認定 NPO 法人
日本システム監査人協会報
2015 年 8 月号
No 173
No. 173（2015 年 8 月号）＜7 月 25 日発行＞

＜不審メールに注意 ＞

ウイルス感染を目的とした添付ファイルが付いているかも

安易に不審メールを開かないよう注意しましょう。！

写真提供：仲会長

巻頭言

『 制御システムおけるセキュリティ動向 』

会員番号:1750 舘岡均(副会長)

最近は国内外にて、標的型サイバー攻撃による甚大な被害が頻繁に発生し、大きな脅威となっています。このような業務システムにおけるセキュリティ脅威の他に、制御システムにおけるセキュリティ脅威も注目されています。

社会・産業基盤を支える産業用の制御システムは、エネルギー分野（電力、ガス等）や石油・化学、鉄鋼業等におけるプラントや機械・食品等の生産・加工ラインなどにおけるシステムであり、従来はセキュリティ強固な固有のシステムで構成されてきました。

しかし、業務システムにおいて圧倒的な規模で普及した PC やサーバ、ネットワークの利便性、コストメリット、知識・技術共有のメリット、等々から、制御システムにおいてもその汎用技術が活用され、その結果、セキュリティの脆弱性をも引継いでしまいました。社会・産業基盤のシステムがサイバー攻撃を受けた場合には、社会にとって健康、安全、環境をも脅かす甚大な被害となることから、急務の課題となり、官民あげて対策の準備が進められ、2014 年 4 月に CSMS（Cyber Security Management System for IACS（Industrial Automation and Control System））、制御システムに関するセキュリティマネジメントシステム認証制度が発足しました。

システム監査においては、セキュリティについての視点も重要な一つとなっており、より範囲を広げて関心を持ち、技術向上に努めていきたいものです。

以上

＜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＞

2015.7

めだか　【 システム監査人の喜び 】

2015年6月30日、政府は、「日本再興戦略」改訂2015を閣議決定しホームページに公表している。日本再興戦略の中には、ITにかかわるロボット開発やビッグデータへの投資を企業に促すほか、IoT、AIの活用の促進に言及している。日本再興戦略の要旨は次のようなものである。

「日本再興戦略」改訂2015を閣議決定

平成27年6月30日、デフレ脱却に向けた動きを確実なものにし、将来に向けた発展の礎を再構築する「『日本再興戦略』改訂2015」を閣議決定しました。アベノミクスは、デフレ脱却を目指して専ら需要不足の解消に重きを置いてきた「第一ステージ」から、人口減少下における供給制約を乗り越えるための対策を講ずる新たな「第二ステージ」に入りました。アベノミクスの「第二ステージ」」では、設備や技術、人材等に対する「未来投資による生産性革命の実現」と、活力ある日本経済を取り戻す「ローカル・アベノミクスの推進」の二つを車の両輪として推し進めることによって、日本を成長軌道に乗せ、世界をリードしていく国とします。

「日本再興戦略」改訂2015－未来への投資・生産性革命－の本文（第一部　総論）

「日本再興戦略」改訂2015－未来への投資・生産性革命－の本文（第二部及び第三部）

「日本再興戦略」改訂2015－未来への投資・生産性革命－の工程表

「日本再興戦略」改訂2015－未来への投資・生産性革命－の改革2020プロジェクト・工程表

「『日本再興戦略』改訂2015」総論概要

「これまでの改革の主な成果と新たな取組」

「3つのアクションプランの概要」

「『改革2020』プロジェクト」

http://www.kantei.go.jp/jp/headline/seicho_senryaku2013.html#c16

上記に先だち、「『責任ある機関投資家』の諸原則《日本版スチュワードシップ・コード》」と、上場会社が株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で透明・公正かつ迅速・果断な意思決定を行うための仕組みを意味するコーポレートガバナンス・コードが策定・公表され実施に移されている。機関投資家に投資先企業やその事業環境等に関する深い理解に基づく建設的な「目的を持った対話」（エンゲージメント）を行うことを求め、積み上がった内部留保の活用策など、投資先企業との対話を通じて中長期的に企業価値を高め投資リターンを拡大することを狙う、また、上場会社は、株主と対話し、コーポレートガバナンス・コードに示される規範を、会社の業種、規模、事業特性、機関設計、会社を取り巻く環境等によって適用を工夫し履行することになる。

世の中が激しく動く中で情報システムの監査に当るシステム監査人は、情報システムのリスクに応じたコントロールが適切に整備・運用されているか、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点検し、代表者に報告を行う責任を負う。その壁は高くかつ厚いがそれを乗り越えることにシステム監査人の喜びがあると思う。

（空心菜）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

＜目次＞

2015.7

投稿【　システム監査人の魅力　】

会員番号　0557　仲　厚吉　（会長）

日本年金機構や東京商工会議所など世の中を震撼させる情報漏洩事件が発生しています。7 月 9 日の朝、ニュースがあり、米国で 7 月 8 日、米ユナイテッド航空（United Airlines）がコンピューターの故障により一時運航停止となり、朝のラッシュ時の空港は数千人の旅客で混雑したと伝えられました。ユナイテッド航空でこうしたトラブルが起きるのはこの 6 週間で 2 度目といいます。ユナイテッド航空のシステム障害が起きた直後には、ニューヨーク証券取引所（New York Stock Exchange、NYSE）で技術的な障害により全ての株式の取引が停止する事態が起きたと伝えられています。2 件のシステム障害が連続して起きたことから、サイバー攻撃ではないかとの懸念の声が上がっていたが、今のところ、関連性はないとみられており、「今も調査中だ。」と国土安全保障省（Department of Homeland Security、DHS）の報道官が回答したと伝えられています。

情報システムが、利用目的に合って安全、有効かつ効率的に機能するよう再発防止に努めていただきたいものです。独立行政法人 情報処理推進機構（IPA）は、「情報セキュリティ 10 大脅威 2015」を発表し、2014 年において社会的影響が大きかったセキュリティ上の脅威について、「10 大脅威執筆者会」の投票結果に基づき、次のように順位付けしています。これは、我が国における脅威であり、システム監査人は、リスク対策に万全をつくすように努め、システム監査人の魅力を向上していただきたいと思います。

1	インターネットバンキングやクレジットカード情報の不正利用～個人口座だけではなく法人口座もターゲットに～
2	内部不正による情報漏えい～内部不正が事業に多大な悪影響を及ぼす～
3	標的型攻撃による諜報活動～標的組織への侵入手口が巧妙化～
4	ウェブサービスへの不正ログイン～利用者は適切なパスワード管理を～
5	ウェブサービスからの顧客情報の窃取～脆弱性や設定の不備を突かれ顧客情報が盗まれる～
6	ハッカー集団によるサイバーテロ～破壊活動や内部情報の暴露を目的としたサイバー攻撃～
7	ウェブサイトの改ざん～知らぬ間に、ウイルス感染サイトに仕立てられる～
8	インターネット基盤技術を悪用した攻撃～インターネット事業者は厳重な警戒を～
9	脆弱性公表に伴う攻撃～求められる迅速な脆弱性対策～
10	悪意のあるスマートフォンアプリ～アプリのインストールで友人に被害が及ぶことも～

