認定 NPO 法人
日本システム監査人協会報

2015 年 11 月号
No 176

No. 176（2015 年 11 月号）＜10 月 25 日発行＞

マイナンバー制度が施行されました。この機会に

『システム監査人の未来』

について考えてみませんか？

＜注目記事＞

写真提供：仲会長「秋の蝶」

巻頭言　『システム監査人の未来 ― 未来のシステム監査人を育てる』

会員番号 1342　安部晃生（副会長）

今月号からの会報の四半期テーマは「システム監査人の未来」です。10 年後、20 年後のシステム監査人がどのようになっているか、想像してみるのも楽しいものです。

金融機関でシステム監査に携わってきた者として、これまでのシステム監査の状況を振り返ってみると、システム監査が本格的に金融機関に導入され始めたのは、2000 年問題対応の頃でした。その当時と比べてみると、システム監査の必要性の高まり、監査手法の高度化の進展には目を見張るものがあり、わずか 15 年で、よくぞここまでといった感があります。マイナンバー制度もスタートし、10 年後、20 年後には、システム監査の必要性は一層高まっていることでしょうし、それに伴って監査手法もさらに高度化しているでしょう。

その一方で、将来のシステム監査について、心配なことが一つあります。それは、情報処理技術者試験で、システム監査の受験者が減少傾向であることです。システム監査ができる人を増やさない限り、システム監査の広がりを期待できないのではないかと危惧してのことです。

こうしたことから、システム監査人の育成が、私のミッションだと考え、同じ監査部署の後輩の指導にあたってきました。しかし、システム監査人の育成は、監査部署の後輩だけに限ったものではないことに、先日気がつきました。システム部門に対して講演をする機会を得て、システム監査人の観点に立って開発・運営の現行業務を見直そうと話したところ、その気になってくれた方が多かったのです。考えてみると、被監査部門は監査で指摘されたくはないのだし、どういった観点でシステム監査をするのかを被監査部門に伝えていきさえすれば、各自が監査人の立場で考えてくれるのではないでしょうか。そうした活動が、未来のシステム監査人を育てることにつながっていくような気がします。

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＞

2015.10

めだか　【　システム監査人の未来　】

日本証券取引所に上場している企業はコーポレートガバナンスの適用が求められている。創業は難しく、上場はさらに難しい。しかし、「創業は易く守成は難しい」ともいう。これは、唐の太宗が側近に「帝王の業は創業と守成と、どちらが難しいか。」を尋ね、自ら、「創業の難事は過去のこと。今は守成の難事にあたろう。」と語ったという故事による。

コーポレートガバナンスは、企業に「守成」を求めた上で、さらなる成長を求めているといえよう。先日、滋賀県安土町を旅行する機会があったが、ここは織田信長が、安土城を築いた土地である。ご存知のように織田信長は、創業の道なかば、本能寺の変で家臣の明智光秀に討たれている。“参考資料”には、次のような記述がある。

“安土町の「信長の館」には、安土城天守閣の最上部が再現されています。織田信長のつくった安土城天守閣は六層だったのですが、上の二層が特徴的で、五層目が朱塗りの八角形、一番上の六層目は黒塗り四角形。四角い巨閣の上に八角形と四角形を積み上げたのですから、これほど不安定な構造はありません。耐久性より生きている今の訴求力を尊ぶ信長の思想と人生がよくあらわれているといえるでしょう。”

安土町にある「信長の館」を訪ねてみると、五層目は朱塗りの八角形、内部は、真っ赤な柱や床、金箔のふすま絵、そのふすま絵は「釈迦十大弟子の図」である。八角形の内陣中央に信長座所があり、釈迦やまわりの十大弟子が信長を見る空間になっている。また、外陣の廊下は、龍が内陣を取り巻くように描かれている。安土城の天守閣は、天下統一を全国に発信する意図でデザインされていたと思う。

本能寺の変の後、安土城は焼け落ち、豊臣秀吉が明智光秀を倒して大坂城で天下人になるが、豊臣政権も「守成」には至らなかった。一方、徳川家康の幕府は、「守成」のための制度を備えていた。「奉行」は、執行するに当って「目付」の連著がなければ、幕府の決裁を得られない仕組みになっていて、まさに、相互けん制を重視する内部統制になっていた。また、家柄にかかわらず新井白石などの有能な人材をどんどん登用している。徳川幕府による平和は、ペリーの黒船艦隊が浦賀沖に現れる幕末まで、2世紀を超えて続いた。

企業がコーポレートガバナンスを求められる時代にあって、システム監査人は、企業がIT（情報技術）の利用においてリスクに応じたコントロールを適切に整備・運用しているか、また情報システムがその目的に照らして有効であるかを監査し、代表者に報告を行う。システム監査人の未来は、コーポレートガバナンスにシステム監査人が期待される役割を果たすことにあると思う。

（空心菜）

参考資料：「大激震　堺屋太一かく語りき」　堺屋太一 著　株式会社実業乃日本社

（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＞

2015.10

投稿【　システム監査人の魅力　】

会員番号　0557　仲　厚吉　（会長）

当協会は、システム監査を核に情報セキュリティなどの研究活動を行っています。日本規格協会より「情報技術－セキュリティ技術－情報セキュリティガバナンス JIS Q 27014:2015」が 2015 年 7 月 21 日付で発行され、同規格は、情報セキュリティガバナンスについての概念及び原則に基づくガイダンスを示しています。また、同規格が引用する規格は、ISMS として、2013 年時点で国内 7,084 件が認証登録されている「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項 JIS Q 27001:2014」です。ISMS で達成すべきことは、リスクマネジメントプロセスを適用することによって、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることであるとしています。

情報セキュリティに関して標的型攻撃などのリスクが増加しており、重要な社会インフラの操業中断を狙った標的型攻撃もあることから、CSMS 認証基準（IEC 62443-2-1:2010）が規定されています。CSMS 認証基準は、事業上の根拠、リスクの識別・分類及びアセスメント、リスクの優先順位のアセスメント、関連するリスクの識別及び優先付け、リスク許容度の確立、CSMS によるリスクへの対処、リスクマネジメント及び管理策の導入、上位レベル及び詳細なリスクアセスメントの更新、CSMS の監視及び改善などを要求しています。CSMS は ISMS のマネジメントシステムや管理策と共通する部分が多く、両者の共通要件と固有要件を特定し、CSMS を構築する際、CSMS 固有要件の適用を行っていくようユーザーズガイドに書かれています。 http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS111-12.pdf

IT ガバナンス（JIS Q 38500:2015）は、適用することで当該組織が 6 原則に基づいた IT の利用に関連した活動に、評価（Evaluate）、指示（Direct）、モニタ（Monitor）ができるようになるとしています。情報セキュリティガバナンス（JIS Q 27014:2015）は、適用することで当該組織が 6 原則に基づいた情報セキュリティに関連した活動に、評価（Evaluate）、指示（Direct）、モニタ（Monitor）、及びコミュニケーションができるようになるとしています。

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

当協会では、IT ガバナンス（JIS Q 38500:2015）にかかわるセミナーを、2015 年 12 月 14 日（月）18 時 30 分より、第 209 回月例研究会（機械振興会館地下 2 階ホール・神谷町）で開催します。システム監査人の魅力は、IT ガバナンス、及び情報セキュリティガバナンスの普及活動を通じて、IT 監査人として健全な情報化社会の発展に資するなかに育まれていくと思います。

参考：「[2013 年改正対応]やさしい ISO/IEC27001（JIS Q 27001）情報セキュリティマネジメント 新装版」
　　高取敏夫・中島博文 著　日本規格協会

＜目次＞

2015.10

第２０６回　月例研究会　（２０１５年９月１５日開催）

会員番号 0056　藤野明夫

【講演テーマ】「マイナンバーがもたらす社会の大変革　－制度施行直前チェックを含めて－」

講師:一般財団法人　日本情報経済社会推進協会(JIPDEC)

常務理事・電子情報利活用研究部　部長　坂下　哲也　氏

日時:　2015 年 9 月 15 日(火曜日)18:30～20:30

場所:機械振興会館　地下 2 階ホール

【講演骨子】

いよいよ 2016 年1月から「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」(平成 25 年法律第 27 号;以下「番号法」)が施行され、個人番号(以下、「マイナンバー」)・法人番号の利用が開始される。一方で、7 月時点での JIPDEC のセミナーアンケートでは、準備を進めている事業者は 30%程度しかおらず、周知が足りない状況である。マイナンバーは、国内に住民票を有する全ての国民に付番され、一生変わらないものであることから、その管理には十分な注意が必要である。

一方で、全ての国民にユニークな識別子が付与されることによって、オンライン上での本人確認や、添付書類の削減などが期待されており、その利活用についての検討も活発に議論されている。

本講演では、マイナンバーを取り扱う事業者が留意するポイントの解説、現在検討されている利活用ソリューションの紹介と、それによる社会インフラの変化について解説する。また、IT が進展することによって、様々なデータを利用するにあたり、事業者が対応すべきポイントについて解説する。

【講演概要】

はじめに

本日は、以下の三点についてお話しする。一点目は、法人番号を含むマイナンバー制度の概要と事業者が気を付けるべきポイント、二点目はマイナンバーの利用について、最後にマイナンバー、マイナンバーカード及びマイナポータルの活用による産業構造の変化に向けた取り組みについてご紹介する。

〔報告者注:以下、参照の便宜のために、参照すべき資料の URL は本文の当該説明部分に記載した。〕

Ⅰ．マイナンバーについて

法人番号を含む制度の概要と事業者が行わなければならないこと等についてご説明する。

１．制度の概要

マイナンバー制度の概要について説明する。

１）番号法とは

2013年に「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」(平成 25 年法律第 27 号、以下「番号法」)が成立した。従来の個人情報保護法の特別法としての位置づけである。現行の個人情報保護法にある常時 5000 件以上の個人情報を取り扱うという枠はない。番号法は個人情報保護法の特別法であるから、とくに定めがないものは個人情報保護法の規定がそのまま適用される。したがって、マイナンバーの管理については個人情報保護法の安全管理規定に適応しなくてはならない。

