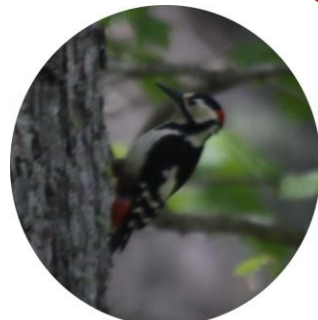


特定非営利活動法人
SAAJ 日本システム監査人協会報

2014 年 9 月号

No 162

— No. 162 (2014 年 9 月号) <8 月 25 日発行> —

残暑、初秋 季節の変わり目**今月号も巻頭言から、
話題満載 目次で検索 !!**

アカゲラ 写真提供: 柴田 幸一 会員

巻頭言**テーマ : SAAJ の活動に望むこと****会員番号 0281 力 利則 (副会長)**

SAAJ 会員になった時に会報に一言寄せた時から、早や 10 数年が過ぎました。今回巻頭言として、自分の反省も含めて SAAJ の活動に望むことを3点述べたいと思います。

(1) その1～SAAJ 会員になったら研究会に参加しよう！～

会員の皆様は研究会に参加していますか？まずは研究会に登録して積極的に参加しましょう。研究会は相互啓発の場であり会員同士を知ることでもでき社外活動として有意義な場です。特に30代、40代の若者たち！にはどれか一つ位は参加して欲しいです。SAAJ としても世の中の動向を掴み新しい研究会を発足させるなど多くの会員の参加を募っていききたいと思います。

(2) その2～SAAJ 活動をまわりに広く知ってもらおう！～

システム監査は、独立的な第3者の立場の取り組みなので、組織の主体者である経営者や幹部層・CIO、システム管理者に十分にその活動を知ってもらわないと成り立ちません。頼まれて！認められて！ナンボの世界だと思います。そのためにはSAAJ 広報活動に積極的に取り組み、SAAJ が発行する各種アウトプットを広く経営者、幹部層・CIO、システム管理者に読んでもらう工夫が重要だと思います。今年度に入って広報活動が強化されましたが、会員一人ひとりの心がけも大事だと思います。SAAJ のしおり、小冊子、会報等を使って様々な場で自ら広報して頂きたいと思います。

(3) その3～システム監査をビジネスとして確立しよう！～

公認会計士は自立してビジネスが成り立っています。それに対してシステム監査人は、CSAになったとしてもビジネスとして生計を立てているケースはあまり聞きません。内部監査としてはだいぶ認知されてきましたが、外部監査の役割はまだ十分には果たせていないと思います。上記(2)の活動とともに連携を取り、法制化や制度化への働き掛けもしながら、ビジネスとして確立できるように風穴を通していきましょう。

私はシステム監査に出会って人生が変わった一人です。いい経験をさせて頂いていると思います。独立した第三者が広くシステムを評価して、監査意見・提言をトップに伝えることは重要だと考えています。トップから見て経営に役立つ監査を繰り返し行っていかなければシステム監査は成り立ちません。JIS化が予定されている「ITガバナンス」にも経営に役立つシステム監査の重要性が謳われています。ぜひ会員の皆様の力！！でSAAJ の活動を盛り上げていき、経営に役立ち、社会に貢献する活動に繋げていきましょう。

<目次>

巻頭言	1
【SAAJの活動に望むこと】	
1. めだか	3
【次世代のためのシステム監査】	
2. 投稿	4
【次世代のためのシステム監査】	
【コラム ITサービスマネジメント奮闘記(メルマガ編)】	
3. 本部報告	7
【第 192 回月例研究会(2014 年 7 月開催)】	
「クラウドサービス利用のための情報セキュリティマネジメントガイドラインの概要及び改訂について」	
講師:経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐 上坪健治 氏	
特定非営利活動法人 日本セキュリティ監査協会(JASA) 事務局長 永宮直史 氏	
【情報セキュリティ監査研究会だより No.17 ーパーソナルデータの利活用に関する 制度改正大綱(検討会案)】(連載)	
【「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」 ～「経済産業省ガイドライン」の読みこなしポイント～	
4. 支部報告	22
【近畿支部報告「第147回定例研究会」:「暗号通貨ビットコインの脆弱性と可能性」】	
【近畿支部 システム監査体験セミナー(入門編)】	
5. 注目情報	26
【経済産業省】「経済団体に対して個人情報保護法等の遵守に関する周知徹底を要請した」(8 月 18 日)	
【IPA情報】「プレス発表:注意喚起「ウェブサイトの改ざん回避のために早急な対策を」	
6. セミナー開催案内	27
【協会主催イベント・セミナーのご案内】	
【外部のイベント・セミナーのご案内(会報担当収集分)】	
7. お知らせ	29
【新たに会員になられた方々へ】	
【協会行事一覧】	
8. 会報編集部からのお知らせ	31
【会報テーマについて、会報記事への直接投稿(コメント)の方法、投稿記事募集】	

めだか 【 次世代のためのシステム監査 】

公共機関の情報システムは社会インフラであり、その障害は多くの人々に被害をもたらすリスクとなる。リスクへの予防措置として公共機関の情報システムにシステム監査が求められるべきと思う。中でも公共機関の情報システムで個人情報を取り扱う情報システムの構築や保守は、障害が起きないよう、また法令等への準拠や本人同意の利用目的に齟齬が生じないようシステム監査を制度化又は法制化するように求めている。

曾野綾子さんの著書「幸せは弱さにある」を読み返してみた。本の中で、「第三章 人との関係で大切なこと」のひとつとして、“「決してあきらめない粘り強い生き方」を私たちはできるか”とある。次の引用文章は、『ルカによる福音書』の11-5～10に於いて、夜遅くやって来た旅行中の友だちにパンを与えるという話にもとづいている。

「あなたがたのうちの誰かに友だちがいて、真夜中にその人のところに行き、次のように言ったとしよう。『友よ、パンを三つ貸してください。旅行中の友だちがわたしのところに立ち寄ったが、何も出すものがないのです』。すると、その人は家の中から答えるに違いない。『面倒をかけないでください。もう戸は閉めたし、子どもたちはわたしのそばで寝ています。起きてあなたに何かをあげるわけにはいきません』。しかし言うておく。その人は友だちだからということで起きて何かを与えるようなことがなくとも、執拗に頼めば、起きて来て必要なものは何でも与えるであろう。そこで、わたしは言うておく。求めなさい。そうすれば、与えられる。探しなさい。そうすれば見つかる。門を叩きなさい。そうすれば、開かれる。誰でも、求める者は受け、探す者は見つけ、門を叩く者には開かれる。」

著者は、この話のポイントは二つあると書いている。一つは、いまでもアラブの砂漠の民の間では「宿を借りに来た旅人には、その人が誰であろうと、パンと水を与えなければいけない」としていること、つまり、「受けることだけでなく、与えることが人間の自立の証である」ということ。二つ目のポイントは、相手にとって与えることが人間の自立の証であれば、「相手に、どんなに拒まれようとも執拗に頼めば、望むものが手に入る」ということ。ここでは、そのような場面での「しっこさ」の大切さが物語られている。

本気で、公共機関の情報システムで個人情報を取り扱う情報システムの構築や保守は、障害が起きないよう、また法令等への準拠や本人同意の利用目的に齟齬が生じないようシステム監査を制度化又は法制化するように求めるのであれば、「しっこく」、粘り強く、求めていると思う。



引用書籍：「幸せは弱さにある」 曾野綾子 著（イースト新書016）

（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＞](#)

投稿【 次世代のためのシステム監査 】

会員番号 0557 仲 厚吉 (会長)

台風 11 号は西日本に大きな被害をもたらしました。西日本の会員の皆様にはいかがでありましたかと案じています。次世代のためのシステム監査は防災にも取り組んでいく必要があると思います。9 月になると防災に係る行事が多くあります。当協会では、9 月の月例研究会で、「首都直下地震の被害想定」の警告 ～情報システムのバックアップは本当に機能するか～(仮題) を、9 月 18 日(木) 18 時 30 分～20 時 30 分、機械振興会館にて、当協会元理事で会員でもある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 氏を講師にお願いして開催します。

当協会では 2014 年 2 月の第 13 期通常総会に、「リーマンショックに立ち向うガバナンス-新 COSO の簡単な理解 - 米国中央政府の Green Report を中心として」をテーマとして、日本 IT ガバナンス協会会長 システム監査学会会長 松尾 明 氏 をお招きし、特別講演を開催しました。本講演では、はじめに、講演の目的である新 COSO の簡単な理解として、「CLICK, CHANGE or DIE」の理解、即ち、インターネットの時代には、「インターネットから情報をクリック、ダウンロードし、そして利用し変化しなければ、死あるのみ」、これが新 COSO の本質である、との説明を聴き、また、新 COSO と改訂の理由、Green Report の定義、新 COSO の 17 の指針、判断基準のデザイン、モニタリング、オブジェクトと COBIT、COBIT の変化など、IT ガバナンスの全般にわたる今後の方向性について聴講しました。

IT ガバナンスは、ISO でも、ISO/IEC 38500 として国際標準になっており、現在、ISO/IEC 38500 の JIS 規格化が進んでいます。IT ガバナンスは、6つのプリンシプル、Responsibility、Strategy、Acquisition、Performance、Conformance、Human behavior で構成され、PDCA を回して、システム監査はその C の役割を担います。IT ガバナンスは、JIS 規格になると社会的な認知に拍車がかかることが期待でき、システム監査人として JIS 規格の発行が待ち遠しい思いです。当協会では、ISO/IEC 38500 の JIS 規格が発行され次第、部会・研究会活動を通じて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。また、当協会の会員が参加している IT Audit の ISO 化の取り組みは、システム監査学会等と協力し ISO/IEC 38500 の JIS 規格化の進捗に並行して進めていきます。

当協会では、2007 年の「システム監査これからの 10 年」アンケートの集計・分析結果に基づいて、「システム監査のこれからの 10 年に向けた提言と当協会の今後の取り組み」についてまとめ、2008 年 2 月 18 日の創立 20 周年記念講演会で発表を行いました。ホームページに 2008 年 3 月 12 日付けで報告資料を掲載しています。このシステム監査これからの 10 年の提言と取り組みに関して、2014 年 8 月 9 日に、システム監査活性化委員会が開催されました。同委員会では、「システム監査のこれからの 10 年に向けた提言と当協会の今後の取り組み」を見直し、残る 4 年間に取り組むべき協会活動の方向性を確認しました。

