認定 NPO 法人
日本システム監査人協会報
2018 年 6 月号
No 207
No.207（2018 年 6 月号）<5 月 25 日発行>

今月号の注目記事

『めだか【システム監査基準／システム管理基準について】』と『システム監査基準・管理基準の改訂作業について（2）』です。

写真提供：仲厚吉

巻頭言

『協会事務局長を拝命して』

会員番号 2581 斉藤 茂雄（事務局長）

第 17 期総会後の役員改選に続く理事役割分担再編成により、この度事務局長を拝命致しました。事務局長とは言ったものの名ばかりで、前事務局長が整備した詳細な事務マニュアルで目先の作業をこなしながら、ようやくよちよち歩きしているところです。

役職を拝命して、中長期の何か自分なりの目標を掲げなければと思いながら、無為に日々が過ぎてしまいます。しかし一つ思うのは、協会は創立 31 年になりますが、設立当時の先達の協会に掛けた情熱を忘れてはならないということです。今、事務局作業の傍ら、先輩が撮り貯めた総会や月例研究会などの 200 本近いビデオテープをデジタル化しています。ここには、当時の若々しい理事や会員が、システム監査や ICT の動向を懸命に学び、真剣に議論している姿があります。これら先輩の精神を絶やさず、更に一層世の中に貢献すべく、協会の発展のために力を尽くさなければならないと感じています。

協会の活性化については「システム監査活性化委員会」はじめ、各支部・部会・研究会がそれぞれの活動テーマを通じて大いにご努力されているところです。事務局としては皆様の活動の縁の下で、効率的で、効果的で、皆様が気持ち良く活動できるための環境整備と支援ができればまずは役割達成かと思いますが、皆様からのご提案があれば受け止め、展開する役割でもあると考えています。加えて、具体性のない話も宜しくないので、まずは自分ができることとして、例えば身の回りから一人でも多く入会を募り、有意な活動をしていただくことも大事な役割と考えているところです。

皆様の、事務局へのご支援・ご協力よろしくお願い致します。

以上

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。

<目次>

2018.5

めだか 【 システム監査基準／システム管理基準について 】

経済産業省より 2018 年 4 月 20 日付けで「システム監査基準」、「システム管理基準骨子」及び「システム管理基準」が公開され、次のように解説されている。

システム監査制度は、経済・社会において必要不可欠な情報システムに想定されるリスクを適切にコントロール・運用するための手段のひとつであり、経済産業省では、システム監査を実施する監査人の行為規範及び監査手続の規則を規定した「システム監査基準（平成 16 年 10 月 8 日改訂）」、システム監査人の判断の尺度を規定した「システム管理基準（平成 16 年 10 月 8 日改訂）」を策定し、公表しています。

しかし、両基準は公表から 10 年以上経過しており、管理基準の内容である IT ガバナンスや事業継続管理が国際規格化されるとともに、技術の進展に伴う新たな開発手法の発生等社会状況の変化が生じ、基準の改訂が喫緊の課題となっておりました。こうした状況を踏まえ、経済産業省は、「システム監査に関する検討会」を開催して改訂の検討を行い、有識者やパブリックコメントにおけるご意見等を踏まえ、「システム監査基準」及び「システム管理基準」を改訂いたしました。

また、「改訂のポイント」には、次のような趣旨が述べられている。

従来のシステム管理基準においても、「IT ガバナンス」の概念や業務継続計画について定めていましたが、その公開後、「IT ガバナンス」についての JISQ38500 や業務継続についての JISQ22301 等の国際規格が成立したため、これらの国際規格との整合性をとるとともに、米国における IT ガバナンスの規格であり、国際的に影響力を有する COBIT 等の内容を踏まえた見直しを行いました。

従来のシステム管理基準では、企画、開発、運用及び保守という概念を前提としたウォーターフォール型のシステム開発を前提としていましたが、短期間での反復した開発を行うアジャイル型のシステム開発における取扱いについても管理策として含め、また、クラウドの利用等を念頭に置いた、整理等の見直しを行いました。

従来のシステム監査基準及びシステム管理基準は、項目の詳細についての説明がなく、運用において、各項目の内容を解説した資料を参照することが必要となっていたため、今回の見直しにより、システム監査基準には「主旨」及び「解釈指針」を、システム管理基準には「主旨」及び「着眼点」を併せて記載することにより、基準の記載内容に基づく運用が行いやすくなるよう見直しを行いました。また、システム監査基準において、実務への適用を踏まえて監査実施の流れに沿った構成の見直しを行いました。

SAAJ では、5 月 19 日（土）午後に機械振興会館で「システム監査基準／管理基準の改訂について」をテーマにした第 232 回特別月例研究会を開催する。システム監査人として、受講したい研究会である。(空心菜)

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

<目次>

2018.5

【時事論評】サイバーセキュリティ教育の欺瞞と絶望

会員番号 0707 神尾博

1.「教えない」という欺瞞？

企業等の組織内部向けのセキュリティ教育資料が、IPA（情報処理推進機構）や IT ベンダにより出版され、中にはネットで無料配布されているものもある。中身を眺めると、比較的 IT 初心者にも理解しやすく、また主要なインシデントや対処法が一通りは網羅されているようだ。

ところが、どうも建前上は公言できない、すなわちタブー視されている事項というものも、多々あるように見受けられる。次節以降で適宜述べていくが、載録しないこと自体は作成者/発信者の総合的な判断という論理もあろう。しかし一方で知る権利という考え方からは、情報操作、すなわちある種の欺瞞という捉え方もありではないか。

そこで本稿において、こうした文書の中で触れられてはいないことに違和感を覚えたものの中から、いくつかを紹介し関係者に一石を投じておきたい。

2.サイバーセキュリティ経営ガイドライン

一般社員への教育について述べる前に、優先度から対経営幹部への啓蒙について見てみよう。まず頭に浮かぶのが、2016 年に公表された IPA の「サイバーセキュリティ経営ガイドライン」だ。内容は別にして、最も注目すべきは「法的拘束力がない」ことである。そうは言うものの、リーダーシップやリスク管理、インシデントへの対応の体制や手順の確立等の、ガバナンス/マネジメント部分については、世情/常識からいっても無視するわけにはいかないだろう。