なお、2015 年 9 月 3 日に成立した改正法により、番号法と同時に個人情報保護法も改正され、現行の個人情報保護法の「個人情報取扱事業者」の定義にある常時 5000 件以上の個人情報を取り扱う事業者という枠が撤廃された。

番号法の最も大きな特長は、利用目的を法のなかで限定していることである。現時点では、マイナンバーは社会保障と税、災害対策以外の目的で取得してはいけない。一意性が担保されるからといって、社員番号などに利用してはいけない。マイナンバー占いなどはあり得ない。

個人情報保護法とのもう一つの大きな相違点は、目的外利用等に対する直罰（最高４年以下の懲役・200 万円以下の罰金（併科あり）、さらに違反者が属する法人も罰せられることがある（両罰））が規定されていることである。

個人に対する発番（市区町村が通知）と併せて法人番号も発番（国税庁が通知）され、平成 28 年１月以降の申告書等で使用される。マイナンバーと異なり利用目的は限定されず、社内の取引先の管理コードなどに利用できる。また、国税庁の「法人番号公表サイト」に公開される。

２）個人番号利用事務と個人番号関係事務

個人番号を取り扱う事務は番号法により「個人番号利用事務」と「個人番号関係事務」に区分される（表1．参照）。事業者は個人情報関係事務の実施者となり「個人情報関係事務実施者」と呼ばれる。個人情報関係事務とは、国の行政機関等が行う個人番号利用事務の処理に関し、他人の個人番号を記載した書面の提出等を行う事務のことである。

表１．個人番号利用事務と個人番号関係事務

種類	定義	事例
個人番号利用事務	・その事務処理に個人番号を利用するもののうち、番号法（番号法別表1）、及び自治体の条例で定められるもの ・その実施を行う者を「個人番号利用事務実施者」という。	・市町村で予防接種を実施する。（予防法第５条は番号法別表１で規定） →予防接種の委託をうけた医療法人は、個人番号利用事務を行う。（医療法人は、個人番号利用事務実施者となる。）
個人番号関係事務	・国の行政機関等が行う個人番号利用事務の処理に関して、法律・条令の規定に基づき他人の個人番号を記載した書面の提出等を行う事務 ・その実施を行う者を「個人番号関係事務実施者」という。	・従業員への所得税の課税には、所得税法の規定により源泉徴収が実施される。 →源泉徴収義務者となる当該事業者（事業主）は、個人番号関係事務を行う個人番号関係事務実施者となる。 →その委託を受ける事業者があれば、同様に個人番号関係事務実施者となる。

３）マイナンバー制度の目指している方向

第6回マイナンバー等分科会（2014 年 11 月 11 日開催）において発表された中間とりまとめには、目指すべき社会像として、以下が明示されている。

・誰もがより安全・安心にインターネットを利用できる基盤を持つ社会

・誰もが必要な時に自身の情報にアクセスし、利活用でき、サービスへの満足度が向上する社会

・国・地方・民間の様々な手続き・サービスが、シームレスかつ効率的に連携し、広く電子的に完結できる社会

４）事業者が取得すべき個人番号

事業者は従業員等の個人番号を税務申告、届出、社会保険関係の書類等に記載する義務を負う。取得の対象者は、以下の三種である。

まず、従業員とその扶養家族（パート、アルバイトを含む）である。雇用契約の締結時点で番号の提供を求めることができる。短期であっても、源泉徴収票を出すものは全て対象である。

次に、株主・出資者等に対する配当等の支払調書に番号を記載する義務を負う（ただし、3 年間の猶予期間あり）。また、持ち株会に従業員等が入会する場合等においても提出する書類等に番号を記載する義務を負う。

三番目は、取引先（不動産の貸主、外部人材など）に対する報酬、料金、契約及び賞金の支払調書などに番号を記載する義務を負う。この場合、契約締結時点で番号の提供を求めることができる。

なお、受入派遣社員については、派遣会社で税・社会保障の処理を行う場合、番号の取得は不要である。

５）いつから個人番号を法定調書に記載するのか

源泉徴収票については、2016 年1月 1 日以降の支払いに係る給与所得分から記載しなければならない。また、雇用保険関係は 2016 年の届出から、健康保険関係は 2017 年の届出から記載しなければならない。なお、国民健康保険組合については、2016 年1月1日から各種届出書等に記載しなければならない。また、既存の従業員・被扶養者分の個人番号については、2016 年1月以降いずれかの時期に、健康保険組合・ハローワークに報告することとなる予定である。

各種法定書類の様式については、国税庁が下記 URL に公開している「国税分野における社会保障・税番号制度導入に伴う各種様式の変更点」を、ご確認されたい。

http://www.nta.go.jp/mynumberinfo/pdf/mynumber_modification.pdf

２．事業者が行うべき対策等について

事業者がマイナンバー制度実施に向けて、行わなければならない対策等について説明する。

なお、事業者が行うべき対策については、特定個人情報保護委員会が下記 URL に公開している「特定個人情報の適切な取扱いに関するガイドライン（事業者編）」（以下「ガイドライン」）を、参照されたい。

http://www.ppc.go.jp/files/pdf/261211guideline2.pdf

このガイドラインは、個人情報保護法の規制がかかるため、安全管理措置は「経済産業分野における個人情報保護ガイドライン」がベースになっている。このガイドライン中で「しなければならない」、「してはならない」は、法律に基づくものであるので、事業者は必ず対応しなければならない。また、「望ましい」は、可能な限り対応措置をとることを推奨している。なお、「特定個人情報」とは「マイナンバー＋個人情報」になっているものをいう。

１）従業員等への周知

10 月より簡易書留で通知カード（マイナンバーを本人に通知するカード）が世帯主へ発送される。通知カードは、住民票を置いている住所へ送付される。送付される簡易書留には、世帯全員分の通知カードが封入されている。事業者は、個人番号を取得しなくてはならないので従業員等へ「紛失しない」、「誤って捨てない」、「みだりに人に教えない」、「写メを取って SNS にアップしない」ように周知する必要がある。

２）規約等の整備

「ガイドライン」では、特定個人情報の取扱いについて、規約等を整備することを求めている。求められている規定、様式類は、①特定個人情報の保護方針を示す書類、②特定個人情報管理についての規定、③本人確認の手順の規定、④特定個人情報の管理簿である。上記に付随して、特定個人情報取扱いの同意書・誓約書などの作成、就業規則等の変更、雇用契約書の変更、業務フローなどの作成が必要になる。

なお、「ガイドライン」には、中小規模の事業者に過大な負担を強いることを避けるために「中小規模事業者」の特例的対応を記載している。「中小規模事業者」とは、原則として、従業員の数が 100 人以下の事業者で、事務で取り扱うマイナンバーの数量が少なく、また特定個人情報等を取り扱う従業者が限定的である等の事業者をいう。これらの事業者には、上述の規程類の整備までは求めず、簡易的な対応を可能にしている。詳しくは、「ガイドライン」を参照されたい。

３）利用目的の通知

マイナンバーは税・社会保障・災害対策以外の利用を厳しく禁じられている。事業者はマイナンバーの取得にあたって、法定調書へ記載する必要がある人（従業員とその扶養家族、パート、アルバイト、株主等）に事前に利用目的を知らせることが必要である。知らせる方法として雇用契約への記載、社内掲示板への記載、社内研修などの方法がある。

なお、事業者が作成する法定調書ばかりでなく、従業員等が作成する法定調書（年末調整、扶養控除異動申告書、児童手当など）も利用する旨も通知することを推奨する。

４）特定個人情報の取扱いに関する安全管理措置

特定個人情報の取扱いについて、漏えいや改ざん、成りすまし等を防止するため、以下のような安全管理措置を取らなければならない（図1．参照）。なお、本件についても、「ガイドライン」をご一読いただきたい。

・本人確認の上、マイナンバーを取得する。
・マイナンバーを保管する場所と、取り扱う場所をしっかり分ける。
・委託する場合は、マイナンバーがしっかり管理できることを確認する。
・不要になったマイナンバー（例：法定保存期限が過ぎた帳票など）は速やかに消去・廃棄する。

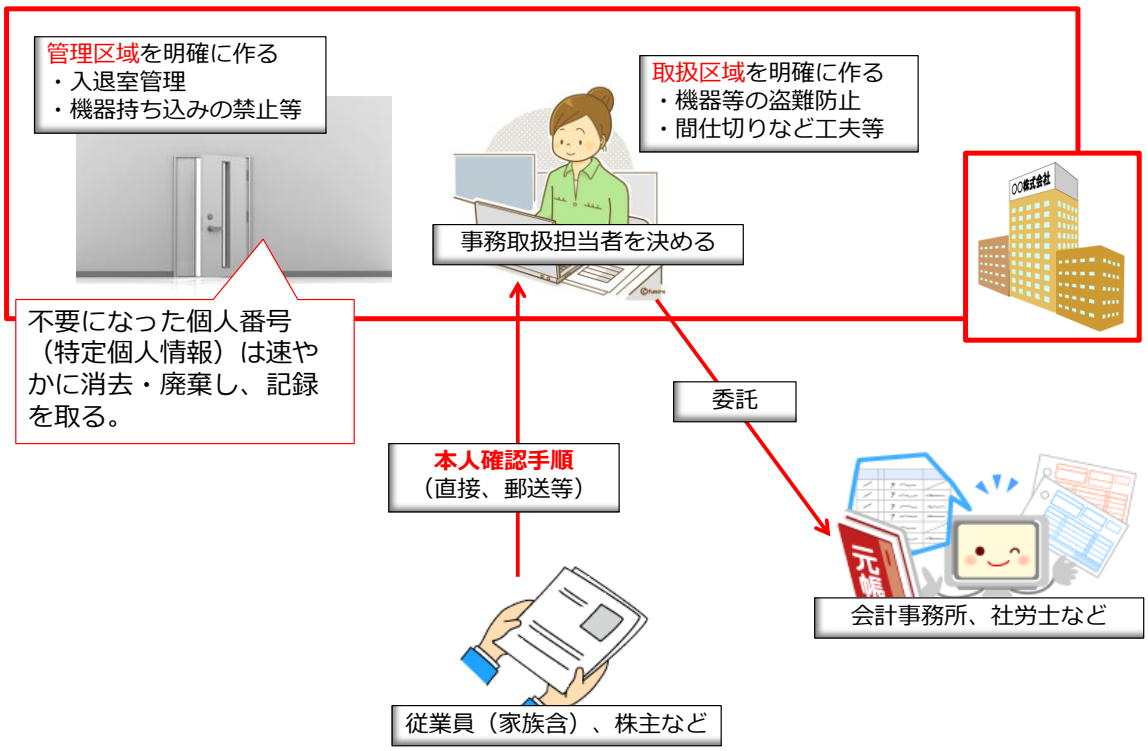


図１．必要な安全管理措置

以下に、これらについて具体的措置を示す。

ｉ）取得時の本人確認について

個人番号の取得は、右の方法で行う。社員（パート・アルバイトを含む）に、「通知カード」を持参するように連絡し、通知カードに記載されている「個人番号」を取得する。代理人による対応も可能である。代理人は、委任状、本人の身元を確認する書類（学生証又は法人若しくは官公署が発行した身分証明書若しくは資格証明書）を持参する必要がある（図2．参照）。法定代理人の場合は、戸籍謄本が必要である。また、間違って、他人の番号を取得しないように気を付ける。