2015 年 7 月分の第 204 回月例研究会は、次の方にご講演をいただきます。
講師 ： 独立行政法人 情報処理推進機構 （IPA）
技術本部　セキュリティセンター　情報セキュリティ技術ラボラトリー　主任研究員　渡辺　貴仁　氏
テーマ ：「最近の情報セキュリティ脅威と対策の解説」

次号以降の会報で、ご講演の要旨をお伝えいたします。

以上

＜目次＞

2015.7 投稿

【 基礎的自治体のシステム・トラブルに見る、自治体のシステム運用・監査の課題 】

会員番号 1566 田淵隆明 （近畿支部法制化研究会）

§1. 発生したシステム・トラブルの概要

昨年、2014 年 8 月 4 日、東京都心からほど近い某基礎的自治体の基幹システム(外部のデータ・センタのクラウドを使用)が丸一日停止し、住民票の発行や転入・転出の受付、婚姻届・出生届の受理などの重要業務が停止した。原因調査の結果、Web システムの手前の負荷分散装置(Load Balancer, 以下 LB)が過負荷になっていたことが原因と判明した。この件は、某有名ビジネス誌にも掲載され、全国的な話題となった。

§2. 2014 年 10 月の決算委員会で判明したこと

この問題は住民にとって非常に重要な問題であるため、再発防止策も含めて、直後の同自治体の議会でも取り上げられた。2014 年 10 月の決算特別委員会での情報システム担当者の答弁により判明したことは以下のとおりである。

①当該自治体の CIO に「システム監査技術者」の資格を有する人がいる。
②「情報セキュリティ監査」として、年に 1 回の有資格者による外部監査を実施している。
③過負荷になった原因は、ファーム・ウェアの更新漏れであった。監査で見落とした原因は、監査のタイミングの問題であった。監査の頻度の見直しも含めて検討する。

高信頼性のデータ・センタでは、SPF(Single Point of Failure)を作らないような設計にしており、負荷分散装置自体も冗長化しており、更新版のファーム・ウェアに問題があるリスクもあるので、更新処理は時差更新とするのが当然である。

ただ、この段階では、「基幹システムが停止した原因」は判明したが、「復旧に長時間を要した原因」は判明していなかった。何故なら、通常、LB の過負荷であれば再起動により問題は解消するからである。

§3. 2015 年 3 月の予算委員会で判明したこと

今回の問題は負荷分散装置のトラブルであったが、データベースでの障害が発生した場合は、データの一部消滅など、更に住民の被害は大きくなる。そこで、データベースの障害対策についても取り上げられた。2015 年 3 月の平成 27 年度の予算特別委員会での情報システム担当者の答弁により判明したことは次のとおりである。

①有資格者による外部監査「情報セキュリティ外部監査」を年に 1 回実施しているが、「公認情報セキュリティ主任監査人」、「公認情報システム監査人(CISA)」、「システム監査技術者(SYS-AUDIT)」を有する外部の専門事業者が実施している。

②監査対象は、個人情報を取り扱うシステム、庁内外の広範囲で利用されるシステム である。

③毎年、1 所属について実施しており、2007 年より 9 所属 14 システムについて外部監査を実施 している。

④現在、「情報セキュリティ外部監査」のほか、基幹システムの契約に基づく「データ・センタ監査」と「住基ネット監査」を実施している。

⑤個人情報保護の観点から、新たな監査を検討している。
⇒「システム監査技術者」の資格を有する CIO アドバイザーなど外部の有資格者の助言を受けつつ、頻度も含めて、監査のありかたを再検討している。

⑥情報政策課の職員は「技術職」でなく「事務職」であるため、「データベース・スペシャリスト」や Oracle Master のようなデータベースの有資格者は未配置。
⇒ただし、「ITC 人材育成指針」に基づき、必要なスキルアップは実施している。
また、「データベース・スペシャリスト」などの資格取得は励行している。

⑦バックアップは毎日取得しており、データベース自体のミラーリングは実施している。

⑧しかし、バックアップ媒体の多重化は行っていない。ただし、データ・センタ自体の二重化は検討中である。

⑨消費税の複数税率化に関する「システムへの影響調査」は、計画的に実施する。
⇒2014 年 4 月の「5%⇒8%」においては、介護保険システムに改修が発生した。

---

①についてであるが、外部監査のメンバーの有資格者の中に、「システム監査技術者」や CISA はいるものの「CSA(公認システム監査人)」はいなかった。

③については、5 月の取材により、監査対象が一巡するのに約 20 年掛かることが判明した。つまり、一度もチェックを受けずにライフサイクルの終焉を迎えるシステムが存在することになる。監査頻度については大きな課題があると思われる。現在、大手企業の監査は四半期決算を行っている。やはり、四半期単位で(巡回監査で良いので)システム監査を実施するべきである。

①③④⑤に関連して、監査項目がセキュリティに偏していることも判明した。法制化推進グループの中には、ICT (Information Communication Technology)と IT の用語の違いに留意するように指摘している人もいるが、総務省は ICT を経産省は IT を標榜している。地方自治のしくみの関係上、地方自治体に対する国の窓口は総務省である。総務省が郵便や通信を管轄していることもあって、地方自治体のシステムの運用・監査では「通信」と「セキュリティ」と「プライバシー」(個人情報保護)偏重になりがちなのかもしれない。

しかし、通信(Communication)に傾注しすぎているのは、IOT/M2M やビッグデータや AI 等の最新のトレンドからみれば些か時代遅れの感がいなめない。また、この現象を助長している背景には、経産省にも問題があると言わざるを得ない。「システム管理基準」と「システム監査基準」は 2004 年以降、全く改訂されていない。「日進月歩」ならぬ「秒進分

歩」と言われる IT の世界の現状を鑑みるとき、これはまさに驚愕の事態である。経産省筋の情報からすると、情報セキュリティやプライバシー保護に忙殺されているようであるが、ここは増員してでも、「システム管理基準」と「システム監査基準」の最新版を最低でも 2020 年には出すべきである。

⑥については、地方公務員法の問題に遡る。多くの自治体において、情報処理システムの管轄は総務部や総務課となっている。つまり、「技術職」ではなく「事務職」のポストしかない。そのため、ベンダのコントロールが困難である。この点については、法改正も含めた対応が必要であろう。特に、データベースが破損した場合の被害は甚大であるため、データベースの有資格者の配置や技術職の配置を可能にする手立てが急務である。

