特定非営利活動法人
日本システム監査人協会報

2015 年 1 月号
No 166

No. 166（2015 年 1 月号）＜12 月 25 日発行＞

プライバシーマークに関わる実務者必見！！
協会では『6ヶ月で構築する個人情報保護マネジメントシステム実施ハンドブック』を刊行いたしました。
関連記事をご覧ください。　⇒特別頒布のご案内はこちら

今年も、話題満載の会報をお届けしていきます。


京都永観堂

巻頭言

2015 年の年頭にあたって

会員番号 0577　仲 厚吉（会長）

年頭にあたって、ひとこと、ご挨拶を申し上げます。

当協会は、2008 年 2 月 18 日の創立 20 周年記念講演会で「システム監査のこれからの 10 年に向けた提言と当協会の今後の取組み」について発表を行っており、昨年、これを見直し、残る期間に取り組むべき協会活動の方向性を確認し、システム監査の活性化に取り組んでおります。

2014 年 6 月 24 日に閣議決定された「世界最先端 IT 国家創造宣言」では、“閉塞を打破し、再生する日本へ”、“世界最高水準の IT 社会の実現に向けて”を基本理念に、情報通信技術（IT）によって革新的な新産業・新サービスの創出と全産業の成長促進、利便性の高い電子行政サービスの提供、オープンデータの活用推進に加えて、東京オリンピック・パラリンピック等の機会を捉えた最先端の IT 利活用による「おもてなし」の発信や、国際貢献及び国際競争力の強化に向けた国際展開等を宣言しています。2015 年より「世界最先端 IT 国家創造宣言」に沿った政策が実行されていくものと思われ、協会としても、政策に沿った活動に取り組みます。

当協会は、毎年2月に通常総会を開催しています。2014 年は、IT ガバナンスについて、日本 IT ガバナンス協会会長・システム監査学会会長の松尾明氏に特別講演をお願いし、分かりやすい講義でたいへん好評でした。2015 年は、IT 人材の育成について、独立行政法人情報処理推進機構（IPA: Information-technology Promotion Agency, Japan）に特別講演をお願いしています。

会員の皆様には、通常総会（2015 年 2 月 20 日金曜日午後）へのご出席を、お願い申し上げます。

＜目次＞

各行から Ctrl キー+クリックで
該当記事にジャンプできます。
（各記事末尾には目次へ戻るリンク有）

＜目次＞

2014.12

投稿　【　ASEAN 情報セキュリティ研修　参加報告　】

会員番号　0898　竹下　和孝

システム監査が目的とする情報システム活用による経営効率への貢献やビジネスパフォーマンスへの寄与は、セキュリティ対策を計画するうえでも役立つと考えています。情報セキュリティ監査だけでは、どうしても業績向上や経営品質向上への貢献、セキュリティ活動の有効性が表現しにくいため、活動予算の確保や経営者の理解を得ることが難しい場面があるからです。

そこで、課題分析や問題解決への視点が経営への貢献に直結するように、情報システムと情報セキュリティ確保の効率性や有効性評価の観点からモニタリングやコントロールを組み立て、情報セキュリティ活動への取り組みを強化するよう、もっと経営者の意思決定を支援してはいかがでしょうか。そのようなシナリオで研修企画した内容が、参加者からも評価いただいたようなので紹介します。

急激に増加する情報セキュリティ被害に悩む ASEAN 諸国から、セキュリティ対策の実践力を高めるための研修ができないかとの要請があり、経済産業省の委託事業である「貿易投資促進事業（制度・事業環境整備）」として研修実施することになりました。この研修での私の役割は、研修期間5日のうち初日から4日目まで。情報セキュリティ対策の組織作りを目的とする集中トレーニングのカリキュラムを企画し、教材作成と講師を担当するというものです。

1. セキュリティ研修の背景と目的

（セミナー表題と主催者ロゴ。主として重要インフラ運用組織むけに案内された）

失われた20年と言われる中でも、IT 活用の場面は急激に進展し、国内の事業者・個人はその先頭に立ち試行を繰り返してきました。多くの失敗もありました。日本的な慣習の良さは、その失敗を相互に学び共有し、同じ間違いを繰り返さないように組織内・業界内で競争して品質を高めてきたことでしょう。

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

ASEAN 諸国との間では、最新のセキュリティ事故と解決策を CSSC(Control System Security Center)、JPCERT/CC(Japan Computer Emergency Response Team Coordination Center)、NISC(National Information Solution Cooperative)などから紹介することは、数年前から年に数回の交流がもたれていたようです。

しかし、いかに優れたセキュリティ技術、セキュリティ対策を講じた機器や装置であっても、情報機器を利用し運用するのは「人」であり「組織的な活動」です。組織で働く人々が日夜の運用に従事しているわけです。

JIPDEC は ISO/IEC27001:2013（JISQ27001:2014）に基づく国際規格の制度運用や活用を推進していますが、ASEAN 諸国の重要インフラ等を運用する組織が直面していると思われる課題を把握しているわけではありません。

私は JIPDEC で ISMS 認定審査員として、また技術専門部会委員として ISMS 適合性評価制度の運営に参加していることから、今回講師として依頼を受けました。手探りながらセキュリティ上の課題分析、セキュリティ強化のための組織づくり、管理策の選定の手法や点検、監査、マネジメントレビューの方法など、ISO/IEC27001:2013 に基づく国際規格の活用方法を提供して、実践方法を演習形式のノウハウとして紹介すればよいのではないか、との仮説を立てました。その後は、研修しながら参加者の課題や問題意識、関心や反応に合わせ調整していくようにしました。

さらに一方向の講義ではなく双方向のコミュニケーションができる研修スタイルとの要望があり、今回の ASEAN 諸国向けに現地で実施する研修は、ケーススタディと演習を中心の4日間とするカリキュラムを作成しました。

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

しかもインターネットを経由した情報アクセスの広がりから通信事業者の連携や国際的な対策が求められます。そこでは可用性や完全性を損なう時だけでなく、利用がピークとなる時の需給バランスを失うことでも情報伝達やサービスは停止し、経済活動への支障をきたしてしまいます。

今回の研修会場となったタイのバンコクでは、政情不安、デモや大規模水害による工業団地の浸水が事業活動に影響を及ぼしたことは記憶に新しいことです。研修は APEC や ASEAN 会議の時期と前後して、ASEAN（本部はジャカルタ）の発祥地であるタイのバンコクで開催することが決まりました。

課題は、情報セキュリティ活動をどのように考え、計画し、実質的な対処の準備を進めておくか、ということです。事故を起こした後での対策なら比較的容易にセキュリティ活動への予算配分や活動の優先度を高めることができるでしょう。それでも、予算や人員、スキルなどは最小限しか割り当てられず、不可欠な水準での準備ができる状況ではないのです。未知の分野が多いからです。

ISO31000 が定める「不確かさ」を想定して、想定外の状況は少なくなったとはいえ、それらのリスクを想定内の事象としてどこまで備えるかは永遠の課題でしょう。被害の想定や許容水準を設定することは容易ではありません。要するに、わからないことだらけです。 しかも入念な事前対策を行っても、被害発生を防止できるわけではありません。

今回の演習参加者への事前調査では、ISO/IEC27001 の基礎知識は習得済みとのことでしたが、セキュリティ体制の構築や運用を議論するほどの理解や実践経験は十分でないことがわかり、参加者の経験の幅に合わせて演習成果の目標レベルを調整する必要もでてきました。慣れていない ISO 用語や英語（私のブロークンな英語も原因のひとつ）に戸惑ったであろう参加者は、配布されたテキストと英語版の ISO 解説書を片手に奮闘しました。

2. 研修の進め方

初日にISO/IEC 27001概要説明、ISMS適合性評価制度の概要を説明しました。受講者には英語での意思疎通が可能なこととの条件をつけてあったため、英語で説明している講師のほうが緊張します。国際的な英語力調査の結果

の通り、参加者の中には達者な英語力による発言や発表もありました。研修講師として、4日間もの連続した講義と演習指導を英語で実施するのは初めての経験でした。受講者との質疑対応を終えて安堵する間もなく、翌日の演習のシナリオを調整しました。その場の対応だけで精一杯で、講義録を残すことも忘れていました。

初めてのことばかりで、設定したシナリオも、実施中に補正をしながら進めたわけです。

さらに、2日目から4日目までのケーススタディでは、情報セキュリティの理解だけでなく、組織内での実践能力の向上を図るため、ケースに示した課題を各自が検討し、チームを組んでグループで問題解決するという手法を採用しました。演習で作成した資料は会場の前方スクリーンに映し出して、直ちにフィードバックしながら情報共有する手法も、参加者の理解と情報共有を促したようで好評でした。参加者の表現では、このようなアトラクティブな研修に参加したことがない、とのことでした。冬季に入ったとはいえ南国のタイですから、外の通りでは半袖シャツでも汗が出てきます。エアコンの効いたホテルの研修会場とはいえ、舞台裏での講師は冷や汗ダクダクです。

初日に出された質問、Human Error と ISO/IEC 27001 の関連の補足説明をした後で Case1～Case4 のケーススタディを始めました。講義形式の研修では、質問をうけて課題を把握しない限り、受講者の理解度や期待を確認することが難しいものですが、質問が多く出されると、質問の意味を理解することも大変です。

個人演習、グループ討議、各グループの成果を発表して意見交換、講師から講評する方式としたことは参加者の理解を深めるためには効果的だったようです。講師2名で分担して各チームの議論が活性化するよう支援します。

一般的には現地が抱えている課題を把握・分析して、状況に合わせて改善提案、問題解決するコンサルティング的な内容が期待されます。今回は直前に実践応力を高めるための双方向コミュニケーション形式を要請されため、事前調査の方法もなく時間の余裕もありません。現地事情を推定しながら、新規に研修カリキュラムを作成したわけですが、ケース研修の当日は、ファシリテーションに集中するようにしました。

研修を始めてわかったことですが、参加者側の実態としては課題の認識はあるものの、現在がちょうど問題点の振り分けや具体策の検討段階にある状況のようでした。そのため、用意したシナリオについて、好意的に受け止めていただいたようです。ISMS を教科書としてセキュリティ対策強化をすすめる準備段階のニーズと合致したようです。

3. ISMS（ISO/IEC27001:2013）に関する研修内容

情報セキュリティ事故の原因として、人によるエラーの統計資料、原因分析やリスク分析・評価に基づく組織作りと、今後は人が起こす犯罪などへの取り組みを通じて ISMS 活動の重要性を説明しました。さらに ISMS の管理策概要を説明し、国内での ISMS 構築実践事例紹介、および ISMS 認証の仕組みや ISMS の運用を広めるため認証・認定の体制を紹介しました。

ISO の規格が使用する英文の表現は、抽象的で一般的には短期間での理解は難しい。このため説明も難しく、参加者が理解できるよう具体的な事例で解説を補う必要があります。今回は担当した講師側が海外拠点での事業活動、IT プロジェクトの運用経験、国内での情報セキュリティ研修の指導経験、および ISO 規格に関する国際会議での活動などの経験を持っており、組み合わせ協力して対応しました。

3.1 ISMS 実践(ケーススタディ)

ISMS 実践のためのケーススタディは次のタイトルの通り用意しました。

1) Case1 True/false questionnaire(2 名グループ)
2) Case2 Select controls from the ISO/IEC 27001(2 名グループ)
3) Case3 Find Solutions:information leakage(5-6 名グループ)
4) Case4 Find Solutions:Services Provided by Third Parties(同上)
5) Case5 Find solutions:Physical protection and entry/exit control(同上)
6) Case6 Find solutions:Suffered and damaged by hacking(同上)
7) Case7 Find Solutions:Risk Assessment(同上)
8) Case8 Find Solutions:Internal Audit and Management Review(同上)

ケース1－2は基本的な理解があれば回答できる基礎知識を問うもの。後半は、具体的な問題解決、および組織的な対応を問う内容です。

2日目研修参加者(ケース初日)に対し、Human Error と ISO/IEC 27001 の関連の補足説明をした後、Case1～Case4 のケーススタディに挑んでもらいました。

参加者の理解を深めるために、個人演習、グループ討議、各グループの成果を発表して、講師が講評する方式としました。この個人演習、グループ討議中は、メンバー同士の議論はタイ語で議論を深めてもらい、講師は適宜、グループ討議の場面を巡回して、個別の質疑や相談に応じました。

3日目研修参加者(ケース2日目)に対して、グループ討議は前日と同じメンバーとしてCase5～Case6のケーススタディに取り組みました。各グループの発表内容は、スキャナでスクリーンに表示して各グループの代表者(順番)にプレゼンしてもらったのですが、成果物として職場へ持ち帰りたいとの要望がでてきたため、スキャンした資料を後日配布するようにしました。

4日目研修参加者(ケース3日目)に対し、Case7～Case8 のケーススタディを行い、グループ討議のメンバーは前日と同じとしましたが、同じ職場のチームが結合して8-10 人ほどの大所帯となっていたグループもありました。

Case Study 形式にも慣れてきたようだったので、各グループにプレゼンをして頂いた後、他のグループから質疑、コメントを求める形式としたことも、より活発な意見交換を促したようです。

3.2 国内事例紹介と情報セキュリティリスク分析

担当したセッションで最も積極的なフィードバックがあったテーマが、初日に説明した国内事例紹介とリスクアセスメントの一部として実施したリスク分析のためのケース教材でした。

国内事例紹介では、すでに 10 年来 ISMS を運用している組織が、どのように組織的な取り組みを進めてきたか、その準備、運用の課題、進め方などを紹介した内容です。 ISO/IEC27001:2013 では、ISO31000 のリスクの考え方を採用しているため、リスクアセスメントの手法が一部変更されています。どのように考えるか悩んでいたところ、ケースでの演習が大変参考になったとのフィードバックもあり、狙い通りの影響を与えることができたと思います。

当初の発表は文字だけの原稿だったのですが、次第にフローチャートやイラストを書き込んだものもでてきました。協働作業を通じて友好なチームの雰囲気を作ることができた効果も大きかったようです。

その結果、日本の ISMS 実践事例を学んだだけでなく、実戦経験を学び、情報セキュリティ対策の進め方に対する考え方の変化を実感したとの多くの前向きのフィードバックが寄せられました。

ISO/IEC27001:2013 という国際規格を国内の ISMS 実践経験を中心に構成した研修は、現地のニーズに応える内容で期待に沿うことができ、また解決策として CSMS、CSSC など国内事例を紹介できたようです。

（写真は、Case－Day3参加の皆さん、事務局、と講師）

最終日には講師チームのまとめとして講評することになりました。

参加者の多くがエンジニアであることを意識して、「シーロム通りの３人のエンジニア」のエピソードを創作して激励しました。

そしてエンジニアの日常業務には単調な面も多いけど、当たり前のことを着実に実行して

「一緒に安全で快適な町を守ろう」

とまとめたところ、ちょっと感動、という参加者もいて、握手を求められました。

今回の研修は情報セキュリティ専門家としての役割でスタートしたのですが、業務プロセス、組織行動、動機付けや組織経営に深く関与してきた CSA としての経験が大きく役立ったようです。

4. 余談と油断

現地で用意いただいたスキャナのドライバが、一般に（日本国内で）普及しているものとは違っていたようで、パソコン接続に手間取ってしまいました。複数のパソコンで試行した後、作業用に持参していた旧モデルのパソコンで認識できたので、急遽、パソコンの役割と配置を変更して対応しました。また、研修会場と宿泊したホテルが提供する Wi-Fi 接続速度も遅く、容量が大きいファイルを操作する場合は、パソコン内に取り込んでおく必要性を感じました。

さらに、電源コンセントの形状も、国によって異なるため変換プラグを携行しますが、今回は宿泊先でパソコンを利用しようとしても通電しません。近所のコンビニ（なんと、国内の有名店舗が 8000 店舗も展開中）で、現地のプラグを購入したもののやはり通電しない。試行錯誤の結果は、主電源が入っていなかったのです。照明以外を集中管理する操作パネルがあり、タイ語表記の下に英文があったのですが、部屋の明かりが暗くてよく見えなかったのです。

最後になりましたが、今回の貴重な機会を提供いただいた METI、JIPDEC、研修アレンジいただいた HIDA（海外産業人材育成協会）、講師チームとして随所で支援いただいた JIPDEC 畔津さん、および研修・演習実施に参画いただいた受講者の皆様方に、改めて感謝します。いっしょに安心安全なセキュリティ環境を守っていきましょう。

以上

＜目次＞

2014.12

めだか　【　情報システム部門のためのシステム監査　】

2015年（平成27年）の干支は「乙未」（きのとひつじ）である。十二支（じゅうにし）は、子・丑・寅・卯・辰・巳・午・未・申・酉・戌・亥の12種類からなっていて「未」は8番目である。十干（じっかん）は、甲・乙・丙・丁・戊・己・庚・辛・壬・癸である。干支（かんし、えと）は、十干と十二支を掛けた120通りではなく、十干と十二支を順列にならべていき最小公倍数の60通りとなる。「乙未」は干支の組み合わせの32番目で、前は「甲午」、「乙未」、次は「丙申」である。60年に一度、同じ干支が回ってくる。還暦である。ちなみに前回の「乙未」は、1955年、日本の高度経済成長の開始（1955年～1957年の神武景気から）の年であった。