相対で取得が難しい場合（株主、遠方の社員等）は、以下の方法で対応することも認められている。

郵送等による対応、すなわち、通知カードの写し、本人であることを確認する書類の写しの送付を受けることで取得することも可能である。郵送には、書留など配達記録郵便の利用を推奨する。また、本人であることを確認する書類の写しは、確認が終わったら、速やかにシュレッダー等で廃棄する。

通知カードの画像送信による対応も可能である。本人であることを確認する書類の画像を、電子メールで送付させる。送信時に、メールアドレスを間違えないように注意することが必要である。本人であることを確認する書類の写しは、確認が終わったら、速やかに削除する。

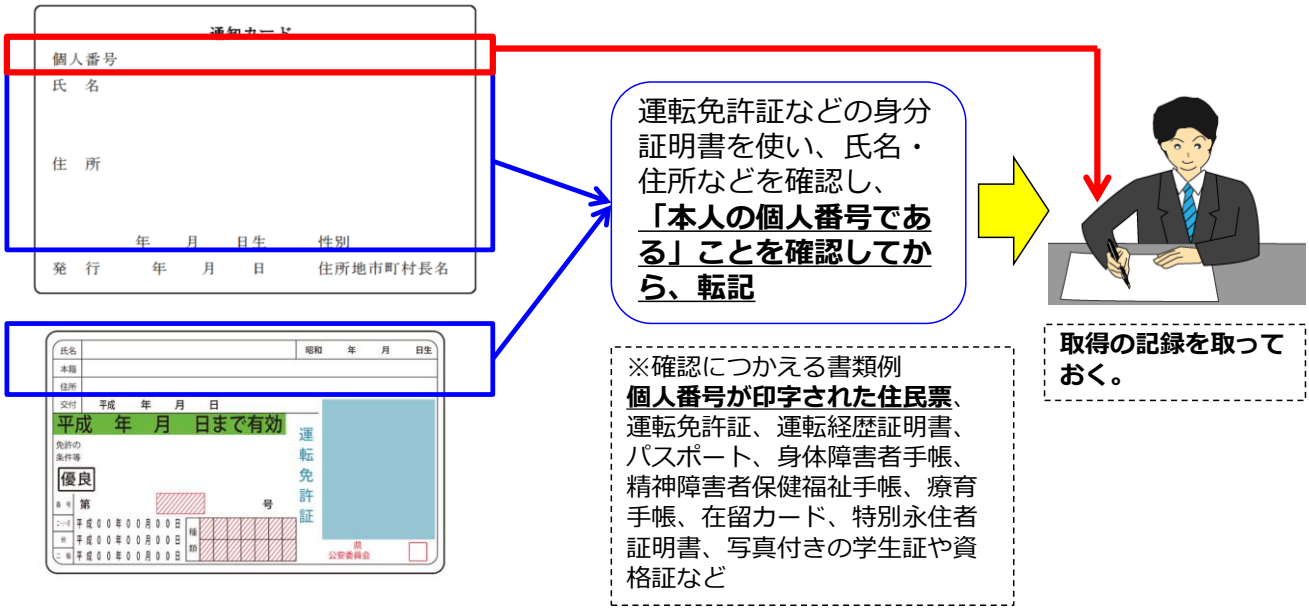


図２．個人番号取得時の作業イメージ（本人確認を含む）

ii）アクセス制御等の物理的安全管理措置

ガイドラインにおいて重視されているのは、アクセス制御等の物理的安全管理措置である。システム化が進んでいる事業者における物理的安全管理措置の例を図3. に示す。

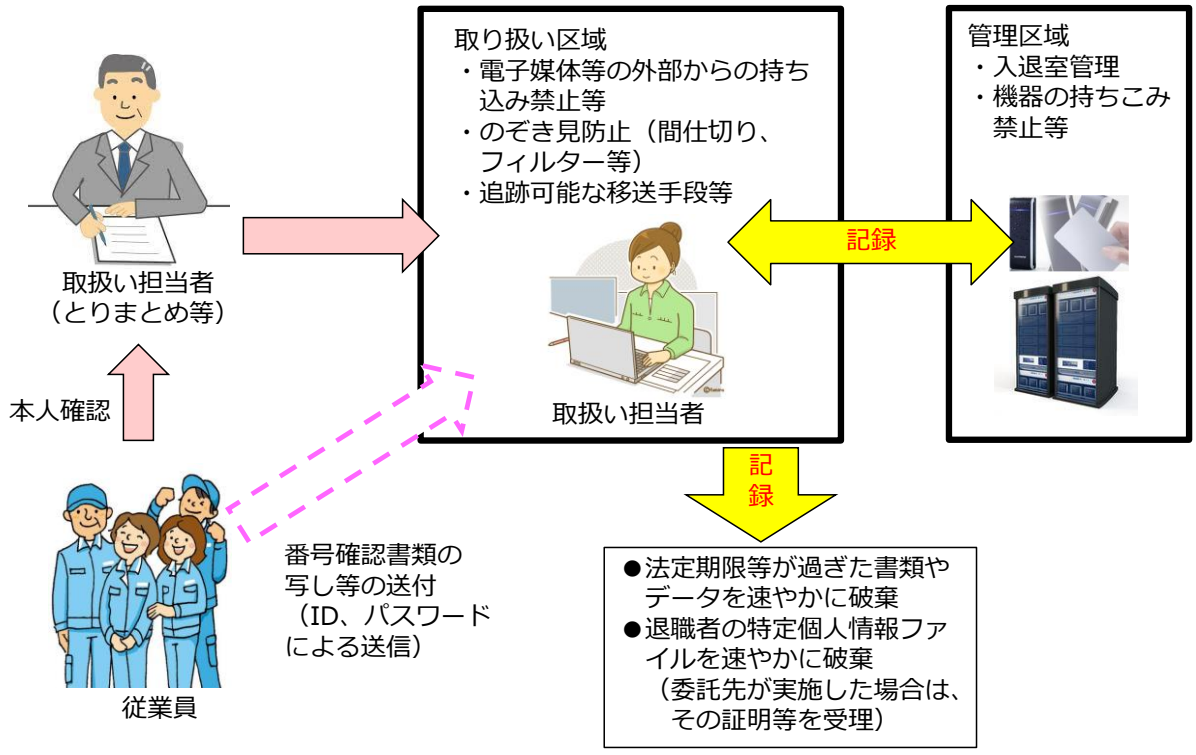


図３．物理的安全管理措置の例

図3. に示すように、個人番号取り扱い区域を限定し、個人番号を保管するサーバは、みだりに立ち入ることのできない管理区域に設置する措置をとらなければならない。

ⅲ）個人番号の保管について

個人番号は、税や社会保障でのみ取り扱うものであり、源泉徴収票や社会保険などの取り扱いにしか使えない。また、その取り扱いを行う人にしか教えてはいけない。社員（パート、アルバイトを含む）から個人番号を預かったら、鍵がかかる引出し、棚や書庫、金庫等に保管して、しっかり管理しておくことが必要である。

ⅳ）パソコン等を使って個人番号を入出力する場合の留意点

使用するパソコンは、ログイン ID/パスワードで他の人が勝手に使えないように管理する。共用のパソコンを使う場合、個人番号を扱うアプリケーション（Excel などの表計算ソフト、給与計算ソフト、財務ソフトなど）を、他の人が勝手に使えないように保護する。また、個人番号を取り扱うアプリケーションを立ち上げたまま、長時間、席を離れないように気を付ける。パソコン等でプリントアウトを行ったら、速やかに出力した帳票を保管し、速やかにアプリケーションを終了する。

ⅴ）消去・廃棄について

源泉徴収票・社会保険の届出等の控えは、法律で指定された期限まで、施錠できる場所で保管し、法律で指定された期限がきたら、速やかに消去・廃棄しなければならない。また、エビデンスとして、消去・廃棄の記録を必ず取らなければならない。

ⅵ）番号法における委託について

個人番号を利用する事務（利用事務、関係事務）の委託を受けた事業者は、委託者（委託元事業者）自らが果たすべき安全管理措置と同様の措置を講じることが求められる。また、委託を行う者は、委託を受ける者を適切に監督しなければならない。さらに、委託先は、委託者の許可を得て再委託を行うことができるが、再委託を行う（一次）委託先は、再委託先に対して安全管理措置に関する監督の責務を負う（図4. 参照）。委託者は、委託先に対して直接的監督義務を負い、さらに、再委託先に対して間接的監督義務を負う。委託先は、再委託先に対して直接的監督義務を負う。

図４．委託時の監督義務

委託者は、委託先の選定に際し、委託先選定規定を作成し、①規定、②体制、③人的安全管理措置、④従業者の役割・責任の明確化、⑤組織的安全管理措置の周知・教育、⑥技術的安全管理措置の確認、⑦利用者の認証・許可・監査及び監査証跡の記録について、委託者のセキュリティ・ポリシーと同等以上か、確認する。なお、上記の要件は既存の認証（プライバシーマーク、ISMSなど）で代替できる。