⑦については、その後の調査により、障害発生時には前日のバックアップに戻ってしまうのではなく、障害直前までの復旧が可能である(アーカイブ・ログ・モード)であることが判明した。これについては良いのであるが、⑧にあるように、バックアップ媒体の二重化が出来ていないのは大問題である。高信頼性のデータ・センタであれば、同一サイト内でのバックアップ媒体の多重化、及び、定期的な遠隔地へのバックアップ(東日本と西日本など。電力会社まで分けたり、プレートまで分けるケースもある)を行うのが当然である。1カ月あたり数千円のクラウド・サービスでも、この程度のことはできている。しかも、このデータ・センタの供用開始は 2013 年のことであり、「3.11」の後である。「3.11」の教訓が生かされておらず、大きな問題と考える。また、トラッシング対策等についても気になるところである。

⑨については、システム企画時の「将来拡張性」の考慮不足であり、これを見逃したベンダ内部の監査体制の問題である。

§4. 2015 年 5 月の取材で判明したこと

5 月下旬に当該自治体の役所を取材し、§2 で残った疑問である「復旧に長時間を要した原因」が判明した。このデータ・センタは他の 3 つの自治体と共同利用になっており、データベース・サーバ、アプリ・サーバ、Web サーバは全て独立していたが、何故か、負荷分散装置(LB)の乗っている筐体のみ分離されていなかった。障害発生当時、同自治体のシステム担当者は、「他の自治体と共用でないならば再起動したが、他の自治体のシステムを”巻き沿い”にするリスクを回避するため、止むを得ず、夕方の業務終了時刻を待って再起動した。すると、障害は解消した」とのことであった。

BCP において、「障害発生時の影響範囲の局所化」は、基本中の基本である。従って、この時点においては、担当者の判断は正解であったと思われる。しかし、負荷分散装置の乗っているサーバが、他の自治体と「一連托生」というのは理解に苦しむ。現在は分離したそうであるが、もし「一連托生」でなければ、直ちに再起動が可能であったことを考えると極めて遺憾である。

§5. 自治体首長との会談・陳情での話

6 月下旬、当該自治体の首長に会うことが出来た。その際には、食品安全の話や、自転車の安全対策、鉄道の混雑緩和などの話をした後に、この問題をお尋ねしたが、「一連托生」に問題の本質があったということについては良く理解しておられた。

§6.監査人としての課題

ここで、我々システム監査人はどう考えるべきだろうか? システムの監査の頻度の改善は当然である。また、「負荷分散装置の一連托生」(SPF)と「バックアップ媒体の二重化未実施」については、そのような設計を行いサービスを提供したベンダの責任は重大である。しかし、それを見逃したシステム監査人の責任も問われるべきである。特に、同自治体の場合は、システム監査人は一般競争入札で決定しており、最安値を入札したところが落札している。しかし、今回の問題を鑑みると、システム監査人も玉石混交であることを改めて実感させられた。システム監査人の資質を担保する上でも、他の資格よりも取得が困難であり、幅広い知識を求められる CSA の価値が再評価されるべきなのではないだろうか?

また、以前から、我々の研究会で提案している「IT 事業者評価制度」の評点を入札資格にするなど、行政側でも資質の確保に努めるべきであると思われる。

また、本来、CSA は「システム監査技術者」及び「CISA」の上位の資格である。従って、今後とも一層の普及啓発を行う必要があると考えられる。

§7. 他の自治体での調査

実はこの自治体は、全国平均からみれば富裕な自治体であり、情報システムの要員も充実した自治体である。従って、他の自治体、特に町村レベルの自治体においては、更に多くの問題が内在しているのではないかと容易に推察される。マイ・ナンバー制度施行が迫る中、今回のことは、非常にリスクがあることがお分り頂けると思われる。現在は、国民年金機構の情報流出問題により、情報セキュリティだけに議論が集中しているが、行政としては、緊急点検を実施するとともに、システムの信頼性・可用性への対応も必要である。(現在、筆者の情報提供を受け、他の自治体でも調査が行われている。)

終わりに、本件について、様々な示唆・助言を頂いた力利則副会長、吉田博一元近畿支部長、近畿支部のシステム監査法制化推進プロジェクトの神尾博副主査、中田和男氏に深く御礼申し上げたい。

(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＞

2015.7

第２０３回　月例研究会　（２０１５年６月開催）報告

会員番号　1760　斎藤由紀子　（個人情報保護監査研究会）

【講演テーマ】個人情報保護法及び番号利用法の改正～パーソナルデータの利活用をめぐる制度の見直し～
【講師】慶應義塾大学総合政策学部教授　新保史生　氏
【日時】　2015 年 6 月 16 日（火曜日）18:30～20:30
【場所】　機械振興会館　地下 3 階　研修 2 号
【テーマ】　□制度見直しに向けた取り組みの経緯
　　□個人情報保護法の改正案
　　□番号利用法の改正案

１．日本の現行の個人情報保護制度（抜粋）

(1) OECD プライバシー8原則

①収集制限の原則
②データ内容の原則
③目的明確化の原則
④利用制限の原則
⑤安全保護の原則
⑥公開の原則
⑦個人参加の原則
⑧責任の原則
1980 年採択

(2)「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（1988 年 12 月 16 日法律第 95 号）
(3) プライバシーマーク制度の運用開始（1998 年 4 月 1 日）
JIS Q15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」(1999 年制定、2006 年改正)
(4) 個人情報の保護に関する法律　(2003（平成15）年　法律第57号)・・・→　2005 年4月1日全面施行

２．過剰反応からいつの間にか過小評価へ

(1) 2006 年 2 月 28 日「個人情報保護の円滑な推進について」（個人情報保護関係省庁連絡会議申合せ）

- 過剰反応の問題について
  - 大規模災害や事故等の緊急時における家族等への情報提供、捜査関係事項照会への回答は、あらかじめ本人の同意を得なくても提供できる。
  - 入学時や新学期の開始時に、あらかじめ個人情報の取扱いについて保護者の同意を取得する等の手続きを明確化すれば、学校や地域社会における緊急連絡網等の名簿の作成が可能。

(2)　2012 年 11 月 29 日「IT融合フォーラムパーソナルデータワーキンググループ(～2013.4.10)