次世代のためのシステム監査へ会員の皆様のご協力をお願い申し上げます。

[＜目次＞](#)

【コラム】ITサービスマネジメント奮闘記（メルマガ編）

会員番号 1706 下田あずさ（近畿支部 IT サービス G）

1. 頼まれてしまったが（企画フェーズ）

SAAJ近畿支部のITサービスグループ（通称:ITSG）では、同支部Webサイト(<http://www.saaik.org/>)やメーリングリスト（以下:ML）の運用、メールアドレス(@saaik.org)の管理、メールマガジンの発行を行っている。その中で今回はメルマガに関する立ち上げプロジェクトの裏話を、この場を借りて公表させて頂く。

時はさかのぼり2012年7月。定例研究会に子連れ（第一子である長女、当時2歳を連れていた）で出席した私に、帰りがけに声をかけてくださった方がいた。SAAJ会報でもおなじみの神尾博氏（2013年度の会報アワードも受賞！）である。たじろぐ私と、泰然と見守る長女に向かって開口一番……

「ITSGにて、メールマガジンを発行したい」「いきなりだが、メルマガのテンプレート（ひながた）を作ってくれないか」「半分期待しているが、残り半分は期待していないので、肩の力を抜いてやってみて！」……なんだかよく分からないが、唐突に頼まれてしまった。これがそもそものきっかけである。

メルマガと言っても、一体なんなのだろう？ コンセプトとしては、仮に「支部活動やプロジェクトの可視化による活性化」と設定することにして、分からないなりにまずは構想してみることにした。

手法としては、プロトタイプ法を採用。と言えば聞こえが良いが、要するに手探りである。とにかく、このようにして私の「企画フェーズ？」は始まった。

2. まずは枠組みから（概念設計・基本設計フェーズ）

さて気軽に言うてくださったものだ、なぜ私に？等、ナゾはうずまくものの、まずはテンプレート作成である。意見や改善案を伺うにしても、たたき台がないと始まらない。私は、イメージづくりから開始だなと考えた。

今までに自分が購読してきたメルマガのうち、好印象を持っていたものをいくつか眺めてみた。……ふむふむ、読みやすさ（見た目、並び等）と、コンテンツの面白さの、両方の要素があるという印象を受ける。まずテンプレート作成とのことだったので、なるべく読みやすそうな構成になるよう、メルマガのパーツを探すことにする。

インターネットで「メーリングリスト」「テンプレート」等のキーワードで検索した。無料素材のサイトをいくつか閲覧し、シンプルかつ好みの（笑）パーツを取得。そこから若干のアレンジを加え、「SAAJとして格調の高いイメージ」を目指してテンプレートを作成。また、簡易版ではあるが具体記事を載せた「例あり」バージョンも作成し、完成イメージを持ちやすくした。これらの案をITSGのMLに投げて修正意見を待つことに。

これは「アジャイル開発」に近い。アジャイル開発の秘訣は「まずはやってみる」「トライ&エラー」ではないだろうか。パーツも、作ってみてイメージを確認し修正していく為、たたき台があると作業が前に進みやすい。

ここまでのいわゆる概念設計・基本設計フェーズに当たる。たたき台を提出してみると、お！「期待以上、意外と完成度が高いではないか」「『例あり』バージョンをブラッシュアップすれば、すぐに創刊号が発行できるのではないか」との反応……滑り出し順調？！そしてやりとりの中で下田がメルマガ編集長に就任することに。

3. みんなでワイワイガヤガヤ（詳細設計・プログラミングフェーズ）

たたき台を作成したことで、まずはみんなでワイワイガヤガヤと意見交換が出来る段階になった。

どのようにしてディスカッションを行ったか？ ITサービスG用のMLを徹底活用である。ML上でのやりとりは非常に活発だった。『例あり』バージョンに肉付けや修正を行っていく形なので、具体的な話が進めやすい。

冒頭の挨拶文、発行元の表記方法、バックナンバーの扱い、発行日や発行間隔の記載、発行時のメールサプ

ジェクト、各コンテンツの掲載順序といった内容についての検討はもちろんのこと、適宜の改行、1行あたりの文字数といった見やすさの観点での修正もどんどん取り込まれていく。また、各コンテンツの紹介者(すなわち記者の名前)を入れることにより、「顔の見えるメルマガ」を目指すことにした。このように、出てきた案を取り込んだ「改善版」を改善案もどんどん出てきて、それを随時、取り込んでいく。

創刊号として原稿を準備しつつ、テンプレートを形にしていっていった。掲載するコンテンツとしては、定例研究会情報、セミナー情報、サイト更新情報、特集……等々、いずれも「近畿支部や同会員の関連する活動内容やトピック」という視点が前提である。またメルマガ発行を通じて、従来のサイト更新やセミナー情報についてもより一層、こまめな発信とコンテンツ収集が必要だということが、メンバ間での共通認識として挙がってきた。

この段階で、各パートを部品化、分担化し、後々の毎号の編集の効率化を考えた。各パートの担当者が作成した原稿を基に、なるべく「コピー＆ペースト」での編集作業が出来るように、というスタイルも確立されていった。部品化や分担化による効率化、これが後々にも効いてくる(当時はそこまで想像していなかったが……)。

4. 最後のブラッシュアップ (テスト&最終レビューフェーズ)

各パートについて考慮した際、情報発信としてタイムリーかつ過不足なくということを念頭に置いたものの、ひととおりの案が出そろって、あそび心も欲しくなる。全体を眺めたうえでのバランスもあるな…… お、編集後記を誰が担当したか、の箇所にひっそりと編集者名を付け加えてみたらどうだろう。後に「あんた誰やねん？」というタイトルの巻頭言にて名乗らせて頂いたが、編集後記には創刊号から(あ)として登場していたのである。

また、「メールサブジェクトの串団子」(各号のメールサブジェクト横に『- ○○○●』- ○○●○』等の串団子のような記号を付与したもの。●を1、○を0として2進数で読み解いてみると……)についても、グループ内でのブラッシュアップの中で出てきた案である。なんだろうこれ？と思うかも、ちょっとしたITクイズ的な戯れ。

さらに、近畿支部理事の要望により、毎号の先頭に巻頭言を入れることになった。当初の編集メンバの自己紹介から次第に随筆的な内容に推移していき、単なるニュースの羅列といったダイレクトメール臭が消されたことで、支部会員間のコミュニティ性のあるものにつながっている。

5. 何事も継続的改善 (保守フェーズ)

こうして開発とテスト、レビューフェーズが終わり完成。ところがここからPDCAサイクルを回すことも肝要だ。今後の持続性を高め、さらに改善していくには、どうしたらいいか。ここでコンテンツ&タレントマネジメントシート(通称:C&Tシート)が登場する。

表形式にて、毎号ごとに各パーツの記事内容や担当者、今後の予定や実績、進捗状況などを並べてすべての見える化を試みたもの。フォーマット自体も随時更新されており、抜け漏れの防止や担当者の偏り防止、全体進捗管理など、生産性を高める工夫もなされている。

C&Tシートは「誰でもできる」編集業務を目指したものである。編集長の私が第二子出産に伴い産休でお休みさせて頂いていた際、C&Tシートおよび部品標準化のおかげで、代理も滞りなく進めて頂けた。

とは言いつつ、ここまでメルマガを形にするまでに、多くの方のご理解とご協力があったことは間違いない。是松徹主査をはじめとするITSGとメルマガ読者の皆様に感謝しつつ、今後もより一層、効率的作業かつスピード感のある話題提供を心掛けていきたい。

【参考】SAAJ近畿支部メルマガURL: <http://www.saaik.org/?cat=8>

[＜目次＞](#)

第192回 月例研究会 (2014年7月3日開催)

会員番号 1459 武安真児 (情報セキュリティ監査研究会)

【講演テーマ】クラウドサービス利用のための情報セキュリティマネジメントガイドラインの概要及び改訂について

【講師】経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐 上坪健治 氏

特定非営利活動法人 日本セキュリティ監査協会(JASA) 事務局長 永宮直史 氏

【日時】2014年7月3日(木曜日)18:30~20:20

【場所】機械振興会館 地下2階ホール

【講演骨子】:講演者より

本年3月、経済産業省では「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を改訂しました。

新ガイドラインは、JIS Q 27002:2006(ISO/IEC 27002:27005)における実施の手引をベースに、クラウドサービス利用における情報セキュリティ管理の確立、導入、運用、監視、見直し、維持及び改善のために必要な情報を提供するものです。本講演では、新ガイドラインの趣旨と概要を中心に解説するとともに、改訂によって生じた主要な変更点についても紹介します。

【講演概要】

講演は、経済産業省商務情報政策局情報セキュリティ政策室 室長補佐 上坪健治氏により行われました。

I. 情報セキュリティマネジメントガイドラインの概要

経済産業省では、2011年4月に「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」(以下「旧ガイドライン」という。)を作成しましたが、2014年3月に改訂を行い、2013年度版として新たに公表しました(以下「新ガイドライン」という。)

本講演では、新ガイドラインの概要と改訂内容について説明します。

クラウドコンピューティング(以下「クラウド」という。)は、新ガイドラインでは「共有化されたコンピュータリソース(サーバ、ストレージ、アプリケーションなど)について、利用者の要求に応じて適宜、適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態」と定義しています。

また、クラウドは、世界各地にあるコンピュータ群を仮想化等の先端技術で巨大な1つのコンピュータとして扱えるようにしたもので、提供されるリソースにより、SaaS、PaaS、IaaS に分類されます。

新旧ともにクラウドセキュリティガイドラインは、システム環境が従来のオンプレミス環境からクラウドサービス利用へ急速に変化する中で、必要とされる情報セキュリティ分野の規範として、ISO 27001 や ISO 27002 を利用しつつ、クラウドサービスを利用する上で必要な部分に対応させるために、新たに規定したものとして位置づけられます。