委託者は、委託先と、安全管理措置を遵守させるために必要な契約を締結しなければならないが、この契約には、①秘密保持義務、②事業所内からの特定個人情報の持出しの禁止、③特定個人情報の目的外利用の禁止、④再委託における条件、⑤漏えい事案等が発生した場合の委託先の責任、⑥委託契約終了後の特定個人情報の返却又は廃棄、⑦従業者に対する監督・教育、⑧契約内容の遵守状況について報告を求める規定（書面の提出などで定期的な報告を受ける、必要に応じ現地監査を行う等）などを盛り込まなければならない（「ガイドライン」、P20）。

なお、特定個人情報をクラウドによって取り扱う場合についても、クラウド事業者を選択する際に、適切なガバナンスを有する事業者を選択するとともに、合意事項として、責任分界点等を取り決めておく必要がある。

vii） 記録について

運用記録等は、特定個人情報の事故の原因究明や、訴訟等において、「故意ではなかった」、あるいは「安全管理措置に問題はなかった」ことを示す客観的な証拠としても大変重要である。「ガイドライン」においても、「組織的安全管理措置」の中で、運用記録を残すことを重要視している。記録を残すタイミングを以下に示す。

・個人番号を取得する段階（記録の例：本人確認記録など）
・個人番号を利用する段階（記録の例：処理記録、ログインや入出力のシステムログ、入退室記録など）
・個人番号を保存する段階（記録の例：処理記録、システムログ、入退室記録など）
・個人番号を提供する段階（記録の例：持ち出し記録、送信記録、配達記録など）
・個人番号を削除・廃棄する段階（記録の例：処理記録、裁断記録、マニュフェストなど）

viii）業務フローの平準化について

安全管理措置の一環として、業務フローを作成・検討し、個人番号を取り扱う業務がきちんと運用されるようにすることが必要である。個人番号の取扱いを通じて、事故等が発生しないように BPR（Business Process Re-engineering）を行うことが望ましい。自治体における特定個人情報保護評価も同じ観点で実施されている。業務フローの作成・検討にあたっては、標準的な業務にすること、誰がやっても質が同じになること、効率的な作業になること、進捗管理が可視化できること等を考慮する。

ix） 特定個人情報を含む安全管理措置が十分であることの対外的な明示について

事業者として、対外的に特定個人情報を含む安全管理措置が十分であることを明示する方策を表2．に示す。

表２． 対外的な明示の方策

	対応策	メリット	デメリット
1	プライバシーマークを取得する。	“既にプライバシーマークを取得している情報保有機関については、情報保護評価書にその旨を記述することで、個人情報保護に対して適切な体制をとっていることを宣言することができる”と記載（平成 25 年度政府「中間整理」他）があり、当該認証によって、特定個人情報を含む安全管理措置が十分であることが対外的に明示できる。	・時間を要する。 ・費用がかかる。 ・法人格を持っていることが必要である。
2	特定個人情報を取り扱う部署を新設し、その部署において ISMS を取得する。		
3	自己宣言（自治体の評価書などを活用してチェックする等）	・自社のペースで準備ができる。 ・費用も少ない。 ・法人格を持っていなくてもできる。	・事故があった場合に十分な説明ができるかどうか
4	しっかり管理できる事業者へ委託する。	・本人確認、安全管理措置の全て、または一部のリスクを転嫁できる。	・『しっかり管理できる』宣言ができる委託先が必要。

Ⅱ．マイナンバーの利用について

マイナンバーは、現在、社会保障、税及び災害関連における利用に限定されているが、2015 年 9 月 3 日に、番号法の改正法が成立した。これにより新たなマイナンバーの利活用の道が開かれた。これを含め、今後のマイナンバー利用の拡張について説明する。

１．改正番号法によって実現できること

改正番号法には、預貯金への付番、及び、特定健診（メタボ健診）の結果や予防接種の履歴情報を共有するための番号活用が盛り込まれた。

3 年後を目処に、預貯金に個人番号を紐づける。当初は新規開設の口座が対象（既存口座は窓口において勧奨）である。銀行等による社会保障制度の資力調査、国・地方による税務調査等の効率化を図ることが目的である。具体的な効果としては、給付付き税額控除の実現が挙げられる。今回の改正では、預金保険機構を番号法における「個人番号利用事務実施者」として位置付け、マイナンバーの利用を可能にする。

また、検診情報等での個人番号利用も盛り込まれた。これにより、乳幼児が受けた予防接種の記録を個人番号で管理する、あるいは、健康保険組合が、特定健診（メタボ検診）の情報を個人番号で管理するといったことが実現する。転居した場合でも、個人番号で紐づけされているので、転居先の自治体で当該情報を活用し、予防接種や保健指導を行うことができる（図5．参照）。

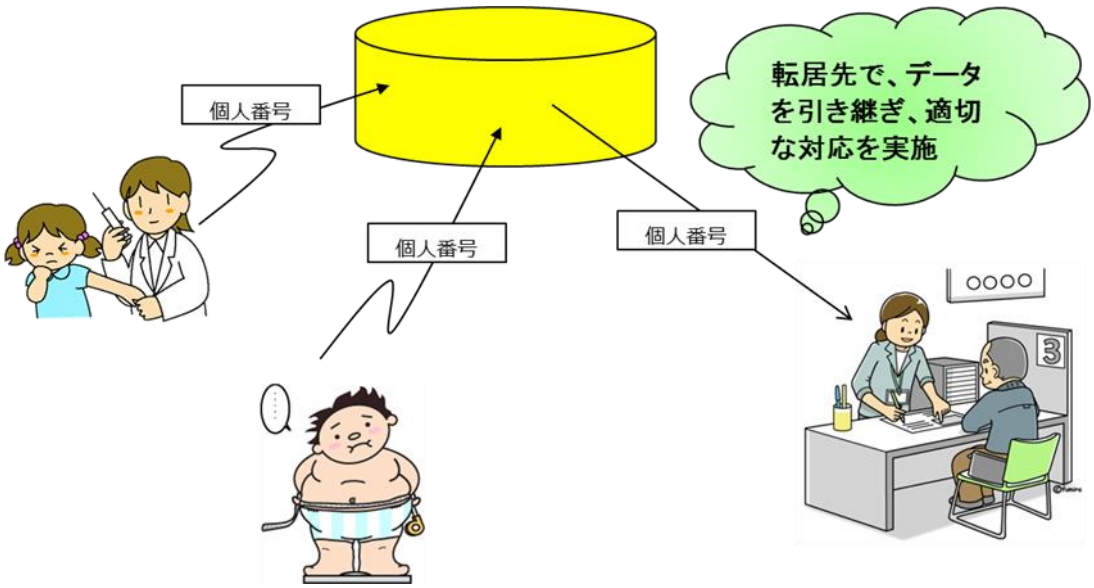


図５．検診、予防接種等での利用のイメージ

２．マイナンバーで便利になることは何か

個人番号の導入によって、所得や他の行政サービスの受給状況を把握しやすくする等により、公平・公正な社会が実現する。また、添付書類の削減など行政手続が簡素化され行政が効率化すると同時に国民の利便性が向上する。

添付書類の削減等を例示すると、①児童手当の新規認定に際し課税証明の提出が不要になる、②ばらばらに申請していた「出生届、健康保険の加入、家族に給付される乳幼児医療費助成、児童手当金、出産育児一時金、出産手当金、育児休業給付金、高額医療費」を一括で申請することができる、③死亡届、年金受給停止届、介護保険資格喪失届、住民票の抹消届、世帯主の変更届、遺言書の検認等が一括で対応可能になるといったことである。

マイナンバーは、「正確な本人確認」ができる重要な社会基盤である。まずは行政分野で大きな制度変化が起きることが期待される。

まず、税制の面であるが、あらかじめ所得などの金額が印刷された申告書（税務署が送付前に本人の所得等を印刷

する)をベースにして確定申告を行う記入済み申告書制度の導入が考えられる。これが実現すると、企業側の年末調整作業が廃止され、家族のプライバシー情報を会社へ提出する必要がなくなる。

現金支払い時に領収書を発行してもらうことにより、現金領収書制度による経済活性化が期待できる。この制度は、韓国で既に導入され、正確な売上捕捉のために利用されている。

土地・家屋の所有者・相続者を明確にすることができる。農地台帳・森林台帳へ適用し、所有者を明確にすることにより、農地・森林の再開発等に利用することができる。

家族制度に関しては、個人が完全に特定できるので戸籍制度の必要がなくなり、事実婚を前提とした家族関係登録などが実現するかもしれない。

当初の目的である社会保障、医療保険、年金制度の一元化が実現し、さらに税と一体化することにより、公平・公正な社会の実現が期待できる。

なお、地方自治体の業務、約 2000 のうち、現時点で 150 ほどが電子化される見込みである。さらなる利活用の推進によって、残りの 1850 の業務のどこまでが電子化されるか、今後の進展に期待したい。

Ⅲ．マイナンバー、マイナンバーカード及びマイナポータルによる産業構造の変化に向けた取り組み

マイナンバー制度の発足にともない、希望者に個人番号カード(以下、マイナンバーカードという)が交付される。このマイナンバーカードの利用により、行政はもとより民間においてもネットワーク上であらゆる手続きが完結する社会が実現する可能性がある。最後にマイナンバーの利用によって、どのような変化が起きるかを瞥見したい。

１．マイナンバーカードとマイナポータルについて

10 月から開始される番号の通知カード送付の封筒に、個人番号カード(マイナンバーカード)交付申請書が同封される。この申請書には、通知カードに記載の住所、氏名、生年月日、性別が印字済である。交付希望者は、この申請書に署名し、電話番号、個人番号カードへの点字表記希望の有無、個人番号カードに搭載する電子証明書の発行希望の有無等を記載する。さらに顔写真(4.5cm×3.5cm)を添付して、同封される返信用封筒に封入し、郵送により申請する。1か月後に住民票を有する自治体から発行が通知されるので、「通知カード、本人確認書類(運転免許証など)」を持って、自治体窓口で受領する。なお、交付開始は 2016 年 1 月以降である。また、交付手数料は、初回は無料となっている。マイナンバーカードの様式を図6．に示す。