システム監査でいうと、前回の「乙未」の1955年から30年経った1985年（昭和60年）に、経済産業省がシステム監査基準を制定している。パソコンが現われ情報化社会が言われ始めた頃である。現在の基準は、2004年（平成16年）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、内部統制制度の開始、つまり金融証券取引法（日本版SOX法）の成立を契機に、2007年（平成19年）に、財務報告に係るIT統制ガイダンスとして追補版が公表されている。また最近では、2014年（平成26年）に、公益財団法人 金融情報システムセンター（FISC）が、「金融機関等のシステム監査指針（改訂第3版）」を発刊している。今に目を向けると、情報システム部門のためのシステム監査は、情報システムを対象とする内部監査であり内部統制でも重要であることをアピールしていきたい。

次回の「乙未」は、2075年である。今年誕生する人が60歳になっている社会である。日本の社会や人口構成はどうなっているのであろうか。国土は海に囲まれ、その国土に住む人たちは、今と同様、地震、津波、台風に脅かされているだろうが、情報技術（IT）の発達により、今よりは前もっての対応ができるようになっているだろう。また、社会は人とアンドロイドが平和に共存し、家庭では鉄腕アトムやドラえもんが人や犬猫といっしょに住んでいる風景が目に浮かぶ。そう考えると、情報技術（IT）発達の健全性（Integrity）が、次回の「乙未」に向けた重要成功要因（Critical Success Factors）であると分かる。

ただし、情報技術（IT）の発達が人を傷つけたりしないようITガバナンス（Corporate Governance of Information Technology）が必要である。そして、ITガバナンスのCheck機能を担うシステム監査は、情報技術（IT）発達の健全性に必須であることをあらためて社会に訴えていきたい。2014年12月14日に衆議院議員総選挙が行われ、与党が定数の3分の2を超えた。この結果、2014年6月24日閣議決定の「世界最先端IT国家創造宣言」は加速して実現の方向に進んでいくと思う。2015年（平成27年）は、システム監査人が、「世界最先端IT国家創造宣言」の方向性を良く認識し、システム監査に当る年になる。

（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＞

2014.12

めだか　【　情報システム部門と共に、情報システム部門の為に　】

私が以前勤務していた銀行では、「店部と共にある監査」「店部の為にある監査」という言葉を、内部監査部門の行動指針としていた。営業店や本部の抱えている問題点を見つけて、その対応策をいっしょになって考え、内部監査部門の立場からアドバイスをする。それが、内部監査部門のミッションであるとの考え方である。

その例に倣うなら、システム監査人は、監査対象部門である情報システム部門に対して、「情報システム部門と共にあるシステム監査」「情報システム部門の為にあるシステム監査」を目指して、監査を行っていく必要がある。

ともすれば、監査側で情報システム部門の問題点であると考えた事項を、一方的に情報システム部門へ伝えて、対応させることを以って、監査の役割を果たした気になりがちである。しかし、それでは、「監査部門　対　情報システム部門」の対立の構図を生むだけであり、「情報システム部門と共にあるシステム監査」とはいえない。

また、監査で発見された情報システム部門の問題点を、単に、表面的・羅列的に列挙し、改善を求めただけでは、「情報システム部門の為にあるシステム監査」とはいえない。発見された情報システム部門の問題点の真の原因は何かを、情報システム部門と共に検討し、真の問題点に対する改善策を求めて、初めて「情報システム部門の為にあるシステム監査」を行ったといえるであろう。

では、システム監査人が、「情報システム部門と共にあるシステム監査」「情報システム部門の為にあるシステム監査」を実践していくためには、どのように対応していけばよいのであろうか？

一つ、お勧めしたいのは、「コーチング」である。

監査部門が指摘事項として情報システム部門に求めた改善事項が、効率的・効果的に対応されるためには、情報システム部門が自ら改善の必要性を納得し、積極的に改善にあたっていくことが必要である。

そのためには、監査部門が一方的に指摘事項を押し付けるのではなく、情報システム部門における問題点の真の原因、その問題点が抱えるリスクなどについて、情報システム部門の認識を確認し、情報システム部門と監査部門とがしっかり議論をしたうえで、認識を合わせることが必要である。

そうした情報システム部門の認識の確認を通じて、問題点の真の原因、リスク状況を気づかせるのが、コーチングである。「答は自分の中にある」は、コーチングでよく言われる言葉だが、システム監査においては、「答は監査対象部門（情報システム部門）にある」である。「情報システム部門の話をよく聞いて、その中から相手に答を見つけてもらう」ことを意識して監査にあたるとよいだろう。

第二にお勧めするのは、「モニタリングの活用」である。

これまでは、監査対象部署の問題点は、往査の中で見つけるのが基本であった。しかし、往査では、頻度的にも、期間的にも、監査範囲・監査深度に限界がある。そうかといって、往査の頻度を上げるのは、監査部門にとっても、監査を受ける側にとっても負担が大きい。

そこで、昨今重要度が増してきたのが、「モニタリング」である。普段の「モニタリング」の中で対象部署に問題点が生じていないかをチェックし、疑問があればその都度、対象部署に確認をしていく。こうしたモニタリングを強化していくことが、結局のところ、問題点の早期発見・改善につながり、情報システム部門に対する監査部門の存在意義を高めることになるだろう。

システム監査人として、これからも、「情報システム部門と共にあるシステム監査」「情報システム部門の為にあるシステム監査」を目指して、監査にあたっていきたい。　　（やじろべえ）

（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＞

2014.12

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）

年頭に当たって、ひとこと、ご挨拶を申し上げます。

当協会では、2008 年 2 月 18 日の創立 20 周年記念講演会で「システム監査のこれからの 10 年に向けた提言と当協会の今後の取組み」について発表を行っています。システム監査活性化委員会では、「システム監査のこれからの 10 年に向けた提言と当協会の今後の取組み」を見直し、残る期間に取り組むべき協会活動の方向性を確認しました。その中で情報システムの有効性の監査がテーマのひとつとしてとりあげられています。情報システム部門のため、情報システム構築プロジェクトが失敗なく、また情報システムが有効であるようシステム監査あるいはシステム管理のポイントを研究していくことは有意義であると考えています。

昨年 6 月 24 日に閣議決定された「世界最先端 IT 国家創造宣言」では、“閉塞を打破し、再生する日本へ”、“世界最高水準の IT 社会の実現に向けて”を基本理念に、情報通信技術（IT）によって革新的な新産業・新サービスの創出と全産業の成長促進、利便性の高い電子行政サービスの提供、オープンデータの活用推進などへ取り組むことに加え、新たに、東京オリンピック・パラリンピック等の機会を捉えた最先端の IT 利活用による「おもてなし」の発信や、国際貢献及び国際競争力の強化に向けた国際展開等を宣言しています。同宣言の中で、政府は、IT ガバナンスの強化、すなわち、政府 CIO による IT ガバナンスを強化し、攻めの IT 投資と無駄の徹底排除を図り、政府全体を通じた戦略的な IT 投資管理を実現するとしています。また、政府における IT 人材の育成を図るため、研修プログラムの見直し・充実を政府横断的な取組みとして実施するとしています。

IT ガバナンスは、ISO/IEC 38500 として国際標準になっており、ISO/IEC 38500 の JIS 規格化が進んでいます。IT ガバナンスは、6つのプリンシプル、Responsibility、Strategy、Acquisition、Performance、Conformance、Human behavior で構成され、Plan-Do-Check-Act を回します。システム監査はその Check の役割を担います。当協会は、ISO/IEC 38500 の JIS 規格化に合わせて、IT ガバナンスの要素であるシステム監査について部会・研究会活動を通じシステム監査の制度化等を提言していくよう取り組みます。IT 人材の育成については、当協会は、高度情報処理技術者試験合格者、公認会計士（CPA）、ISMS 主任審査員、プライバシーマーク主任審査員等への公認システム監査人（CSA、ASA）資格認定制度を通じ、実績にもとづく資格認定と、継続教育受講実績による資格更新認定を行っています。また、月例研究会によるセミナーや会報掲載の部会・研究会報告等により最新の情報を提供しています。

当協会は、毎年2月に通常総会を開催しています。昨年は、IT ガバナンスについて、日本 IT ガバナンス協会会長・システム監査学会会長の松尾明氏に特別講演をお願いし、分かりやすい講義でたいへん好評でした。今年は、IT 人材の育成について、独立行政法人情報処理推進機構（IPA: Information-technology Promotion Agency, Japan）に特別講演をお願いしています。同機構は、ソフトウェア及び情報処理システムが社会を支える基盤であることから、技術・人材の両面からソフトウェア及び情報処理システムの健全な発展を支えるインフラ機能を提供している団体です。

会員の皆様には、通常総会（2015 年 2 月 20 日金曜日午後）へのご出席を、お願い申し上げます。

＜目次＞

2014.12

第１９７回　月例研究会　（２０１４年１１月１９日開催）報告

会員番号 0056　藤野明夫　（情報セキュリティ監査研究会主査）

【講演テーマ】　「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

【日時】　2014 年 11 月 19 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】

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活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。

【講演概要】

はじめに

経済産業省の CIO 補佐官として、主にアイデンティティ、とくに ID 連携トラストフレームワークを担当している。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についてご紹介する。

なぜ、マイナンバーとアイデンティティが関係するか。それは以下の理由による。

現在、日本では、行政に関わる手続きが、すべてネットワーク上の電子的処理で完結するものはひとつもない。たとえば、何かの手続きで、情報処理技術者試験の合格を証明する必要がある場合、必ず紙による合格証かそれに代わる資料を紙媒体で添付しなければならない。

今回の番号法成立によるマイナンバー制度の発足で、初めてネットワーク上で電子的に本人を確認できる仕組みができた。ただし、マイナンバーそのものは、その直接的な利用が、行政に関わるいくつかの手続きに法律で限定されていて、民間活用は許されていない。マイナンバー制度によるネットワーク上での電子的な本人確認を民間で活用するとすれば、民間の事業者は本人の確認に際しマイナンバーそのものにアクセスすることなく、単に本人であるか否か、Yes か No かの回答を得られれば足りるとする ID 連携トラストフレームワークの仕組みを活かすのが最も相応しい。

もし、これが実現すれば、事業者は従来の方法よりはるかに信頼性の高い本人確認ができ、さらに、その取引に必要にして十分な最小限のアイデンティティに関する情報を取得でき、しかも、個人を特定する情報を保有するという大きなリスクをとる必要がなくなる。また、利用者からみれば、自身を特定する情報を事業者が保有することがないことが保証されていることで、安心して取引ができることになる。ネットワーク上でのビジネスの拡大に大きく資することになるであろう。

なお、番号法により、法人にも法人番号が付与され、法人名、本社所在地がインターネットで提供される。

Ⅰ．マイナンバー制度について

マイナンバー制度の民間利用について説明する前に、マイナンバー制度そのものを理解していただく必要があるので、その骨子を説明する。なお、「マイナンバー」と「個人番号」は同じものであるが、以下、制度面を説明する際には「マイナンバー」、マイナンバーそのものを指す場合は「個人番号」という表記をする。

１．マイナンバーとは

マイナンバーは、行政を効率化し、国民の利便性を高め、公平・公正な社会を実現する社会基盤である。その目的ゆえ、マイナンバーそのものは行政機関しか利用することができず、また、その利用目的も法律により限定されている。

2015 年 10 月から、住民票を有するすべての人に、一人一つの番号（12 桁）が付与され、市区町村から住民票記載の住所にマイナンバーの通知カードが送付される。マイナンバーは、番号が漏えいし不正に使われる恐れがある場合を除き、生涯変更されない。

2016 年 1 月から、社会保障、税、災害対策の行政手続で、マイナンバーが必要になる。なお、マイナンバー制度の番号そのものを参照することができるのは、この、社会保障、税、災害対策分野において法律で定められた行政手続に限定される。具体的な利用の場面を以下に例示する。

・毎年 6 月の児童手当の現況届の際に、市区町村にマイナンバーを提示する。
・厚生年金の裁定の際に、年金事務所にマイナンバーを提示する。
・証券会社や保険会社等にマイナンバーを提示し、法定調書に記載する。
・勤務先にマイナンバーを提示し、源泉徴収票に記載する。

上記のような場面で利用するため、民間事業者も、税や社会保険の手続で、マイナンバーを取り扱う。マイナンバーを記載した源泉徴収票や支払調書、被保険者資格取得届などを行政機関等に提出する必要があるからである。

前述のとおり、マイナンバーは、法律で決められた行政手続きでのみ利用することが許されている。したがって、マイナンバーに関して、上記のような必要な手続き以外の目的での利用や、不正な入手、あるいは、不当な提供は、直接罰で処罰される。

２．個人番号カードについて

前述の通知カードには顔写真がないので本人確認には使用できない。そこで、本人の希望に応じて顔写真付きの個人番号カードが発行される。この個人番号カードは、個人情報の基本四情報（氏名、住所、生年月日、性別）に加えて、顔写真が券面の表面に貼付され、裏面に個人番号（マイナンバー）が記載される予定である。表面のみで身分証明書として利用可能にするためである。個人番号を裏面に記載するのは、金融機関、レンタルビデオショップ等で本人確認をした証拠として個人番号カードのコピーをとることがあるが、その際に個人番号もコピーされてしまうのを防ぐためである。なお、個人番号カードには IC チップが内蔵されているが、その空き領域は、国の行政機関、地方公共団体の機関等が法令で定めることにより、印鑑登録証、公共施設の予約等、種々の目的に利用することができる。

３．マイナンバー制度における安心・安全の確保と情報連携について

マイナンバー制度（社会保障・税番号制度）における国民の懸念と、それに対する保護措置について、以下に説明する。

番号制度に対する国民の懸念は、次の三点であろう。一つは、個人番号を用いた個人情報の追跡・名寄・突合が行われ、集積・集約された個人情報が外部に漏えいするのではないかといった懸念、二つ目は、個人情報の不正利用（例：他人の個人番号を用いたなりすまし）等により財産その他の被害を負うのではないかといった懸念、三つ目は、国家により個人の様々な個人情報が個人番号をキーに名寄せ・突合されて一元管理されるのではないかといった懸念である。

これらの懸念に対して、制度面とシステム面の両面で保護措置を講じている。まず、制度面であるが、以下の 5 点の保護措置を講じている。

① 番号法の規定によるものを除き、特定個人情報の収集・保管、特定個人情報ファイルの作成を禁止（番号法第 20 条、第 28 条）
② 特定個人情報保護委員会による監視・監督（番号法第 50 条～第 52 条）
③ 特定個人情報保護評価（番号法第 26 条、第 27 条）
④ 罰則の強化（番号法第 67 条～第 77 条）
⑤ マイ・ポータルによる情報提供等記録の確認（番号法附則第 6 条第 5 項）

システム面では、以下の 4 点の保護措置を講じている。

① 個人情報を一元的に管理せずに、分散管理を実施
② 個人情報を直接用いず、符号を用いた連携を実施
③ アクセス制御により、アクセスできる人の制限・管理を実施
④ 通信の暗号化を実施