クラウドの安全指針策定と国際標準化の流れを見ても、国際規格である ISO/IEC 27002:2005 から日本の規格の JIS Q 27002:2006 が策定され、次に、この JIS Q 27002:2006 をベースに 2011 年 4 月に旧ガイドラインが作成され、さらに、2014 年 3 月に環境変化に対応した改訂版として新ガイドラインが作成されました。

今回、新ガイドラインへの改訂と同時に、「クラウドセキュリティガイドライン活用ガイドブック」(以下「活用ガイドブック」という。)を新たに作成しましたが、この活用ガイドブックでは、具体的な利用シーンに応じたガイドラインの解説を行っています。

また、旧ガイドラインは、ISO/IEC の情報セキュリティに関する専門部会(JTC1/SC27/WG)に提案されていましたが、この専門部会で日本の提案が基礎となったクラウドセキュリティの標準化が行われつつあり、ISO/IEC

27017:2015 として、2015 年に発行される予定になっています。

クラウドを利用する上では、クラウド特有のリスクがあり、そのリスクへの対応が必要となりますが、クラウド事業者と利用者間で情報セキュリティポリシーの不整合が存在し、データ管理のレベルが異なることなどにより、不正なデータ取得によるウイルス感染や、適切なアクセス権の設定不能、また、ライフサイクル管理が困難になるといったリスクが発生します。

さらに、クラウドを利用すると、通常利用者がハードウェアの保有、管理、運用といった自社で行ってきた業務を外注することになるため、物理的なガバナンスの確保が難しくなるとともに、社内にスキルが蓄積出来なくなり、システムの構築・運用・管理に関するリテラシーが低下するという問題が起こります。

これらの利用者の不安を防ぐには、懸念事項は何かをしっかりと分析し、原因に対して管理策を講じることが必要になります。

クラウドを利用する上で発生するリスクを回避するために、クラウド事業者とクラウド利用者がお互いに協力・連携して情報セキュリティ対策を実施し、安全・安心なクラウドサービス利用環境を保証するための枠組みを構築することが必要となります。このようなリスクへの対応が、クラウドセキュリティガイドラインの目的です。

II. 旧ガイドラインの策定

旧ガイドラインの策定では、アンケートを実施して情報セキュリティ対策のニーズの調査を行いました。実施したアンケートの中では、クラウド事業者による情報セキュリティ対策の第三者評価及び情報セキュリティマネジメントシステムの国際基準への適合性評価の要望が多いことが分かりました。

また、クラウドセキュリティガイドライン(初版)が出来た背景としては、クラウドの黎明期の 2008 年からの 3 年間でも多くのインシデントが発生していて、クラウドに対してルールが必要になったこともありました。

そこで、ガイドラインの内容と構成は、JIS Q 27002:2006 の章立てに 1 対 1 に対応させ、クラウド利用者の具体的な対策とクラウド事業者の実施が望まれる事項を分けて記述しました。

具体例をスライド 10 ページにあげていますが、オンプレミスを想定して作成された JIS Q 27002:2006 では、情報システムの「利用」という形態をとるクラウドには、管理策の「実施の手引」をそのまま適用することはできませんので、「クラウド利用者のための実施の手引」、「クラウド事業者の実施が望まれる事項」及び「クラウドサービスの関連事項」の 3 つに分けて記載しています。

III. 新ガイドラインの改訂と活用ガイドブックの作成

新ガイドラインの改訂の理由は、以下のとおりです。

①クラウドを本格的に運用していく過程で、大規模な障害や障害対応過程での情報漏えい等が発生したことにより、リスクが顕在化した。

②事業者の情報開示のあり方を詳細に反映することが必要になった。

③国際的な動向を踏まえることが必要になった。

④抽象的な条文だけでなく、具体的な利用シーンに応じた対策についての解説が欲しいという声があった。

これらの要望等を踏まえ、新ガイドラインと活用ガイドブックを作成しました。

ところで、新ガイドラインとは別に、総務省から「クラウドサービス提供における情報セキュリティ対策ガイドライン～利用者との接点と事業者間連携における実務のポイント～」が今年 4 月に発表されています。何が違うのかよくご質問を受けるので、経済産業省のガイドラインとの違いを説明します。総務省のガイドラインは、クラウド事業者のなかでは SaaS 事業者が多いため、SaaS 提供におけるアプリケーションに関わる領域に特化して、実務の詳細を記述して

いますが、経済産業省のガイドラインは、クラウド利用者と事業者の双方を対象とした内容になっており、SaaS 事業者も含めた汎用性を持っています。

また、「クラウド情報セキュリティ管理基準」が日本セキュリティ監査協会から発表されていますが、こちらは対策技術の実装について、参照する基準が必要になったときに利用するものになっています。

IV. ガイドライン改訂の4つの背景とポイント

ガイドラインの改訂は、前述の4つの背景により行われました。

- (1) 大規模な障害や障害対応過程での情報漏えい等が発生したことによるリスクの顕在化
 - (2) 事業者の情報開示のあり方を詳細に反映することの必要性
 - (3) 国際的な動向を踏まえる必要性
 - (4) 具体的な利用シーンと対策に関する解説の要求
- これらのそれぞれについて説明します。

1. 顕在化したリスクに関する改訂

改訂を行うにあたって、発生した以下のリスクの事例を参考としました。

- ① データ消失を伴う障害の発生(ファーストサーバー事件等)
 - ② 電源系のトラブルに起因する長期間のサービス停止を伴う障害の発生(Amazon、Microsoft、Salesforce.com のサービスの停止等)
 - ③ 容量・能力管理に関する障害の発生(Amazon、Microsoft Azure のサービスの停止等)
- 新ガイドラインは、これらに対応した改訂を行っていて、具体的な変更点は以下のとおりです。
- (1) 情報のバックアップ(簡条 10.5.1)
- バックアップ取得に関する要求事項をさらに明確化しました。
- (2) 事業継続計画の策定・実施(簡条 14.1.3)
- 旧ガイドラインでは、利用者・事業者の基準やシステムの冗長化を図る観点が記述されていなかったため、記述を追加しました。
- (3) 容量・能力の管理(簡条 10.3.1)
- 旧ガイドラインでは、事業者への要求事項や関連情報が規定していなかったため、新たに記述を追加しました。

2. 事業者の情報開示のあり方に関する改訂

事業者の情報開示のあり方については、以下の考え方にに基づき改訂しました。

- a) 利用者への情報提供について事業者自らが方針を定めて利用者に提示し、利用者は提示された方針及び方針に基づき提供された情報によってクラウドサービス利用に係るリスクを評価する。
- b) クラウド事業者は、クラウド利用者との合意に基づき情報を開示する。
- c) クラウド利用者には、クラウド事業者から情報を得た範囲で自らの責任においてリスクアセスメントを行い、対応や対策を決定する責任がある。

具体的な変更点は以下のとおりです。

- (1) 操作手順書(簡条 10.1.1)

クラウド事業者の情報提供に関する方針を定め利用者に提供することを求めるとともに、クラウド利用者が管理をクラウド事業者の外注するからといって丸投げにするのではなく、クラウド事業者の情報提供方針を確認することが

望ましいとしました。

(2) 第三者によるサービスの変更管理(簡条 10.2. 3)

クラウド事業者は、情報セキュリティに影響する可能性がある第三者サービス提供に変更があった場合は、通知の方針を定めて、新たに事例が設けられた通知事項についてクラウド利用者に通知することが望ましいとするとともに、クラウド利用者も変更管理プロセスに基づき必要な対応を実施することが望ましいとしました。

(3) 責任及び手順(簡条 13.2.1)

責任と手順についても改訂が行われ、事業者が情報提供の方針を定めてクラウド利用者に提示することを求めています。

3. 国際的な動向

前述のとおり、クラウドセキュリティガイドラインを国際標準化する作業が行われていますが、2015 年に ISO/IEC 27017 が発行されると、新ガイドラインはそれに合わせて役割を終える予定です。

(1) 分類の指針(簡条 7.2.1)

データの分類項目の例を明確化しました。事業者だけでなく、利用者もきちんと資産に対するチェックを行うことが示されています。クラウドサービスは事業者と利用者が相互に協調することが必要であることの一例です。

(2) モバイルコードの管理策(簡条 10.4.2)

事業者は方針を定め、クラウド利用者に提示し、方針に対する協力を求めるとともに、クラウド利用者も悪意のあるコードに関する事項について、クラウド事業者の情報提供方針を確認することが期待されています。

(3) ネットワーク管理策(簡条 10.6.1)

通信傍受が話題になっていますが、利用者と事業者ともに暗号化やアクセス制御等に注意することを記述しています。

(4) ネットワーク領域分割(簡条 11.4.5)

仮想化を行う場合、ネットワークの仮想環境の分離があいまいであると問題が発生するため、基盤についての管理を利用者も事業者もきちんと行ってほしいということを新規に記述していて、さらに、クラウド利用者からネットワークを分離する機能の使用について、必要に応じて情報を要求するケースについて記述しています。

4. 活用ガイドブックの作成

活用ガイドブックは、以下の 5 部構成になっています。

1. はじめに
2. クラウドセキュリティとは
3. クラウドサービスにおけるリスク
4. クラウド利用者のためのガイドライン活用
5. クラウド事業者のためのガイドライン活用

ガイドブックは、ガイドラインを読む前に読むと、ガイドラインを理解しやすいと思われます。とくに「3. クラウドサービスにおけるリスク」では、クラウドサービスにおける様々なリスクについて解説されていて、これとガイドラインの参考となる項番が対応付けられているため、ガイドラインの重点項目がわかる構成になっています。

また巻末に、付録として契約書等の書式のサンプルを用意しました。実務において有益な内容になっているかと思いますが、ぜひご参照ください。

V. 今後の動向

1. クラウド情報セキュリティ監査制度

クラウドセキュリティをきちんとセキュリティ基準に基づいて行っていることを外部に示して信頼性を向上するために

は、本来外部の専門家の確認を受けることが望ましいことです。しかし、外部の専門家による監査は一般にコストも時間もかかるので内部監査をきちんと行い、さらに当該内部監査について信頼性があることを確認できれば、コストや時間をそれほどかけずに信頼性を向上することができます。この内部監査の信頼性を確認する制度が、クラウドセキュリティ情報監査制度で、予定では今年度中に実施できる見込みです。