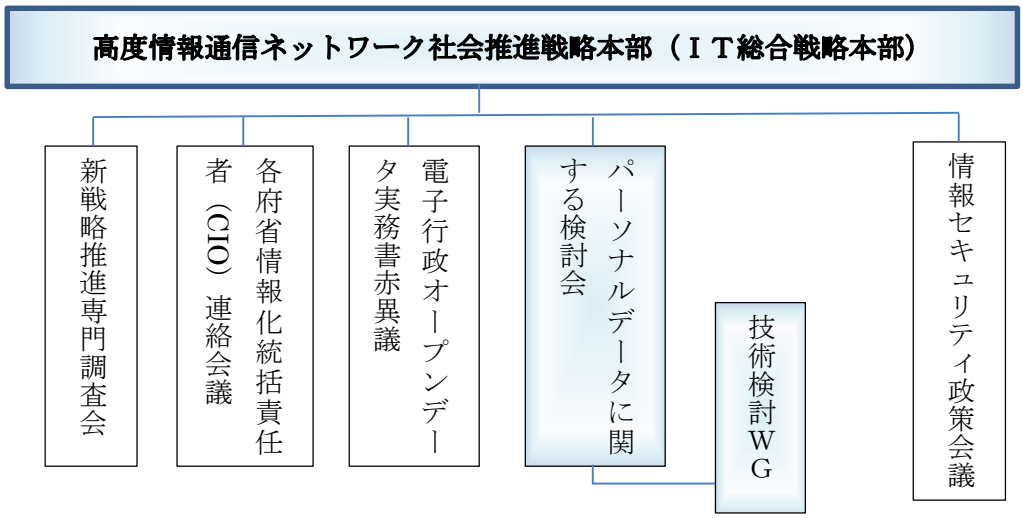
- 便利で種々多用なサービスが日々新たに登場　～ビッグデータ活用と脱法的なパーソナルデータの利用～
  - 利用者：利便性やポイントなど、利用しなければ「損」であるという意識の広がり
  - 事業者：取得される「大量のデータ」を有効活用しないことは「損」であるという認識

この両者の損得勘定が、不透明で不可解な情報の取扱いを結果的に許容する現状を招いている

- ネット上で問題が指摘される事例の増加
  - 個人情報（PII）と非個人情報(Non-PII)を区別しない取り扱いの問題
  - 取扱う情報が、法令において明確に禁止されていない問題

「いわゆるビッグデータ」の取扱いにあたっては、法令遵守や
「個人の権利利益保護」への取り組みが軽視される傾向があることは否めない

３．制度見直しに向けた取組み：パーソナルデータに関する検討会（2013.9.2-2013.12.10）



（※SAAJ 注：新保史生教授は「パーソナルデータに関する検討会」委員としてご参加）

５．個人情報保護法改正案

1. 個人情報の定義の明確化		
	修正	(1)個人情報の定義
2. 適切な規律の下で個人情報等の有用性を確保するための規定の整備		
	新設	(1)匿名加工情報に関する規定
	微修正	(2)利用目的の制限の緩和
	修正	修正(3)情報の利用方法からみた規制対象の縮小
3. 個人情報の保護を強化するための規定の整備		
	新設	(1)要配慮個人情報に関する規定
	新設	(2)第三者提供に係る確認及び記録の作成の義務付け
	新設	(3)不正な利益を図る目的による個人情報データベース提供罪
	修正	(4)本人同意を得ない第三者提供への関与（オプトアウト規定の見直し）
	削除	(5)小規模事業者の適用除外
	修正	(6)個人情報取扱事業者による努力義務への個人データの消去の追加
	修正	(7)開示等請求権の明確化
4. 個人情報保護委員会の新設及びその権限に関する規定の整備		
	新設	(1)個人情報保護委員会の主な権限
	新設	(2)個人情報保護指針の作成への関与
5. 個人情報の取扱いのグローバル化に対応するための規定の整備		
	新設	(1)国境を越えた個人情報の取扱いに対する適用範囲に関する規定の整備
	新設	(2)外国執行当局への情報提供に関する規定の整備
	新設	(3)個人データの外国にある第三者への提供の制限

(1) 目的に関すること(第一条関係)　　(SAAJ 注:赤字は改正ポイント)

この法律は、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とするものとすること。

(2) 定義に関すること(第二条関係)

1 (省略)

2 この法律において「個人識別符号」とは、次のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものとすること。

(一)特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した符号であって、当該特定の個人を識別することができるもの

(二)個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの。

3 この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

(3) 国及び地方公共団体の責務等に関すること(第二章関係)

政府は、国際機関その他の国際的な枠組みへの協力を通じて、各国政府と共同して国際的に整合のとれた個人情報に係る制度を構築するために必要な措置を講ずるものとすること。

(4) 個人情報取扱事業者の義務に関すること(第四章関係)

1 適正な取得

個人情報取扱事業者は、一定の場合を除き、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならないものとすること。

2 データ内容の正確性の確保等

個人情報取扱事業者は、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならないものとすること。

4 第三者提供の制限

(一)一定の場合にあらかじめ本人の同意を得ないで当該本人が識別される個人データを第三者に提供することができる旨の規律について、当該規律の対象となる個人データから要配慮個人情報を除くとともに、当該規律により個人データを提供するためには、一定の事項を個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出なければならないものとすること。

(二)個人情報保護委員会は、(一)の届出があったときは、個人情報保護委員会規則で定めるところにより、当該届出に係る事項を公表しなければならないものとすること。

5 外国にある第三者への提供の制限

個人情報取扱事業者は、外国にある第三者に個人データを提供する場合には、一定の場合を除き、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならないものとすること。

6 第三者提供に係る記録の作成等　　（SAAJ 注：赤字は改正ポイント）

個人情報取扱事業者は、個人データを第三者に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名等の記録を作成し、一定の期間保存しなければならないものとすること。

7 第三者提供を受ける際の確認等

個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、当該第三者による当該個人データの取得の経緯等を確認するとともに、当該個人データの提供を受けた年月日等の記録を作成し、一定の期間保存しなければならないものとすること。

8 開示等

（一）本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの開示を請求することができるものとするとともに、一定の場合において、当該保有個人データの内容の訂正、追加若しくは削除、利用の停止若しくは消去又は第三者への提供の停止を請求することができるものとすること。

（二）本人は、（一）による請求に係る訴えを提起しようとするときは、一定の場合を除き、その訴えの被告となるべき者に対し、あらかじめ、当該請求を行い、かつ、その到達した日から二週間を経過した後でなければ、その訴えを提起することができないものとすること。

(5) 匿名加工情報取扱事業者等の義務に関すること（第四章第二節関係）

1 匿名加工情報の作成等

（一）匿名加工情報を作成するときは、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするために必要なものとして個人情報保護委員会規則で定める基準に従い、当該個人情報を加工しなければならないものとすること。

（二）匿名加工情報を作成したときは、加工の方法に関する情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、これらの情報の安全管理のための措置を講じなければならないものとするとともに、個人情報保護委員会規則で定めるところにより、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならないものとすること。