これらの保護措置の全体像を図 1 に示す。

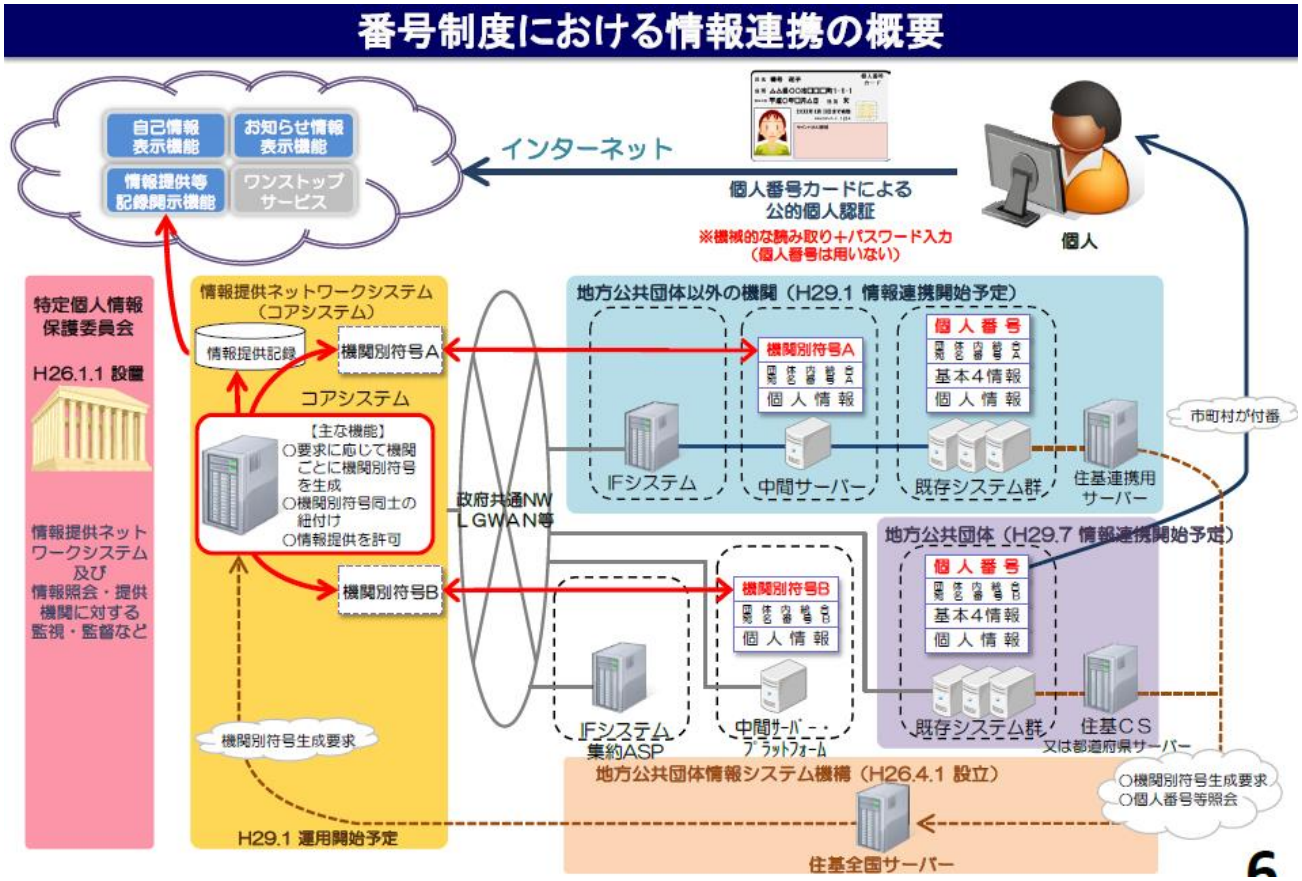


図1　番号制度における情報連携の概要

図1をベースに、マイナンバー制度における情報連携に関する安心・安全の確保について説明する(図中の地方公共団体以外の機関とは、厚生労働省、国税庁等である)。

国の行政機関や地方公共団体の個人情報の連携は、個人情報の一元管理の懸念をなくすために、直接、個人番号で連携をすることをせずに、情報提供ネットワークシステム(コアシステム)というものを介して情報をやり取りする(図1左から二番目の囲み)。各行政機関は元々個人番号を持っているが、データを他の機関とやり取りするときは個人番号を外す。外した上で個別の機関ごとに、機関別符号A、機関別符号Bという別の符号に置き換える。要は私の個人番号が2種類になる。私の番号は、行政機関の間で連携する場合、たとえば、厚生労働省のなかでは機関別符号Aの「123」となる。逆に地方公共団体では、機関別符号Bの「456」になる。これらを一人の人だと認識しているのは情報提供ネットワークシステム(コアシステム)だけである。要するに、連携の要求に応じて機関毎に符号を生成して、コアシステムで、機関別符号同士の紐付けを行う。これが一元管理ができない仕組みである。

なお、スウェーデン等はこういう仕組みをとらず一つの番号を全ての業務で共有するやり方もある。各国によって様々である。

異なる行政機関の間での情報連携の際には、コアシステムにどのような連携(情報提供)が行われたかを情報提供記録(ログ)に残す。情報連携の際は、必ずコアシステムを経由するので、このログを見れば、どこでどういう情報提供が行われたかを知ることができる。

本人がこの情報提供記録を閲覧できるようにした仕組みがマイ・ポータルと呼ばれているものである。このマイ・ポータル(情報提供等記録開示システム) は、番号法施行後一年を目途に設置し (番号法附則第 6 条第 5 項)、以下の機能を持つことを予定している。

① 情報提供記録表示：自分の特定個人情報を、いつ、誰が、なぜ情報提供したのかを確認する機能
② 自己表示機能：行政機関などが持っている自分の特定個人情報について確認する機能
③ プッシュ型サービス：一人一人に合った行政機関などからのお知らせを表示する機能 (個別設定により、子どもが学齢になったので小学校入学の手続きの案内を送る、あるいは、確定申告の案内を送る等)
④ ワンストップサービス：行政機関などへの手続きを一度で済ませる機能

この①は、制度面での保護措置の⑤をシステム上で実現するものである。これにより、本人は、目的外利用がされたか否かを知ることができる。また、①は番号法附則第 6 条第 5 項に、②は同条第 6 項第 1 号に、③は同条同項第 2 号に、④は同条同項第 3 号にそれぞれ対応する。

以上がマイナンバー制度の概要である。

Ⅱ．民間でのマイナンバー利活用の検討

2014 年 5 月 16 日に発表された、IT 総合戦略本部新戦略推進専門部会マイナンバー等分科会の中間とりまとめ(案)(以下、「中間まとめ」)には、「世界最先端の IT 利活用社会」のインフラとして、マイナンバー制度の普及と利活用を図るため、国・地方・民間が連携して取り組むべきことが謳われている。以下、この中間とりまとめに沿って、民間でのマイナンバー制度の利活用について紹介する。

１．個人番号カードの普及・利活用について

前述のごとく、個人番号カードは、身分証明書として機能し、さらに、内蔵する IC チップの中に種々の情報を保存することができるので、行政及び民間において、以下のような活用シーンが期待される(図2参照)。

まず、職場、役所、病院等で必要な健康保険証、印鑑登録カード、公務員身分証明書等のカード類を個人番号カードに一体化/一元化する。さらに、対面と書面による本人確認手段を、個人番号カードを活用することにより電子

的な本人確認に代え、官民の様々な手続きをネットワーク上で電子的に終始、完結できるようにする。また、個人番号カードを利用して、窓口外、時間外の利用が可能なコンビニ等で、行政機関、金融機関等のサービスをいつでも受けられるようにする等である、

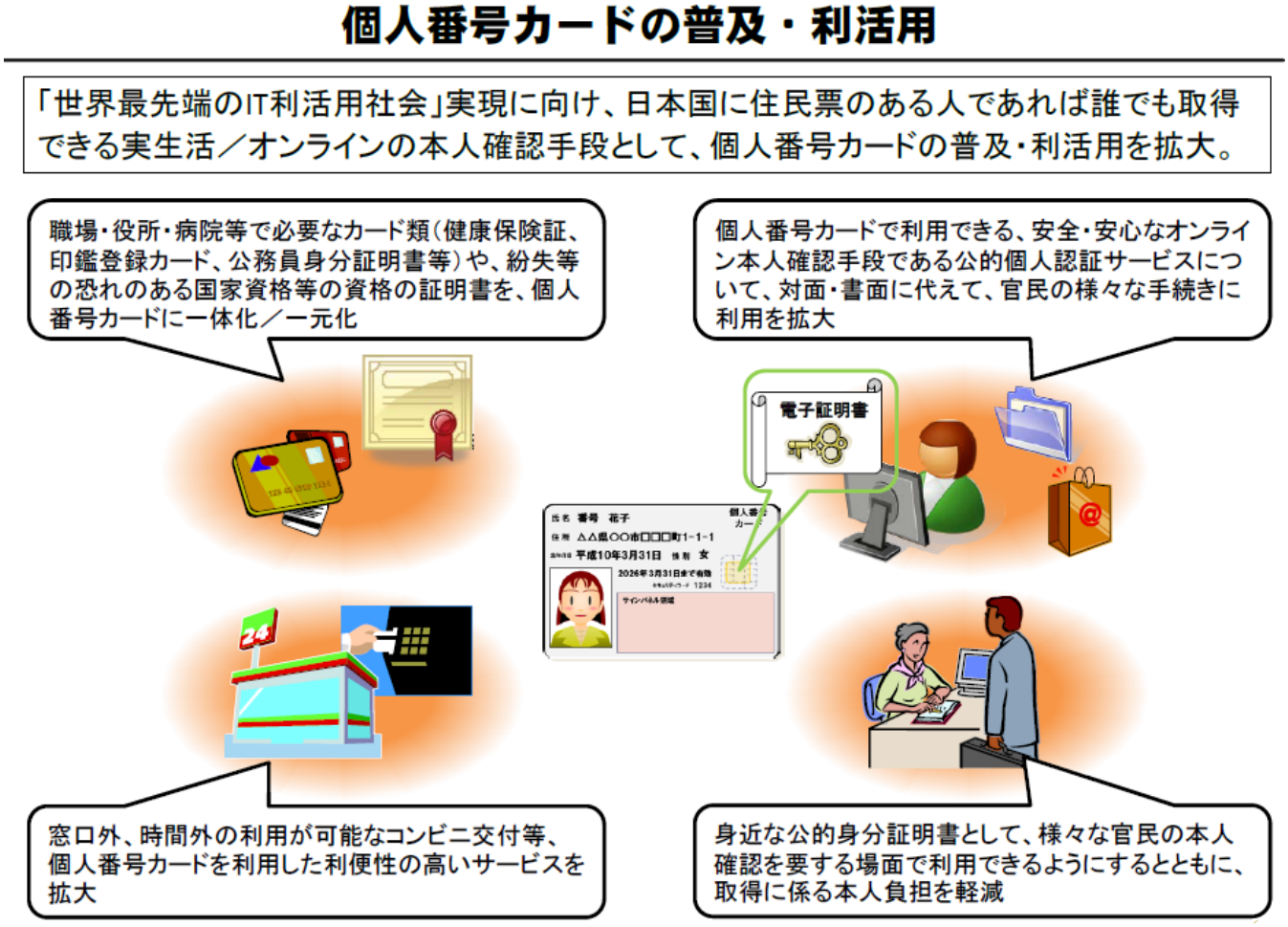


図2　個人番号カードの普及・利活用のイメージ

2．マイポータル/マイガバメントについて

中間まとめの利活用各論の二点目は、マイポータルである。中間まとめには、「利用者の特定個人情報等の閲覧を可能とする情報提供等記録開示システム（マイポータル）を拡張し、暮らしに係る官民の利便性の高いオンラインサービスを、誰もが安全かつ手軽に利用できる「マイガバメント」を構築する（※名称については見直しを検討）。」と謳っている。マイポータル/マイガバメントの概要を図 3 に示す。

提供する主なサービスは、以下のとおりである。

① 利用者の自己情報の閲覧：利用者の特定個人情報や医療・健康・介護等に係る自己情報を、マイポータルや公的個人認証を利用して、分かりやすく、タイムリーに、必要に応じ閲覧可能に

② プッシュ型サービス：利用者に係る情報に基づき、その利益になる情報（政府広報等のお知らせ、子育て等のサービス情報、給付金等の資格通知、権利の得喪に係るアラート等）を提供

③ ワンストップサービス：引越しや死亡等のライフイベントの際に必要となる官民の様々な手続きを、オンラインで一括化

マイポータル/マイガバメントでは、利便性の高いサービス利用に必要な基盤を確立する。これは、手続き等が対面処理や紙媒体の書類の提出を必要とせず、すべて電子的に完結するよう、必要な情報をデータで入手・利用する仕組み（マイポータル/電子私書箱）である。これを確立することにより、たとえば、生命保険料控除証明書等をデータで受信し、そのまま e-tax による確定申告等に利用するといったことが実現する。

さらに、シームレスな官民サービスを利用可能とする、本人確認に係る官民連携基盤を確立する。たとえば、e-tax で確定申告し、そのままネットバンキングで納付するといったことが実現する。

今後は、サポートを受けながらの利用や代理人による利用に係る環境整備やスマートフォンや CATV 等、利用チャンネルや認証手段を拡大していく。

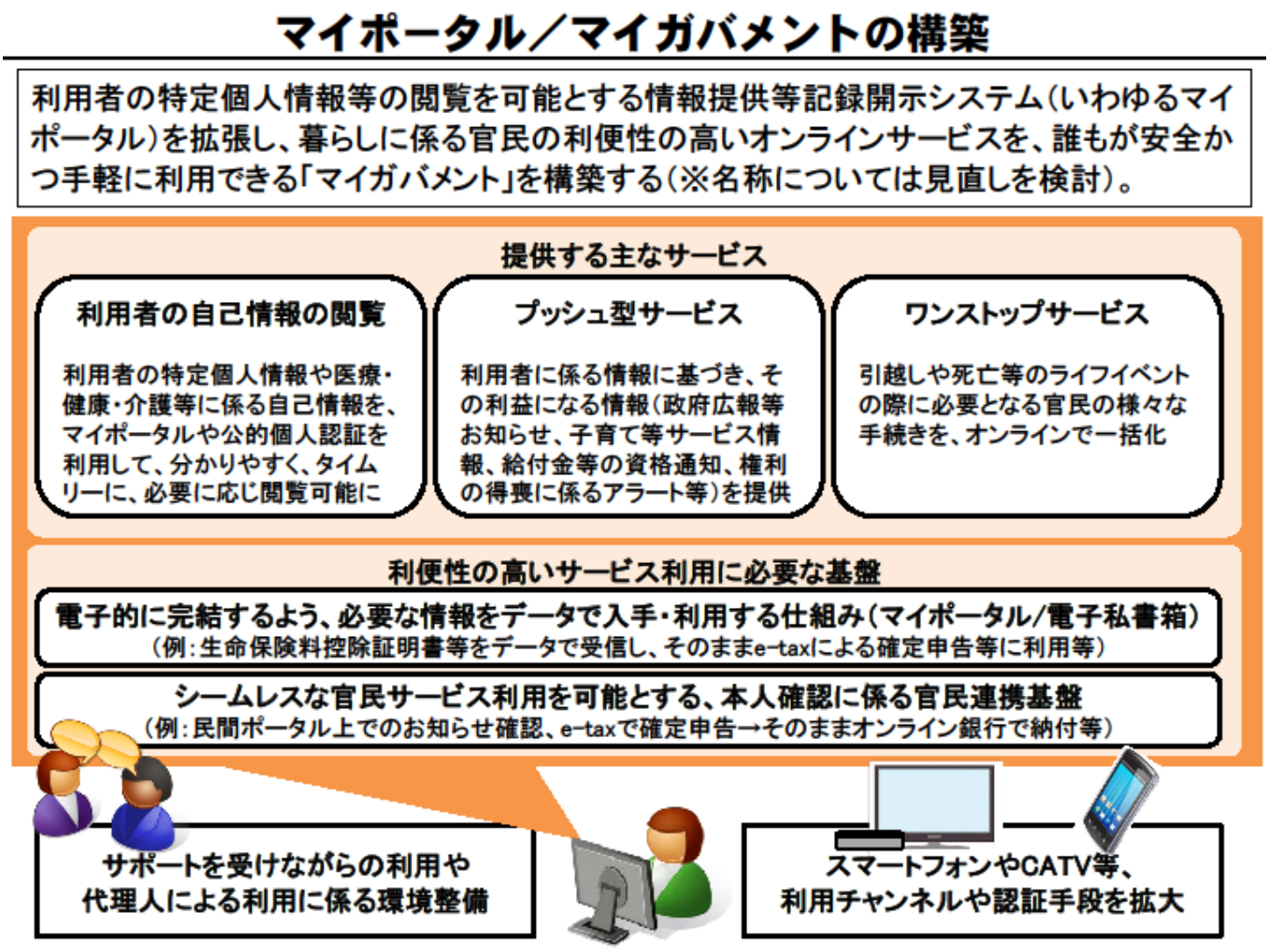


図3　マイポータル/マイガバメントの概要

マイガバメント活用の例として、マイガバメントを利用したライフプラン情報連携サービスを紹介する（図 4 参照）。

左上のマイポータルは、法定の狭い意味のマイポータルである。ここに自己情報表示として自分の社会保険料納付状況、納税情報がある。これと、保険会社のアカウントを結びつけて自分の保険情報、銀行の貯蓄情報等のデータをマイガバメントに集約し、ファイナンシャルプランナーからトータルなライフプランサービスを受けることができる。この連携が無限に広がるのは不都合なので、一定の枠（図 4 の赤い破線枠）を設ける。官民連携は行うがある程度の枠内に収めようということである。そのバランスを取るのが「トラストフレームワーク」である。