なお、マイナンバーカードの交付にともない、住基カードは終了する。

図６．マイナンバーカードの様式

マイナンバーカードには顔写真が貼付されているので、運転免許証等と同様に、これだけで本人確認ができる身分証明書として機能する。ただし、裏面に記載される個人番号は、番号法の制約を受けており、目的外で裏面を見せたり、

コピーを求めたりしてはいけない。

希望により公的個人認証（JPKI）を搭載することができる。これにより、従来の署名認証機能（e-tax など）に、利用者証明認証機能（マイナポータルのログインなど）を追加することができる。マイナンバーカードでは、電子署名と電子利用者証明の検証者の範囲を拡大し、行政機関だけでなく総務大臣の認定を受けた民間企業も対象になる予定である。

マイナンバーカードの利用の場を大きく広げるマイナポータルについて説明する。マイナポータルとは、別名「情報提供等記録開示システム」といい、個人情報のやりとりの記録を、本人がインターネット上で確認できるシステムである。2017年１月から利用可能になる予定である。ちなみに、以前は「マイ・ポータル制度」と呼ばれていたが、2015 年４月に正式名称が「マイナポータル」に決まった。

マイナポータルでは、自分の個人情報をいつ、誰が、なぜ提供したかの確認、行政機関などが持っている自分の個人情報の内容の確認、行政機関などから提供される一人ひとりに合った行政サービスなどの確認の三つのことができる。個人のパソコンでの利用を想定しているが、パソコンがない人でもマイナポータルを利用できるよう、公的機関への端末設置を予定している。マイナポータル利用の際に、なりすましにより特定個人情報を詐取されることのないように、マイナンバーカードのICチップに搭載される公的個人認証を用いたログイン方法が採用される。

以上のように、マイナンバーカードによる公的個人認証を経たマイナポータルの利用により、例えば各種社会保険料の支払金額等、確定申告等を行う際に必要となる情報の入手がネット上で行えるようになる。 また、引越し等において官民横断的な手続のワンストップ化や納税などの決済をキャッシュレスで電子的に行うサービスも検討されている。

２．マイナンバー、マイナンバーカード及びマイナポータルのさらなる利活用の推進について

マイナンバー、マイナンバーカード及びマイナポータルのさらなる利活用の推進について、事例によって紹介する。

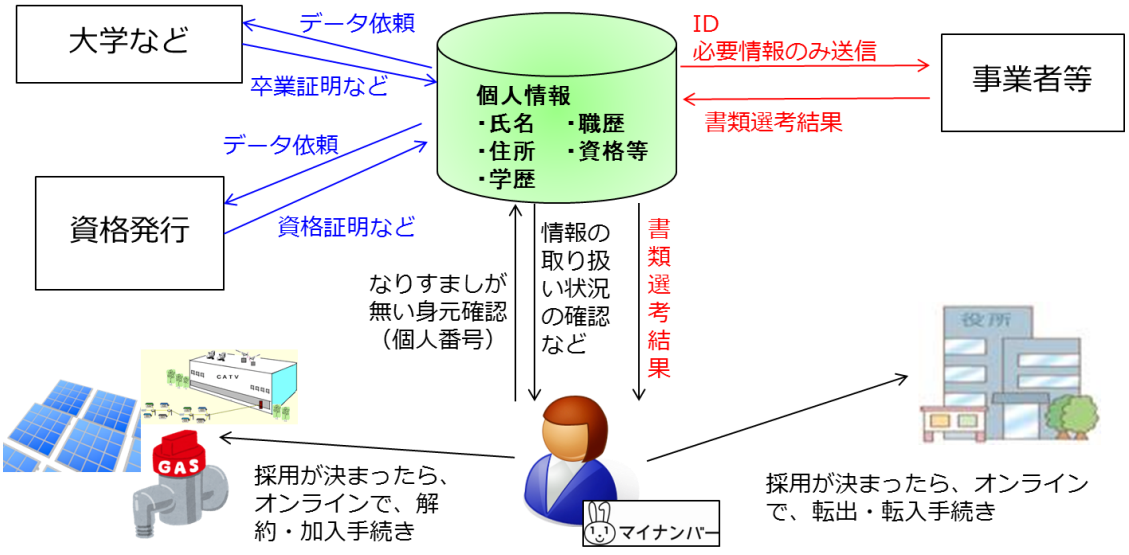


図７．マイナンバー、マイナンバーカード及びマイナポータルの転職にともなう諸手続きでの利用

最初に紹介するのはマイナポータルの転職活動への適用である（図7．参照）。転職を希望する人は、マイナポータルによって、大学等の資格の発行元等に各種資格情報の提供を要求する。このとき、マイナンバーカードによって本人確認が行われているので、資格の発行元は個別に確認をとる必要なしに各種の資格情報を提供できる。また、転職先の事業者には、資格情報等必要な個人情報のみが送信される。採否の決定も事業者からマイナポータルに通知される。転職にともなう引越に際し、役所への転出及び転入手続きや、転出、転入にともなうガス、水道、電気等の契約の解除及び新規の締結手続きも、マイナポータルにより本人のパソコン上で一元的に行うことができる。

マイナポータルを含む当該利用者の情報を、マイナポータル上のアプリケーションが本人の代理として収集し、利用する仕組み（ネット上の代理人）も検討されている。各種控除等を含む納税のためのデータ収集と処理を、まずはマイナポータルが本人に代わって実施し、その結果をサービス事業者に預けることにより、ほとんど本人の手を煩わすことなく納税手続きが完結する。図8. を参照されたい。

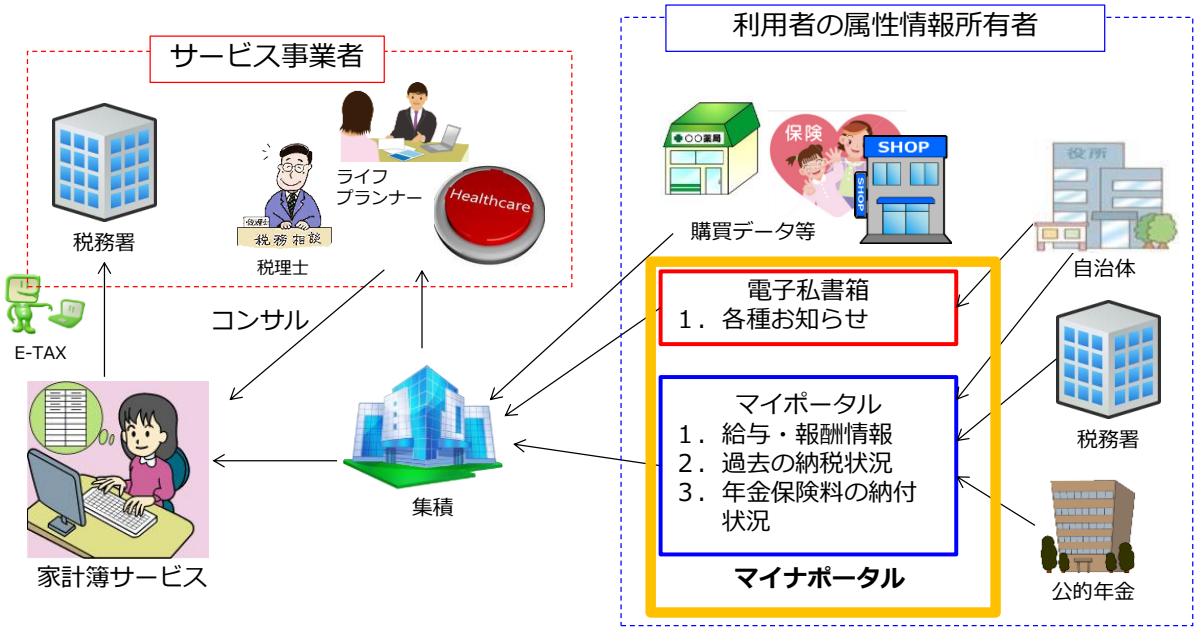
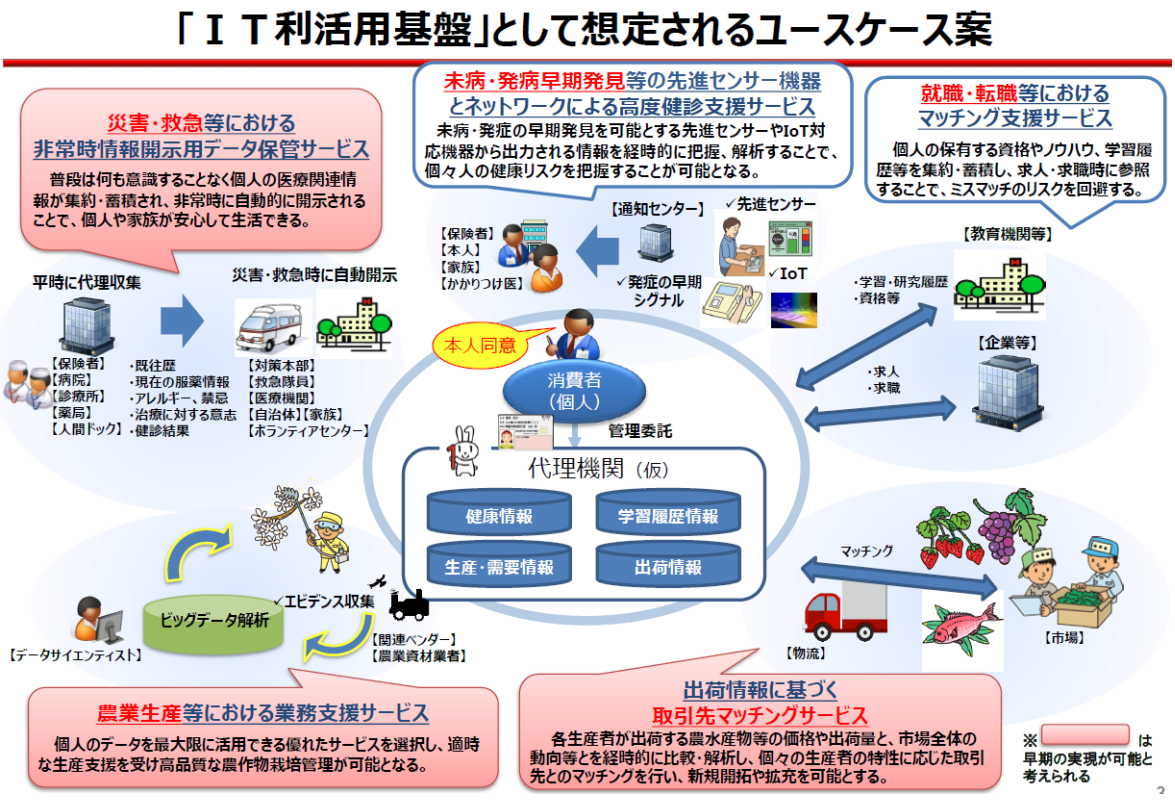