（三）匿名加工情報を作成して自ら当該匿名加工情報を取り扱うに当たっては、当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該匿名加工情報を他の情報と照合してはならないものとすること。

2 匿名加工情報の提供

匿名加工情報取扱事業者は、匿名加工情報を第三者に提供するときは、個人情報保護委員会規則で定めるところにより、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならないものとすること。

3 識別行為の禁止

匿名加工情報取扱事業者は、匿名加工情報を取り扱うにあたっては、当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、加工の方法に関する情報等を取得し、又は当該匿名加工情報を他の情報と照合してはならないものとすること。

4 安全管理措置等

匿名加工情報取扱事業者は、匿名加工情報の安全管理のために必要かつ適切な措置、匿名加工情報の取扱いに関する苦情の処理その他の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、

かつ、当該措置の内容を公表するよう努めなければならないものとすること。

(6) 監督に関すること(第四章第三節関係)　　(SAAJ 注:赤字は改正ポイント)

1 個人情報取扱事業者の監督を行う主体を主務大臣から個人情報保護委員会に改めるとともに、匿名加工情報取扱事業者の監督を個人情報保護委員会が行うものとすること

2 報告及び立入検査、指導及び助言(省略)

3 権限の委任

個人情報保護委員会は、緊急かつ重点的に個人情報等の適正な取扱いの確保を図る必要があることその他の政令で定める事情があるため、必要があると認めるときは、政令で定めるところにより、2による権限を事業所管大臣に委任することができるものとすること。

5 事業所管大臣の請求(省略)

(7) 民間団体による個人情報の保護の推進に関すること(第四章第四節関係)

1 認定個人情報保護団体の認定及び監督を行う主体を主務大臣から個人情報保護委員会に改める

2 個人情報保護指針(省略)

(8) 個人情報保護委員会に関すること(第五章関係)

1 所掌事務

(一)基本方針の策定及び推進に関すること。

(二)個人情報及び匿名加工情報の取扱いに関する監督並びに苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関すること((四)に掲げるものを除く。)。

(三)認定個人情報保護団体に関すること。

(四)特定個人情報の取扱いに関する監視又は監督並びに苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関すること。

(五)特定個人情報保護評価に関すること。

(六)個人情報の保護及び適正かつ効果的な活用についての広報及び啓発に関すること。

(七)(一)から(六)までに掲げる事務を行うために必要な調査及び研究に関すること。

(八)所掌事務に係る国際協力に関すること。

(九)その他法律に基づき委員会に属させられた事務

(9)雑則に関すること(第六章関係)

1 適用範囲

この法律の一定の規定は、国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報又は当該個人情報を用いて作成した匿名加工情報を取り扱う場合についても適用するものとすること。

2 外国執行当局への情報提供

個人情報保護委員会は、この法律に相当する外国の法令を執行する外国の当局に対し、その職務の遂行に資すると認める情報の提供を行うことができるものとすること

(10)罰則に関すること(第七章関係)

個人情報取扱事業者若しくは従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、一年以下の懲役又は五十万円以下の罰金に処するものとすること。

６．Ｑ＆Ａ

Q1:グローバル化に対応する規定の整備について、日本と同等のレベルの外国政府（執行当局）には個人情報を移転できると言っても、実際に海外の政府を認定することができるのでしょうか。

A1:日本と同等と認定するノウハウが明確ではない状態では、相当揉める可能性も出てくると予想されます。認定しないという選択肢という考えもあるようで、今後どうなるのかは注視していく必要があるでしょう。

Q2:クラウドサービスの委託について、クラウド利用の場合、海外にデータを置く可能性があります。どこまで評価しなければならないのでしょうか。

A2:契約先のデータセンターが、実際にどこに置いているのかまでの確認までは求めていません。しかし、委託先が一定の安全管理体制を整備していることを約款や報告等で確認は必要です。

Q3:匿名加工情報について、内部監査の証跡にある個人情報の記載を塗りつぶす等の対応をすると、匿名加工情報の取り扱いとなるのでしょうか。

A3:事業者内部における匿名加工情報についても取扱いにあたっての公表義務の対象となります。しかし委員会規則に基づいて加工する匿名加工情報と、そもそも個人情報には該当しない情報は匿名加工情報ではないので公表義務からは除外されるため、いろいろな工夫があると思われます。

Q4:国際的な評価について、今回の法改正について、国際的にはどのように評価されているでしょうか。

A4:第三者機関として、個人情報保護委員会が設置されたことが、プライバシー・コミッショナー会議への正式参加の可能性をはじめとして、国際的にも重要な評価がなされると考えられます。また、利活用推進を目的としながら、要配慮個人情報を明記したり小規模事業者の適用除外を撤廃するなど、厳しい規定も定められたことが、非常に高く評価されています。

Q5:欧米の取り組みとの比較について、日本の取り組みとして不足しているとすれば何があるでしょうか。

A5:公的部門に委員会の権限が及ばないことは最大の欠点です。OECD ガイドラインも、執行機関が官民双方に対し権限を及ぼすことを求めています。しかし、今回の年金機構の事件についても委員会は何もできません。総務省で行政機関を対象とした検討を継続していますが、このまま決着するのであれば、国際的な理解は得られず、十分性認定の評価を得ることはできないと言えるでしょう。

１０．報告者所感

講演冒頭に、社保庁の年金記録問題（2007年）、年金機構の125万件流出（2015年5月）の事件発生が、法制定・改正に及ぼす影響について言及され、また最後のＱ＆Ａに応じて「公的部門への執行権限」という課題が残されていると締めくくられたことは、我が国の個人情報保護の今後について示唆に富むものであった。

我々システム監査に携わる者として、実務レベルに関係する、施行令、施行規則、個人情報保護委員会規則等が民間事業者に与える影響について、地道な研究活動を続けていく重要性を痛感する講演であった。

以上

＜目次＞

2015.7

北信越支部 「2015 年度 福井県例会 報告」

会員 No. 1281　北信越支部 宮本 茂明

以下のとおり2015年度福井県例会を開催しました.