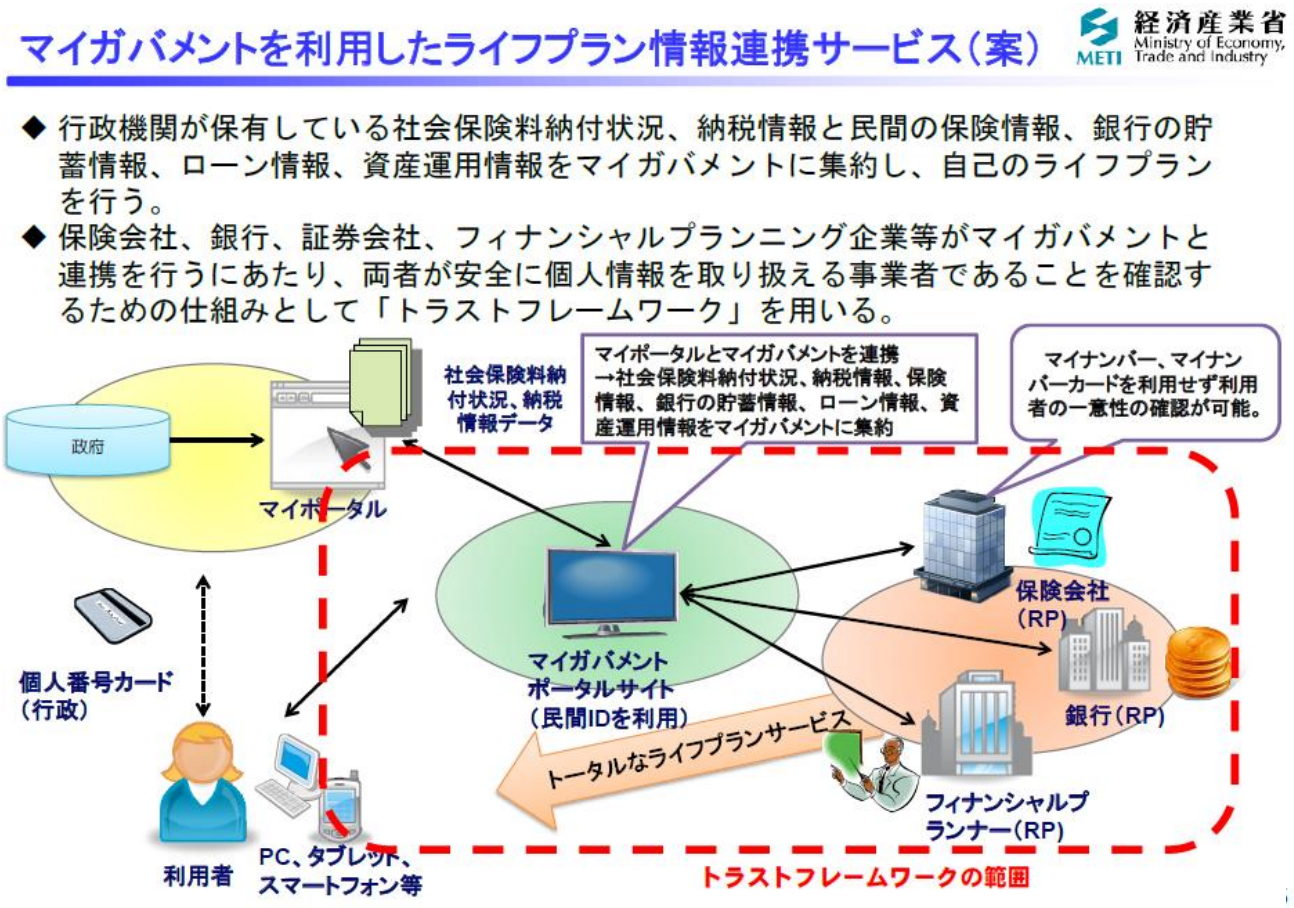


図 4　マイガバメントを利用したライフプラン情報連携サービス

ここで、「トラストフレームワーク」という言葉が初めて出てきたが、その説明は後述する。まずは、「トラストフレームワーク」による官民連携の仕組みのイメージを掴んでいただきたい（図 5 参照、図中の「RP」等の用語については後述する）。図の左端の「政府」は、特定個人情報保有機関である霞が関の行政機関である。赤の破線枠がマイガバメントトラストフレムワーク（仮称）の範囲である。このマイガバメントトラストフレームワークのポイントを以下に示す。

① 個人番号とマイガバメントのユーザ ID は、一意にならないよう関連づけられる（マイガバメント領域で管理されるユーザ ID や属性情報は利用者同意で提供可）。

② 上記に伴い、利用者がマイポータルから自己の情報を個人番号と紐付かないデータとして取得できる場合は、名寄せのリスクが低くなること等から、マイガバメントでは、ID/パスワードなど既存の本人確認手段が利用可能になり、また、利用者本人の同意に基づき自己の情報を外部サービスに提供することが可能になる。

③ マイポータルを含めたトラストフレームワークが形成できた場合、マイポータル経由で、プッシュによる自己情報取得ができる可能性もある。

④ 利用者は、マイガバメントを含むトラストフレームワーク参加サービス（図 5、民間サービス A、B、C）ごとに、サービスを受ける都度、IdP の個人情報連携を許可することにより、サービスの選択が可能になる。

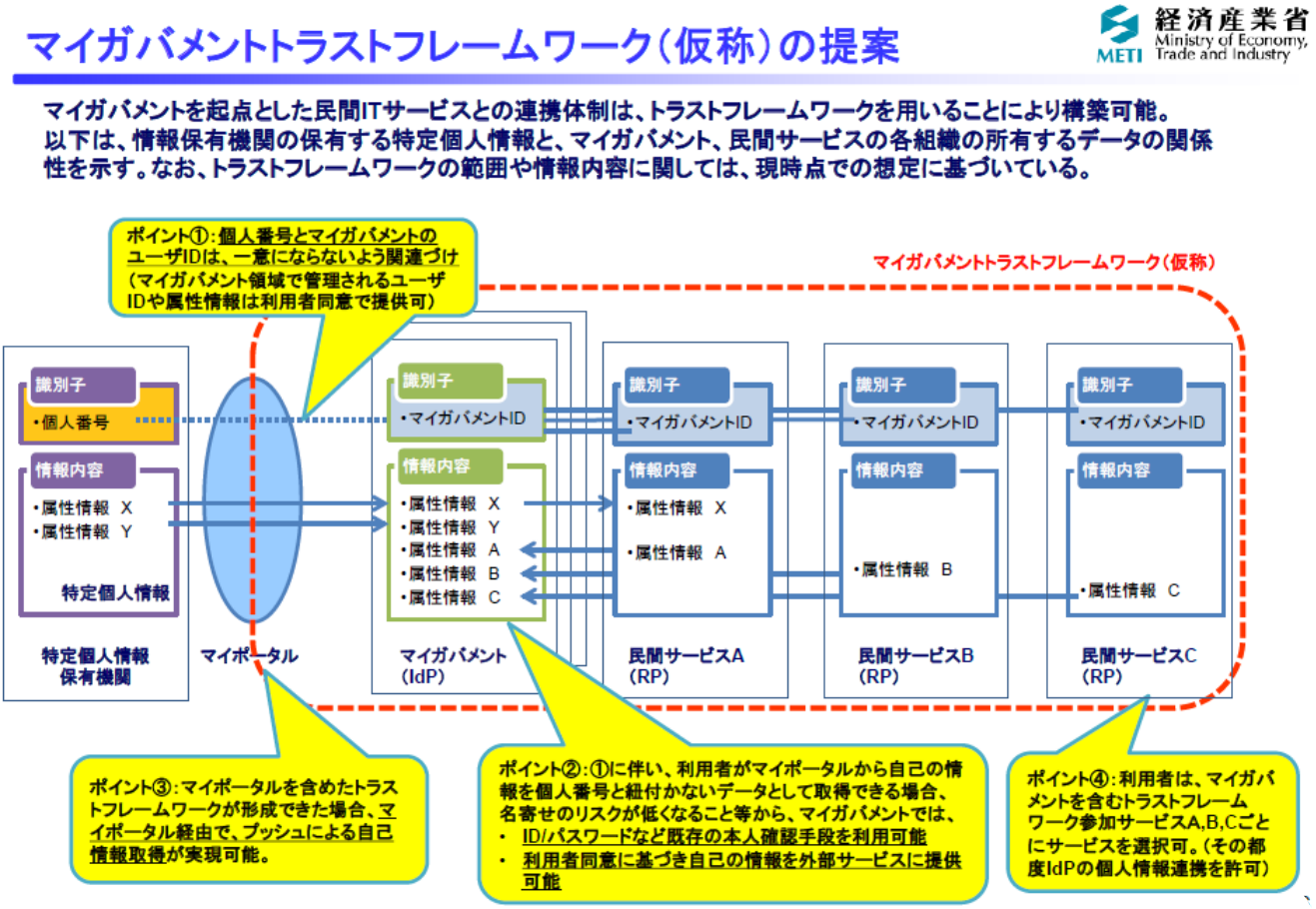


図 5　マイガバメントトラストフレームワーク

マイポータル/マイガバメントの説明の延長でトラストフレームワークに触れざるを得なくなり、説明が前後してしまったが、次項でトラストフレームワークについて説明する。

3．ID 連携トラストフレームワークについて

ID 連携トラストフレームワークの正式名称はアイデンティティ連携トラストフレームワークである。アイデンティティの利活用の促進とアイデンティティの安全な流通手段の確保との両立を目指す。ここで言う ID は、アイデンティティ（属性集合体）のことであり、ユーザ ID の ID とは異なるものである。ユーザ ID は本人を識別する識別子たる文字列であって、ID（アイデンティティ）の要素の一つである。ID の要素には、ユーザ ID、氏名、住所、メールアドレス、所得、家族構成等、個人に関するあらゆる情報が含まれる。すなわち、ここでいう ID はその人を示す属性情報の集合体である。

ID 連携トラストフレームワークとは、インターネット上（非対面の環境）で、利用者のデータ（個人に関する情報の集まり）やサービスの受け渡しを行う企業群が、「利用者がその相手を信用して利用者本人の情報利用を任せられる（信用、信頼）」状態であることを保証する枠組みのことである。図 6 に ID 連携トラストフレームワークのイメージを示す。

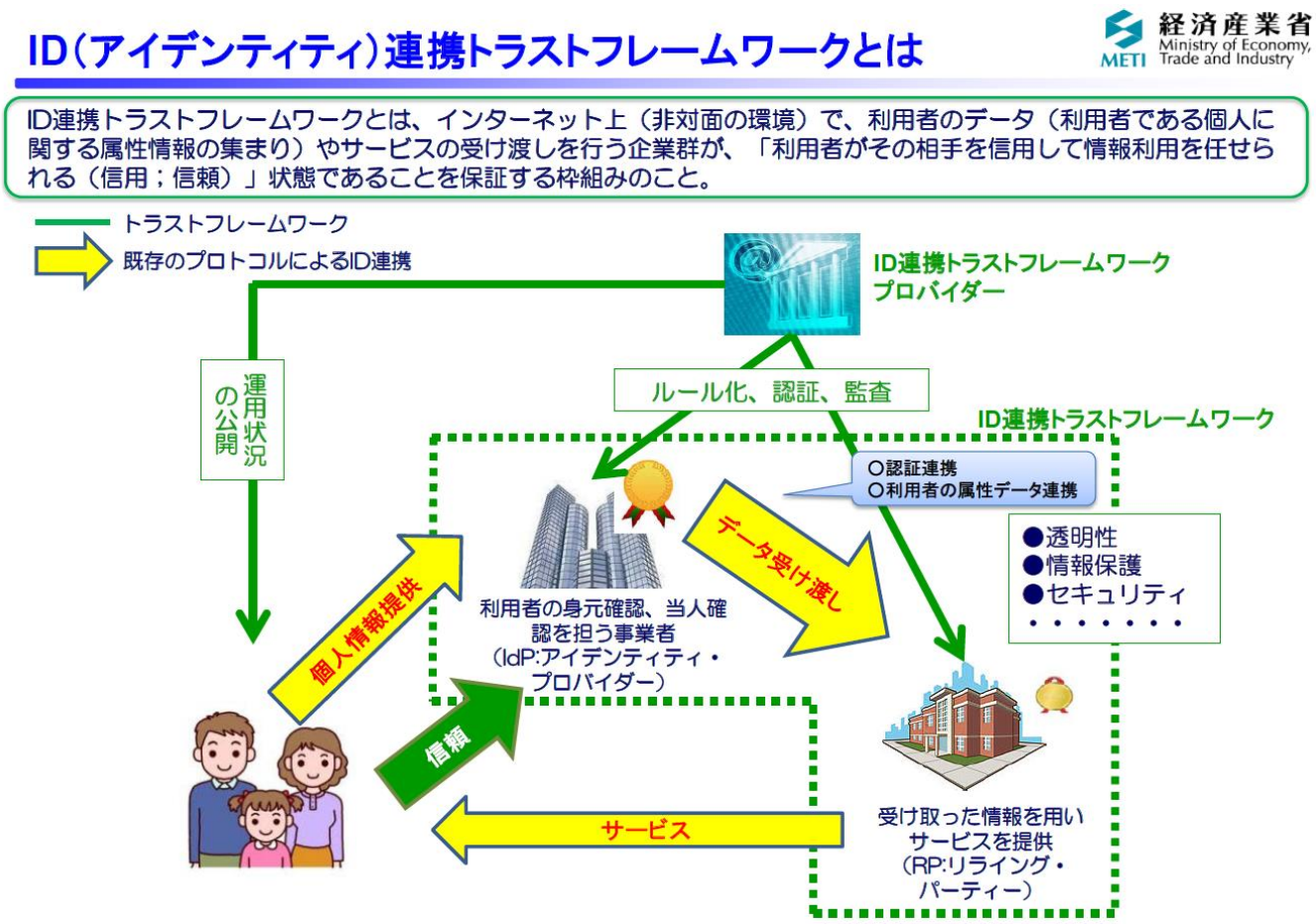


図 6　ID 連携トラストフレームワークのイメージ

ここで、利用者の身元確認、当人確認を担う事業者を IdP（アイデンティティ・プロバイダー）という。IdP は、利用者を認証する主体である。

また、受け取った個人情報をもとに利用者にサービスを提供する事業者を、RP（リライング・パーティ）という。RP は、IdPから、サービスの提供に必要な個人情報のみを受け取る。パスワード等の不要な情報は受け取らない。

ID 連携トラストフレームワークでは、そのトラストフレームワークに一つ、TFP（トラストフレームワーク・プロバイダー）と呼ばれる第三者機関がある。TFP は、トラストフレームワーク内のルールを作って、組織をチェック・監査して IDP や RP を認証することにより、上述の定義にある「利用者がその相手を信用して利用者本人の情報利用を任せられる（信用、信頼）」状態であることを保証する。TFP は、そのトラストフレームワーク全体の維持・管理の責任を負う監督者的役割を果たす。

ID 連携トラストフレームワークには二つの機能がある。一つは情報連携、すなわち、属性データ（ID）の授受である。もう一つは認証連携である。まず、認証連携について図 7 により説明する。

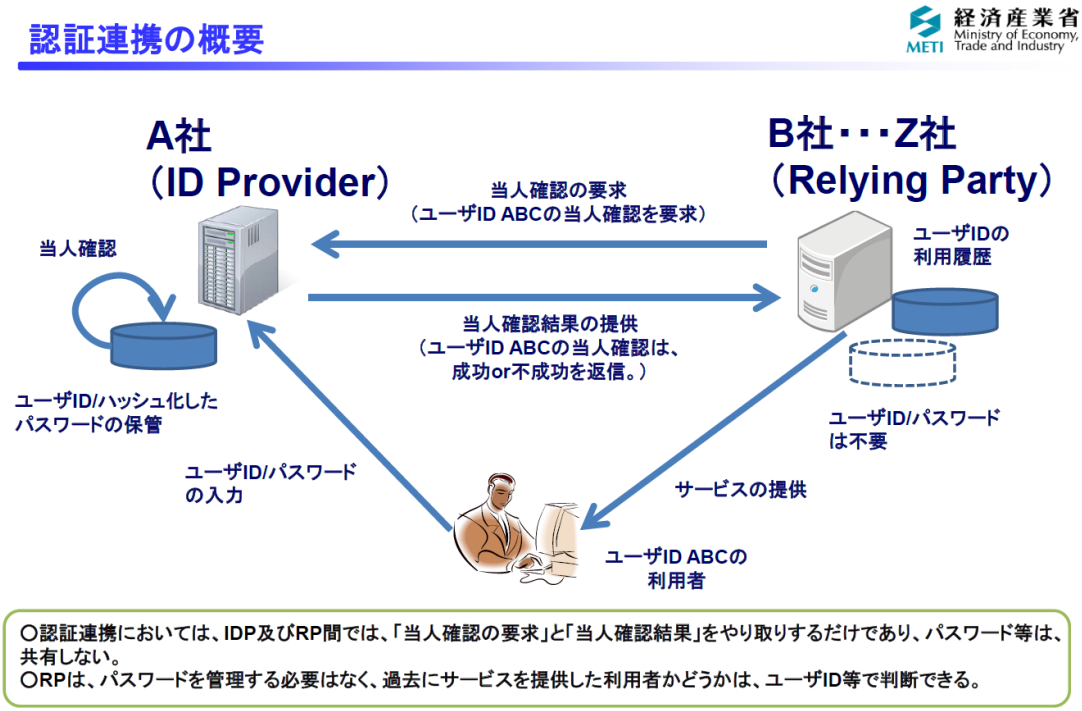


図 7　認証連携の概要

まず、利用者は、ユーザ ID とパスワードを IdP に登録する。次に、RP に対してサービスの提供を申し込むと、RP は、IdP である A 社に対して当人の本人確認の要求を行う。これに対して、IdP たる A 社は、本人確認が成功したか不成功であったかという情報だけを返す。このとき、パスワードは送らない。RP は、本人確認が成功したときのみ、利用者に対してサービスを提供する。 次に、利用者の属性データ連携を図 8 により説明する。