一方で技術的な知識についてはどうだろうか？ネットには JR 宝塚線脱線事故の判決の例を挙げ、この国の司法は「経営幹部は物理学の法則への理解はなくてもよい」と考えているとの意見がある。この「文系脳は免罪符になっている」との見解が当を得ているなら、IT 分野においても適用される可能性は大である。

「経営者は SE 出身とは限らない。それほど熟知しなくても良いはず。いや不案内で通用するなら、わざわざ火中の栗を拾うことはない」と解釈し、このリスク「回避」を選択する経営者が現れることは、火を見るよりも明らかだ。

ところが「AI をビジネスにする/生かすなら、経営者は本質や技術への造詣/理解が必要」という意見も飛び交い始めた。さて「AI 技術は理解しているが、セキュリティはわかりません」が通用するだろうか？ここは法的リスクを「受容」の上で、AI とセキュリティの両方を自己啓発するか、教育を受けて頂くしかないだろう。

3.国家の諜報活動

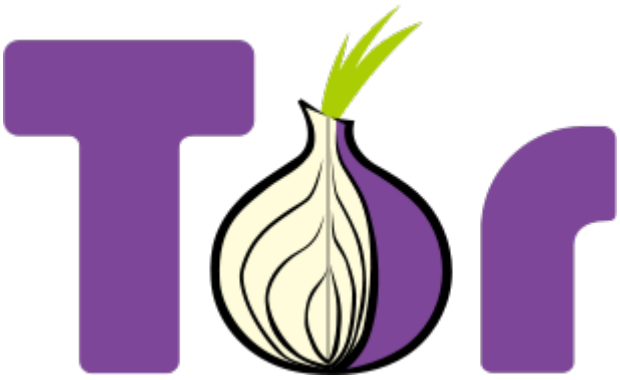
2013 年のスノーデンによる、NSA（アメリカ国家安全保障局）の大規模なネットの諜報活動の暴露は、全世界を震撼させた。日本では、NSA 程のすべての通信データの収集というわけでは無いが、1999 年の通信傍受法に加え、2017 年のテロ等準備罪へと、徐々に適用範囲が拡大されている。こうした国家の治安機構によ

る情報収集は、ビジネスや日常生活に直結するサイバーセキュリティの問題ではなく、国民の言動への監視の是非/程度という社会の在り様への捉え方であるから、セキュリティ教育には関係ないというご意見もあろうが、果たしてそう断言できるのだろうか。

実は 2018 年には欧州某国の外務省が、同国首相の海外訪問の際に同行する企業等に「持参する PC や携帯電話からは機密情報は削除しておくように」との指示を出している。傍受を想定してのものだという。わが国でも、無法地帯への出張に際しては、盗難のリスク対策のため同様の命令をしている政府機関や企業もあるだろう。海外支店での不正の証拠としてフォレンジック用の HDD を国外に持ち出そうとしたところ、盗賊に持って行かれた企業のエピソードを、数年前に聴講したことがある。国家はさておき、犯罪組織による通信の傍受や IT 機器の盗難については、海外出張者へはもれなく教育を実施しておくことが不可欠である。

4.深層ウェブと Tor

数年前と違い、この 2018 年現在では「深層ウェブ（Deep Web）」をご存知の方も多いだろう。一般の検索エンジンでは表示されない場所で、規模は表層ウェブの数百倍とも言われている。中でも闇ウェブ（Dark Web）は、麻薬、覚醒剤、拳銃等の取引や、性的な違法コンテンツが UP されている、いわゆるネットの無法地帯である。セキュリティ教育の場で「素人が無防備に覗くことは危険が伴う。したがって存在そのものについて触れるべきか？」は、意見が分かれるところだろう。



ところが、それ以上に悩ましい事案がある。深層ウェブへのアクセスは、Tor（トーア：The Onion Router）のような、オニオンプロトコルを実装したブラウザを使用するが、実はこのツールは匿名性確保にはきわめて有効な手段なのだ。簡略に説明すると、目的の通信先/相手へダイレクトではなく、それぞれの秘密鍵を持つ何人かをリレーしながら、対応する公開鍵を使った多層の暗号を解除していくという方式である。ネット上のデータ量が十分に多ければ、通信経路の秘匿が可能という。ただし通信内容の秘匿には TLS（Transport Layer Security）等と組み合わせる必要がある。つまり送信元すらも隠したい通信については、理論上は「Tor を使え」は、技術論としてはまさしく正解なのである。

一方で、Tor のような技術が存在することについては、一般社員と異なり、システム運用/セキュリティ管理者には、必須の知識であることは疑いようもないだろう。

5.チップ内バックドア

2018 年初頭の CPU 脆弱性騒動については記憶に新しいが、これはメーカサイドの意図しないバグに起因するものである。一方ですでに 2010 年以前から、ハードウェアに故意に仕組まれるチップ内バックドアの可能性も、取り沙汰されていた。たとえば、米国防総省の元幹部は著書の中で、政府機関や電気通信事業者での、通信機器の選別/使用制限の必要性について言及している。やっかいなことに、一般にこうした脆弱性はハードウェア交換でしか対処できない。

2005 年にパソコン事業を売却した IBM 社内では、2015 年から MAC への切り換えが進んでいる。ヘルプデスク利用者の大幅削減効果があるというが、国外製の不正回路対策ではないかという疑念も浮かぶ。Apple 社は、FBI（連邦捜査局）の「iPhone へのロック解除機能の開発命令」を拒否しているくらいのツワモノだからだ。一方で東アジア製のスマホについては、2014 年頃から相次いでバックドアの発覚が報道されている。ところがわが国では、政府機関や自治体等が「バックドアの発覚歴のあるメーカの製品は使うな」とは、公式にはなかなか発言できないだろう。貿易摩擦や外交問題に発展しかねないためだ。

個人の場合は購入機器の嗜好の問題だが、一般組織では一考を要するテーマだ。たとえば、確かに Windows パソコンの特定ベンダ・特定機種への統一は、MAC 程では無いにしろ、内部向けヘルプデスク等の運用コストの削減への寄与が期待できる。しかし、その場合でもリスクアセスメントの実施と経営幹部への報告は言わずもがな、リスク洗い出しはサイバー戦争の際の社内パソコン全滅にまで、視野に入れたものでなければならない、そういう時代の到来だろう。