図８．納税手続きにおけるネット上の代理人のイメージ

最後に、「IT利活用基盤」として想定されるマイナンバー、マイナポータル等のユースケース案を図9. に示す。



出典：第９回マイナンバー等分科会資料

図９．「ＩＴ利活用基盤」として想定されるマイナンバー、マイナポータル等のユースケース案

図 9.に示すように、普段は個々の病院等で厳重に管理され開示されることのない医療情報等を災害・救急時に開示するための事前の保管サービス、未病・発病早期発見等の先進センサー機器をネットワークに接続して実現する高度検診支援サービス等、これまで技術的には可能であっても個人情報保護の観点から実現できなかった種々の高度かつ重要な活動が、マイナンバー制度の強固な本人確認機能と安全管理機能により実現されるようになるであろう。

おわりに

本日は、はじめに、ご参加の方々が強い関心をお持ちの、間もなく送付が開始される個人番号に関して、事業者が実施しなければならい各種の措置を中心にご説明した。お役に立ったであろうか。次に、マイナンバー、マイナンバーカード及びマイナポータルの利活用によって、社会がどのように変化していくかを瞥見した。マイナンバー制度の導入により、行政はもとより民間においても、これまで紙媒体を通じて行なってきた各種の手続きの多くがネット上で完結するようになる。そうなると日本の社会全体が大変革を遂げざるを得なくなる。その辺りの見通しについて少しでもご理解いただけたら幸いである。

【報告者の所感とお詫び】

個人番号送付開始の 2 週間前、番号法及び個人情報保護法の改正法成立の 2 週間後という絶妙のタイミングで開催された文字どおり時宜を得た講演であった。また、上記のタイミングに相応しい内容の濃い講演であった。講演後、たいへん活発な質疑が行われたが、紙面の都合で割愛させていただいた。深くお詫び申し上げる。

【参考情報】

政府マイナンバー・コールセンター

0570-20-0178（平日 9:30 から 17:30；土日祝日、年末年始を除く）

〔URL〕

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

・JIPDEC 支援サイト
http://www.jipdec.or.jp/project/mynumber_support.html

〔本文中で参照した政府のＷｅｂ公開資料〕

・「特定個人情報の適切な取扱いに関するガイドライン（事業者編）」 2014 年 12 月 11 日、特定個人情報保護委員会
http://www.ppc.go.jp/files/pdf/261211guideline2.pdf

・「国税分野における社会保障・税番号制度導入に伴う各種様式の変更点」 2015 年 8 月、国税庁
http://www.nta.go.jp/mynumberinfo/pdf/mynumber_modification.pdf

〔書籍〕

・影島広泰著『マイナンバー制度への実務対応』（清文社）
・榎並利博著『マイナンバー制度と企業の実務対応』（日本法令）
・袖山喜久造『マイナンバー制度と企業の実務』（税務研究会出版局）
・JIPDEC 編『特定個人情報保護評価の進め方』（アマゾン・プリントオンデマンド）
・瀬戸洋一他著 『プライバシー影響評価 PIA と個人情報保護』（中央経済社）

〔文献〕

・坂下哲也「個人番号関係事務実施者としてのマイナンバー対策について」（『自治体ソリューション』2015 年 6 月号）

以上

＜目次＞

2015.10

中部支部報告　【　西日本支部合同研究会　ｉｎ　ＧＩＦＵ　】

会員番号　1711 澤田裕也(中部副支部長)

１．はじめに

2015年9月5日(土)、6日(日)岐阜市にて開催した「西日本支部合同研究会 in GIFU」について報告する。
「西日本支部合同研究会 in GIFU」のコンセプトは以下のとおり。

社会保障・税に関わる番号制度、ビッグデータの利活用など、社会や組織の活動における情報システムの利用が益々浸透し、社会の発展をけん引するものとなってきました。そして、情報システムの利用に関わるリスク管理の対象範囲・領域が拡大・変質し、改めて健全な情報化社会の発展に寄与するシステム監査の重要性を認識しないわけにはまいりません。

そこで、本研究会では、『社会と組織のためのシステム監査』をテーマとして、西日本支部の会員各位の発表と、情報化社会の発展に貢献するシステム監査の在り方・今後について議論してまいります。

２．一日目(研究会)

(1)本部挨拶、基調講演(斎藤副会長)

監査の最新動向の説明も交えた本部挨拶の後、基調講演「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」発行の経緯と「読者用ダウンロードサイト」のご紹介いただいた。

ハンドブックの概要、ダウンロード可能な様式、著者間のWebでの情報共有等説明いただいた。ハンドブックおよび様式を活用するとともに、情報共有の方法も支部活動で参考にしていきたい。

(2)北信越支部(長谷部　久夫氏)

「重要インフラにおける情報セキュリティ管理PDCAサイクルの実効性確保とその監査について」

政府の動向(第3次行動計画)を踏まえ、情報セキュリティPDCAサイクルをまわすための課題および対応策案、監査をするにあたってのポイントについて発表いただいた。非常に時間をかけて議論、整理したことがよくわかり、中部支部活動でも参考としたい。

(3)中四国支部(溝下　博氏)

「システム監査実務再考(振り返り)～J-SOX、Pマーク審査のL型実務を中心に～」

監査について日頃感じていること等を中四国支部のメンバーで議論した結果を発表いただいた。ここで書くことができないような生々しい内容で、資料配布がないのも納得した。発表を聞いていて共感することがとても多かった。

(4)九州支部(諸藤　雅之氏)

「保健医療福祉分野のシステム監査とガイドライン」

ご自身の資格維持経験を踏まえ、医療情報システム監査人の試験制度と関連ガイドラインの説明をいただいた。私自身、医療分野の情報システムについて触れる機会がほとんどなかったので学ぶことも多く新鮮であった。

(5)近畿支部(松井 秀雄氏)

「保証型システム監査を可能にするアプローチ」

近畿支部にて実際に行った保証型監査をもとに、監査の分類、監査手順、言明書の考え方について発表いただいた。私も以前日本セキュリティ監査協会の保証型監査プロジェクトに参加して難しさも感じていたこともあり、保証型監査の実例を目の当たりにすることができ感慨深かった。

(6)中部支部(大友 俊夫氏)

「基礎自治体におけるITマネジメント力強化の取組」

ガバナンス強化にあたり、組織風土や関係者を変えるための方法と苦労を教えていただいた。少しずつでも自分の仕事に取り入れていきたい内容であった。

３．一日目(交流会)

交流会は長良川鵜飼。ここ数日の雨がうそのような好天。各支部から差し入れいただいたお酒を鵜飼船で味わいながら研究会の内容、出身地ネタ等で盛り上がった。鵜飼は迫力満点の総がらみを間近で見ることができ非常に満足度の高いものであった。

４．二日目（施設見学と街なか歩き）

今年7月に開館したばかりのぎふメディアコスモス(中央図書館、市民活動交流センター等からなる複合施設)について、街づくりのなかでの位置づけ、施設の建設コンセプトについて紹介いただいたのち、自由見学した。

大雨のため、後半の街なか歩きは残念ながら中止となった。

５．さいごに

多くの協力をいただいて2日間の合同研究会を無事終えることができた。講演者、出席者、後援団体、中部支部スタッフにこの場を借りてお礼を申し上げたい。また、本合同研究会の成果を踏まえ、監査の普及・監査人の知識向上につながる活動を引き続き推進していきたい。

研究会の様子

鵜飼船での懇親会

鵜飼

以上

＜目次＞

2015.10

支部報告　【　システム監査体験セミナー（入門編）開催結果報告　】

会員番号　1345 広瀬克之　（近畿支部）

１．セミナー名称　：　システム監査体験セミナー（入門編）
２．開催日時　　：　２０１５年８月２９日（土）　１０時～１７時
３．開催場所　　：　大阪大学中之島センター　３０２号室

４．開催概要

近畿支部では、2015年8月29日(土)、大阪大学中之島センターを会場として、システム監査体験セミナー(入門編)を開催しました。今回は、これまで数年に渡って開催してきた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から、「セキュリティ」・「マイナンバー」・「指摘文書作成」という3つのテーマに関する内容で10時から17時まで、6名の方に参加頂いて実施しました。コースの概要は以下の通りです。

(1)　システム監査の進め方　＆　ケース演習Ⅰ

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、「システム監査の進め方」の講義を行いました。その後、本日最初の演習として、実際に起こったセキュリティ事故を題材としたケーススタディを行いました。受講者を2チームに分けて、事故の内容を理解した後、インタビュー項目を想定し、チェックリストのまとめ・報告を行っていただきました。

(2)　指摘文書トピックス

長年、大手電気機器メーカの内部監査人としてさまざまな経験をしてきた協会会員の体験を、有効な指摘文書を作成する上での考慮点・工夫点に焦点を当て、トピックス的に解説しました。

(3)　ケース演習Ⅱ

午後から実施した演習は、本年間もなく個人あてに通知される個人番号(マイナンバー)に関するテーマとしました。協会の会員でマイナンバーに詳しい弁護士・福本先生に、まずマイナンバー法に関する主旨を1時間講義いただき、その後、マイナンバー導入において陥りやすい取り扱いの間違いを含んだ人材派遣会社の事例を学習しました。マイナンバーをどのように取り扱うのか経営者の認識、情報システム課長の認識を把握し、ヒアリング項目をまとめて、システム課長にのヒアリング、指摘のまとめ、グループ報告、評価の手順で進めました。