2. クラウド情報セキュリティの国際標準化

国際規格である ISO/IEC 27017 の標準化は、2011 年 5 月から行っていて、それと並行して、ISO/IEC 27036-4: 供給者関係の情報セキュリティの標準化に向けた議論も行っています。

また、クラウドセキュリティ監査制度に関する議論や、クラウドリスクの管理フレームワークに関する議論も行っています。

これらは、2014 年 10 月をもって基本的な議論が収束し、骨子が決まる状況であると聞いています。

今後はこれらの周辺の部分についての議論を行い、来年秋ごろに正式な ISO/IEC 27017 のスタートが出来ればという状況になってきています。

VI. 資料

ガイドライン及び活用ガイドブックは、以下のホームページに掲載されています。

- ・新ガイドライン及び活用ガイドブックの原文

<http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html>

- ・旧ガイドラインの原文

<http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html>

VII. 質疑

質疑では、特定非営利活動法人 日本セキュリティ監査協会 (JASA) 事務局長 永宮直史氏と経済産業省商務情報政策局情報セキュリティ政策室 室長補佐 上坪健治氏のお二人に回答していただきました。

最初に、すでに参加者から事前に受け付けた質問について、回答が行われました。

質問1: クラウド利用者が安心してクラウドサービスを利用するために、クラウド事業者が必要な情報を利用者に開示しなければならないが、そのための制度面の方策はありますか？

回答1: クラウド情報セキュリティの認証制度までは話が進んでいませんが、ISO/IEC 27017 が発行されるまでには議論をしなければならないと言われています。事業者が内部監査を行う時の管理基準は作りましたが、監査をして欲しいとの要望がありますので、まず監査制度を立ち上げようとしています。

質問2: クラウドサービスのプライバシー保護に配慮したデータの利活用・流通はどのように考えればよいでしょうか？

回答2: 新ガイドラインは、プライバシー保護については範囲外としています。セキュリティとプライバシー保護には密接な関係がありますが、本来、別のものです。クラウドにおける PII (個人の識別) は、現在並行して ISO/IEC 27018 で検討されていて、これに基づく対策が本来、必要になるものと思われます。

質問3: 従来の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」の利用・適用実績はどれくらいありますか？

回答3:実績については調査をしていません。ただし、情報セキュリティに関心の高い大手の企業では、事業者に対してチェックリストを作成して、履行状況を確認したと聞いています。

質問4:本来、クラウド利用者にとってのクラウドの価値はその利用の手軽さにあると思われませんが、ガイドラインが求めているものは手軽さに反するという批判は無いでしょうか？

回答4:手軽さに反するという批判は無いと思いますが、「厳格に守って下さい」では厳し過ぎると言われることは理解できます。

JASA のホームページに「クラウド情報セキュリティ管理基準」を掲載していますが、この中の「基本言明要件」が、中小事業者が利用できるセキュリティ基準になりますので、管理策の判断基準としてください。

なお一言申し上げておきたいのが、新ガイドラインは、法令ではありませんので、それ自体には罰則はありませんが、会社経営者が負う「善管注意義務」を測る尺度になり得るということです。事業者・利用者いずれの立場でクラウドを利用するにせよ、システムの運用姿勢に問題があり、損害賠償等の問題が発生した場合、会社経営者の過失の判断基準の一つとして新ガイドラインが用いられ得るということをご認識ください。

質問5:「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」で触れられている範囲内でのセキュリティ事故はどのようなものがありましたか？

回答5:新ガイドラインは、利用者側の目線で書かれているので、利用者がどのような事故が起きているかを把握することは難しいと思われます。事業者側から聞いた話では、クラウドの管理者権限の乗っ取りと利用者の安易なサーバの消去がセキュリティ上のリスクになるということです。

質問6:小企業の場合は、自社で情報システムを管理できないためにクラウドサービスを利用するのですが、クラウドを利用する場合、サービス事業者任せにすることができず、利用者自身で実施しなければならない事項があると思われます。何を実施しなければならないかについての一般的な例がありますか？

回答6:クラウドは、それぞれサービスが異なるため、クラウドに一般的なものというのはありません。自社で対応できない場合には、そのサービスを提供してくれる事業者を選定して依頼する必要があります。

質問7:クラウドサービスを利用する場合、監視のためのログ取得とチェックについて、利用者が行わなければならない部分についての基準はありますか？

回答7:クラウドは、サービス内容が事業者によって異なり、同じ事業者でも異なるサービスを提供しているため、基準となるものはありません。自分ができることに合ったクラウド・サービスを選択してください。

質問8:クラウドの事業者やサービスを検討して選択することも、利用者にとっては技術力と工数が必要になると考えられますが、第三者の立場で選択の相談に乗ってくれる機関は無いでしょうか？

回答8:民間の SI 事業者さんがこういったサービスを行っているところがあります。コンサルタントといえばコンサルタントですが、よく分かっているので、心配であればそういうところを利用することも考えられます。

最後に会場から、以下の質問がありました。

質問:いわゆる自称クラウド事業者に関してそのようなあまり信頼できない事業者への対応はどうすればよいでしょう?

回答:そのような自称クラウド事業者を排除できるかは疑問です。クラウドは、もともと設備から出た概念ではなく、サービスから出た概念ですので、「御社はクラウドでは無い」と明確に言うことができません。しかし、透明性は必要で、例えば、日本では食品については食品衛生管理制度があります。おいしいかどうかはわかりませんが食中毒を起こさないことの線引きが明確にできます。今後、クラウドサービスが公共サービスになって行くと考えられますが、最低限の品質を確保するためにも、監査制度を現在、作っています。

質問:クラウド・イン・クラウドの問題で、ユーザからは表に出ているクラウド事業者しか見えないため、その後ろにいるクラウド事業者が見えませんが、利用者から見て安心できないのではないのでしょうか?

回答:クラウド事業者は、後ろのクラウド事業者についても安全性を明確にしなければなりません、それが出来ない場合には、後ろの事業者に問題が起きた場合、その全ての責任を表に出ているクラウド事業者が取する必要があります。

以上

[＜目次＞](#)

【パーソナルデータの利活用に関する制度改正大綱(検討会案)について**－ 情報セキュリティ監査研究会だより No. 17 －】(連載)**

会員番号 0056 藤野明夫(情報セキュリティ監査研究会)

はじめに

情報セキュリティ監査研究会では、アン・カブキアン著、「プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流」をテキスト(以下、左記の書を「テキスト」と称します)として、「プライバシー・バイ・デザイン」の意義、影響、PIAやシステム監査との関係などを、2013年8月から議論しております。

今回は、先ごろ発表されパブリックコメントが募集されました「パーソナルデータの利活用に関する制度改正大綱(検討会案)」について、ご紹介いたします。この大綱は、大きな社会的、ビジネス的、技術的な意義を持つビッグデータの利活用と、それとはトレードオフの関係にある個人情報の保護について、事業者側と個人情報の主体である個人との間で適切な妥協点を見出すため、新たな法制度と施策を打ち出そうというものです。その意味で、従来、トレードオフの関係にあった個人情報の利用と保護の関係を、企業と個人の双方に利益をもたらす関係に転換することを目指すプライバシー・バイ・デザインの考え方と通じるところがあり、連載の途中に挟むことにいたしました。

本報告は、情報セキュリティ監査研究会内部の検討結果であり、日本システム監査人協会の公式の見解ではないことをお断りしておきます。また、我々の力不足のため、誤りも多々あるかと存じます。お気づきの点がございましたら適宜ご指摘いただきたいと思います。ご興味のある方は、毎月20日前後に定例研究会を開催しておりますので是非ご参加ください。参加ご希望の方、また、ご意見やご質問は、下記アドレスまでメールでご連絡ください。

[security ☆ saaj.jp](mailto:security☆saaj.jp) (発信の際には“☆”を“@”に変換してください)

【参考資料等】**<テキスト>**

堀部政男／一般財団法人日本情報経済社会推進協会(JIPDEC、以下、同じ)編、アン・カブキアン著、JIPDEC 訳「プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流」、2012年10月、日経BP社

<資料1> IT総合戦略本部、2014年6月19日了承、「パーソナルデータの利活用に関する制度改正大綱(検討会案)」

http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryoku2.pdf

【報告】「パーソナルデータの利活用に関する制度改正大綱(検討会案)について」

政府のIT総合戦略本部は、6月19日に開催された第12回パーソナルデータに関する検討会で、「パーソナルデータの利活用に関する制度改正大綱(検討会案)」を了承した。これは、制定後、10余年が経過した個人情報保護法を新たに生じた課題に適合させるため、改正しようというものである。以下、資料1に沿って、その趣旨、基本的な枠組み、今後のスケジュールを紹介する。詳細は、資料1をご参照いただきたい。

I 制度改正の趣旨**1. 背景**

今年で個人情報保護法(以下「現行法」という。)の制定から10余年が経過したが、この間の情報通信技術の飛躍的な進展は、いわゆるビッグデータの収集・分析を可能とし、新産業・新サービスの創出や種々の課題の解決に大きく貢献するなど、我が国発のイノベーション創出に寄与するものと期待されている。特に、ビッグデータの中でも個人の行動・状態等に関する情報に代表される、利用価値が高いとされているパーソナルデータについては、最新の高度な情報通信技術を用いることにより、本人の利益のみならず公益のために利活用することが可能となってきた。しかし同時に、自由な利活用が許容されるのかが不明確な「グレーゾーン」が発生・拡大し、パーソナルデータの利活用に当たって、保護すべき情報の範囲や事業者が遵守すべきルールが曖昧になりつつある。

一方、現行法の制定以来、個人情報及びプライバシーという概念が広く認識されるとともに、パーソナルデータの悪用への危惧等により、従来以上の注意を払ったパーソナルデータの取り扱いを望む消費者の声が拡大しつつあり、パーソナルデータが適正に取り扱われることを明らかにし、消費者の安心感を生む制度の構築が望まれている。

これらを背景に事業者もグレーゾーンを意識し、社会的な批判を懸念して、パーソナルデータの利活用を躊躇する「利活用の壁」が出現しており、我が国においてパーソナルデータの利活用を阻む要因になっている。