6.「教えられない」という絶望？

概して「教えるリスク」が「教えないリスク」より強大な場合は、教えないという選択が定石である。もっともその場合は、もはや「教育」にはならないが。

締め括りに、情報漏洩に関する教育のジレンマについて述べておく。セキュリティ教育の場では、当人が監視されている事実と罰則を教えるのが、統計上の裏付けからも極めて有効であると言われている。だが、たとえば不正競争防止法等、情報漏洩を取り締まる法律が少ない現状を、これとセットで説明してしまっては、むしろ「合法の範囲内なら OK」と寝ている子を起こすことにもなりかねない。逆に触れなければ、会場にこうした事情をよく理解している聴講者がいた場合には、質疑応答で講師が凍りつくこともあり得る。この類の課題/疑問は枚挙に暇がない。なお、情報漏洩前提時代における教育以外の対処については、機会があれば後日改めて採りあげてみたい。

最後に、今回の論考を通じ、サイバーセキュリティ教育が奥の深いテーマであることを改めて思い知らされたという所感とともに、本稿作成に際して貴重なご助言を頂いた安本哲之助氏への謝辞も付け加えておきたい。

（このコラム文章は、記事提供者の個人的な意見表明であり、SAAJ の公式見解ではありません。画像の出典はウィキメディア・コモンズです。：Picture by The Tor Project, Inc.）

<目次>

2018.5

第２３０回月例研究会：講演録

テーマ：【残念な BCP とこれからの BCP】

会員番号 2574 竹原 豊和 （月例研究会）

【講師】東京海上日動リスクコンサルティング株式会社 ソリューション創造本部

主幹研究員 兼 立教大学 21 世紀社会デザイン研究科特任教授

指田 朝久 氏

【日時・場所】2018 年 3 月 14 日（水）18：30 – 20:30、機械振興会館 地下 2 階ホール（神谷町）

【テーマ】テーマ ： 「残念な BCP とこれからの BCP」

【要旨】

BCP の普及とともに策定された BCP が機能しないことも課題である。内閣府の事業継続ガイドラインも第三版に改訂されており、初期に策定した企業ではキャッチアップが必要である。

ここでは熊本地震での BCP の発動事例を紹介するとともに、機能しない BCP の課題を指摘し、残念な BCP を是正改善するための最新情報を提供する。

最後に内閣官房が開始した BCP に関するレジリエンス認証制度をご紹介する。

【講演録】

1．最近の製造・サービス停止事例

BCP は様々な企業や組織にて作成しているが、必ずしもうまくいかないのが実情である。2005 年に BCP のガイドラインが策定されたが、現在においては時代遅れな内容となっている。

BCP のテーマを考えた場合、「製品やサービスをいかに継続するか」となるが、最近の製品・サービス供給停止事例は多岐にわたる。「工場火災」「倉庫火災」「ワナクライ：コンピュータウイルス」「熊本地震」「テキサス州ハリケーン」「部品供給停止（政治的リスク）」「北海道じゃがいも不作」「博多道路陥没事故」「福井大雪」など様々である。

よくある BCP は「地震を想定している」が、地震以外でも製品やサービスの供給は停止する。

2．熊本地震を振り返る

熊本地震は他の震災と同様に多大な被害を出しているが、実は特異な地震となっており、震度 7 が 2 回、その他にも「水枯れ」や「長周期地震動階級 4（最大）」という状況があった。特に、この「長周期地震動階級 4（最大）」により、免震の建物が被災することとなった。免震の建物が被災することで、病院や庁舎が利用できなくなったのである。

熊本地震では様々なことが指摘されたが、その中でも「耐震性の無い市庁舎の被害」や「市町村の業務継続計画の問題」「学校教室などの避難者への提供と授業の再開への対応の遅れ」といった自治体における BCP に関する問題が露呈した結果となった。

当然、企業においても同様に BCP への考え方を改める必要性が出た地震であった。内閣府で「企業の事業継続に関する熊本地震の影響調査」が行われ、今後取り組みたいこととして 5 割以上の企業が BCP の見直し

の必要性を認識する結果となった。

3. 残念な BCP

BCP を策定することで BCP が機能すると思っているが、時代が経過し、機能しなくなった残念な BCP が増えてきている。BCP を策定しているはずなのに、うまくいっていないのである。

そんな残念な BCP の特徴として「経営者の BCM への関与度合いが低い」「適切な BCM 推進体制がされていない」「BCP と名前がついているが中身は防災計画」「既存の BCP の見直しができていない」「BCP の周知と教育ができていない」「継続的改善の仕組みができていない」「中小企業では BCP の策定率が低い」ことが考えられる。

残念な BCP の具体例をいくつか抜粋すると「優先順位がない」「代替戦略がない」「防災と BCP を勘違いしている」「BCP の文書量が膨大になっている（文書のメンテナンスができない）」「定期的な BCP の見直しが行われていない」「本社機能の継続性確保・強化がない（本社の被災を想定していない）」「グループ企業、取引先企業との連携に不備がある（全体的な指導ができない）」ことが挙げられる。

4. 事業継続のポイント

事業継続のポイントとして重要なことは「目標を定めるが、すべてに対応するわけではなく、優先順位を設定すること」となっている。また、BCP は防災ではなく、「被害にあう（被災）ことを前提として考える」ことも重要である。必要となる業務を予め選択し、代替を前もっと準備する必要があるのである。

BCP の普及率について考えた場合、大企業だと策定済が 60%となっているが、これが中堅企業の場合だと、30%となっている。特に都内中小企業の BCP 策定率は 6%となっており、中小企業における BCP への対応はまだ不足している状況となっている。

国の動きとしては 2013 年 6 月に内閣府事業継続ガイドライン（第三版）が策定されている。また、2015 年には市町村のための事業継続計画作成ガイド、2016 年には大規模災害発生時における地方公共団体の事業継続の手引きが策定され、2016 年 4 月には内閣官房レジリエンス認証制度（BCP の認証制度）がスタートしている。国際標準としても、BCP の認証規格として 2012 年 5 月に ISO22301 が制定されている。