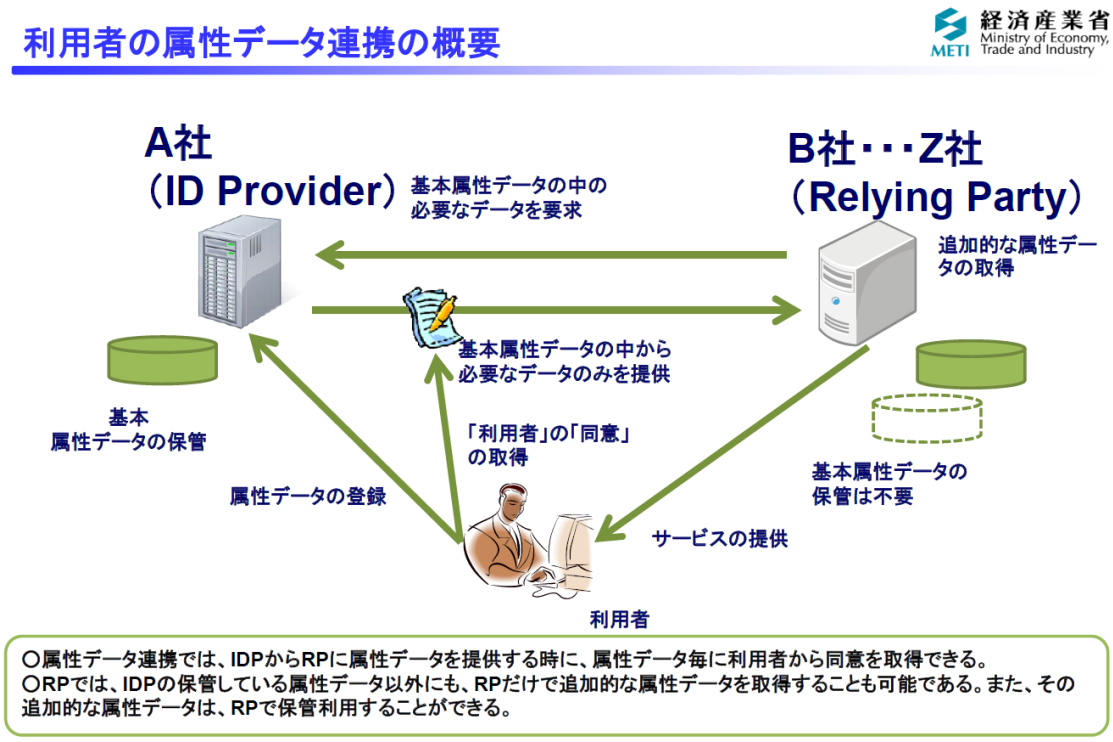


図 8　利用者の属性データ連携の概要

RP は、本人確認が成功すると、IdP たる A 社に、サービスに必要な属性データ（ID すなわちアイデンティティである氏名、住所等）を要求する。このとき、IdP たる A 社は、利用者本人に、要求された属性データをRPに提供してよいか否かについて確認し、同意を得る（そのトラストフレームワークのルールにより同意なしの提供も可とすることができる）。属性データの提供を受けたRPは、受領した属性データに基づき利用者にサービスを提供する。

利用者の画面の遷移により連携のイメージを説明したものが、図 9 である。

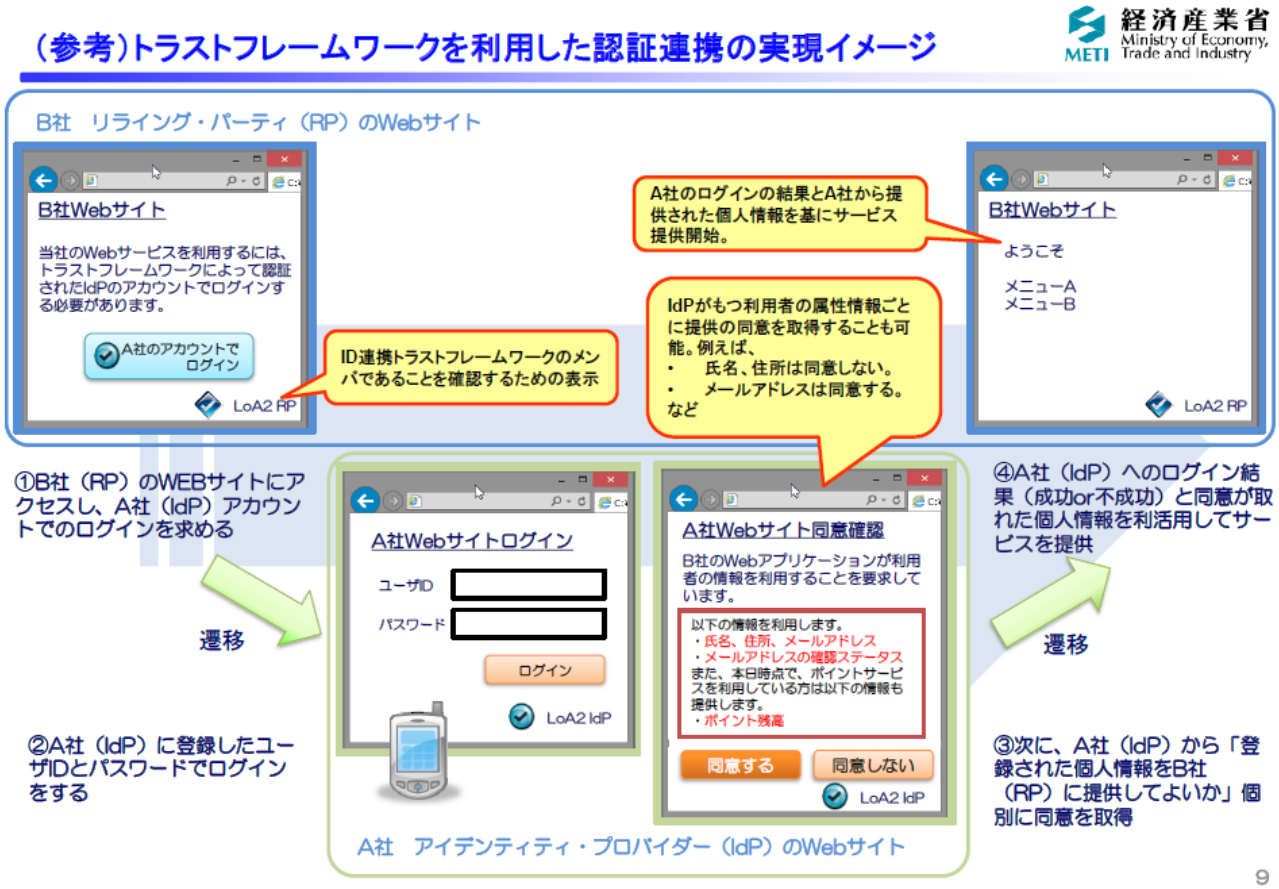


図 9　認証連携と属性データ連携における利用者側画面の遷移

利用者がB社の提供するサービスを受けようとして、①B社の当該サービス提供サイトにアクセスすると、図 9 の左上の画面が表示され、IdPのアカウントでのログインを求められる。画面はIdPたる A 社のサイトに遷移し、②A社に登録したユーザ ID とパスワードでログインする。このログインが成功すると RP たる B 社から必要な属性データの提供を IdP たる A 社に求める。A 社側は、利用者に対して、求められた属性データの提供可否の同意を、データ別に利用者に求める。この入力が完了すると画面は自動的に B 社サイトに遷移し、④B 社は、A 社から提供される利用者の同意が取れた属性データを利活用して、利用者にサービスを提供する。

なお、認証方式は SAML、OpenID Connect 等を想定している。もちろん、それ以外でも技術的に使用できるものは、使用しても問題ない。

最後に米国におけるトラストフレームワークについて、一言、触れたい。

6. 米国におけるトラストフレームワークについて

米国においては、GSA（U.S.General Services Administration）の ICAM（Identity、Credential and Access Management）Division が、トラストフレームワークのルール作りを行っており、このルールのなかに、TFP（トラストフレー

ムワーク･プロバイダー)認定等のルール、“Trust Framework Provider Adoption Process”がある。これに基づいてICAM Division が TFP の認定を行っており、すでに、四つの TFP が認定されている(表1参照、なお、TFP、IdP、RP等については、図 6 を参照されたい)。

また、一つのトラストフレームワーク内のIdP、RP 等の事業者の認定は、そのトラストフレームワークの TFP が行う。

なお、表1中の「LoA」とは、保証レベル(Level of Assurance)のことで、信頼性の保証の強さを示す指標である。

表1　米国における認定済みトラストフレームワーク一覧

認定済み トラストフレームワーク・ プロバイダ	特徴	IdP認定実績
InCommon	• Internet2（教育・研究機関向けネットワーク提供コンソーシアム）により運営される団体。 • 大学、非営利団体、研究機関などに対して、Bronze （LoA１相当） とSilver（LoA２相当）の認定サービスを実施。	• バージニア工科大学（Bronze及びSilver） • ネブラスカ医療センター大学（Bronze）
Kantara Initiative	• 2009年米国にてアイデンティティ関連の仕様やソリューションの相互運用を促進する業界団体（非営利団体）として設立。 • オンライン・アイデンティティに関連する法人会員のメンバーで運営される組織。	• シマンテック社：Norton Secure Login Service（LoA２～３） • ベライゾン社：Universal Identity Service（LoA１～３） • MITRE社： MITREid OpenID 2.0（LoA１） • エクスペリアン社：Precise ID（身元確認ベンダーとしてLoA２～３）。
Open Identity Exchange	• 2011年米国政府CIOの要請に基づき、OpenID Foundation（OIDF）とInformation Card Foundation（ICF）が非営利団体としてOIXを設立。 • オンライン・アイデンティティに関連する法人会員のメンバーで運営される組織。 • 米国政府の最初の認定トラストフレームワーク・プロバイダ。	• グーグル社（LoA１） • エクイファックス社（LoA１） • ペイパル社（LoA１） • ベリサイン社（LoA１） • ウェイブシステムズ社（LoA１） • 山形大学（LoA１） • ベライゾン社（LoA１～３）
SAFE-BioPharma	• 製薬関連の企業・団体のメンバーで運営される組織。製薬業界標準の電子署名ソリューションの普及活動を実施している団体も参加している。 • NIH（National Institutes of Health）、VA（Veterans Administration）、FDA（Food and Drug Administration）のオンラインサービスへのアクセスが可能な認証サービスの認定が中心。	• ベライゾンビジネスUIS社（LoA２～３） • Cegedim Relationship Management（LoA１） • AYIN International（身元確認ベンダーとしてLoA２～３） • エクイファックス社（身元確認ベンダーとしてLoA２～３）

講演、以上

【質疑】

Q1－1:個人情報保護法では、本人が第三者に個人情報の提供を拒否する権利があるが、ID 連携トラストフレームワーク内の RP(サービス提供事業者)に対して、個人情報の提供を拒否する権利があるのか。

A1－1:ID 連携トラストフレームワーク内の RP への提供であっても、IdP から個人情報を提供する際は本人の同意を取るのが原則である。図8と図9を参照されたい。これにより、第三者提供に対する本人の拒否権は担保される。

Q1－2:ID 連携トラストフレームワークのなかで、本人が、自身の個人情報の削除を求めることは可能か。

A1－2:標準プロトコル上はないが、日本で先行的に ID 連携の IdP を務めているヤフーでは実装しており、ログリストを後から見て、どこそことのデータ連携を削除せよと依頼して削除することができると聞いている。

Q2:ID 連携トラストフレームワークで代理人の制度は考えているか。

A2:マイナンバー制度のなかには、代理人の話が出てくるが、ID 連携トラストフレームワークでは、代理人を設けることは想定していない。

Q3：ID 連携トラストフレームワークにおける民民間の紛争において、ADR による紛争解決は考えているか。
A3：民民間の紛争解決には ADR が必要であると思う。これからの議論である。

Q4－1：米国の TFP（トラストフレームワーク・プロバイダー）の認定の仕組みと実績は、講演の最後の部分（報告者注、表1等）で分かったが、日本では、TFP はどこが務めるのか。
A4－1：マイガメントトラストフレームワークは政府が絡むので、TFP は政府が関係する機関がやることになると思うが、民民間のトラストフレームワークの TFP は民側でやるべきである。
Q4－2：筋論としてはそのとおりだと思う。米国は民主導の国であるからそれでよいだろうが、日本の風土では、民主導で TFP のような仕事をすることができるのであろうか。
A4－2：確かに民側で TFP を担うのは難しいであろう。しかし、ID 連携トラストフレームワークの趣旨に鑑みると、政府が主導権をとるのではなく、民側が自発的、自律的な運営を行うべきである。日本でも、民主導の認証制度で成功している例が一つある。それはプライバシーマーク認定制度である。立ち上がり時点では政府が絡んだが、現在は、民間主導で実施され、定着している。民民間のトラストフレームワークもこれを手本として、民主導で推進すべきと思う。

Q5：未成年者は、ID 連携トラストフレームワークに入ることができるか。
A5：未成年者の法定の権利の行使は、代理人によらなければならない。よって、ID連携トラストフレームワークでも同意、許諾等をすることができないので、ID 連携トラストフレームワークに入ることはできない。もともと、ID 連携トラストフレームワークは、一億国民全員が入ることを考えていない。これに対して、マイナンバーは全員に付与され、生まれてから死ぬまで基本的には同一の番号が使用される。
個人的には、ID連携トラストフレームワークの識別子としての ID は、目的に応じて複数持ってもかまわないと思っている。仕事で用いるID、消費者としてのID、趣味人としてのIDという具合である。例えば、デンマークでは、ビジネスマンとして、また、住民として ID を複数、取れる。二つまでは無料で三つ目以降は有料である。

Q6：ベネッセの個人情報漏えいなどを考えると、マイナンバーは、源泉徴収票への記載などで金融機関等、民間で取扱われるので、漏えい、不正利用等のリスクがあるのではないか。また、コンピュータで一元管理すること自体に問題があるのではないか。
A6：マイナンバーそのものは一人に一つであるが、先ほど説明したとおり、一元管理できないよう、情報連携はコアシステムを経由して行う（報告者注、図1参照）。ID/パスワードによる本人確認は、すでにリスト攻撃に耐えられず、たいへん脆弱なものになっている。そのためマイガバメントトラストフレームワークでの認証としては、複数要素認証を視野にいれた認証方法の検討が必要だと考えている。

【図表の出典】

・図1：内閣官房　社会保障改革担当室、「番号制度の概要」(2014.11) ⇒ 図1：スライド 6
http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/h2611_gaiyou_siryou.pdf
・図2、図 3：IT 戦略本部　新戦略推進専門調査会、「マイナンバー等分科会　中間取りまとめの概要」(2014.05.28)
⇒ 図2：スライド 2、図 3：スライド 3
http://www.kantei.go.jp/jp/singi/it2/senmon/dai5/sankou4_1.pdf
・図 4、図 5、図 6、図 9：経済産業省、「トラストフレームワークを用いた個人番号の利活用推進のための方策」(2014.4)
⇒ 図 4：スライド5、図 5：スライド6、図 6：スライド4、図 9：スライド9
http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number/dai3/siryou3.pdf

・図 7、図 8:経済産業省主催シンポジウム、「ID 連携トラストフレームワークが築く社会」(2014.10.23 開催)資料の経済産業省発表スライド「政府の IT 戦略と経済産業省の取り組み」⇒　図 7:スライド7、図 8:スライド8
http://www.meti.go.jp/policy/it_policy/id_renkei/sinpojiumutoukyo.pdf

・表1:一般財団法人日本情報経済社会推進協会(JIPDEC)、「平成 25 年度電子経済産業省構築事業『ID 連携トラストフレームワーク』の構築のための実証事業報告書」(2014.3)、54 ページ
http://www.meti.go.jp/policy/it_policy/id_renkei/houkokusyo.pdf

【参考ウェブサイト】

(1)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

(2)マイナンバー等分科会
http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number.html

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

【報告者所感】

たいへん新鮮な内容の講演であった。マイナンバー制度のアーキテクチャについて、これほどきちんとした説明を聴くのは、ほとんどの参加者にとって初めてではないか。行政機関間での情報連携がすべてコアシステムを経由して行われ、その記録が保管されることにより、行政機関間での情報提供の履歴を本人が閲覧できるという説明で、マイナンバー制度に対する懸念がかなり解消されたと思う。

この、情報連携の記録閲覧に使用されるマイポータルを、マイガバメントトラストフレームワークや、さらには、民間の ID 連携トラストフレームワークまで拡張する話は圧巻であり、ID 連携トラストフレームワークが、ますます深化するデジタルネットワーク社会の社会インフラとして重要な位置を占めることを、予感させるものであった。

報告者として謝らなければならないことが二点ある。

一点は、講演の内容が広範なものであったため、紙面の都合で報告内容をかなり割愛せざるを得なかったことである。個人番号と同時に付与される法人番号の紹介と ID 連携の保証レベルに関する説明を、重要な内容であるにもかかわらず全面的にカットした。

二点目は、ID 連携トラストフレームワークの説明が十分できなかったことである。ID 連携トラストフレームワークは、その仕組みを理解するのにはかなりの時間を要し、とても一講演の中に収まるものではない。おそらくこの報告だけではご理解いただけないと思う。ID 連携トラストフレームワークについて詳しく知りたい方は、参考ウェブサイト(3)にアクセスし、そこに紹介されている資料を参照されたい。また、当協会の2014年の会報、5月号(158号)、6月号(159号)、7月号(160 号)及び10月号(163 号)の「情報セキュリティ研究会だより」に、ID 連携トラストフレームワークの紹介記事が連載されているので、こちらも参照されたい(会報のバックナンバーは、協会のホームページからダウンロード可能)。