(4)　ケース演習Ⅲ

監査実施の場面では、効果的な指摘文書の作成能力が必要です。外部監査員として多くのISOを中心とした監査の経験を持つ協会会員から、ISO規定・内部監査基準などが要求している報告・指摘文書の要件を解説し、何点からの指摘事例を、受講者が修正し、どのような考えで作成していくかを解説しました。

５．受講者の皆様の感想

受講された皆様からは、「マイナンバー」に関するご意見を中心に以下のようなお声を頂きました。

＜マイナンバーに関するテーマ＞

・マイナンバーに関する演習については、マイナンバーに特化した視点で考えるのか、監査一般的な視点で考えるのか、その他前提を含め、明確にした方が論点が見えたと思う。

・マイナンバーについては「何となく知っている」レベルだったので、本質について理解が深まった。

・マイナンバーについて、もう少し時間をとってほしかったが、適時でもあり有益度が高いと思う。会社内でもフィードバックしたい。

＜セミナーの進め方・全般について＞

・グループワークは、個人で考えたことを形にできて、かつ、チームワークの大事さも身に染みましたので、勉強になった。

・グループ演習の時間がもう少し長い方がなお良かった。まとめる時間がうまく取れなかった。

・グループワークや監査文書作成は、最初に規範を示しておく方がよい。人によっては、見当違いなことをやり続けるリスクがあります。

・グループ討議は初対面の者同士なので、スタッフが進行の手助けをする等、時間を有効に使えるよう考慮してもらいたい。

上記の他、時間・費用に対して「満足」とのご意見や、演習テーマの条件等が「わかりづらい」、「事前にシステム管理基準等の準備が必要」、「技術者試験の論文の添削講座など、監査人の仕事の広報や後輩育成の施策を考慮してはどうか」などの、ご意見がありました。

６．感想

今回、申し込み者10名に対して出席者が6名という今までにない、欠席率となりました。（これまでの欠席率はセミナー全体で5%程度）。今後、申し込み者との連絡を密にする等、欠席率の減少の工夫が必要になりました。受講生の皆さんは、システム監査の学習になじみが薄い方と、豊富な経験者の方が参加されましたが、上記のご意見を参考に今後とも、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

＜目次＞

2015.10

支部報告　【　近畿支部　第１５４回定例研究会　】

会員番号 1779 山本全（近畿支部）

１．テーマ　「ツールが無くてもここまでできる SAP ERP 内部統制監査」

２．講師　三洋電機株式会社 品質・業務推進センター IT 統制推進部
浦上豊蔵 氏　梅谷正樹 氏　下田あずさ 氏　木ノ原真由美 氏　中川昭仁 氏

３．開催日時　２０１５年９月１８日（金）　１８：３０～２０：３０

４．開催場所　大阪大学中之島センター　７階　講義室７０２

５．講演概要

(1) 三洋電機㈱でのシステム監査の歴史

1987～1990年頃をシステム監査黎明期としており、他社に比べ早くから取組みを開始。以降中断時期を挟み、システム監査を再開したのは 1999 年からで、拡大契機となったのは 2007 年のJ－SOX対応。2000年問題を機に海外子会社に標準システムとして導入したSAPシステムは、「J-SOX 以前に導入されたため内部統制が十分に考慮されていない」という課題があった。 さらに、国内事業所での SAP 導入拠点が少なく、SAP 監査に対する知見が監査人に全くない状況であった。そのような経緯からSAP監査技法の確立と内部統制の高位平準化が、システム監査部門にとって大きなテーマとなっている。

(2) SAP 監査のグローバル傾向

浦上氏

アプリケーションそのものの機能について、ERPであっても自動化統制（正当性、網羅性、正確性）は要求される。パッケージ特有の内部処理ブラックボックス化という現実をふまえ、①ERP導入時に想定したデザイン通りに利用するような統制があるか　②ブラックボックスの前後IN／OUTで正当性、網羅性、正確性が保たれているか　③不適切なプログラム変更が行われていないか、を主要な評価視点とする。SAPでは標準プログラムの改修やDBテーブルの変更は「モディフィケーション」と呼ばれており、これを行うことはERP適用メリット自体を否定することとなるため「原則行わない」が一般認識である。モディフィケーションを行わない限りはSAP標準機能で統制が保証されていると見なすのが海外監査法人における一般的な考えで、自動化統制の評価に重きを置かない傾向があることが、これまでの海外拠点の外部監査支援を行う中で判った。

一方、不備指摘事項として主に外部監査で取り上げられたのは

① 職務分掌の逸脱
　初期導入時/組織再編時に職務を十分に考慮せず，必要の無い権限を付与

② 高権限の限定付与の未実施
　高権限の過剰な付与や，高権限操作者に対するモニタリングの未実施

といったアクセス権限管理に関わるものがほとんどであった。

(3) 職務分掌の評価(職務の分離と実行権限の付与)


梅谷氏

SAPには業務処理に結びつく「トランザクション」と呼ばれる機能単位が6万個以上存在する。その中から統制に関わる重要トランザクションを特定して権限付与の妥当性を評価する必要がある。それが十分でなかったことが前項に述べた不備指摘につながっている。重要トランザクションの例は下記の通り。

・マスターデータ(取引先・品目・勘定科目)の登録・更新
・伝票(受注・出荷・発注・検収・請求・会計等)の登録・更新
・与信限度額の変更
・ユーザ ID 情報の登録・変更

最近の傾向として「不正防止」観点が重要視されており、「衝突する特定トランザクションの付与を禁止し、不正の機会を抑止」することをねらいとした取組みを行っている。

一般的な不正リスクシナリオ(架空受注,出荷/架空債権計上,入金による横領等)を想定し、それを防止できる職務分掌(SOD)ルールを考え、衝突回避すべきトランザクションの組合せを定義するという作業を行った。これを元に個々の SAP システムの運用ルールを照合し整備状況を確認している。

また実際のコントロール運用として、トランザクションに紐づく SAP 内の定義データに対する検査を行っている。

① ロールの SOD チェック
ロール/トランザクション表から、衝突するトランザクションのパターンを持つロールを検出する

② ユーザの SOD チェック
ユーザ/トランザクション表を作成し、衝突するトランザクションのパターンを持つユーザを検出する

2種類のチェックを実施するために独自のツールを作成しており、同様の機能を持った市販の高額ツールに代替できる効果を創出している。

(4) SAP 標準機能を活用した監査手法


下田氏

ここでは主にSAPにおける高権限IDの管理に焦点をあて、予め備わっている標準機能を活用工夫することで十分なコントロールを実装できること、そして監査にも利用できることをデモを織り交ぜて紹介があった。

高権限IDを①オールマイティ(SAP*等) ②アプリ用の重要なパラメータ等設定ID ③IDの登録・修正・削除が可能なIDと定義している。①については「特に強権なビルトインIDは人による使用がなされていないこと」、またその他の①と②③共通観点では「実行可能IDの存在・付与が限定されていること」が管理ポイントとなる。そしてこれらの条件抽出・棚卸は標準機能を活用することで十分実用的な運用とその検証が可能ということである。

また高権限以外の観点で重要なアクセス権限管理ポイント「不要ユーザ(退職者等)の抽出」「プロファイルパラメータによるセキュリティ設定状況」についても標準機能の活用で容易に確認可能であることも解説された。

(5) 内部統制レベルアップへの取り組み

SAP内部統制を維持するために、システム環境面、教育面での取り組みを継続して行っている。


木ノ原氏

システム環境面においては①SAP社が提供している仮想企業環境“IDES”を PC サーバー上に構築し、機能検証に役立てていること ②本番環境に対する監査人用ロールとして SAP_ALL_DISPLAY を新バージョンの環境でも利用できるようにし、監査作業が業務に影響しないような工夫がされている。

次に教育面においては、監査人および被監査部門向けにSAPの“概要”“ITGC”“ITAC”で構成された「内部統制基礎講座」研修が用意されている。実務場面ではそれに対応する形でSAP「自己点検支援ツール（かんたん！チェックシート）」「ITGC監査マニュアル」「ITAC監査マニュアル」が作られている。

また、SAP不正リスク監査にスコープした社内研修コースも別途用意されている。

６．所感

自分自身被監査部門の立場でSOX対応を8年間続けているが、パッケージか否かに関わらず「アプリ仕様そのもの」を主だって評価する段階は過ぎ、「ITと人をつなぐ接点が適正管理されているか」がより重要な評価視点になっていると実感している。その意味でも今回の発表の背景にある課題認識は十分共感できるものであった。

SAPという「自社の手の内に無い」しくみに対し、権限コントロールに責任が持てるよう社内監査部門の立場で徹底的に創意工夫されていることが良く理解できた。パッケージといえどもコントロールするにはそのしくみを深く理解する必要があり、その労を惜しまず地道な取組みを続けられたことが成果に結びついているのだと考える。本日は実機デモも交え、実務者視点からも大変有意義な講演を頂戴しました。

以上


中川氏


情報交換会

以上

＜目次＞

2015.10

注目情報（2015.9～2015.10）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■【注意喚起】「特定の組織からの注文連絡等を装ったばらまき型メールに注意」

2015年10月9日

独立行政法人情報処理推進機構

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は 10 月 8 日以降、“特定の組織からの注文連絡”や“複合機からの自動送信”等を装った Word 文書ファイルが添付された不審なメールに関する相談が相次いだことから、当該メールに関して注意喚起を行います。