BCP とは供給責任を果たすための事前対策のことである。したがって、どの顧客に、どの製品をいつまでに届けるか、ということを考える必要がある。分析検討のポイントにおいて「BIA」は非常に重要となる。すべての業務はできないため、誰を（どの顧客を）優先するか、何を（どの製品を）優先するか、をしっかりと検討する必要がある。但し、検討しそれを決定するのは経営者となる。現場レベルでそれを決定することは経営と反しており、「優先順位」「選択」はトップダウンにより実現する必要がある。

また、企業として「復旧をしない」「この業務は（被災を境に）停止する」という選択肢も十分に考えられる。業務停止時間が長い場合、影響が大きく顧客が戻ってこないこともある。非被災地の顧客がどれだけ待てるのか、ということは目標復旧時間を決める際には非常に重要であり、目標復旧時間はお客様目線で決めることが重要となる。

5. 事業継続の具体的取組事例

BCP の計画策定のポイントとして代替戦略と早期復旧戦略のふたつを考える必要がある。この際の代替戦略においては、被災していない別の場所での製造やサービス供給を行うこととなるが、そうなると中小企業単体での対応は難しくなる。この際に、「お互い様協定」といった形で同業他社と組む戦略もありえる。

具体的には、横浜市の企業と新潟市の企業でお互い様協定を結び、BCP における代替戦略としている。また、四国地方、中国地方・山陰地方の企業でも同様の取組が進められている。

BCP 戦略の作りこみとして、サプライチェーンのデータベース化とシミュレーションを実施していることや、特注品から汎用品へと設計段階からの検討などを行っている最先端事例がある。また、緊急設計変更を行うための設計要員の増員を検討し、人材育成へも力を入れている事例もある。この場合、平時の特需の際にも対応ができるため、企業にとっては BCP が特需対応の有用な対策となっている。また、ある漁協では販路の代替確保を行っている事例もある。

BCP を策定するもしないも企業の自己責任であるため、BCP を策定しないという選択肢もあると考える。但し、サプライチェーンを考えた場合には BCP の策定が発注要件になりつつあるし、地場産業等の場合、自治体を含めた協力体制が構築されるため、各企業に求められる BCP は何であるかというのも踏まえて策定を検討していく必要がある。

6. レジリエンス認証制度

レジリエンス認証制度は 9 つの項目からなる認証制度となっており、少なく、わかりやすい項目であるが、しっかりとポイントをおさえている項目となっている。

レジリエンス認証制度の狙いとしては、「継続的に運用できる能力に着目」と「BCP の代替戦略を確認」することとなっている。継続的に運用できる能力の中には「見直しできる能力」「運用の中核人物の能力・コンピテンシーに注目」「人材育成と組織力を担保する訓練に注目」という重要ポイントがあり、BCP の内容を確認する訓練をしっかりとおこなっていることや、経験と知識がある要員が BCP 関連の事務局に在籍しているか、ということも審査対象としている。

7. まとめ:これからの BCP

これからの BCP を考える際に、「今の BCP が本当の BCP かどうか、機能しているかどうかを見直す」必要がある。BCP の主体は経営者・事業部門であり防災部門が実施するものではない。

また、代替戦略として特殊製品だけではなく、汎用品を活用していくことも重要となる。BCP は定期的な見直しも必要であり、その際の目標復旧時間は必ず顧客目線で決定することが重要である。

BCP は経営者と社員が一貫となって取り組むこと、そして BCP は企業にとってなんのために存在しているのか、優先すべき製品・サービスは何か、必要な定期訓練やその見直しは行っているかについてもしっかりと考える必要がある。

最後に、内閣府事業継続ガイドライン第三版等の最新のガイドラインを活用して勉強をしていくことも重要であり、オールリスクと代替戦略について留意し、正しい BCP を策定、運用していくことが重要と考える。

【所感】

今回の御講演の中では「熊本地震」という我々に身近な災害を事例としてお話しいただき、普段から災害やBCP について意識はしているが、今まで以上に BCP の重要性を肌で感じることとなった。

私自身、特に重要に感じたキーワードは「優先順位付け」と「代替戦略」であるが、そもそも BCP は被災したことを大前提として考えていく必要があるため、どのように被害を最小にするか、ではなく被害にあった場合において、どのように製品やサービスを継続していくか、という視点で考える必要性を切に感じた。

システム監査という視点で考えた場合、BCP を継続的改善が行える体制になっているのか、防災視点での BCP となっていないだろうか、という部分が非常に大事になるのではないか、と感じた。

以 上.

<目次>

2018.5

本部報告 PMS 要求事項【JIS Q 15001:2017】と「個人情報取扱規程」の事例 管理策 3

会員番号 1760 斎藤由紀子 （個人情報保護監査研究会）

旧 JIS では、”事業者の代表者”としていた用語は、新 JIS で、”トップマネジメント”に変更されました。用語は変わりましたが、PMS におけるトップマネジメントの責任、個人情報保護管理者と個人情報保護監査責任者が、組織内部に属するものでなければならないことは、旧 JIS の規格と変わりはなく引き継がれています。なお、内部規程に”代表者”と記述されているものを訂正することまでは求めていません。
今回も、附属書 A（規定）および附属書 B（参考）の要求事項を確認しつつ、できるかぎりシンプルな規程として「3300 個人情報取扱規程」のサンプルをご紹介したいと思います。

※ この連載を基にした HTML 版を公開しています。
規格本文＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/000JISQ15001_2017.html
管理策 1＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/001JISQ15001_2017.html
管理策 2＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/002JISQ15001_2017.html
管理策 3＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/003JISQ15001_2017.html
引用：日本規格協会「日本工業規格 JIS Q 15001:2017 個人情報保護マネジメントシステム要求事項」