以上

＜目次＞

2014.12

第 25 回ＣＳＡフォーラム開催【システム監査法制化・制度化に向けて】

会員番号　6005　斉藤　茂雄　（CSA 利用推進 G）

今回のフォーラムはSAAJ近畿支部から田淵隆明様を講師としてお招きして、理事会テーマである法制化検討PJの会合を兼ね開催しました。ご承知のように近畿支部では早くからシステム監査法制化研究会を組織し、研究を進めております。今回関東地区では初めての成果報告となりましたが、情報システムが社会の重要インフラとして浸透している中で、情報システムによる事故やトラブルを未然防止するためのシステム監査法制化の必要性について、具体的でわかりやすいお話をいただきました。参加者からは、法制化実現には課題も多く、業界によっても温度差があることから、業界毎のフレームワークやアプローチが必要、日本内部監査協会、日本 IT ガバナンス協会など他団体とも連携して進めていくことが望ましい、などといった建設的な意見が多く出され、大変有意義な2時間でした。

開催の概要は以下です。終了後講師を囲んで短時間ですが懇親会を実施しました。

タイトル：「システム監査法制化・制度化に向けて」

概要（当日使用スライドより）：

スライド目次：

0. 近畿支部における法制化研究会の活動の歴史及び目標
1. システム監査の法的義務化・「システム監査人」の選任義務化
   - 1．1　最近のシステム開発の動向
   - 1．2　今、やるべきこと(システム監査の法的義務化)
   - 1．3　プログラム準備金の復活
   - 1．4　公共システム・重要インフラ等の外部監査の義務化
2. 新しい IT 事業者評価制度の創設
   - 2．1　新しい「 IT 事業者評価制度」の在り方とは？
   - 2．2　特別に考慮した事項
3. 企業経理における研究開発費の資産計上の復活
   - 3．1　企業経理における研究開発費の資産計上の復活
   - 3．2　会計制度の変遷
4. ソフトウェアに対する製造物責任法(PL 法)の適用
   - 4．1　製造物責任法とは
   - 4．2　ソフトウェアと PL 法
   - 4．3　組み込み以外のソフトウェアでの問題事例

開催日時： 2014 年 11 月 21 日(火) 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＞

2014.12

新入法人会員紹介　【　特定非営利活動法人 東京 IT コーディネータ　】

会員番号　6068 矢野　一男 （法人部会）

新たに法人会員となられた**特定非営利活動法人 東京 IT コーディネータ様**より、メッセージをいただきました。

NPO法人 東京ITコーディネータは、平成26年4月に設立満10年になりましたが、現在は、複数の資格と多分野の経験を持つコンサルタント16名で構成しており、中堅・中小企業のIT経営の支援を中心に、コンサルティング分野及び研修分野に携わっております。例えば、PマークやISMSの認証取得支援、内部統制の構築支援等について多くの実績を有しております。

システム監査については設立当初より手がけており、近年は複数の会員が日本システム監査人協会(SAAJ) の公認システム監査人の資格を取得し、監査品質の向上に努めております。

常に、ベンチャー精神とボランティア精神を両立させながら、中堅・中小企業の経営基盤の強化を中立的な立場から支援することを目指しております。

この度、SAAJの法人会員になったことを機に、より多くの業種・業態の中堅・中小企業の方々との出会い、そしてご支援できることを期待しておりますので、宜しくお願い致します。

ホームページ ： http://www.npo-tokyoitc.jp/

＜目次＞

2014.12

～「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５
2-2-3-3. 従業者の監督（法第２１条関連）2-2-3-4. 委託先の監督（法第２２条関連）

会員番号　6005　斉藤茂雄　（個人情報保護監査研究会）

2-2-3. 個人データの管理（法第１９条～第２２条関連）

2-2-3-3. 従業者の監督（法第２１条関連）

法第２１条
個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

安全管理措置を遵守させるよう、従業者を監督する際は事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じることが必要です。

※個人情報保護監査研究会注:「従業者」には雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）だけではなく、取締役、執行役、理事、監査役、監事、派遣社員等も含まれます。

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

※個人情報保護監査研究会注:2014年9月26日のGL改正案では、随所に上記中小企業者云々の追記があります。これは、大規模な個人情報漏えい事件を受け、事業者の安全対策措置の強化を求めていますが、一方では中小企業者に過剰な負担を強いない配慮といえます。

【従業者に対して必要かつ適切な監督を行っていない場合】

事例1）従業者が、安全管理規程等に従って業務を行っていることを確認せず、結果、個人データが漏えいした場合

事例2）規程等に違反してパソコン又は外部記録媒体を持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】

個人データの取扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリングを実施する場合は、次の点に留意する。

- モニタリングの目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
- モニタリングの実施に関する責任者とその権限を定めること。
- モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程を策定するものとし、事前に社内に徹底すること。
- モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。

2-2-3-4. 委託先の監督（法第２２条関連）

法第２２条

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

事業者が、個人データの取扱いを委託する場合、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、事業の性質及び個人データの取扱状況等に起因するリスクに応じた、必要かつ適切な措置を講じることが必要です。

「必要かつ適切な監督」には、委託先を適切に選定すること、必要な契約を締結すること、委託された個人データの取扱状況を把握することが含まれます。

※ご参考（2014年9月26日に追加された、経産省GL改正案。）

（略）必要のない個人データを提供しないようにすることは当然のこととして、特に、中小企業者においては、自ら又は委託先の事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

（略）個人データの取扱状況を把握することが含まれる。

なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

※個人情報保護監査研究会注：中小企業者での措置の追記については先の従業者の監督と同様に、中小企業者に過剰な負担を強いない配慮といえます。また委託元が優先的な地位を利用して委託先に過度な負担を強いることが無いよう付記されました。

①委託先の選定

委託先の選定に当たっては、個人データの安全管理措置が、法で求められる安全管理措置と同等であることを確認する。また、委託先の評価は適宜実施する。

※個人情報保護監査研究会注：経産省GL改正案では、委託先企業からの大規模な個人情報漏えい事件の事例を踏まえ、委託先での安全管理措置の徹底と委託元による実地検査が今回追記されました。

※ご参考（2014年9月26日に追加された、経産省GL改正案。）

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第20条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、個人情報保護管理者（CPO）等が、適切に評価することが望ましい。

（ア）組織的安全管理措置

- 個人データの安全管理措置を講じるための組織体制の整備
- 個人データの安全管理措置を定める規程等の整備と規程等に従った運用
- 個人データの取扱状況を一覧できる手段の整備
- 個人データの安全管理措置の評価、見直し及び改善
- 事故又は違反への対処

（つづき）

（イ）人的安全管理措置

- 雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結
- 従業者に対する内部規程等の周知・教育・訓練の実施

（ウ）物理的安全管理措置

- 入退館（室）管理の実施
- 盗難等の防止
- 機器・装置等の物理的な保護

（エ）技術的安全管理措置

- 個人データへのアクセスにおける識別と認証
- 個人データへのアクセス制御
- 個人データへのアクセス権限の管理
- 個人データのアクセスの記録
- 個人データを取り扱う情報システムについての不正ソフトウェア対策
- 個人データの移送・送信時の対策
- 個人データを取り扱う情報システムの動作確認時の対策
- 個人データを取り扱う情報システムの監視

②委託契約の締結

委託契約には、安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における個人データの取扱状況を把握することを盛り込む必要があります。

③委託先における個人データ取扱状況の把握

※個人情報保護監査研究会注：経産省GL改正案では、委託元による委託先の監査の実施とともに、再委託・再々委託についても、安全管理措及び監査等による監督を行うよう明記されました。個人情報保護法では、監査については踏み込んでいませんが、経産省GL改正案により、委託先の安全管理措置の実施を確実なものにするため、監査の重要性が、より明確に示されたと言えます。

※ご参考（2014年9月26日に追加された、経産省GL改正案。）

委託先における委託された個人データの取扱状況を把握するためには、定期的に（少なくとも年1回）、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者（CPO）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

（略）

委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人情報の扱い方法等について、委託先から事前報告又は承認を求める、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施する

（略）

【委託を受けた者に対して必要かつ適切な監督を行っていない場合】

事例1）安全管理措置の状況を把握せず外部の事業者に委託した場合で、委託先が個人データを漏えいした場合

事例2）安全管理措置の内容を委託先に指示せず、結果、委託先が個人データを漏えいした場合

事例3）再委託の条件に関する指示を行わず、委託先が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

- 委託元及び委託先の責任の明確化
- 個人データの安全管理に関する事項
- 個人データの漏えい防止、盗用禁止に関する事項
  - 委託契約範囲外の加工、利用の禁止
  - 委託契約範囲外の複写、複製の禁止
  - 委託契約期間
  - 委託契約終了後の個人データの返還・消去・廃棄に関する事項
- 再委託に関する事項
  - 再委託を行うに当たっての委託元への文書による報告
- 個人データの取扱状況に関する委託元への報告の内容及び頻度
- 契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
- 契約内容が遵守されなかった場合の措置
- セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

※個人情報保護監査研究会注：経産省GL改正案が、8月に続けて10月にも示されたのは、委託先からの情報漏えい事件が社会問題になっているためと思われます。 委託先からの情報漏えいは、委託元にその責任があり、自社と同様の安全管理を行わせると言っても、実際にどこまで委託先に要求してよいのか、企業の悩みどころでした。 経産省GL改正案では、委託先を管理する細かな手法まで踏み込んで示され、確実な安全管理がなされるよう配慮されています。

次回は、「2-2-4.第三者への提供（法第23条関連）」の読みこなしポイントを掲載します。

バックナンバー目次 http://1.33.170.249/saajpmsMETIGL/000METIGL.html

（↑バックナンバー目次のURLが変更となりました。）

（注）

「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」（平成26年12月12日 厚生労働省・経済産業省告示第4号）が公表されました。

改正の要点については、次回掲載します。

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

■

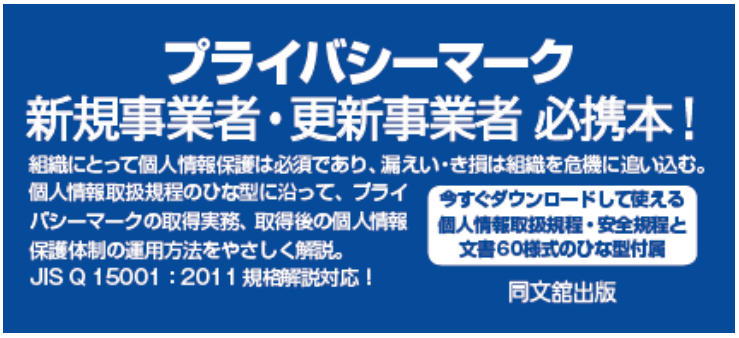
＜目次＞

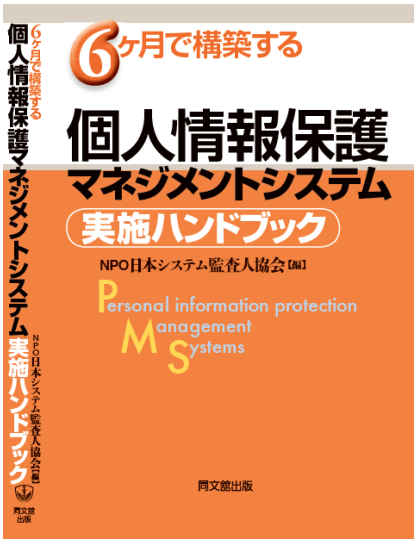
2014.12

６か月で構築する【個人情報保護マネジメントシステム実施ハンドブック】刊行

会員番号　1760　斎藤由紀子　（個人情報保護監査研究会）

１．「個人情報保護マネジメントシステム実施ハンドブック」
　　がついに、本になりました！

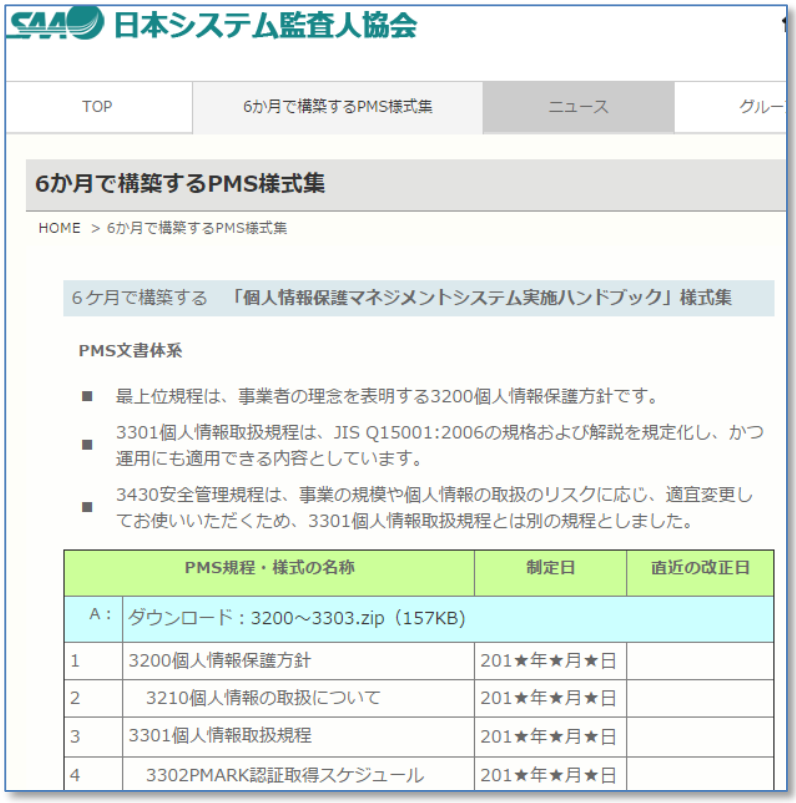




価格：2700円（＋消費税）　A5版　188ページ
ご購入は、アマゾンから、または以下のサイトから！！

http://www.e-hon.ne.jp/bec/SA/Detail?refBook=978-4-495-20121-0&Rec_id=1010

ひな形のダウンロードページ



※ひな形のダウンロードを
　ご希望の方は、
　ご購入後に、
　ＰＭＳ読者会員登録が必要です。
　詳細は本誌に！

！注目お得情報！：今なら次のページを印刷して出版社にFAXすると、特別価格で購入できます。

特別価格：2500円（送料・消費税込）

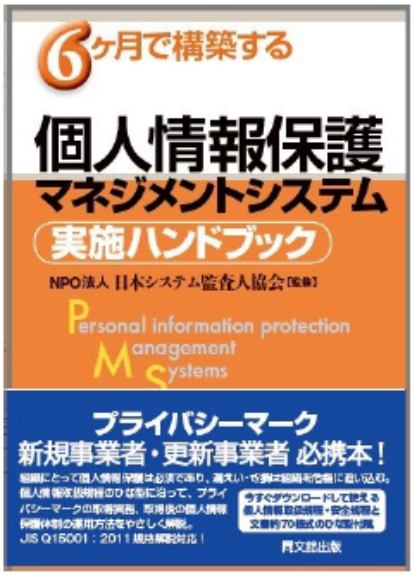
＜目次＞

特 別 頒 布 のご 案 内

プライバシーマーク新規事業者・更新事業者必携本！

6ヶ月で構築する
個人情報保護マネジメントシステム
実施ハンドブック

NPO法人**日本システム監査人協会【監修】**



A5判・208頁・並製
本体価格2,700円(税抜)

JIS Q15001：2011規格解説対応！

個人情報取扱規程のひな型に沿って、プライバシーマークの取得実務、取得後の個人情報保護体制の運用方法をやさしく解説！

【目次】

今すぐダウンロードして使える
個人情報取扱規程・安全規程と文書約70様式のひな型付属！

◆**申込方法**　同文舘出版宛てに、FAXまたは郵送で以下の申込書を使ってお申し込みください。
同文舘出版株式会社　〒101-0051　東京都千代田区神田神保町1-41
TEL 03-3294-1801　　FAX 03-3294-1807

◆**支払方法**　現品到着後、同封の請求書によりお支払い願います。

※特別頒布価格は、以下申込書利用者限定で、書店ではお申し込みできません。

お申込みはFAXで　同文舘出版　03-3294-1807

同文舘出版(担当：福井)行き　　平成　年　月　日

書　名	特 別 価 格	ご 注 文 冊 数
6ヵ月で構築する 個人情報保護マネジメントシステム実施ハンドブック (ISBN：978-4-495-20121-0)	定価2,916円＋送料を →2,500円 (税・送料込)	

貴社名　　貴部門名　　ご担当者名
お届け先住所　　〒　　TEL (　)

※ご記入いただいた個人情報は、お申込みをいただいた書籍の発送目的のためにのみ使用させていただきます。

2014.12

支部報告　【　西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ　報告　】

会員番号　1709　荒町　弘　（近畿支部）

近畿支部が事務局となり、「西日本支部合同研究会　in　OSAKA」を開催しました。

・テーマ:「ICTによる災害に強いしなやかな社会の実現とシステム監査の重要性」
・日時:2014年11月29日（土）　～　11月30日（日）
・場所:国際カンファレンスプラザ　Ａ－3会議室（大阪市）
・主催:特定非営利活動法人日本システム監査人協会
　　北信越支部，中部支部，近畿支部，中四国支部，九州支部
・後援:経済産業省近畿経済産業局，ISACA大阪支部，日本ITストラテジスト協会
　　特定非営利活動法人 ITコーディネータ協会，システム監査学会
・次第:
　「大震災が情報システムに訴えていること」
　　日本システム監査人協会　副会長　中山　孝明様
　「クラウドソーシングによる災害対策」
　　近畿支部　吉田　博一様（前　近畿支部長）
　「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」
　　北信越支部　支部長　宮本　茂明様
　「グローバル展開している自動車部品製造業者の国際間 BCP 事例紹介」
　　中部支部　原　善一郎様（元　中部支部長）
　「事業中断計画とシステム監査」
　　九州支部　副支部長　舩津　宏様
　「近畿支部BCP研究プロジェクト活動報告」
　　近畿支部 BCP 研究プロジェクト　金子　力造様