URL：http://www.ipa.go.jp/about/press/20151009.html

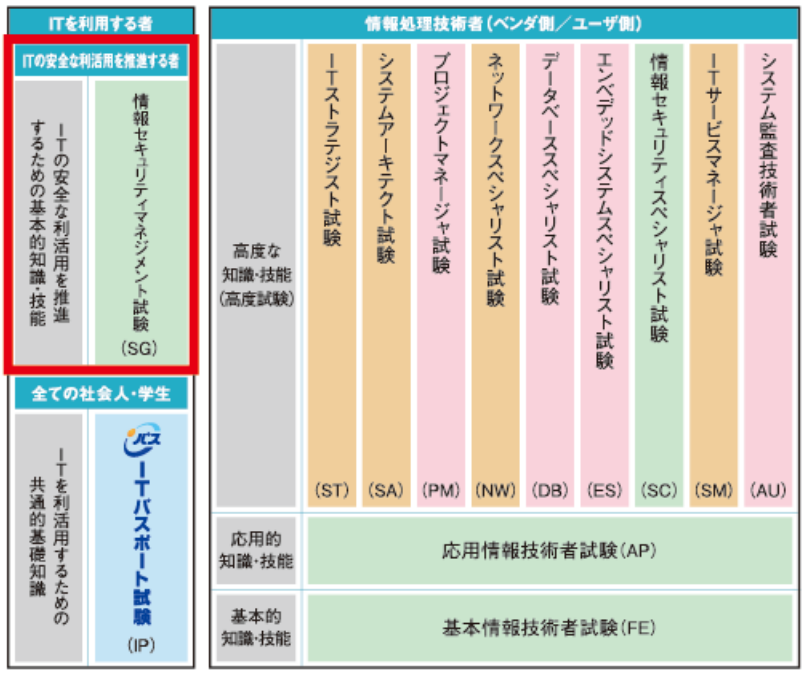
■【国家試験「情報セキュリティマネジメント試験」の創設と実施について】

2015年10月16日

独立行政法人情報処理推進機構

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、国家試験「情報処理技術者試験」の新たな試験区分として「情報セキュリティマネジメント試験」が経済産業省によって創設されたことを受け、平成28年4月から実施することを10月16日に公表しました。あわせて、同試験の出題範囲・シラバス・サンプル問題などの詳細情報をIPAのウェブサイトで公開しました。

URL：http://www.jitec.ipa.go.jp/sg/



情報処理技術者試験の試験体系

＜目次＞

2015.10

【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第208回	日時:2015 年 11月19日(木)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「リスクマネジメントと危機管理　　～想定内と想定外:原点に戻って考える～　」
	講師	東京海上日動リスクコンサルティング株式会社 上席主席研究員　指田　朝久　氏
	講演骨子	地震、水害、火山噴火、テロ、株価の暴落、粉飾決算、情報漏洩、ハッキング、コンピュータウイルス、法令違反など様々な企業や組織をゆるがす事態が発生している。 これらについて危機管理あるいはリスクマネジメントと説明されるが、その言葉の意味は使用する人々によって様々である。また東日本大震災の教訓として想定外に備えることが示されているが、これらはリスクマネジメントや危機管理のどの領域に対応するのであろうか。 今日はこれらの言葉の使い方について原点にもどって考察する。
	お申込み	日本システム監査人協会ホームページ
第209回	日時:2015 年12月14日(月曜日)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「IT ガバナンスの JIS 化」(仮題)
	講師	日本 IT ガバナンス協会(ITGI Japan)　　副理事長　梶本　政利　氏 認定 NPO 法人　日本システム監査人協会　副会長　　力　利則　氏
	講演骨子	詳細確定次第、HPでご案内いたします。
第210回	日時:2016年1月21日(木曜日)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「最近の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」(仮題)
	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	詳細確定次第、HPでご案内いたします。

【外部主催イベント・セミナーのご案内】

■ＩＳＡＣＡ東京支部 2015 年　月例会予定（東京）

日時: 2015 年 11 月例会　11/25(水)開催予定　18:30-20:10(受付開始:18:00) 2015 年 12 月例会　12/22(火)開催予定　19:00-20:40(受付開始:18:30)	
詳細	http://www.isaca.gr.jp/education/index.html

＜目次＞

2015.10

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。

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/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

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
　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。

ご意見募集中

・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。

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。

＜目次＞

2015.10

協会からのおしらせ 【年会費納付時期について 】

会員番号 1760 斎藤由紀子 （事務局長）

会員各位

いつも、協会活動へのご協力を賜りありがとうございます。

早速ですが、会員規程に従い、2016年度年会費の請求書を、2015年12月1日付で発送いたしますので、ご準備のほどよろしくお願い致します。

【会員規程】 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf

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

【2016年度会費請求の内容】

＜金額＞ 正会員個人:　￥10,000－　（消費税非課税）

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

＜払込期限＞2016年2月末日

なお、正会員団体に限り、事業年度予算等の事情による、「納付期限延長願い」をご提出いただくことで、納入期限の延長が可能です。（原則2016年4月末期限。ただし時期についてはご相談ください。）

お申し出先: http://www.saaj.or.jp/toiawase/index.html （事務局）

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

加入者名:日本システム監査人協会事務局

銀行振込口座:みずほ銀行八重洲口支店（普通）2258882

口座人名:特定非営利活動法人日本システム監査人協会

トクヒ）ニホンシステムカンサニンキヨウカイ

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

（会員番号が付けられない場合は、メールで振込内容をお知らせください。）

【2015年度会費未納の場合】

一部の会員の方について、2015年度会費のお支払が確認できません。2015年12月31日までに納付が確認できない場合は、除名処分となりますので、至急お手続きいただきますようお願い致します。

なお、http://www.saaj.or.jp/kenkyu/index.html の「会員ログイン画面へ」から、会員ページにアクセスしていただきますと、会費のお支払状況をご確認いただくことができます。

【ご寄附のお願い】

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

＜寄附金額＞￥3,000/一口　　ご寄附は、何口でも承ります。

＜振込先＞ご寄附は、協会会費に合算して、会費振込先にお振込みください。

＜東京都への個人情報の提供＞法令に基づき、寄附者名簿（氏名、ご住所）を、認定NPO法人所轄庁の東京都へ報告致します。何卒ご了承賜りますようお願い致します。

【会費、ご寄附等に関するお問い合わせ先】：http://www.saaj.or.jp/toiawase/index.html （事務局）

＜目次＞

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更・追加された予定			2015. 10
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**
10 月	8:　理事会	23:　第 207 回月例研究会	18:秋期情報処理技術者試験
11 月	12:理事会 13:予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/8〆切) 18:2016 年度年会費請求書発送準備 23:会費未納者除名予告通知発送 30:本部予算提出期限	中旬:秋期 CSA 面接 19:第 208 回月例研究会 20:CSA･ASA 更新手続案内 〔申請期間 1/1～1/31〕 27:CSA 面接結果通知	
12 月	1:2016 年度年会費請求書発送 2016 年度予算案策定 10:理事会:2016 年度予算案 会費未納者除名承認 第 15 期総会審議事項確認 11:総会資料提出依頼(1/8〆切) 15:総会開催予告掲示 18:2015 年度経費提出期限	10:CSA/ASA 更新手続案内メール 14:第 209 回月例研究会 18:秋期 CSA 認定証発送	
2016 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1 月	8:総会資料(〆) 16:00 13:総会･役員改選の公示 14:理事会:通常総会資料原案審議 15:総会開催案内掲示･メール配信 20:2015 年度決算案 23:2015 年度会計監査 26:総会申込受付開始(資料公表) 31:償却資産税･消費税	1-31:CSA･ASA 更新申請受付 20:春期 CSA･ASA 募集案内 〔申請期間 2/1～3/31〕 21:第 210 回月例研究会	8:会計:支部会計報告期限 25:SAAJ 創立記念日
2 月	4:理事会:通常総会議案承認 25:法務局:資産登記、活動報告提出 理事変更登記 **29:年会費納入期限**	1～3/31:CSA･ASA 春期募集	**22:第 15 期通常総会･特別講演**
3 月	1:東京都へ NPO 事業報告書、役員変更届提出 7:年会費未納者宛督促メール発信 10:理事会	2:第 211 回月例研究会 上旬:CSA･ASA 更新認定書発送	
2015 年	**過去に実施した行事一覧**		
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 中旬　認定委員会:新規ASA認定証発行 28 日第 201 回月例研究会	19 日　2015 年春期情報技術者試験
5 月	14 日　理事会 29 日　年会費未納者宛督促メール発信	中旬　認定委員会:新規 CSA 面接 29 日第 202 回月例研究会	
6 月	3 日　認定 NPO 法人東京都認定！ 4 日　会費未納者督促状発送 11 日　理事会 12 日～会費督促電話作業(役員) 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)	10 日　認定委員会:CSA 面接結果通知 16 日　第 203 回月例研究会 18-19 日　事例研:第 27 回システム監査実践セミナー(日帰り 2 日間コース)	
7 月	8 日　支部助成金支給 9 日　理事会	1 日　秋期 CSA･ASA 募集案内 〔申請期間 8/1～9/30〕 14 日　第 204 回月例研究会 20 日　認定委員会:CSA 認定証発送	14 日　支部会計報告〆切
8 月	(理事会休会) 29:中間期会計監査	1:　秋期 CSA･ASA 募集開始～9/30 24:　第 205 回月例研究会	
9 月	10:理事会	15:　第 206 回月例研究会	5-6:西日本支部合同研究会 (開催場所:岐阜)

＜目次＞

2015.10

会報編集部からのお知らせ

1. 会報テーマについて
2. 会報記事への直接投稿(コメント)の方法
3. 投稿記事募集

□■ 1. 会報テーマについて

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。11 月号から 1 月号までは、「システム監査人の未来」をテーマといたします。皆様の幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマも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)

□■ 会報投稿要項 (2015.3.12 理事会承認)

・投稿に際しては、Wordの投稿用フォーム(毎月メール配信)を利用し、会報部会(saajeditor@saaj.jp)宛に送付 して下さい。
・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
・特定非営利活動促進法第2条第2項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
・原稿の掲載、不掲載については会報部会が総合的に判断します。
・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

会報記事は、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。
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: 認定NPO法人 日本システム監査人協会 会報編集部
〒103-0025 東京都中央区日本橋茅場町2－8－8共同ビル6F

■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】 http://www.saaj.or.jp/toiawase/

■会報は会員への連絡事項を含みますので、会員期間中は、会員へ配布されます。
会員の所属や登録メールアドレス等の変更は、当協会ホームページ会員サイトより変更してください。
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。
【会員でない方の送付停止】 http://www.skansanin.com/saaj/register/

■□■SAAJ会報担当
編集委員: 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子、西宮恵子、藤野明夫
編集支援: 仲厚吉 (会長)、各支部長
投稿用アドレス: saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)

＜目次＞