赤字：【2006 年版 JIS】から追加、変更となった規格

青字：PMS 監査研究会のコメント

A.3.3.4	資源、役割、責任及び権限 2006：3.3.4	トップマネジメントは、少なくとも、次の責任及び権限を割り当てなければならない。 トップマネジメントは、この規格の内容を理解し実践する能力のある個人情報保護管理者を組織内部に属する者の中から指名し、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。 個人情報保護管理者は、個人情報保護マネジメントシステムの見直し及び改善の基礎として、トップマネジメントに個人情報保護マネジメントシステムの運用状況を報告しなければならない。 トップマネジメントは、公平、かつ、客観的な立場にある個人情報保護監査責任者を事業者の組織内部に属する者の中から指名し、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。 個人情報保護監査責任者は、監査を指揮し、監査報告書を作成し、トップマネジメントに報告しなければならない。監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保しなければならない。
	附属書 B.3.3.4	"資源"とは、個人情報保護マネジメントシステムの確立、実施、維持及び継続的改善に必要な資源（本文の 7.1）であり、具体的には人員、組織の基盤（規程、体制、施設、設備など）、資金などをいう。 個人情報保護管理者は、個人情報保護マネジメントシステムを理解し、実施・運用できる能力をもった者であることが望ましい。 個人情報保護管理者は、当該組織に係る個人情報の管理の責任者である性格上、いたずらに指名する者を増やし、責任が不明確になることを避けることが望ましい。したがって、事業部が複数あり個人情報保護管理者を複数名指名する場合には、当該者間での役割分担を明確にすることが望ましい。 個人情報保護管理者は、社外に責任をもつことができる者（例えば、役員クラス）を指名することが望ましい。 個人情報保護監査責任者は、社外に責任をもつことができる者（例えば、役員クラス）であって、個人情報保護管理者と同格又は上席者の中から指名されることが望ましい。

	【P マーク審査のポイント】 ・**「個人情報保護体制」（体制図）の整備** 個人情報保護管理者は、トップマネジメントの代理者として、また個人情報保護監査責任者は、トップマネジメントからの任命により監査を行う立場であることが体制図に示されていることが重要です。 また体制図には「個人番号関係事務責任者」「個人番号関係事務担当者」を含めておく必要があります。 ・**「PMS に関する責任と権限一覧表」の整備** 旧 JIS（2006 年版）では、個人情報管理台帳の承認者、リスク分析表の承認者、各ただし書き適用時の承認者、苦情対応の承認者、是正処置立案の承認者など、各フェーズにおいて承認者が誰かを規定しているかどうかを審査していました。新 JIS では、あらためて「PMS に関する責任と権限一覧表」を整備しておけば、各項目で規定せずとも問題ないことが明確にされています。　ただし、各フェーズで規定されている内容を訂正する必要はありません。

【3300 個人情報取扱規程】サンプル

3.3.4　資源、役割、責任及び権限

当社は PMS を確立し、実施し、維持し、かつ改善するために役割、責任及び権限を定め、「3341-01 個人情報保護体制別紙：3341-02PMS に関する責任と権限一覧表」で文書化し、トップマネジメントの承認を得て、従業者に周知する。またその管理に必要な資源を用意する。

2　トップマネジメントは、経営最高責任者として個人情報保護に関するすべての責任と権限をもつ。

3　個人情報保護管理者は、トップマネジメントに PMS の見直しおよび改善の基礎として PMS の運用状況を報告する。

4　個人情報保護管理者は、個人情報の取り扱いを総括するために「事務局」を設置し、事務局長を任命する。

5　個人情報保護管理者は、リスクの顕在化又はそのおそれがあると判断した場合は、個人情報の取り扱いを監督するために、全社の各部門の責任者を対象に「管理委員会」を招集することができる。

■

A.3.3.5	内部規程 2006： 3.3.5	組織は、次の事項を含む内部規程を文書化し、かつ維持しなければならない。 a)個人情報を特定する手順に関する規定 b)法令、国が定める指針その他の規範の特定、参照及び維持に関する規定 c)個人情報保護リスクアセスメント及びリスク対策の手順に関する規定 d)組織の各部門及び階層における個人情報を保護するための権限及び責任に関する規定 e)緊急事態への準備及び対応に関する規定 f)個人情報の取得、利用及び提供に関する規定 g)個人情報の適正管理に関する規定 h)本人からの開示等の請求等への対応に関する規定 i)教育などに関する規定 j)文書化した情報の管理に関する規定 k)苦情及び相談への対応に関する規定 l)点検に関する規定 m)是正処置に関する規定 n)マネジメントレビューに関する規定 o)内部規程の違反に関する罰則の規定 組織は、事業の内容に応じて、個人情報保護マネジメントシステムが確実に適用されるように内部規程を改正しなければならない。
	附属書 B.3.3.5	“内部規程を文書化し、かつ、維持する”とは、手順として確立したルールを文書化しておくことによって担当者が変わっても個人情報保護水準の継続性が保つことをいう。ルールが明文化されていないことも個人情報保護リスクの一つである。 内部規程の文書化には、A.3.3.3 によって実施した個人情報保護リスクの特定・分析及び対策に基づく手順の文書化が含まれる。個人情報保護リスクの特定が十分になされていればその対策を内部規程として文書化する作業は容易である。内部規程の文書化とは、基本となる規程を形式的に定めるだけでなく、それを受けて細則、マニュアル、チェックリストなどを作成し、どのような行為をなすことが望ましいか、又は望ましくないのか、従業者が具体的に規範を参照できるように構成することである。内部規程は、必ずしも形式的に一本化される必要はなく、例えば、内部規程の違反に関する罰則は、就業規則で規定してもよい。

		A.3.3.5d)は、個人情報を保護するための組織規程を含む。組織規程には、組織の各部門及び階層における権限及び責任が含まれる。
	【P マーク審査のポイント】 ・新 JIS 規格の付属書 A では、A.3.7.3 マネジメントレビュー、A.3.8　是正処置　となりました。しかし、A.3.3.5 では、旧 JIS からの移行を考慮し、m)是正処置に関する規定、 n)マネジメントレビューに関する規定と順序が逆になっています。規程は組織が定める規程体系でよく、どちらでもかまわないとされています。 ・o)罰則の規定としては、「個人情報取扱規程」等で、” 当社の PMS に故意に違反した者、あるいは自らの職務を適正に遂行しなかった従業者（協力会社員は除く）は「就業規則」に従い懲戒の対象となるとともに、会社に損害を与えた場合は、損害賠償請求を行うことがある。”と規定しておくとよいでしょう。	