このような現状に鑑み、データ利活用による産業再興を掲げる政府としても、特に利用価値が高いとされるパーソナルデータについて、「利活用の壁」を取り払い、個人情報及びプライバシーの保護を図りつつ、新産業・新サービスの創出と国民の安全・安心の向上等のための利活用を実現する環境整備を行うことが求められている。

また、OECDのプライバシーガイドラインの改正、米国の消費者プライバシー権利章典の公表、EUの個人データ保護規則案の可決など、関連する諸外国での法整備に配慮し、制度の国際的な調和を図る必要がある。

2. 課題

このような背景から生じる様々な課題は、以下のとおり。

(1) 「利活用の壁」を取り払うために

i) グレーゾーンへの対応

パーソナルデータの「利活用の壁」を生じさせている「グレーゾーン」の要素は、

- ① 「個人情報」の範囲についての法解釈の曖昧さ、
- ② 特定の個人が識別された状態にないパーソナルデータであっても、特定の個人の識別に結びつく蓋然性が高いなど、その取扱いによっては個人の権利利益が侵害されるおそれがあるものに関して、保護される対象及びその取扱いについて事業者が遵守すべきルール

の曖昧さ、である。データ保有の現状や利活用の際の問題を踏まえつつ、これらの曖昧さを解消していく必要がある。

ii) 個人の権利利益の侵害を未然に防止するために

本人が意図しない目的でパーソナルデータが利用されるなどの不安を解消し、消費者が安心してデータを提供できる環境を整備することが重要で、個人の権利利益の侵害に結びつくような事業者の行為を未然に防止することが必要である。

(2) 機動的な対応を可能とするために

技術や意識が時代とともに急速に変化していく中で、それらによって生じるグレーゾーンや個人の権利利益の侵害のおそれの解消を、制定・改正等に厳格な手続を要する法律の規定のみで行っていくことには限界がある。そこで、法律で定めるべき範囲と政省令や規則、ガイドライン等で対応すべき範囲とを適切に分けるとともに、機動的な対応を可能とする上で有益な民間の自主的な取組を補助し促進できるような制度が必要である。

(3) 確実な制度執行を行うために

事業者によるルールの遵守を確保し、消費者の信頼を得るためには、制度執行を行う主体が独立し、公平な立場にあることが求められる。また、前述の民間の自主的な取組を実効性あるものとするためにも、その認定等に関わる公的な機関が必要である。

(4) 制度の国際的な調和のために

企業活動のグローバル化に対応するために、国際的に調和のとれた信頼性のある制度の整備が必要である。

II 制度改正内容の基本的な枠組み

パーソナルデータの利活用促進に向け、課題の解決のためにとるべき法的措置の枠組みは以下のとおりである。

1. 本人の同意がなくてもデータの利活用を可能とする枠組みの導入等

パーソナルデータの利活用により、多種多様かつ膨大なデータを、分野横断的に活用することによって生まれる

イノベーションや、新ビジネスの創出等が期待される。この際、目的外利用や第三者提供に当たって、本人の同意を必要とする現行法の仕組みは、事業者にとって負担が大きく、「利活用の壁」の一つとなっている。そこで、現行法の趣旨を踏まえつつパーソナルデータの利活用を促進するために、現行法に加え新たに一定の規律の下で原則として本人の同意が求められる第三者提供等を本人の同意がなくても行うことを可能とする枠組みを導入する。具体的には、「個人の特定性を低減したデータ」への加工と、本人の同意の代わりとしての取扱いに関する規律を定める。

また、医療情報等のように適切な取扱いが求められつつ、本人の利益・公益に資するために一層の利活用が期待されている情報も多いことから、萎縮効果が発生しないよう、適切な保護と利活用を推進する。

2. 基本的な制度の枠組みとこれを補完する民間の自主的な取組の活用

グレーゾーンの内容や個人の権利利益の侵害の度合いは、技術の進展状況や個人の主観等複数の要素により時代とともに変動するものであり、これらに機動的に対応するため、法律では大枠を定め、具体的な内容は政省令、規則及びガイドライン並びに民間の自主規制ルールにより対応することとする。主な改正事項は以下のとおり。

- ・ 事業者がパーソナルデータの利活用に躊躇しないよう、「個人情報」の範囲を明確化し、個人の権利利益の侵害が生じることのないよう取扱いに関する規律を定める。
- ・ 技術の進展に迅速に対応することができる制度の枠組みとする。
- ・ パーソナルデータの利活用の促進と個人情報及びプライバシーの保護を両立させるため、消費者等も参画するマルチステークホルダープロセスの考え方を活かして、民間団体が業界の特性に応じた具体的な運用ルール(例:個人の特定性を低減したデータへの加工方法)や、法定されていない事項に関する業界独自のルール(例:情報分析によって生じる可能性のある被害への対応策)を策定し、その認定等実効性の確保のために第三者機関が関与する枠組みを創設する。

3. 第三者機関の体制整備等による実効性ある制度執行の確保

法令や民間の自主規制ルールを実効性あるものにするために、以下の独立した第三者機関の体制を整備する。

- ・ 法定事項や民間の自主規制ルールについて実効性ある執行を行うため、国際的な整合性も確保しつつ、第三者機関の体制を整備する。
- ・ 第三者機関については、番号法(注)に規定されている特定個人情報保護委員会を改組し、パーソナルデータの保護及び利活用をバランスよく推進することを目的とする委員会を設置する。
- ・ 第三者機関は、現在個人情報取扱事業者に対して主務大臣が有している機能・権限に加え、立入検査等の機能・権限を有し、民間の自主規制ルールの認定等や、パーソナルデータの国境を越えた移転に関して相手当事国が認めるプライバシー保護水準との適合性を認証する民間団体の認定・監督等を実施する。
- ・ 現行法の本人からの個人情報の開示等の求めについて、請求権に関する規律を定める。

改正に当たっては諸外国の制度や国際社会の現状を踏まえた国際的に調和のとれた制度とすることを目指す。

(注)行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)

Ⅲ 今後のスケジュール

改正法の施行時期等については、制度設計や法案の成立時期により今後変わり得るが、以下を目途とする。

- (1) 平成27年(2015年)1月以降、可能な限り早期に関係法案を国会に提出する。
- (2) 改正法の成立後、可能な限り早期に第三者機関を設置し、業務を開始するとともに、周知及び準備が必要な部分を除き早期に施行する。
- (3) その後、可及的速やかに残りの部分についても施行する。

以上

[＜目次＞](#)

～「経済産業省ガイドライン」の読みこなしポイント～

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」

会員番号 1760 斎藤由紀子（個人情報保護監査研究会）

現在「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（以下、経済産業省ガイドラインと呼ぶ）」の改定に向けて作業が行われています。「個人情報保護監査研究会」では今月号より、現行の「経済産業省ガイドライン」（策定：2004/10/22厚生労働省・経済産業省告示第4号、最終改正：2009/10/09厚生労働省・経済産業省告示第2号）の中で、特に民間事業者が知っておくべき、読みこなしポイントを連載でご紹介します。

なお、これからの記述は、「経済産業省ガイドライン」の本文そのものではありません。事業者が自社に適用する場合は、必ず、以下の経済産業省ガイドライン（2009/10/09 厚生労働省・経済産業省告示第2号）を参照してください。

http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

「経済産業省ガイドライン」（2009/10/09改定版） 目次（本号内容）

1. 目的及び適用範囲	1
2. 法令解釈指針・事例	2
2-1. 定義（法第2条関連）（2-1-1～2-1-13の目次省略）	2
2-2. 個人情報取扱事業者の義務等	14
2-2-1. 個人情報の利用目的関係（法第15条～第16条関連）	14
2-2-2. 個人情報の取得関係（法第17条～第18条関連）	20
2-2-3. 個人データの管理（法第19条～第22条関連）	24
2-2-3-1. データ内容の正確性の確保（法第19条関連）	24
2-2-3-2. 安全管理措置（法第20条関連）	25
2-2-3-3. 従業員の監督（法第21条関連）	37
2-2-3-4. 委託先の監督（法第22条関連）	38
2-2-4. 第三者への提供（法第23条関連）	40
2-2-5. 保有個人データに関する事項の公表、保有個人データの開示・訂正・利用停止等 （法第24条～第30条関連）（2-2-5-1～2-2-5-7の目次省略）	47
2-2-6. 苦情の処理（法第31条関連）	58
2-2-7. 経過措置（法付則第2条～第5条関連）	59
2-3. 民間団体付属の研究機関等における個人情報の取扱いについて	60
3. 「勧告」、「命令」及び「緊急命令」についての考え方	60
4. ガイドラインの見直し	62
5. 個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格	65
別添 クレジットカード情報を含む個人情報の取扱いについて	65

——目次以上——

1. 目的及び適用範囲

「経済産業省ガイドライン」は、経済産業省が所管する分野における事業者等が、個人情報の適正な取扱いの確保のため、具体的な指針として定めたものです。「[個人情報の保護に関する法律](#)」施行後、いち早く告示されたのが「経済産業省ガイドライン」で、その後各省庁のガイドライン策定のベースともなりました。

経済産業省が所管する分野における事業者であっても、従業員の個人情報(雇用管理に関するもの)については、※1「[雇用管理における個人情報保護に関するガイドライン](#)」(2012/5/14厚生労働省告示357号)や、※2「[雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について](#)」(2012/6/11告示)との整合性に留意する必要があります。

※1、2: 個人情報保護監査研究会の追記。現行の「経済産業省ガイドライン」では旧版を記載している。

各省のガイドラインにおいて共通して言えることですが、「しなければならない」としている規定については、それに従わなかった場合は、主務大臣(ここでは経済産業大臣)により、法の規定違反と判断されることがあります。一方、「望ましい」と記載されている規定については、法の規定違反と判断されることはないとしています。

2. 法令解釈指針・事例

2-1. 定義(法第2条関連)

※個人情報保護監査研究会注:ここからは、できる限りポイントを絞って記述します。不明な点は本文を参照してください。http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

2-1-1. 「個人情報」

「[個人情報の保護に関する法律](#)」では、「個人情報」とは“生存する個人に関する情報”と限定していますが、「[経済産業省ガイドライン](#)」では、“死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。”としています。なお、外国人も含まれることについても明記しています。