・日時:2015 年 6 月 13 日(土) 13:00-17:00　　参加者:10 名

・会場:福井市地域交流プラザ (AOSSA)

・議題:1.研究報告

「システム案件起案段階でのシステム監査のあり方」

小嶋 潔 氏

2. 西日本支部合同研究会「社会と組織のためのシステム監査」-北信越支部報告検討

・北信越支部報告:

「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」

3. SAAJ 中部・北信越支部・JISTA 中部合同研究会 企画検討

・開催日程:11 月開催で調整, 開催場所:福井市地域交流プラザ

◇研究報告

「システム案件起案段階でのシステム監査のあり方」

報告者 (会員 No. 1739　小嶋　潔)

1. はじめに

私の勤務先の銀行におけるシステム監査の過程で日頃感じている問題点に対して課題と解決策を検討し、システム監査によりシステムリスクの軽減に繋がるような議論を展開できればということで、本日の報告を行います。

2. システム監査について

(1)システム監査の実施方針

・当行では、監査の着眼点として、FISC(金融情報システムセンター)のシステム監査指針を参考にすると共に、金融検査マニュアル、財務報告に係る内部統制におけるIT統制の統制目標等を参考にして監査項目を設定してシステム監査を行っています。

・FISCのシステム監査指針の要点項目の内、「システム開発」、「外部委託」については、態勢整備に関する項目以外に、実際のシステム開発や外部委託契約がスタートする前の段階でのチェック項目を含んでいます。

(2)システム方式決定前段階におけるITコントロール運用状況の有効性評価

・一方、これまで私の経験したシステム監査では、システム方式やパッケージあるいはサブシステムが決定された後に、その後の開発過程や運用管理状況を後追いで検証して問題点の指摘や提言を行ってきました。もちろん、勘定系システムの更改のような大規模開発案件については、開発過程でのプロジェクト監査を行っています。しかしながら、システム方式やサブシステムの決定過程に関与して監査したことは、基本的にありません。

(3)システム案件の検討と監査の問題点

・当然ながら、監査部門は業務執行に携わることはできませんので、施策の決定過程に直接関与することはないのですが、最近システム監査を行っていく中で、「関与」する方法を工夫して、決定過程におけるリスク評価が適正に行われるよう、社内の態勢を整備していかなければならないのではないかと考えるようになりました。

・その理由は、システム導入検討時や外部委託先選定時のシステムリスク評価について、態勢的に不十分な状況があると思われるからです。

3. 当行のシステム化案件の決裁と内容の検討

(1)規程上の決裁権限

・規程により、それなりの規模のシステムの導入決定については、最低でも執行役決裁、場合によっては経営会議等の会議決裁が必要で、複数年に亘って大きな費用や投資が必要なものは取締役会を経て決定されることになります。

(2)新商品・新種業務審査

・一方で、新商品や新種業務の取り扱いを開始するにあたっては、新たな各種リスクの介在が想定されることから、事前に法令等遵守、顧客保護等管理上の問題点を検証したうえで、内在するリスクの評価を適切に行う必要があります。しかしながら、規程上すべてのシステム化案件がこの審査を受ける決まりとはなっていないため、網羅的に新システムのリスク評価が行われる体制となっていません。

(3)システム案件の評価

・ところで当行の業務分掌規程により、システム開発案件の査定・調整・統括、コンピュータシステムに関する機器や設備の導入・改廃といった業務は、システム部門の業務分担となっています。

4. システム案件の内容検討

(1)案件の検討

・当然、上記3.(3)の案件検討の過程では、案件起案部署とシステム部門が協力してシステム仕様を固めることになっています。また、サブシステムの導入に関しては「導入時チェックリスト」により、ソフト・ハード・データ・ネットワーク・アクセスに関する管理体制の確認、さらに個人情報を取り扱うシステムであれば技術的安全管理措置に関する確認を行っています。したがって、相応のリスク評価を行ったうえで、案件採り上げとなるはずです。

・但し、リスク評価の観点で行っている「導入時チェックリスト」については、平成 17 年 4 月に制定以来一度も改定見直しを行っておらず、またチェックした結果をその後どう取り扱うか明確な取り決めもないため、適正なシステムリスクの評価となっているか、疑問な面があります。また、現状すべてのシステムについてリスク評価が洩れなく一定のレベルを保って実施される体制とはなっておらず、特に小規模なサブシステムやASPについては、システム部門によるリスク評価が十分に行われないケースが実際に発生しています。

・システムリスクにそれほど関心のない部署が、業務機能にのみ注目してシステムを選定してしまうと、思わぬ落とし穴に落ちてしまいかねないのではないかと危惧しています。実際に、クラウド利用であることの認識なしにサブシステム選定して利用開始し、システム監査において指摘となった事例もあります。

・一般的に一旦導入を決定してしまうと、後戻りするのには大変な労力や費用を要することになり、簡単なことではありませんので、事前の調査やリスク評価が確実に行われてから、採否の稟議が行われるようにする必要があります。

5. 当行における「監査」について

(1)取締役、執行役の業務執行に対する監査

・当行は指名委員会等設置会社であり、取締役や執行役の職務執行を監査する役目は、取締役会や監査委員会が担っています。

(2)内部監査部門の監査

・一方、内部監査部門は、適正かつ効率的な業務運営態勢の構築、運営がなされているかを定期的に内部監査

するもので、あくまで職員の業務執行を把握し、その改善を図る目的のものです。

(3)内部監査部門としての現状に対する問題意識

・前述のとおりシステム化案件の採用決定の際に、リスク評価が一部不十分となっています。

・一方で既存のサブシステムに関しては、FISCの安全対策基準等をベースに作成された「セキュリティチェックシート」を用いて、年 1 回定期的にシステムリスクのモニタリングを行っています。「セキュリティチェックシート」の内容は毎年見直しを加えており、リスク管理/評価の観点で一定以上の効果はあるものと思っています。

・しかしながら、新規のサブシステムに対する「導入時チェックシート」の内容は制定後見直しされておらず、上記「セキュリティチェックシート」との整合性もとられていないため、システム導入検討時のリスク評価に用いるものとしては、不十分な点があることは否めません。

6. 考えられる対応策

(1)システム導入検討時点での牽制

・上述の実態に鑑みれば、システム導入時には決裁が取締役会や経営会議であろうと、稟議決定前にすべからく一定レベルのシステムリスク評価が行われる体制を整えるのが重要であると思われます。

・そのために「導入時チェックシート」と「セキュリティチェックシート」を、共通的に使用可能な「チェック表」に見直しを行い、システム導入検討時も定期的モニタリングにおいても同様のレベルでリスク評価を行うべきです。

・さらにシステム起案時には、必ず網羅的にシステムリスクを評価する規程とし、関係各部署に周知徹底し、チェック洩れを防止できる体制を構築しなければなりません。

(2)何をどのように監査していくか

・まずシステム部門に対するシステム監査において、「チェック表」が整備され、定期的にその内容について見直しをかけているかについて検証します。

・「チェック表」が充分に整備されていることを前提に、すべてのシステムについてこの「チェック表」によるリスク評価が行われていることを、システム部門及び本部各部署の監査時に検証します。

・導入時リスク評価のチェック項目が充足されていなくてもシステムを採用する場合は発生します。このようなシステムに関しては、定期的なリスクモニタリングの際に、導入時チェックで不十分であった項目について改善しているかどうかフォローアップすることが必要です。