【3300 個人情報取扱規程】サンプル

3.3.5　内部規程

JIS Q 15001:2017 要求事項		該当規程・様式
a)	個人情報を特定する手順に関する規程	「3300 個人情報取扱規程」3.3.1 「3305 個人番号関係事務規程」
b)	法令、国が定める指針その他の規範の特定、参照及び維持に関する規程	「3300 個人情報取扱規程」3.3.2 「3320 法令・指針・規範集」
c)	個人情報リスクアセスメント及びリスク対策の手順に関する規定	「3300 個人情報取扱規程」3.3.3
d)	当社の各部門及び階層における個人情報を保護するための権限及び責任に関する規程	「3300 個人情報取扱規程」3.3.4 「3341PMS に関する責任と権限一覧表」
e)	緊急事態(個人情報が漏えい、滅失又はき損をした場合)への準備及び対応に関する規程	「3300 個人情報取扱規程」3.3.7
f)	個人情報の取得、利用、及び提供に関する規程	「3300 個人情報取扱規程」3.4.2.1～3.4.2.9、4 「3305 個人番号関係事務規程」
g)	個人情報の適正管理に関する規程	「3300 個人情報取扱規程」3.4.3 、「3430 安全管理規程」
h)	本人からの開示等の請求等への対応に関する規程	「3300 個人情報取扱規程」3.4.4、4
i)	教育などに関する規程	「3300 個人情報取扱規程」3.4.5
j)	文書化した情報の管理に関する規程	「3300 個人情報取扱規程」3.5
k)	苦情及び相談への対応に関する規程	「3300 個人情報取扱規程」3.6
l)	点検に関する規程	「3300 個人情報取扱規程」3.7
m)	トップマネジメントによる見直しに関する規程	「3300 個人情報取扱規程」3.7.3
n)	是正処置に関する規程	「3300 個人情報取扱規程」3.8
o)	内部規程の違反に関する罰則の規程	「3300 個人情報取扱規程」5、「就業規則」

■

A.3.3.6	計画策定 2006：3.3.6	組織は、個人情報保護マネジメントシステムを確実に実施するために、少なくとも年一回、次の事項を含めて、必要な計画を立案し、文書化し、かつ、維持しなければならない。 a)A.3.4.5 に規定する事項を踏まえた教育実施計画の立案及びその文書化 b)A.3.7.2 に規定する事項を踏まえた内部監査実施計画及びその文書化
	附属書 B.3.3.6	計画は、組織における内部及び外部の課題、並びに利害関係者からの要求事項を踏まえて、長期、中期、短期に策定されることが望ましい。A3.3.6 は、PMS の計画策定に当たり、最低限求められる事項について定めている。 “必要な計画”には、教育、内部監査、安全管理計画（情報セキュリティ対策）、委託先の監督、マネジメントレビュー実施のための具体的な計画を含む。 計画の“文書化”とは、実施のための具体的な計画を、計画書として文書化することをいう。どのような計画書を作成するかについては、A.3.7.3 のマネジメントレビューで把握された課題も踏まえ、組織の置かれた状況などを勘案して、個別に必要性を検討することが望ましい。 A.3.3.6a)の、“教育実施計画書”は、研修の年間カリキュラム、個別の研修プログラム（研修名、開催日時、場所、講師、受講対象者及び予定参加者数、研修の概要、使用テキスト、任意参加か否かの別など）、予算などによって構成する。 “A.3.4.5 に規定する事項を踏まえた教育実施計画”とは、A.3.4.5 の管理策を満たすために具体的な計画を策定することをいう。 A.3.3.6b)の“内部監査実施計画書”は、当該年度に実施する監査テーマ、監査対象、目的、範囲、手続、スケジュールなどによって構成する。

		“A.3.7.2 に規定する事項を踏まえた内部監査実施計画”とは、A.3.7.2 の管理策を満たすよう具体的な計画を策定することをいう。 なお、内部監査の計画には、前回までの見直しの結果についてのフォローアップを含めてもよい。
	【P マーク審査のポイント】 ・計画の種類 ・年間計画書（教育、内部監査、安全管理対策、委託先監督、マネジメントレビュー） ・個別計画書（教育、内部監査） ・計画には、次の事項を含んでいること。 a)実施事項 （対象、実施日、場所、内容・・） b)必要な資源（テキスト、チェックリスト、担当者・・） c)責任者 d)達成期限 e)結果の評価方法（評価表、テスト、アンケート、報告書） ・計画は進捗管理し、結果を評価して、次年度の計画立案を行うこと。	

【3300 個人情報取扱規程】サンプル

3.3.6 計画策定

当社は PMS を確実に実施するために必要な教育、監査などの計画を立案し、トップマネジメントの承認を得て文書化し、維持する。

関連文書：「3303PMS 年間計画書（兼点検表）」
「3451PMS 教育計画書（兼報告書）」
「3721PMS 監査計画書（兼報告書）」

■

A.3.3.7	緊急事態への準備 2006：3.3.7 法第 46 条: 事業所管大臣 法第 47 条: 認定個人情報保護委員会 法第 61 条: 個人情報保護委員会	組織は、緊急事態を特定するための手順、及び特定した緊急事態にどのように対応するかの手順を確立し、実施し、かつ、維持しなければならない。 組織は、個人情報保護リスクを考慮し、その影響を最小限とするための手順を確立し、かつ、維持しなければならない。 また、組織は、緊急事態が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持しなければならない。 a)当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知するか、又は本人が容易に知り得る状態に置くこと。 b)二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること。 c)事実関係、発生原因及び対応策を関係機関に直ちに報告すること。
	附属書 B3.3.7	緊急事態を特定するための手順及び特定した緊急事態にどのように対応するかの手順（対応手順）の策定に当たっては、次のような事項を考慮することが望ましい。 －緊急事態及び事故が最も起こりやすい場面 －予想される被害の規模 －被害を最小限に抑えるための一次的な対処方法 －組織内の緊急連絡網及び組織外への報告手順の確立 －再発防止処置を実施する手順 －緊急時対応についての教育訓練 A.3.3.7 の a)～c)の事項を実施するに当たっては、例えば、どのような場合にどのような手順になるか、法令等に従って対応を定め、その対応に従い実施することが望ましい。 A.3.3.7b)の事案の公表に際しては、公表によって本人などへの二次被害を招かないように、被害の重篤性を踏まえたうえで、公表する内容、手段及び方法を考慮することが望ましい。また、個人情報の取扱いの全部又は一部を受託している受託者については、委託契約において何ら取決めがない場合は、委託者と相談の上実施することが望ましい。 ＝＝表 B.1 表示事項整理表＝＝ 本人に速やかに通知するか、又は本人が容易に知り得る状態に置く □当該漏えい、滅失又はき損が発生した個人情報の内容 可能な限り遅滞なく公表する。 □事実関係、発生原因及び対応策
	【P マーク審査のポイント】 ・「緊急事態発生」時には、代表者の指揮のもとで、規定した対応手順が実施される必要があります。	