※個人情報保護監査研究会注:法律がゆるく、「経済産業省ガイドライン」が厳しいではありません。

法律は、個人情報を、生存する個人(=人間)の権利として捉えているからで、「経済産業省ガイドライン」では補足として、死者に関する情報を一律に排除しているのではないことを説明しています。

【個人情報に該当する事例】として、本人の氏名、生年月日等に加えて、会社における職位・所属、防犯カメラの映像等についても挙げています。

2-1-2. 「個人情報データベース等」(法第2条第2項関連)

「個人情報データベース等」とは、コンピュータを用いるかどうかを問わず、一定の規則(例えば50音順)に従って整理・分類した状態のものを言います。

【個人情報データベース等に該当しない事例】として、“アンケートの戻りはがきが、氏名、住所等により分類・整理されていない状態”を挙げています。

※個人情報保護監査研究会注:分類・整理されていなくても、「個人情報」にあたりますので、安全管理措置が必要です。

2-1-3. 「個人情報取扱事業者」（法第2条第3項関連）

「[個人情報の保護に関する法律施行令](#)」第2条では、個人情報取扱事業者から除外される者として、“事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数(略)の合計が過去6月以内のいずれの日においても5000を超えない者とする。”

と定めていますが、「経済産業省ガイドライン」では、上記に該当しない事業者等についても、“このガイドラインに規定されている事項を遵守することが望ましい。”としています。

※個人情報保護監査研究会注:JIS Q15001:2006(個人情報保護にマネジメントシステム—要求事項)では、期間、件数の定めはありません。一時的に取得した場合、1件でも安全管理措置の対象とします。

件数の数え方としては、“同一個人の重複は除く”としています。例えば従業者や顧客の個人情報は、できる限り「人数」を件数として把握することが適切です。

【特定の個人の数に算入しない事例】として、電話帳やカーナビゲーションなど他人が作成し、不特定多数の者が利用できる状況で、かつ編集・加工しないで利用する場合は、件数に算入しないよいとしています。

【事業の用に供しないため特定の個人の数に算入しない事例】として、倉庫業、データセンター等の事業者が、受託している情報が個人情報かどうかを認識しない場合を挙げています。

2-1-4. 「個人データ」（法第2条第4項関連）

「個人情報データベース等」を構成する個人情報を指し、利用するデータベースの他に、バックアップデータ、出力された紙情報も含まれます。

2-1-5. 「保有個人データ」（法第2条第5項関連）

JIS Q15001:2006(個人情報保護にマネジメントシステム—要求事項)における、「開示対象個人情報」と同じ概念です。個人情報取扱事業者が、本人(又はその代理人)から、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止(以後、開示等という)に応じることができる権限を持っている「個人データ」を言います。受託業務においては、委託元に開示等の権限があり、委託先にはその権限はありません。

「その存否が明らかになることにより、公益その他の利益が害されるもの」については、「保有個人データ」ではないとされています。そのため、本人から開示等の請求があっても、請求に応じる必要はありません。2000年以降、各虐待防止法(児童、配偶者、高齢者、障害者)の施行により、家族であっても本人の委任が明確でない限り、安易に開示しないように注意する必要があります。他にも、企業が不当要求被害を防止するために保有している、総会屋や、悪質なクレマー情報、防衛に関連する機器やソフトウェアの開発担当者情報、要人の行動予定や記録等についても、安易に開示してはならないとしています。

また警察等から、捜査のためとして、本人の同意を得ずに「保有個人データ」の提供を求められる場合があります。これは「その個人データの存否が明らかになることで、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの。」として協力を依頼するものです。その際には、「捜査関係事項照会依頼書」をもらい、提供する理由を明らかにします。

2-1-6. 「本人」（法第2条第6項関連）

「本人」とは、個人情報によって識別される特定の個人をいい、「[個人情報の保護に関する法律](#)」の通りです。

2-1-7. 「本人に通知」

「本人に通知」とは、本人に直接知らしめることをいいます。

【本人への通知に該当する事例】は以下の通りです。

- 事例1) 面談において、口頭又はちらし等の文書を渡す。
- 事例2) 電話において、口頭又は自動応答装置等で知らせる。
- 事例3) 隔地者間において、電子メール、ファックス、郵便等で送付する。
- 事例4) 電話勧誘販売において、口頭の方法による。
- 事例5) 電子商取引において、自動応答の電子メールにて送信する。

※個人情報保護監査研究会注:通知を口頭で行う場合は、伝える内容を手順書、業務フローなどによって文書化しておくことが重要です。

2-1-8. 「公表」

「公表」とは、広く一般に自己の意思を知らせることをいいます。

【公表に該当する事例】は以下の通りです。

- 事例1) 自社のウェブのトップページから1回程度の操作で到達できる場所への掲載
自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備置き・配布等
- 事例2) 店舗販売において、店舗の見やすい場所への掲示
- 事例3) 通信販売において、通信販売用のパンフレット等への記載

2-1-9. 「本人に対し、その利用目的を明示」

本人に対し、その利用目的を明確に示すことをいいます。

【利用目的の明示に該当する事例】は以下の通りです。

- 事例1) 利用目的を明記した契約書等の書面を本人に手渡し、又は 送付する。
- 事例2) ネットワーク上において、自社のウェブ画面上にその利用目的を明記します。その際には、送信ボタンをクリックする前に本人の目にとまるよう配置に留意します。(利用目的の画面に、1回程度の操作で遷移するリンクやボタンを含む。)

2-1-10. 「本人の同意」

「本人の同意」とは、本人(本人確認が前提)の意思表示とともに、その意思表示を個人情報取扱事業者が認識することをいいます。

【本人の同意を得ている事例】

- 事例1) 本人から、同意する旨を口頭又は書面で確認する。
- 事例2) 本人が署名又は記名押印した同意する旨の申込書等文書を受領し確認する。
- 事例3) 本人から、同意する旨のメールを受信する。
- 事例4) 本人による、同意する旨の確認欄へのチェック
- 事例5) 本人による、同意する旨のウェブ画面上のボタンのクリック
- 事例6) 本人による、同意する旨の音声入力、タッチ、ボタンやスイッチ等による入力

※個人情報保護監査研究会注:同意を口頭で得た場合は、録音や応答記録簿などに残すことが重要です。なお口頭同意の記録、書面による同意を問わず、記録には日付が必須です。

2-1-11. 「本人が容易に知り得る状態」

「本人が容易に知り得る状態」とは、本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いていることをいいます。

【本人が容易に知り得る状態に該当する事例】は以下が継続的に行われている状態を指します。

事例1) ウェブ画面中のトップページから1回程度の操作で到達できる場所への掲載

事例2) 事務所の窓口等への掲示、備付け

事例3) 広く頒布されている定期刊行物への掲載

事例4) 電子商取引において、商品を紹介するウェブ画面にリンク先を掲示

※個人情報保護監査研究会注: 事業で取り扱う個人情報の利用目的は、容易に知り得る状態に置いておく必要があります。

2-1-12. 「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」

これは、本人が知ろうとすれば、知ることができる状態に置くことをいいます。

【本人の知り得る状態に該当する事例】は以下の通りです。

事例1) 問い合わせ窓口を設け、口頭又は文章で回答できるよう体制を構築しておく。

事例2) 店舗販売において、店舗にパンフレットを備え置く。

事例3) 電子商取引において、問い合わせ先のメールアドレスを明記する。

※個人情報保護監査研究会注: 遅滞なくとは、ワンクッションにおいて対応する程度を指します。

開示請求が少ない事業者は、開示請求書をダウンロードできる状態にしていなくても、郵送、メール添付ファイルなどの手段で遅滞なく本人に送付すればよいでしょう。

2-1-13. 「提供」

「提供」とは、個人データを利用可能な状態に置くことをいいます。

※個人情報保護監査研究会注: 一般的に「提供」とは、**本人、当該事業者以外**が個人データを利用可能な状態に置くことをいいます。例えば、従業員の顔写真、プロフィールをホームページ上で公開することは提供にあたり、本人の同意が必要です。

提供には、i) 委託、ii) 事業の承継、iii) 共同利用、及び第三者提供がありますが、狭義の提供については、2-2-4. 第三者への提供(法第23条関連)で詳しく述べられています。

次回は、「2-2. 個人情報取扱事業者の義務等」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://www.saaj.jp/saajpmsMETIGL/000METIGL.html>

今回の読みこなしポイントの部分は、「経済産業省ガイドライン」の改定案の対象となっていないませんでした。改定案では、2-2-3-2. 安全管理(法第20条関連)から対象としており、この部分の読みこなしポイントは、会報2014年12月号を予定しています。

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

[＜目次＞](#)

支部報告 【 近畿支部 第147回定例研究会 】

会員番号 169 林 裕正 (近畿支部)

1. テーマ 暗号通貨ビットコインの脆弱性と可能性
2. 講師 京都聖母女学院短期大学 生活科学科 准教授
荒牧総合研究所代表 中小企業診断士 荒牧 裕一氏
3. 開催日時 2014年7月18日(金) 18:30~20:30
4. 開催場所 大阪大学中之島センター 講義室301

**5. 講演概要**

講師は、近畿支部の会員であり、近畿支部において「ソフトウェア著作権研究プロジェクト」の主査を務めておられます。今回は、最近非常に話題となっている「ビットコイン」について、講師ご自身の経験を踏まえ、暗号通貨の脆弱性と今後の可能性についてお話しいただきました、講師による講演の概要は以下の通りです。

「暗号通貨(仮想通貨)ビットコインは、2月下旬に大手取引所「マウントゴックス」の倒産を機に社会問題となりました。しかし、その後も海外での取引は活発に行われています。今回、私自身のビットコインの取引・運用経験を踏まえて、ビットコインの仕組み、脆弱性、ビジネスや投資対象としての可能性等についてお話しします。」

(1) ビットコインの概要

- ・ビットコインは、暗号技術に応用した仮想通貨であり、2009年に「中本哲史」と名乗る人物が考案した内容を元にビットコイン財団が関連プログラムを開発し、公開している。
- ・発行上限は約2100BTCであり、最初の4年でその半分、次の4年で4分の1を発行する。
- ・新規発行は、「採掘(マイニング)」と呼ばれる方法で行われる。
- ・小数点以下8桁まで細分化が可能である。
- ・現在、類似の通貨が多数(数百種)登場している。