2014 年 11 月 29 日(土)、日本システム監査人協会西日本の5支部（北信越、中部、近畿、中四国、九州）合同での西日本支部合同研究会を開催しました。

来年は、阪神・淡路大震災の発生から20年の節目の年となることもあり、統一テーマを「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」と設定し、協会本部および西日本支部の会員各位より発表していただきました。

参加人数は、発表者を含めて総勢57名で、日本システム監査人協会39名（北信越支部3名、中部支部7名、近畿支部22名、中四国支部2名、九州支部3名、他支部2名）、後援団体16名、一般参加2名でした。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

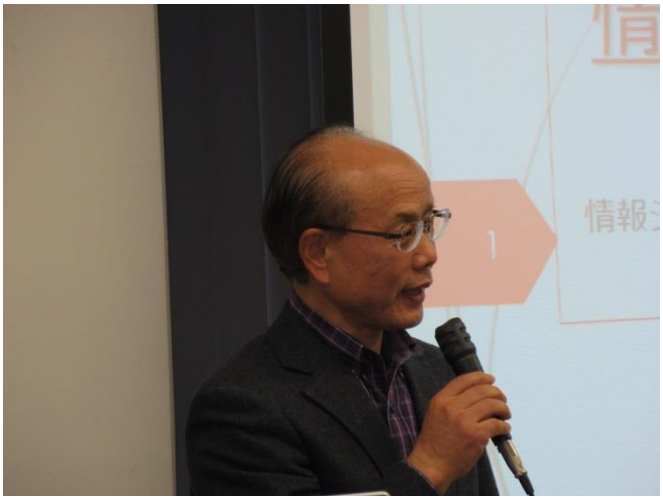
◇発表１　　報告者　会員番号　0264　三橋　潤　（近畿支部）

【講演テーマ】

『大災害が情報システムに訴えていること』

【講師】

日本システム監査人協会　副会長　　中山　孝明様



【講演内容】

大震災による情報システムの被災状況を具体的にみると、既往の災害予防や復旧策の多くが、机上の対策に過ぎないことがよく分かる。大震災の教訓は生かされているか、システム監査はその実用性・実効性を検証しているか、などについて考える。

・阪神淡路大震災では、「不足している対策が分かった」、「おざなりだった訓練や着飾った体制図と画餅だったBCP」等を学んだ。そして、東日本大震災では、「再度、思い知った対策の不備」を痛感した。

・被災で判明した対策不備の実例として、次の様な事項が挙げられる。

被災例：緊急連絡が混乱／輻輳　→　緊急連絡一覧表が役立たなかった。電話連絡が混乱した。

被災例：建物やマシン室が被害大　→　耐震／免震強度が不足。入室不可や室内が使用不可状態に。

被災例：自家発電機が役立たず　→　燃料タンクや配管が耐震不足により故障した。

被災例：業務が復旧／継続できず　→　復旧に必要なデータが使用できず。業務復旧が混乱した。

・以上の対策不備例から、形だけの対策から現実的な対策として、「通信手段、情報収集、情報集中こそ対策の要」を始めに31の項目について列挙した。対策検討のポイントとしては、「標準的なガイドラインは、自社にとっては曖昧だらけ」ということに注意しなければならない。

【所感】

講師は、永年某都市銀行の勘定系システム等の企画／開発／運用などを担当されており、金融庁に勤務されたご経験も有られる。講演では、現実的で具体的な対策の数々を提言していただき、非常に参考になった聴講者も多かったと思われる。私も某コンピュータメーカに勤務していた時に、阪神淡路大震災が発生し、業務停止した数多くの顧客システムを如何にして立ち上げるかを、混乱と錯誤のなかで大変苦労した経験がある。

「備えあれば憂いなし」の格言や、「天災は忘れたころにやってくる」の言い伝えを、肝に銘じておく必要があることを再認識した講演であった。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

◇発表２　　報告者　会員番号　0169　林　裕正　（近畿支部）

【講演テーマ】

『クラウドソーシングによる災害対策』

【講師】

日本システム監査人協会　近畿支部　吉田　博一様

【講演内容】

これまで災害対策は、行政が情報を収集し、避難などの対策を講ずるものであった。海外では、クラウドソーシングのサービスが災害時に活用され，官民連携が進んでいる。日本における官民連携によるレジリエンスな耐災害性の高い社会システムについて、考察する。

・「レジリエント」とは、「弾力的な、柔軟な」の意味であり、「レジリエンス」は、「システムの機能を維持するために変化を吸収する能力」と定義した例もある。

・米国等では「オープンガバメント」と呼ぶ「行政」と「住民」との双方向の協力による施策が進められており、その類型として「クラウドソーシング」が挙げられる。これは、「アウトソーシング」という形で外部の専門業者に業務を委託するのではなく、インターネットを利用して不特定多数の人に業務を委託する形式である。

・クラウドソーシングの例としては、行政への通報処理をWebで実現した米国の「Open311」等がある。

・日本の災害対策は、官主導であるが、行政による情報収集に限界があることや、住民ニーズの把握が不十分であることは解決できていない。しかし、千葉市等で「Open311」に相当する実証実験が開始されている。日本においては災害時に特化した住民との双方向のやりとりは、東日本大震災において一部利用された実績はあるが、組織的な取り組みとはなっていない。平常時から災害時の対応までを考慮したオープンガバメントによる災害対策が有効であると考える。

・　このようなクラウドソーシングなどレジリエンスを取り入れた災害対策は、行政だけでなく、企業等あらゆる組織で取り組む必要がある一方、このようなレジリエンスに対応したシステムに対するシステム監査の手法の確立が課題である。

【所感】

講演者は、これからの住民サービスにおいては、行政側だけでなく、住民を含めた民間との協力が不可欠であると主張している。しかし、有事の際の対応だけでは、いざという場合に機能しないため、平常時から体制を確立しておくことが重要である。今後、更に高齢化社会が進むことを考えると、地域における高齢者の支援活動等と、うまく連携できれば可能性は十分あると思われる。これらのサービスや活動を支えるためICTの活用は必須であり、その分野でシステム監査人の新たな活動範囲が広がることを期待したい。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

◇発表３　　報告者　会員番号　0169　林　裕正　（近畿支部）

【講演テーマ】

『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』

【講師】

日本システム監査人協会　北信越支部　宮本　茂明様

【講演内容】

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として実効性向上を目指したコンティンジェンシープランの策定整備が行われている。これらの取組事例とそのシステム監査について北信越支部会員による意見交換をもとに報告する。

・日銀より東日本大震災における金融機関の対応について2011年6月に報告がなされており、更に2013年1月にBCPの整備状況に関するアンケート調査が公開されている。これらによると、金融機関は全体としては震災後も安定的に業務を継続し、決済機能を維持できたが、一方で認識していなかった課題も浮かび上がった。従来のコンティンジェンシープランで想定していなかった事象が発生し、準備していた対策が十分に機能しなかった事例があった。アンケートの結果によると、例えば震災後に新たに追加した原因事象として、「原子力関連施設の事故」、「計画停電」、「津波」等が挙げられている。また、実効性で不十分であると評価した事項として、「要員の確保」、「マニュアルの整備」がある。

・金融機関ではシステムの共同化が進んでおり、特に基幹系システムについてはバックアップセンターも整備されているが、基幹系以外のシステムについては十分整備できていない事例もある。また、日銀のアンケートでは、従来から認識されていたシステムの切替え時の決済データ欠落への対応が改めて重要であると認識されている。

・これらを踏まえ、金融機関ではコンティンジェンシープランの見直しが進んでいるため、それに対するシステム監査についても、新たな視点も加味して実効性のある監査を実施する必要がある。

【所感】

金融機関は、情報システムの分野においても監督官庁や日銀による検査・考査を受けている。事業継続の分野でもFISCより事業継続計画策定のガイドラインが公開されており、その取組は他業界よりは進んでいると考える。しかし、東日本大震災の経験を踏まえ、見直しが必要な事項も明確になり、その対応が進むものと期待される。システム監査においても行政機関や社会インフラを担う企業との連携等も考慮した新たな監査視点が必要になると思われる。今後の北信越支部での研究活動に期待したい。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

◇発表４　　報告者　会員番号　1710　小河　裕一　（近畿支部）

【講演テーマ】

『グローバル展開している自動車部品製造業者の国際間BCP事例紹介』

【講師】

日本システム監査人協会　中部支部　原　善一郎様

【講演内容】

自動車部品製造業においては、顧客が海外生産に重点を移している現状であり、それに追随して生産の軸を海外へ移さなければ生き残れない状況になりつつある。その海外でも日本と同等の品質を求めたいが、「仕事への執着」や「費用・単価の違い」等、さまざまな困難がある。

一方で、「大災害対策」という面においては、この「グローバル展開」を有効に活用して「強み」にすることができ、その取り組みとして当社が進める国際間ITのBCP/DRに関する活動として下記3つを実現した。

・日本から海外子会社のサーバやパソコンを遠隔修理
・日本＋香港＋USAの3カ所にデータバックアップのミラーサイトとファイルサーバ設置
・TV会議を利用した月例IT会議の実施

また、現在計画中の国際間ITのBCP/DRに関する活動は下記のとおり。

・本社の大災害時に、海外子会社によるミラーサイトでの自立的復旧活動
・海外子会社の近隣会社同士での協力体制構築

国際間BCPの問題点である、人・距離・費用・セキュリティの課題を解決し国際間BCPを確固たるものにしたい。

【所感】

原様は、実施に国際間BCP/DRの構築に従事されており、生々しい分析結果や苦労談を交えて話をして頂いた。実際に現地に何回も行かれており、現地での対応に苦労しておられるため内容もかなり詳細であり、また、海外の事例であるにもかかわらず「すぐそこで発生している驚くべきこと」といった内容のようで、すんなりと頭の中に入ってくる内容でありました。原様の業界だけでなく、さまざまな分野で「海外進出」「オフショア」は拡大していくと思われます。そのような環境を有効に利用する国際間BCP/DRに関する内容は、今後実践しなくてはいけないと考えているかたには特に有用な講演でした。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

◇発表５　　報告者　会員番号　0645 是松　徹　（近畿支部）

【講演テーマ】

『事業中断計画とシステム監査』

【講師】

日本システム監査人協会　九州支部副支部長　　船津　宏様

【講演内容】

事業継続計画では、事業継続にかかるリスクを想定し、BC（Business Continuity）と DR（Disaster Recovery）を検討し、準備を日常の業務に反映する。しかし、多くの中小企業では何処まで実施するか など迷いも多く難しいものである。そこで、DR を伴わない事業継続計画を事業中断 計画として、再起を前提とした事業の撤収の仕方を考え、事業継続計画のひとつの方法論と監査について考察する。

・災害復旧（DR）を考えない事業継続計画、すなわち、事業を一旦放棄する計画を事業中断計画と名前を付けて考えてみた。この計画の目的は、危機・災害の発生に対して、人の安全を前提に現事業が二次災害を引き起こすことなく、地域や顧客などへの影響を最小にして撤収するものである。全てを失っても、信用・信頼を残し、再起を図ることを方針・目的としている。

・事業中断計画では、以下の事項がポイントとなる。

「初動対応」：二次災害の防止、従業員の参集、安否・被災業況の把握

「顧客・協力会社への連絡」：納品遅延・供給停止依頼の連絡

「中核事業継続方針立案・体制確立」：処分・再利用等の方針決定、事業中断体制構築等

「顧客・協力会社向け対策」：取引調整

「従業員・事業資源対策」：応急措置

「財務対策」：運転資金の確保・支払

・事業中断計画は、このポイントが確実にできること、よりスムーズにできることを検討し、計画する。事業所や工場のレイアウト、資材の保管方法や日常の活動 などについて、業務効率化だけでなく事業中断（事業継続）の視点を加えて見直しを行う。

・事業中断計画への監査視点は以下の通りであり、事業継続計画への監査視点にもなり得ると考える。

①「事業中断計画」の視点でのリスクアセスメントは適切であるか

②管理策は、すでに「事業継続日常対応」に反映されるか、「事業継続対応計画」に含まれているか

③「事業継続日常計画」での日常運用や訓練などで、「事業中断計画」は効果が期待できるか

④ 「事業中断計画」は、事業や環境の変化に追従しているか。

【所感】

最初に「事業中断計画」と聞いた時は、ずいぶん開き直った、ある意味無責任な計画だなと思ったが、発表を拝聴し、そうではなく、現実を踏まえ、人の安全と再起前提とした事業の撤収の仕方を考えた計画だということが理解できた。事業中断計画においても、被災直後の非常対応がスムーズにできるように、あらかじめ日常の活動等の中で留意しておくことが重要であり、この点では事業継続計画と同様であると感じた。最後に事業中断計画の検討が、すでに立案済の事業継続計画の網羅性・適切性の検証になり得るとの提言をいただき、改めて実効性のある事業継続計画とは何かを考えるきっかけとなった。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

◇発表６　　報告者　会員番号　1709　荒町　弘　（近畿支部）

【講演テーマ】

『近畿支部BCP研究プロジェクト活動報告』

【講師】

日本システム監査人協会　近畿支部　金子　力造様

【講演内容】

本プロジェクトでは、大災害の経験を踏まえ、IT-BCP と初動対応をテーマに研究を行ってきた。本年度は、その成果を基に IT 部門の初動対応をモデルに訓練を通じた気づきの重要性について提示する。

・ITは、事業継続に必須の経営資源であり、コア業務のみだけでなく社内の全業務と関係している。
・東日本大震災の教訓から、初動のスピードと的確さが復旧に大きく影響するという認識が高まった。
・災害発生直後の対策本部では、意思決定に必要な3つの情報コントロール（情報収集・発信・共有）が重要。
・災害発生後の初動フェーズでは重要業務の仮操業に必要なITが使えるようIT部門はICTインフラに責任を持つ。

経営トップの理解が得られにくく、投資効果が分かりにくいIT-BCPに関する取り組みは後回しにされがちである。IT-BCPの普及のためには、まず取り組むための動機「気づき」が必要なのでは？と考え、今年度はセミナーグループの協力により災害発生直後の初動対応演習を含めたIT-BCP体験セミナーを開催した。

演習では災害発生直後のIT部門の初動についてケースシナリオにもとづき受講生に体験していただいた。災害直後の限られた時間での状況把握・優先順位付け・意思決定・指示出し、という作業を2チームで実施した。インバスケット演習により限られた時間で多数の案件を処理する演習は受講生からも高い評価を得ることができた。演習後は「危機対策本部の実際」と「訓練・演習で鍛えるIT-BCP」の2つの講演も行い、こちらも受講生から高い評価を得られた。

本プロジェクトの最終目的であるIT-BCP監査に向け今後も実践的な普及セミナーを企画していく予定である。

【所感】

今回のセミナーは、IT-BCP普及を支援する本プロジェクトの新たな一歩を踏み出すものであり、訓練を通じて見えてくるIT-BCPの必要性やポイント・気づきがあるということを十分体感してもらえるセミナーでありました。今後も、受講生のレベルを想定しながらステップアップできるセミナーとして進めていきたいと思います。

2014.12

研究会活動報告【「西日本支部合同研究会　ｉｎ　ＯＳＡＫＡ」報告】

◇情報交換会

報告者　会員番号　0645　是松　徹　（近畿支部）

合同研究会終了後、会場の国際カンファレンスプラザからすぐ近くの店に場を移し、情報交換を兼ねて懇親会を開催しました。本部、各支部からのご出席者も参加いただいて総勢26名となり、盛況の内に終了しました。

情報交換会では各支部の活動内容の紹介や、情報共有、また支部活動の他支部への展開等についての相談を行うなど交流を深める場になったと思います。また、本部、各支部、ISACA（後援）からも一言いただき、盛り上がりが一層増すきっかけにもなりました。情報交換会の意義を再認識し、通常の定例研究会後の情報交換会活性化の必要性を改めて感じた次第です。

◇施設見学（2 日目）

報告者　会員番号　1709　荒町　弘　（近畿支部）

研究会 2 日目は大阪府の運営する施設、大阪府「津波・高潮ステーション」の見学を 12 名の参加を得て行いました。水害に関する大阪の歴史や大阪府が進めてきた津波・高潮への対策状況等について理解する場を持つことができました。

学生の修学旅行の見学コースにもなっているようで当日は学生の団体客も訪れていました。

津波・高潮ステーションの紹介ページ
http://www.pref.osaka.lg.jp/nishiosaka/tsunami/index.html

津波・高潮ステーションのマスコットキャラクター「なみのすけ」

◇西日本支部合同研究会を振り返って

報告者　会員番号　1709　荒町　弘　（近畿支部）

今回で 12 回目となる西日本支部合同研究会は関係者のご協力のもと無事開催することができました。

西日本支部合同研究会開催にあたり、ご多忙の中にもかかわらず資料等の準備を行っていただきました発表者の皆様に厚く御礼申し上げます。そして、事務局として運営準備からご協力いただきました支部の皆様、ありがとうございました。