	・「本人への連絡」は最優先とし、二次被害防止の観点から必ず本人に伝わる手段でなければなりません。 ・「個人情報保護委員会」について： ・法的に公正取引委員会と同列の権限を持つ。 ・旧 JIS（2006 年版）で規定していた主務大臣への報告は廃止され、事業者への監督権限が「個人情報保護委員会」に一元化された。ただし、法第 44 条、法第 46 条により、金融庁長官、厚生労働大臣、国土交通大臣、国家公安委員会等の事業所管大臣に権限が委任されることができるとされた。 ・事業所管大臣は、その権限をさらに下位組織に委任することができる。 ・事故発生時の報告先機関は、法第 47 条（認定個人情報保護団体）、もしくは法 61 条（個人情報保護委員会）により明確にされました。加えて、審査を受けた機関（JIPDEC または各指定審査機関）に報告する必要があります。 ・「運用の確認の記録」に、緊急事態が発生したかどうか、発生した場合は規定した通りに対処が行われたかどうか、を含める必要があります。 ・最終的に「是正処置」の手順によって根本的な再発防止策が実施されなければなりません。

【3300 個人情報取扱規程】サンプル

3.3.7 緊急事態への準備・対応

個人情報に関する事故の発生を監視し、検知し、事故が発生したときには緊急対応し、復旧するための手順を確立し、実施し、かつ維持する。

3.3.7.1 緊急事態の定義

個人情報が漏えい、滅失又はき損をした場合に想定される経済的な不利益および社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とする。そのため、事故・事件の影響度に応じて以下の３つのレベルに区分けし定義する。なお、委託先で発生した事故・事件についても同様に取扱う。

レベル	影響度（起こりやすい場面）	予想規模	責任者
A	1.個人情報が社外へ流出（紙、電子データ） 2.個人情報を滅失又はき損しサービス不能状態が継続 3.影響範囲が特定できず被害が拡大するおそれ	多数の顧客	トップマネジメント
B	1.個人情報が社外へ流出（回収可能） 2.個人情報を滅失又はき損しサービス不能状態（短時間） 3,影響範囲が特定でき被害が拡大のおそれがない	特定の顧客	トップマネジメント
C	上記に相当する事態が発生したが、事前に検知した。 その結果、外部顧客、取引先に影響ないと判明した。	被害なし	個人情報保護管理者

3.3.7.2 緊急事態の体制

トップマネジメントは、緊急事態発生時に指揮をとり早期解決を図る。各部門長（管理者）、連絡先（内線番号、携帯電話番号）および具体的な分担は「3371 緊急時連絡網」に従う。

2 各部門長は、「3371 緊急時連絡網」および「3373 事故報告書」を常時使用できるよう準備しておかなければならない。

3 個人情報保護管理者は、「3371 緊急時連絡網」を、毎年事業年度開始日、および組織変更時に見直し、各部門長に配布する。

3.3.7.3 緊急事態発生時の措置

緊急事態発生の発見者は、ただちに部門長に報告しなければならない。以後は下記の手順に従う。

a) 緊急事態発生の報告を受けた部門長は、「3373 事故報告書」の発生速報欄に記入し、「3371 緊急時連絡網」に従って、速やかに個人情報保護管理者に報告する。
b) 個人情報保護管理者は、3.3.7.1 項のレベルＡ、Ｂ、Ｃのいずれに該当するかを判断し、「3373 事故報告書」に追記してトップマネジメントに報告する。
c) トップマネジメントは「緊急対策会議」を招集し、以下の措置について、実施の可否および方法を決定する。

1	本人への連絡（必須）	当該漏えい、滅失又はき損が発生した個人情報の内容を本人に速やかに通知（訪問、電話、メール、郵送など）し、又は本人が容易に知り得る状態（HP掲載など。ただし個人名は非公開）におく。
2	関連会社	親会社、取引先、委託元、提供元、関連会社、グループ会社など
3	関係機関（必須）	個人情報保護委員会、認定個人情報保護団体、審査機関（JIPDEC など）
4	警察	サイバーテロ等のおそれがある場合
5	公表	二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因および対応策を遅滞なく公表する。 ・社内通知 ・自社ＨＰ公表 ・マスコミ発表

d) 特定個人情報の事故が発生した時は、個人情報保護委員会規則第５号「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」を確認し個人情報保護委員会への報告の要否を判断のうえ対応する。

e) 個人情報保護管理者は、前項で講じると決定した措置のために「謝罪文」「公表文」などを作成し、トップマネジメントの承認を得て実施する。

f) 講じると決定した措置は、緊急事態発生後の状況の変化に応じて、速やかに追加措置を講じなければならない。

3.3.7.4 再発防止措置

個人情報保護管理者は、緊急事態が収まり又は最悪の状態から脱した時期に、レベルＡ、Ｂ、Ｃを問わずすべての緊急事態発生について、類似案件が再発しないよう以下の措置を講じる。

a) 緊急事態を発生させた部門長に「3801 是正処置報告書」の作成を指示する。

b) 「3801 是正処置報告書」によって策定、実施された再発防止策について、緊急事態発生部門、および同様の事態が発生する可能性のある部門に対し、臨時の社内教育を実施する。