(2) ビットコインの仕組み

- ・ビットコインそのもののデータは存在せず、デジタル署名を使ったデータだけを管理する。
- ・デジタル署名を使うことにより、正当な権利者からの譲渡であることは保証される。
- ・デジタル署名はコピー可能であるため、二重譲渡は防げない。そのため、「ブロックチェーン」と呼ばれる独自の登録システムにより二重譲渡を監視する仕組みを取っている。
- ・ビットコインを送信には、公開鍵を一部加工してアドレスとして使用する。取引データをブロードキャスト送信し、その取引データがブロックチェーンに登録されることで、正当性を公示する。
- ・送金手数料は自由であるが、高額の方が優先処理される。(0.0001BTC以上が目安)

- ・ビットコインの採掘(マイニング)とは、ブロックチェーンに追加するために必要なキーを計算で見つける作業である。
- ・マイニングのソフトは公開されているので、それをダウンロードして採掘するが、大きな計算パワーを必要とする。
- ・マイニングを集団で行い、成功した場合は仕事量に応じて成果を配分する「マイニングプール」も現れており、個人が比較的小さな計算パワーで参加しても、ビットコインを取得できるようになった。

(3) ビットコインの可能性

- ・投資対象としての魅力がある。相場変動は激しく、マイニングの利回りは3～7%/週。2週間毎に大きく低下。
- ・決済手段として、特に海外への少額送金では手数料が安いと、魅力がある。
- ・寄付や、ネットショップのポイントとして利用できる可能性がある。
- ・将来的には、データの所有権の公示手段として利用できる可能性がある。

(4) ビットコインの危険性

- ・秘密鍵の漏洩や破壊により、利用できなくなる危険がある。
- ・「トランザクション展性(transaction malleability)」と呼ばれる脆弱性がある。マウントゴックスの経営破綻の原因は、本脆弱性を突かれたものであると言われている。
- ・マイニングは、合意形成のプロセスであるため、マイニングに参加する計算パワーの過半数が悪意を持った操作をすれば、正当なプロセスが保証できなくなる可能性がある。(51%アタックと呼ばれる)
- ・サイバー攻撃、不正アクセス、ウィルス被害等の可能性がある。

(5) ビットコインの利用体験

- ・今年からビットコインを利用し始めたが、マウントゴックスについては、申請中であつたため、実損は無かつた。
- ・交換サイトへの不正アクセスで保有するBTCを全額引き出されたが、運用側が不正アクセスによる被害と認めたため、被害額は全額補填された。
- ・その他、売買時の操作ミスは多数、経験した。

6. 所感

マウントゴックス社の経営破綻を契機に暗号通貨についての話題が盛んになり、関係する書籍もいくつかが発刊されました。私もいくつか購読しましたが、自分で実際にビットコインを利用していないため、実際にどのようなものかが十分に理解できませんでした。今回、ご自身でビットコインの取引を行っておられる荒牧先生より、ビットコインの仕組み、脆弱性、今後の可能性についてご講演頂き、理解を深めることが出来ました。暗号通貨の今後については、法規制の整備等まだ不透明と言えるかも知れませんが、同種の暗号通貨が多数開発されていることを考えると、いろいろな課題を解決しながら発展していく可能性は大きいと感じました。今後もインターネットの利活用分野が拡大すると思われますので、インターネットでの利用を前提とした暗号通貨が、国家通貨を補完する形で発展することは十分予想されます。システム監査人としても今後の動向に注目していくべきと考えます。

[本報告作成に際し、下記の書籍を参考に致しました]

- ・斉藤賢爾著 『これでわかったビットコイン』(太郎次郎社エディタス)
- ・吉本佳生・西田宗千住著 『暗号が通貨になる「ビットコイン」のからくり』(講談社 ブルーバックス)

以上

[＜目次＞](#)

支部報告 【 システム監査体験セミナー（入門編） 】

会員番号 1790 吉谷尚雄（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 2014年6月28日（土） 10時～17時
3. 開催場所 大阪大学中之島センター 608号室

**4. 開催概要**

近畿支部では、2014年6月28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。10時から17時までの1日コースで、スーパーマーケットに対するシステム監査のケーススタディを主な内容として、11名の方にご参加いただきました。コースの概要は以下の通りです。

(1) 講義 & チェックリスト作成

最初にセミナーの説明やスタッフ及び受講者の自己紹介を行った後、「システム監査概要」の講義を行いました。その後、本日のケーススタディで学習する内容を監査手順に従って説明し、受講者を2チームに分けて、インタビュー項目の洗い出しを行い、チェックリストをまとめていただきました。

(2) インタビュー & 監査報告書作成 & 監査報告会

午後からは、作成したチェックリストを用いて、店舗営業部とシステム課に対するインタビューを体験していただきました。インタビュー後は監査結果を監査報告書にまとめ、監査依頼者にあたる監査室長以下の被監査組織に対してチーム単位で監査報告していただきました。本セミナーではチェックリスト作成から、監査報告会までをロールプレイで体験いただきましたが、いずれの監査チームとも、監査室長以下からの質問に対して適切に回答されていました。

(3) 監査エピソード

ケーススタディ以外にセミナースタッフの監査経験を基にしたエピソードを紹介しました。1回目は、「プロジェクト監査考察」というテーマで、システム開発や運用フェーズを監査する項目は「システム管理基準」に規定されており、その他、ISO21500（プロジェクト管理）・ISO20000（ITサービス）など、プロセスを確認する規格が存在することを紹介しました。これらを考慮しながら、現実のプロジェクトの運営状況を点検する方法について考察しました。2回目は、「機密書類の廃棄」というテーマで、電子媒体の削除は比較的厳密に管理されているが、紙媒体については不用意に裏紙使用されているリスクが散見されることを説明しました。企業

内でシュレッダー処理する人が多いが、多量の場合は廃棄物として処理される場合が多く、その場合は機密書類の破棄として業者選定に注意が必要なことについて話しました。短い時間ですが、受講者にとっては、今後監査に何らかの関与する際に、有益な内容であったと思います。

5. 受講者の皆様の感想

受講された皆様からは、以下のようなお声をいただきました。

- ・具体例でのシミュレーションは役に立ったと思います。参考になりました。ディスカッションはいろんな方の意見が聞けて楽しかったです。
 - ・ヒアリング以外の監査手続きについても触れてみたい。ロールプレイングの担当者とのやりとりは新鮮。報告会も質疑応答もあり、これまで受講したことがなく新鮮だった。
 - ・教材が非常によく練られた内容で受講生のレベルを問わず学びを得られる深い内容でした。座学だけでなく、他受講生仲間とのワークを通じた体験は自分でこなせている点、未熟な点がはっきりし、役立つものでした。
 - ・具体的な事例で、事前に資料配付があったので、ある程度考えておくことができ、よかったです。これがないと、1日で意見を出し、まとめるのは難しかったと思います。エピソードなど、コーヒープレイク的なお話もあり、楽しく有意義な時間を過ごすことができたと思います。期待以上だったと思います。
- また、上記の他、「考える時間がもっと欲しい」「ヒアリング以外の監査手続きについても学習したい」など、今後の参考となるご意見も頂戴しています。

6. 感想

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、経験者の方が参加されましたが、全体としてシステム監査を体験するうえで有益であったとの感想を多くいただきました。また、セミナー研修時間が短いのご意見や、スタッフの研修生に対する気配りが改善点のご意見もいただき、これらを参考に今後とも、より良いセミナーが提供できるよう努力していきたいと考えています。



以上

[＜目次＞](#)

注目情報 (2014. 07～2014. 08) ※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。

■経済産業省「経済団体に対して個人情報保護法等の遵守に関する周知徹底を要請しました」の公表

(ニュース・リリース 2014 年 8 月 18 日)

経済産業省は、今般、教育関係事業者において極めて多数の個人情報が漏えいするという事案が発生したことを踏まえ、本日、経済団体(日本経済団体連合会、新経済連盟、日本商工会議所、全国商工会連合会、全国中小企業団体中央会)に対し、個人情報保護法等の遵守に関する周知徹底を行うよう、経済産業大臣名による要請文書を発出しました。

個人情報とは、個人の人格尊重の理念の下に慎重に取り扱われるべきものであり、個人情報保護法に基づき、個人情報を取り扱うすべての事業者にとっての極めて重要な義務として、その適正な取扱いが求められています。今般、教育関係事業者において、極めて多数の個人情報が漏えいするという事案が発生し、多くの保護者や国民が不安を感じています。

このため、経済産業大臣名により、本日付で、日本経済団体連合会、新経済連盟、日本商工会議所、全国商工会連合会及び全国中小企業団体中央会の計 5 団体に対し、別紙のとおり個人情報保護法等の遵守に関する周知徹底について要請しました。

具体的には、要請文書において、団体所属の会員各社に対し、①社内の安全管理措置、②委託先及びその先に関与する事業者の監督、③外部からの適正な個人情報の取得、を含めた個人情報保護法等の遵守について、現場担当者にとどまらず、社内全体、委託先事業者等に、周知徹底を図っていただくよう要請しました。

■IPA情報「プレス発表:注意喚起「ウェブサイトの改ざん回避のために早急な対策を」

IPA(独立行政法人情報処理推進機構、理事長:藤江 一正)および JPCERT/CC(一般社団法人 JPCERT コーディネーションセンター、代表理事:歌代 和正)は、ウェブサイト改ざんのインシデント報告が後を絶たないことを受け、ウェブサイト運営者および管理者に対し、改めて点検と備えを呼びかけます。

【概要】:

JPCERT/CC によれば、2014 年 1 月～6 月の期間に報告を受けたウェブサイト改ざんは 2,624 件(*1)でした。前期(2013 年 7 月～12 月)の総件数は 4,378 件(*2)であり、件数そのものは減ってきているものの、依然として月平均 400 件程度の改ざんの報告が続いています。7 月も 388 件の改ざんがあり、この件数は実際改ざんされているウェブサイトの氷山の一角と考えられます。

詳細は、<http://www.ipa.go.jp/about/press/20140813.html> で



[＜目次＞](#)