7. 最後に

・日頃監査業務に従事していると、被監査部署の業務遂行の結果のみを検証して不備を指摘し、改善提言を行うことが中心となります。しかしながら、監査頻度は各部署に対して年に1、2回がせいぜいで、タイミング良くシステム案件に対する検討状況を必ずしも検討段階に検証できるとは限りません。

・業務部署にはリスク目線が乏しい担当者も少なくありません。また、システム部門は日常業務に埋没し、システム開発自体も外部委託中心となって、委託先の管理がメイン業務となっている場合も珍しくありません。そういう状況の中で、システム担当者のリスク感応度も必ずしも高くない場合があります。

・しかしながら、監査に携わる者として、少しでもシステムリスクの低減につながるよう、様々な直面で業務執行にならない範囲で物言うシステム監査人であるよう心掛けていきたいと思う今日この頃です。

以上

＜目次＞

2015.7

支部報告　【　近畿支部第１５２回定例研究会報告　】

会員番号 0645 是松徹 （近畿支部）

１．テーマ　：　「失敗した IT プロジェクトの真の原因に迫るマンダラ図の紹介」

２．講師　：　公認システム監査人　松井　秀雄氏

３．開催日時　：　２０１５年５月１５日（金）　１８：３０～２０：３０

４．開催場所　：　大阪大学中之島センター３階　講義室３０１

５．講演概要　：

「IT プロジェクトで失敗を経験した後、何を学び、何を語り継ぐべき？」との命題を掲げて研究を進め、その成果としてまとめられた失敗を究明する手法である「【IT プロジェクト版】失敗原因マンダラ図」（以後【IT 版】マンダラ図）について、構築の経緯・内容と活用事例等についてご講演いただいた。また、関連して失敗から学んだことを整理し共有する手法である「AAR（After Action Review）」（アメリカ陸軍の事後検証メソッド）について紹介いただいた。

（１）現状と背景

プロジェクトマネジメントに関する手法や文献が世の中に数多く紹介され、知見、ノウハウ等の蓄積も進んでいるように見えるが、プロジェクトの成功率は 31.1%、ユーザー満足度は 10%と低調であり、依然として多くのプロジェクトが失敗している実態がある。 失敗原因として、要件定義不足、プロジェクト管理の不備、システム導入後の効果があいまい、思い込みと確認不足等が事例として公表されている。今回の研究のきっかけは、システム開発の各局面では順調に進捗した（ように見えた）が、いざふたを開けてみると機能不足が判明した失敗事例である。

（２）研究の目的

過去から同じ失敗を繰り返しているのは、真の原因が特定できていないからと考える。そこで、「失敗の真の原因を客観的かつ網羅的に把握する」ことを研究の目的として設定した。研究母体は、関西 IBM ユーザー研究会・IT 研究会分科会であり、アドバイザーとして参画した。

（３）研究内容

①従来の特性要因図やなぜなぜ分析に限界がある中で客観性、網羅性を満たす手法はないか、IT 業界から離れて視野を広げて探索すればどうか、とのアプローチから、失敗学会の「失敗原因のマンダラ図」に行き着いた。

②マンダラ図自体や考え方は流用可能と判断し、IT 業界へ適用できる内容への再構築を検討した。

③検討メンバ各自（各社）の失敗事例から失敗原因を洗い出し、全員分を統合してマンダラ図案を作成した。

④マンダラ図案に対し、以下の観点から整理を行った。

・項目の統合＆削除　・階層の深さ　・各階層の粒度　・言葉の意味　・分類の見直し

⑤最後に、書籍の事例を用いてマンダラ図案の網羅性を精査し、【IT 版】マンダラ図として完成させた。結果として、各社事例(61 事例)と書籍事例(161 事例)をもとに 49 個の失敗原因が抽出できた。

⑥【IT 版】マンダラ図は失敗学会からも一定の評価が得られ、信頼性が確保できたと考えている。

(4)【IT 版】マンダラ図使用方法のご紹介

失敗事例について【IT 版】マンダラ図を使用した分析の流れは以下となる。

Step1:関係者各自が【IT 版】マンダラ図から失敗原因を抽出

Step2:関係者各自が抽出した失敗原因を集約

Step3:失敗原因を選定

Step4:真の失敗原因を特定

Step5:再発防止策を検討

(5) 活用事例

【IT 版】マンダラ図の活用事例として以下が考えられる。

① **プロジェクトの振り返り**:失敗について、網羅的な原因分析と再発防止策の策定が実施できる。

② **システム監査**:真の失敗原因を探り出し、有効な改善提言が表明できる。

③ **若手社員の育成**:上司と若手の共通ツールとして原因分析等に活用し、若手に気付きを与える。

④ **統計:**真の失敗原因と複数の統計項目を組み合わせ、統計情報として管理できる。

(6) 課題

IT プロジェクトの失敗原因を検討する目的で作成したため、IT 運用、IT 企画等の他の用途への適用検討が今後の課題である。

(7) AAR(After Action Review)手法の紹介

グループで以下を討議し、事後検証する手法である。【IT 版】マンダラ図が③で活用できると考える。

① 我々は何をやろうとしたのか?

② 実際には何が起きたのか?

③ 当初の目的と実際の結果の違いは何故起きたのか?

④ 次回なすべきことは何か?

6. 所感

依然として問題が多い IT プロジェクトの真の失敗原因を探り出すツールとして新たに提唱された「【IT 版】マンダラ図」は、その構築過程の確かさから有効性が大いに期待できると感じました。失敗については輻輳した多様な原因があるため、なかなか特効薬はないと考えますが、いずれにしても真の原因を分析し、地道に対策を講じていくことしかないと思います。本マンダラ図を継続してブラシュアップしていただき、有効度を高めていただくことを期待しています。

以上

＜目次＞

2015.7

注目情報（2015.6～2015.7）※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】IPAの注意喚起メールを騙った不審メールに注意！

2015年7月17日 独立行政法人情報処理推進機構

7月17日、IPAの名前を騙った不審メールが出回っていることを確認しました。当該不審メールにはウイルス感染を目的とした添付ファイルが付いているため、安易に不審メールを開かないよう注意してください。

IPAが確認したところ、IPAが7月15日に発信したMicrosoft製品やAdobe製品に関するセキュリティ対策情報が用いられており、IPAからのメールニュースを模した内容となっていました。また、このメールには本来のメールニュースには存在しないはずの圧縮ファイル（.zipファイル）が添付されていました。

IPAが提供情報を分析した結果、添付されていた圧縮ファイルを展開すると、ショートカットファイル（.lnkファイル）が現れ、これはウイルス感染を目的とするファイルであることが確認されました。