統一テーマを、「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」については、あらゆる視点からのご講演を頂戴することができ、新たな発見、気づきが多かったと感じております。

情報交換会にも多数の参加をいただき、支部間での交流を促進する良いきっかけづくりの場になりました。

2 日目の施設見学では、私自身、地元大阪に在住しながらもあまり知らなかった大阪の歴史に触れるよい機会でありました。災害対策を考える方々へのご案内を含め再度訪問したいと思います。

普段なかなかお会いできない本部、各支部の方々と直接お会して情報交換できたことを今後の支部活動に生かしたいと思います。そして、他支部でのイベントへのご協力なども積極的に行っていきたいと思います。

＜目次＞

2014.12

近畿支部報告　【　ＩＴ－ＢＣＰ体験セミナー　開催結果報告　】

会員番号 645 是松 徹（近畿支部）

１．セミナー名称　：　ＩＴ－ＢＣＰ体験セミナー
２．開催日時　：　２０１４年１０月２５日（土）１３：００～１７：００
３．開催場所　：　大阪大学中之島センター　講義室３０３
４．当日参加者　：　受講者　１０名
スタッフ　荒町、尾浦、金子、松井（ＢＣＰ研究プロジェクト）
広瀬、三橋、小河、鬼松、是松（セミナーグループ）

５．開催概要

当セミナーは、ケースシナリオを使った体験演習により IT-BCP のポイントを把握することを狙いとし、今年度から開始した新しいセミナーです。教材を開発したBCP研究プロジェクトとセミナーグループが共同で準備・運営を進めました。

カリキュラムは演習 2 題と2本の講義から成り、演習は受講者 10 名を 2 チームに編成して実施しました。各演習の最後に検討した結果をチーム単位にまとめて発表いただき、講師講評を踏まえて受講者全員で成果の共有を図りました。

５．１　オリエンテーション／事例企業の解説　（荒町氏）

はじめに、当セミナーで把握すべき内容として以下を提示しました。

・初動対応の演習を通じて、IT部門に要求される行動を体験する。
・グループ討議での気付きをもとに、IT－BCPの重要性と自社で取り組む場合のポイントを確認する。
・IT－BCP策定への道筋として、災害対策本部運営の実際や訓練・演習で鍛えるIT－BCPを学ぶ。

その後、演習の対象となる事例企業（スーパー）の概要を説明しました。

５．２　グループ演習　（進行：金子氏）

あらかじめ設定した9つのシーンに対し、各演習のテーマに沿ってIT管理部門としてどのように対処すべきか個人で検討の上、チームとしての見解をまとめました。まとめた内容は、模造紙にシーンごとにポストイットも活用しながら書き出し、2チームそれぞれのリーダ役の方から発表を行いました。

検討内容に対して意図的にタイトな時間設定とし、限られた時間内で多数の案件を一度に迅速に意思

決定する重要性に気付いていただく狙いで、インバスケット研修の手法を採用しました。

(1)演習１（災害発生直後の初動対応）

初動としてIT管理部門はどのように対応すべきかを検討しました。

・優先順位付け、どの部署の誰にどのように指示を行うか等

(2)演習２（ＩＴ－ＢＣＰのポイント検討）

IT管理部門として、何を事前に準備・計画していればより適切な対応が可能であったかを検討しました。

・行動計画／ルール、危機対応時に有効な文書／資料、ダメージを少なくする事前対策等

(3)講師講評／演習の解説　（尾浦氏・金子氏）

各チームの発表内容に対し、講師側から実務体験も踏まえて講評を行いました。また、9つのシーンの設定の背景と初動対応、及びIT－BCP策定のポイントについて解説しました。

５．３ 講義１：危機対策本部の実際　（尾浦氏）

まず、演習課題を全社BCPの視点から掘り下げ、初動段階において全社BCPの発動状況がIT－BCPやIT部門にどのような影響をもたらすか、また、実際の危機対策本部において全社BCPがどのような経過をたどって発動されるかについて、阪神淡路大震災など過去の大災害における初動の実例を交えた解説が行われました。

次に、危機対応の長期化に際してBCPの実効性を大きく阻害する「社内温度差」の防止に触れ、対策本部体制における機能の絞り込みと各班が担う機能の明確化、組織的機能と物理レイアウトの一致、状況認識の共有、引継ぎ、ローテーション終結基準等の重要性について、米国防総省で運用されている現場指揮システムの紹介を交えて解説が行われました。

最後に、常に機能の拡張・統廃合を意識してシステム設計・開発を行ってきた上級IT技術者は、状況変化に強いBCPの策定に必要なスキルを既に有しているとの指摘がなされました。

５．４ 講義２：訓練・演習で鍛えるＩＴ－ＢＣＰ　（松井氏）

訓練・演習を行わないIT－BCPはテストをしていないソフトウェアと同じでバグがたくさん残っており、有事の際の実効性に不安があるという話から講義が始まりました。また、東日本大震災での情報システムへの被害の傾向として、ネットワークの被害が相対的に大きいことがデータとして示され、今後クラウド化が進む中で、この傾向には留意する必要があるとの説明がなされました。

続けて、訓練の話に移り、机上訓練と実機訓練の対比において、実機訓練は本番系システムに与える悪影響や本番系システム停止が困難であること等から、現実的には机上訓練を推奨するとの説明がなされました。そして、有効な机上訓練としてDIG（※）をITに応用する手法が紹介されました。

このIT版DIG訓練の利点として、システム環境全体の可視化ができ、詳しい知識がない人の参加が容易になること、実施が手軽・簡単であること、様々な意見が収集できることがあげられました。

最後に、いざという時に本当に有効か、副作用はないかとの視点から、実機訓練、机上訓練それぞれについてのシステム監査人が意識すべきリスクが示されました。

※D：災害（Disaster）　I：想像力（Imagination）　G:ゲーム(Game)の頭文字をとって名付けられた災害机上訓練のノウハウ。

６．受講された皆様の感想

受講された皆様からは、以下のようなご意見をいただきました。（アンケートから抜粋）

・演習により、5W1H、特に誰が、という指示の重要性等気づきがあり参考になりました。

・BCP、IT-BCPについて、自社の対応を考えるのに役立つ内容でした。

・講義1の単独セミナーを企画いただければ幸いです。ぜひじっくりご教示いただきたいと思います

・演習、実践のヒント、盛りだくさんで、使っていける手法を一つ一つ試していきたいと思います。

・演習は詳しい人の意見が聞けて、いろいろな気付きがありました。

・限られた時間に有益な内容を盛り込まれており、有益でした。

・自分自身で考え、議論し、そして講師に教えてもらうのはよい方法だと思います。

・もっと講師の時間があってもいいかと思いました。

・「IT-BCPが難しい」と思っているのは、専門用語が多いことと、つながりがわからないところで、やはり今日もわからない用語が多かった。

・各グループの演習結果を後で共有いただけると、復習する際に助かります。

７．感想

IT－BCPに関する気付きを提供するという方針で当セミナーを初めて開催しましたが、受講者の感想は概ね好評でした。半日のカリキュラムで演習と講義を体験でき、ダラダラ感がなくコストパフォーマンスが妥当であったととらえていただけたと感じています。一方で、講師の時間が不足、じっくり聞きたいところが時間の関係で割愛されたという感想もいただいており、インプット学習の重要性と演習とのバランスをどうとっていくかが今後の課題の一つだと認識しました。

限られた時間の中で、受講者の皆様には真摯に演習等に取り組んでいただき、また、演習で発表いただいた内容には、講師側で用意していた正解とは異なった視点の優れた解答があり、スタッフ一同大いに勉強させていただきました。

今後とも当セミナーを継続して開催していくべく、近畿支部内でBCP研究プロジェクトとセミナーグループの連携をより強化していくように考えています。

受講者の皆様、スタッフ／関係者の皆様、ご協力ありがとうございました。

以上

＜目次＞

2014.12

注目情報（2014.11～2014.12）※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。

■　「サイバーセキュリティ基本法」が公布(2014/11/12)

各国で深刻化するサイバー攻撃に対し、国の責務と対応指針を明文化した「サイバーセキュリティ基本法」が成立し、平成 26 年法律第 104 号として公布された。

同法は、①日本のサイバーセキュリティに関する施策に関する基本理念と、国および地方公共団体の責務などの明確化、②そのうえで、サイバーセキュリティ戦略の策定および関連施策の基本となる事項の制定、③サイバーセキュリティ戦略本部の設置などを目的とする。

同法では、従来の情報セキュリティ政策会議を格上げする形で「サイバーセキュリティ戦略本部」を設置し、IT 総合戦略本部および国家安全保障会議(NSC)と緊密に連携することとなる。

【サイバーセキュリティ基本法（衆議院 HP)】

http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm

【サイバーセキュリティ基本法の概要（内閣府 HP：PDF)】

http://www.nisc.go.jp/conference/seisaku/dai40/pdf/40shiryou0102.pdf

■　経済産業分野の「個人情報保護ガイドライン」改正（2014/12/12)

経済産業省は、大量の個人情報の漏えい事案等を踏まえ、「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」を改正し、告示・施行した。

主な改正点は、以下のとおり。

(1)第三者からの適正な取得の徹底

・第三者から個人情報を取得する場合には、適法に入手されていること等を確認することが望ましい旨追記。

・適法に入手されていることが確認できない場合は、取引を自粛することを含め、慎重に対応することが望ましい旨追記。

(2)社内の安全管理措置の強化

・外部からのサイバー攻撃対策の追加。

・内部不正対策の組織的、物理的、技術的安全管理措置の項目の追加。

(3)委託先等の監督の強化

・内部不正対策の委託先の安全管理措置の確認、定期的な監査等の追加。

・再委託先以降も同様の措置を行うことが望ましい旨追記。

(4)共同利用制度の趣旨の明確化

・事業者が共同利用を円滑に実施するために共同利用者における責任等を追加。

・共同利用者の範囲の明確化。

(5)消費者等本人に対する分かりやすい説明のための参考事項の追記

・個人情報取扱事業者は、本人に対して、個人情報保護を推進する上での考え方や方針等について、分かりやすい表現で説明するために参考とすべき基準を追記。

http://www.meti.go.jp/press/2014/12/20141212002/20141212002.html

＜目次＞

2014.12

【　協会主催イベント・セミナーのご案内　】

■月例研究会（東京）

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

■近畿支部第１５０定例研究会（大阪）

日本システム監査人協会近畿支部と ISACA 大阪支部の合同講演会

申し込み受付中	日時:2015 年 1 月 16 日(金)19:00～20:30 場所:大阪大学中之島センター　2階　講義室201	
	テーマ	IT-BCP の実効性を高める訓練・演習とその監査
	講師	日本システム監査人協会近畿支部会員　松井　秀雄　氏 (近畿支部　BCP研究プロジェクトメンバー)
	講演骨子	IT-BCP を策定しただけで何の検証も行っていない状態は、コーディングが完了したものの単体テストや統合テストを一度も行っていないソフトウェアの状態に似ており、考慮漏れや記述ミスなどが存在する可能性が強い事から、有事の際に機能しない可能性が強い。当講演では、IT-BCP が有事の際に機能する「実効性」を高めるために ISO22301・ISO27031・IT-BCP ガイドラインなどで求められている事項を紹介します。訓練・演習に実機を使うタイプと机上で行うタイプの両方を紹介し、各々の長所・短所を明らかにします。机上訓練の手法として一部の業界で採用されている DIG (Diaster Imagination Game)を IT-BCP へ応用した事例も紹介します。また、訓練・演習に取組んでいる組織に対する監査の要点について、システム管理基準を踏まえた説明をいたします。
	お申し込み	HPでご案内中です。(http://www.saaj.or.jp/shibu/kinki/kenkyukai150.html)

■システム監査普及サービス(全国)

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

＜目次＞

■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』

■公認システム監査人特別認定講習（東京・大阪）

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

【　外部主催イベント・セミナーのご案内　】

■2014 年度 第 7 回ＪＡＳＡ月例セミナー（東京）

日時：2015 年 1 月 23 日（金） 18:30～20:00 場所：東京都中小企業振興公社 第 1 会議室	
テーマ	パネルディスカッション「大規模機密漏えいリスクへの対処を考える」
パネリスト等	パネリスト：株式会社ディアイティ 情報セキュリティ事業部長 青嶋 信仁 氏 綜合警備保障株式会社 干場 久仁雄 氏 ベーカー＆マッケンジー法律事務所弁護士 松本 慶 氏 モデレータ：特定非営利活動法人 日本セキュリティ監査協会 事務局長 永宮 直史氏
概要	情報セキュリティ対策が官民を挙げて取り組まれている現在にあって、今年、大規模な機密漏えい事案が発生してしまった。技術的にみると最新のデバイスに対する対策漏れという新しい面もありますが、情報セキュリティマネジメントの観点からは「10 年前と全く変わっていない」という厳しい意見が寄せられている。 そこで、IT 技術、セキュリティマネジメント、営業機密法務の第一線で活躍される実務家の皆様に、この事案を分析して頂き、情報セキュリティマネジメントについて、再度、考えてみたい。
詳細	http://www.jasa.jp/seminar/monthly.html

＜目次＞

2014.12

協会からのお知らせ

【ＣＳＡ／ＡＳＡ資格をお持ちの方へ　：資格更新申請手続きについて】

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

・資格認定期限が 2014 年 12 月 31 日で満了となる方について、認定の更新手続を行います。

・資格更新申請の受付期間は 2015 年 1 月 1 日(木)から 1 月 31 日(土)までの 1 か月間です。

・今回の更新対象者は、資格認定番号が下表の方です(2014 年度よりすべて 2 年度ごとの更新です)。

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

・資格更新申請には、更新申請書や継続教育実績申告書などの提出が必要です。準備をお願いします。

・更新手続の詳細は、HP の「CSA の資格をお持ちの方へ」(http://www.saaj.or.jp/csa/forCSA.html)をご覧ください。

＜目次＞

2014.12

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

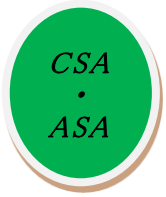
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

・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＞

2014.12

【　ＳＡＡＪ協会行事一覧　】

赤字：前回から変更された予定

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
12 月	1 日 2015 年度年会費請求書発送 2015 年度予算案策定 11 日 理事会:2015 年度予算案、 会費未納者除名承認 12 日第 14 期総会資料提出依頼(1/9〆切) 19 日 会計:2014 年度経費提出期限	6 日 法制化検討 PT 事前打合せ 6 日 事例研:第 16 回課題解決セミナー 10 日 認定委員会:CSA/ASA 更新手続 案内メール発信 16 日 第 198 回月例研究会 20 日 CSA 認定証発送 21 日 第 25 回 CSA フォーラム	13 日 東北支部:支部総会
2015 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1 月	7 日 16:00 総会資料(〆) 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 19 日 会計:2013 年度決算案 24 日 会計:2013 年度会計監査 31 日 償却資産税・消費税	認定委員会:CSA・ASA 更新申請受付 〔申請期間 1/1～1/31〕 20 日 第 199 回月例研究会 20 日 春期公認システム監査人募集案内 〔申請期間 2/1～3/31〕	10 日 会計:支部会計報告期限 16 日 近畿支部:支部総会
2 月	5 日 理事会:通常総会議案承認 6 日 総会資料公表 20 日 第 14 期通常総会・特別講演 25 日 法務局:資産の変更登記、 活動報告書提出 28 日 年会費納入期限	CSA・ASA 春期募集(2/1～3/31)	
3 月	2 日 東京都への事業報告書提出 2 日 年会費未納者宛督促メール発信 4 日 認定 NPO 法人東京都による調査 12 日 理事会	4 日 第 200 回月例研究会	
4 月	9 日 理事会 末日 法人住民税減免申請	認定委員会:新規 CSA/ASA 書類審査	19 日 2015 年春期情報技術者試験
5 月	14 日 理事会 29 日 会費未納者チェック(6 月 1 日督促)	認定委員会:新規 CSA/ASA 面接	
	以下は、昨年:2014 年の行事一覧です。		
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): (実践編)
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 14 日 予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/10〆切) 18 日 2015 年度年会費請求書発送準備 20 日 会費未納者除名予告通知発送 30 日 予算申請提出期限	中旬 認定委員会:CSA 面接 19 日 第 197 回月例研究会 20 日 CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 28 日 認定委員会:CSA 面接結果通知	29 日 西日本支部合同研究会 (開催場所:大阪市)

※注　定例行事予定の一部は省略。

＜目次＞

2014.12

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まいりました。

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」、11 月号から 1 月号までが「情報システム部門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。

2015 年度の年間テーマは、「システム監査人の魅力」です。これまでは「システム監査」に焦点を当ててきましたが、今年度は「システム監査人」に焦点を当てて考えてみたいと思います。次号より四半期ごとに具体的なテーマを設定し、皆様から記事の募集をする予定です。皆様の幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマも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 （「会報掲載論文募集要項」及び「会報掲載論文審査要綱」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、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＞