2014.08

【 協会主催イベント・セミナーのご案内 】

■月例研究会（東京）

第195回	日時:2014年9月18日(木)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	「首都直下地震の被害想定の警告 ～情報システムのバックアップは本当に機能するか～」(仮題)
	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	2013年末に公表された政府の首都直下地震の被害想定は東日本大震災を踏まえて前回2005年に公表された想定を大きく変えている。しかしながらその被害想定の内容はあまり認識されていない。本セミナーでは今回公表された被害想定を解説し、企業はどのように対応すればよいのかについて提言する。このように書くこととありふれた内容に思われるかもしれないが、政府は首都直下地震につきかなり踏み込んだ被害想定を行ったことを理解していただきたい。政府は今回はじめて具体的なライフラインの途絶時間を公表した。その内容をみると情報システムの稼働に大きな影響を与える電力の被害想定が大幅に悪化したことがわかる。また通勤困難、飲食料入手困難さらに非常用発電機に不可欠な燃料の調達困難などがあり、これらを含め政府は過酷事象も想定外としないように求めている。それを踏まえると首都圏における経済活動が困難であり、企業はこれらを正しく踏まえたBCPを構築することが必要である。
	お申し込み	次のサイトでご案内しています。 http://www.saaj.or.jp/kenkyu/kenkyukai195.html

第196回	日時:2014年10月30日(木)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	「オープンデータを中心にIT政策の動向全般」(仮題)
	講師	経済産業省 CIO補佐官 平本健二氏
	講演骨子	10月号で掲載。
	お申し込み	速報、HPでご案内しています。 http://www.saaj.or.jp/kenkyu/kenkyukai_sokuhou201410.html

■中堅企業向け「6ヶ月で構築するPMS」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、様式を用いて、6ヶ月でPMSを構築するためのセミナーを開催します。 詳細をHPでご案内しています。(http://www.saaj.or.jp/shibu/kojin.html)
	基本コース	月1回(第3水曜日)14時~17時(3時間)×6ヶ月 ※他に、月2回の応用コースなどがあります。
	料金	9万円/1名~(1社3名以上割引あり)
	会場	日本システム監査人協会 本部会議室(茅場町)
	テキスト	SAAJ「個人情報保護マネジメントシステム実施ハンドブック」(非売品)

■公認システム監査人特別認定講習の実施(東京・大阪)

申し込み受付中	◎システム監査に関する知識コース(2日コース) 2014年9月14日～15日 ◎論文およびプレゼンテーションコース(1日コース)2014年9月3日
	概要 本講習は、SAAJが認定した特別認定講習実施機関が、CISA、ITコーディネータ、情報セキュリティスペシャリスト、プロジェクトマネージャ等の資格取得者に対し、SAAJの定めるカリキュラムに基づき講習を実施するものです。講習を修了した場合には、「公認システム監査人」、「システム監査人補」の申請の資格要件が得られます。
お申し込み	講習開催スケジュールと申し込み先をHPでご案内しています。 (http://www.saa-j.or.jp/csa/tokubetsu_nintei.html)

■システム監査普及サービス(全国)

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

【 外部のイベント・セミナーのご案内(会報担当収集分) 】

■情報システム・ユーザー会連盟(FISA)

第35回監査講演会のご案内	
日時	2014年10月21日(火) 10:20～17:00
場所	きゅりあん(品川区立総合区民会館／東京・大井町)
テーマ	『情報セキュリティとシステム監査』
概要	サイバーテロ対策や情報漏えいへの対応など各企業のセキュリティは一層重要となっており、システム監査の実施に際しても従来以上に厳格な対応が求められています。そこで本年度は「情報セキュリティとシステム監査」をテーマに、プログラムを企画いたしました。 現在検討されている情報セキュリティの国家資格を含むセキュリティ政策や、システム開発における情報セキュリティ関連の法的課題とシステム監査に関する講演、現場で実務に携わる方々をお招きしてのパネルディスカッションなど多岐にわたる内容となっております。 (詳細は下記 URL より案内状をご参照下さい。)
内容等	申込方法等の詳細はHPで紹介されています https://www.it-user.hitachi.co.jp/pdf/H26syskanannai.pdf

[＜目次＞](#)



新たに会員になられた方々へ

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。

先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

ご確認ください

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

特典

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

ぜひ参加を

- ・各支部・各部会・各研究会等の活動です。 <http://www.saaaj.or.jp/shibu/index.html>
皆様の積極的なご参加をお待ちしております。門戸は広く、見学也大歓迎です。

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.saaaj.or.jp/shuppan/index.html>
システム監査の現場などで広く用いられています。

セミナー

- ・セミナー等のお知らせです。 <http://www.saaaj.or.jp/kenkyu/index.html>
例えば月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。

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.saaaj.or.jp/csa/index.html>

会報

- ・PDF会報と電子版会報があります。 (http://www.saaaj.or.jp/members/kaihou_dl.html)
電子版では記事への意見、感想、コメントを投稿できます。
会報利用方法もご案内しています。 <http://www.saaaj.or.jp/members/kaihouinfo.pdf>

お問い合わせ

- ・右ページをご覧ください。 <http://www.saaaj.or.jp/toiawase/index.html>
各サイトに連絡先がある場合はそちらでも問い合わせができます。

[＜目次＞](#)

2014.08

【 S A A J 協会行事一覧 】			
2014 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
1 月	9 日 理事会:通常総会議案審議 10 日 総会開催案内掲示・メール配信 10 日 役員改選公示 15 日 事務局:総会資料(※) 20 日 会計:2013 年度決算案 25 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 認定委員会:春期公認システム監 査人募集 案内 〔申請期間 2/1～ 3/31〕	11 日 会計:支部会計報告期限 17 日 近畿支部:支部総会
2 月	6 日 理事会:通常総会議案承認 21 日 通常総会・特別講演	CSA・ASA 春期募集(2/1～3/31) 1-2 日 事例研:第 23 回システム監査実 務セミナー(前半)、22-23 日(後半) 5 日 CSA フォーラム 10 日 第 189 回月例研究会	
3 月	1 日 事務局:法務局登記、 東京都への事業報告、変更届提出	1 日 第 13 回課題解決セミナー 25 日 CSA フォーラム	
4 月	1 日 認定 NPO 法人申請準備開始	認定委員会:新規 CSA/ASA 書類審査 25 日 第 190 回月例研究会	20 日 2014 年春期情報技術者試 験(9:30～16:30)
5 月	8 日 理事会 29 日 会費未納督促メール	認定委員会:新規 CSA/ASA 面接 15-16 日 事例研:第 26 回システム監査 実践セミナー 22 日 第 191 回月例研究会	
6 月	12 日 理事会 末日 支部会計報告依頼(※切 7/14) 末日 助成金配賦額決定(支部別会員数)	7 日 事例研:第 14 回課題解決セミナー 10 日 新規 CSA/ASA 承認 10 日 CSA フォーラム	28 日 近畿支部:システム監査 体験セミナー(入門編):
7 月	1 日 会費未納者督促状発送 8 日 支部助成金支給 10 日 理事会	1 日 秋期公認システム監査人募集案内 〔申請期間 8/1～9/30〕 3 日 第 192 回月例研究会 22 日 第 193 回月例研究会	14 日 支部会計報告※切
8 月	(理事会休会) 会費督促電話作業(役員) 23 日 中間期会計監査	秋期公認システム監査人募集開始～9/30 20 日 第 194 回月例研究会 30-31 日 事例研:第 24 回システム監査 実務セミナー(前半)	30～31 日 東北支部:合宿研修会 30～31 日 近畿支部:システム監 査体験セミナー(実践編)
9 月	11 日 理事会	13-14 日 事例研:第 24 回システム監査 実務セミナー(後半) 8 日 第 24 回 CSA フォーラム 18 日 第 195 回月例研究会	6～7 日 中部、北信越支部 /JISTA 中部合同合宿
10 月	9 日 理事会	30 日 第 196 回月例研究会	25 日 近畿支部:IT-BCP 体験セミナー
11 月	13 日 理事会 13 日 予算申請提出依頼(11/30※切) 20 日 会費未納者除名予告通知発送 30 日 予算申請提出期限 30 日 2015 年度年会費請求書発送準備	中旬 認定委員会:CSA 面接 20 日 CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 28 日 認定委員会:CSA 面接結果通知	29 日 西日本支部合同研究会 (開催場所:大阪市)
12 月	1 日 2015 年度年会費請求書発送 2015 年度予算案策定 11 日 理事会:2015 年度予算案、 会費未納者除名承認 12 日 支部会計報告依頼(1/9※切) 第 14 期総会資料提出依頼(1/9※切) 19 日 会計:2014 年度経費提出期限	10 日 認定委員会:CSA/ASA 更新手続 案内メール発信 20 日 CSA 認定証発送	

※注 定例行事予定の一部は省略。

[＜目次＞](#)

会報編集部からのお知らせ

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

□■ 1. 会報テーマについて

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

これまで2月号から4月号までが「公(おおよけ)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」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。

8月号から10月号までの3か月は、「次世代のためのシステム監査」をテーマとすることとしました。次世代に向けてのシステム監査について、皆様からの幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマもちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

- 1)PDF ファイルの全体を、URL (<http://www.skansanin.com/saaj/>)へアクセスして、画面で見る
- 2)PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
- 3)会報 URL (<http://www.skansanin.com/saaj/>)の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボタンをクリックするだけです。動画でも紹介しますので、参考にしてください。

(<http://www.skansanin.com/saaj/> の記事、「コメントを投稿される方へ」)

□■ 3. 会員の皆様からの投稿を募集しております。

分類は次の通りです。

1. めだか (Word の投稿用テンプレート(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (論文投稿規程があります)

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。システム監査にとどまらず、情報社会の健全な発展を応援できるような内容であれば歓迎します。ただし、投稿された記事については、表現の訂正や削除を求め、又は採用しないことがあります。また、編集担当の判断で字体やレイアウトなどの変更をさせていただくことがあります。

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/>

Copyright(C)2014、NPO 法人 日本システム監査人協会

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

■□■SAAJ会報担当

編集委員: 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、中山孝明、藤野明夫

編集支援: 仲厚吉 (会長)

投稿用アドレス: saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)

[＜目次＞](#)