また、メールの件名と本文はIPAが公開している実在のウェブページを元に作成されており、添付ファイルの開封を促すような文面となっています。

https://www.ipa.go.jp/about/press/20150717.html

■【安全なウェブサイトの構築と運用管理に向けての16ヶ条 ～セキュリティ対策のチェックポイント】

最終更新日 2015 年 7 月 14 日 独立行政法人情報処理推進機構 技術本部 セキュリティセンター

ウェブサイトの脆弱性や運用管理の不備を悪用された情報漏えいやウェブページの改ざんなどの事件が多数発生しています。ウェブサイトの改ざんや情報漏えい等の被害が発生すると、サービス停止や顧客への補償等、事業に直接的な影響を受ける可能性があります。

https://www.ipa.go.jp/security/vuln/websitecheck.html

■プライバシーマーク制度における

番号法および特定個人情報ガイドラインへの対応について

http://privacymark.jp/news/2015/0519/index.html

よくある質問と回答 ： 2015 年7月17日追加更新

http://privacymark.jp/reference/pdf/guideline_kaisetsu_FAQ_150717.pdf

一般財団法人日本情報経済社会推進協会（JIPDEC）プライバシーマーク推進センター

＜目次＞

2015.7

【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第205回	日時:2015 年 8 月 24 日(月)　18:30～20:30　場所:機械振興会館　地下 2 階　ホール	
	テーマ	「CSMS(サイバーセキュリティマネジメントシステム)認証と ISMS 認証の今後」(仮題)
	講師	一般財団法人　日本情報経済社会推進協会(JIPDEC) 情報マネジメント推進センタ センター長 高取敏夫 氏
	講演骨子	詳細確定次第、HPでご案内いたします。
	お申し込み	日本システム監査人協会ホームページ
第206回	日時:2015 年 9 月 15 日(火)　18:30～20:30　場所:機械振興会館　地下 2 階　ホール	
	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) 電子情報利活用研究部 部長 坂下 哲也 氏
	講演骨子	詳細確定次第、HPでご案内いたします。
第207回	日時:2015 年 10 月 23 日(金)　18:30～20:30　場所:機械振興会館　地下 2 階　ホール	
	テーマ	「失敗した IT プロジェクトの 真の原因に迫るマンダラ図の紹介」(仮題)
	講師	特定非営利活動法人　日本システム監査人協会 近畿支部　会員　松井　秀雄　氏
	講演骨子	詳細確定次第、HPでご案内いたします。

■システム監査実践セミナー（東京）

第26回	日時:2015年8月29日(土)～30日(日)、9月12日(土)～13日(日)＜1拍2日×2＞ (どちらか一方のみの参加は不可) 時間:土曜は 10:00～19:30、日曜は 09:00～15:00 (進行状況により若干の変更が生じる場合があります。) 会場:晴海グランドホテル(最寄り駅都営地下鉄大江戸線勝どき駅下車徒歩8分)	
	概要	本セミナーは、当協会のシステム監査事例研究会「システム監査普及サービス」で実施したシステム監査事例を教材として、ロールプレイングを中心とした演習によりシステム監査を修得することを狙いとしたきわめて実践的なコースです。 なお、本セミナーを受講した後、事後課題を提出頂き、その内容が適切であると判断された場合には、当協会が認定する公認システム監査人の認定に必要なシステム監査実務を1年間経験したものとみなされます。
お申し込み		HPでご案内中です。 http://www.saaj.or.jp/kenkyu/jitsumuseminar26.html

■システム監査体験セミナー（実践編）（大阪：近畿支部主催）

	システム監査体験セミナー（実践編）	
	概要	・本セミナーは、システム監査を実際に行う機会が少ない現状において、システム監査技術者や公認システム監査人を目指される方、内部監査ご担当者やシステム監査にご興味をお持ちの方々に、模擬体験を通したシステム監査能力向上の機会をご提供することを目的としております。特に内部監査人養成は企業の内部統制整備に欠かせない要件となっており、この機会を利用した監査実務の体験は短期間での養成に最適と考えます。今回の監査テーマは昨年度と同様に「現行システムとユーザニーズの適合性、経営戦略と情報システムとの適合性」という、経営者の視点に立ったテーマと致しました。
お申し込み		HPでご案内中です。 （http://www.saaj.or.jp/shibu/kinki/taiken20151024.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』

【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 8 月例会 8/25（火）開催予定 19:00-20:40(受付開始：18:30) 2015 年 9 月例会 9/30（水）開催予定 18:30-20:10(受付開始：18:00) 2015 年 10 月例会 10/27（火）開催予定 19:00-20:40(受付開始：18:30) 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＞

2015.7

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

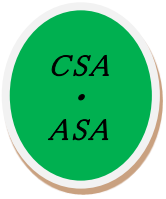
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

・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＞

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2015.7
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**
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 日　中間期会計監査	1 日　秋期 CSA･ASA 募集開始～9/30 24 日　第 205 回月例研究会 29-30 日　事例研:第 26 回システム監査実務セミナー(前半)	
9 月	10 日　理事会	12-13 日　事例研:第 26 回システム監査実務セミナー(後半) 15 日　第 206 回月例研究会	5～6 日　西日本支部合同研究会 (開催場所:岐阜)
10 月	8 日　理事会	23 日　第 207 回月例研究会	
11 月	12 日　理事会 13 日　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 日　2016 年度年会費請求書発送準備 23 日　会費未納者除名予告通知発送 30 日　本部予算提出期限	中旬　認定委員会:秋季 CSA 面接 19 日　第 208 回月例研究会 20 日　CSA･ASA 更新手続案内 〔申請期間 1/1～1/31〕 27 日　認定委員会:　CSA 面接結果通知	
12 月	1 日　2016 年度年会費請求書発送 2016 年度予算案策定 10 日　理事会:2016 年度予算案、 会費未納者除名承認 総会審議事項確認、 11 日第 15 期総会資料提出依頼(1/8〆切) 15 日　総会開催予告掲示 18 日　会計:2015 年度経費提出期限	10 日　CSA/ASA 更新手続案内メール 18 日　秋季 CSA 認定証発送	
2015 年	**以下は、過去に実施した行事一覧**		
1 月	7 日　16:00　総会資料(〆) 8 日　理事会:通常総会資料原案審議 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 26 日　総会申込受付開始(資料公表) 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 20 日　第 14 期通常総会･特別講演 25 日　法務局:資産登記、活動報告提出 28 日　年会費納入期限	CSA･ASA 春期募集(2/1～3/31) 28 日-3 月 1 日　事例研:第 25 回システム監査実務セミナー(前半)	
3 月	2 日　東京都への事業報告書提出 2 日　年会費未納者宛督促メール発信 12 日　理事会	4 日　第 200 回月例研究会 14-15 日　事例研:第 25 回システム監査実務セミナー(後半)	
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)	

■

＜目次＞

2015.7

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。8 月号から 11 月号までは、「システム監査人の喜び」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＞