3.3.7.5 関係機関への事故報告

個人情報保護管理者は、緊急事態が収まり又は最悪の状態から脱した時期に、レベルＡ、Ｂ、Ｃを問わずすべての緊急事態発生について、「3373 事故報告書」を作成し、トップマネジメントの承認を得たうえで「3371 緊急時連絡網」に従い、審査機関である一般財団法人 日本情報経済社会推進協会（JIPDEC）プライバシーマーク事務局事故担当に提出する。

2 あわせて、「3371 緊急時連絡網」に従い、認定個人情報保護団体に報告する。

3 個人番号の漏えいに関する事故の場合は、「3371 緊急時連絡網」に従い、個人情報保護委員会に報告するとともに、一般財団法人 日本情報経済社会推進協会（JIPDEC）プライバシーマーク事務局事故担当に報告する

3.3.7.6 緊急事態に関するマネジメントレビュー

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

■

次回は、3.4 実施及び運用 から考察します。

以上 ■■

<目次>

2018.5

本部報告 システム監査基準・管理基準の改訂作業について（２）

会員番号 0555 松枝憲司（IT アセスメント研究会）

１．システム監査基準・管理基準の公開

システム監査基準及び管理基準が 2018 年 4 月 20 日に公開されました。
http://www.meti.go.jp/policy/netsecurity/sys-kansa/h30kaitei.html
公開された資料は以下の 10 点です。

(1) システム監査基準
(2) システム管理基準（骨子）
(3) システム管理基準
(4) 参照 1 情報セキュリティ管理基準参照表
(5) 参照 2 システム監査基準新旧対照表
(6) 参照 3 システム管理基準新旧対照表
(7) 参照 4 システム監査に関する検討会構成員名簿及びワーキンググループ構成員名簿
(8)「システム監査基準（案）」 及び「システム管理基準（案）」に対する意見公募の結果について
(9) 別紙 1 パブリックコメントの概要及びご意見に対する考え方（システム監査基準）
(10)別紙 2 パブリックコメントの概要及びご意見に対する考え方（システム管理基準）

2. システム監査基準の概要

[1]システム監査の意義と目的

システム監査を次に様に定義している。「システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型である。」また、システム監査の目的を「情報システムにまつわるリスク（以下「情報システムリスク」という。）に適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすこと」としている。従前の基準には、システム監査の定義はなく目的のみ記述されていた。

[2] システム監査基準の意義と適用上の留意事項

情報報システムの安全性、信頼性、準拠性のみならず、戦略性、有効性、効率性等の監査もカバーし、かつ、中小規模の企業や、各府省庁、地方公共団体等、各種組織体が各種目的をもってシステム監査を行う場合にも利用できる、としている。

[3] システム監査上の判断尺度

原則として「システム管理基準」又は当該基準を組織体の特性や状況等に応じて編集した基準・規程等を利用することが望ましい。他のガイドラインや組織体独自の諸規程・マニュアル等を、システム監査上の判断尺度として用いることもできる。特に、情報セキュリティの監査に際しては、「システム管理基準」とともに、「情報セキュリティ管理基準」を参照する。

また、本監査基準の記述形式については、システム監査の実施に際して遵守が求められる「基準」を「しなければならない」と記述し、各基準の補足的な説明や、実務上の望ましい対応や留意事項を「解釈指針」として記述した。

【基準１】システム監査人の権限と責任等の明確化

システム監査の実施に際しては、その目的及び対象範囲、並びにシステム監査人の権限と責任が、文書化された規程等又は契約書等により明確に定められていなければならない。

【基準２】監査能力の保持と向上

システム監査の品質を高め、組織体の状況や IT 環境の変化等に対応して、効果的なシステム監査を実施するために、システム監査人は、適切な研修と実務経験を通じて、システム監査の実施に必要な知識・技能の保持及び向上に努めなければならないとあり、この解釈指針として、

(1)システム監査人に求められる基本的な知識・技能を習得するためには、システム監査技術者、CISA（公認情報システム監査人）等の試験や CSA（公認システム監査人）の認定制度の活用も考えられる。との記述があり、監査基準に当協会の CSA が取り上げられている。

【基準３】システム監査に対するニーズの把握と品質の確保

システム監査の実施に際し、システム監査に対するニーズを十分に把握したうえでシステム監査業務を行い、システム監査の品質が確保されるための体制を整備しなければならない。

次のようなニーズに基づいて、システム監査の目的が決定される、として監査ニーズと監査の目的と監査対象に関する例示がなされている。またシステム監査のニーズに応じて、公表されている各種基準・ガイドライン等を適切に選択し、必要に応じて組み合わせて、判断尺度とすることが望ましいとしている。

【基準４】システム監査人としての独立性と客観性の保持

システム監査人は、監査対象の領域又は活動から、独立かつ客観的な立場で監査が実施されているという外観に十分に配慮しなければならない。また、システム監査人は、監査の実施に当たり、客観的な視点から公正な判断を行わなければならない。

【基準５】慎重な姿勢と倫理の保持

システム監査人は、システム監査業務の計画、実施、及び結果の報告において、システム監査の専門家としての慎重な姿勢で臨むとともに、倫理観を保持し、誠実に業務を実施しなければならない。

解釈指針の中には、「下記の各団体に所属、又は専門資格を認定されているシステム監査人は、各団体で要求される専門職としての職業倫理の遵守が求められる。」として 「特定非営利活動法人日本システム監査人協会」の名前が取り上げられている。

【基準６】監査計画策定の全般的留意事項

システム監査人は、実施するシステム監査の目的を効果的かつ効率的に達成するために、監査手続の種類、実施時期、及び適用範囲等について、適切な監査計画を立案しなければならない。監査計画は、状況に応じて適時に変更できるように弾力的なものでなければならない。

解釈指針として、

(1)監査計画の、中長期計画、年度計画及び個別監査計画に関する説明や、

(2)アジャイル開発手法を採用するシステム開発プロジェクトなどでは、アジャイル開発手法の本来の意義を損なわないように留意しつつ、監査実施のタイミング、サイクル、作業負荷及び監査証拠の範囲･種類などを特定して計画を立案することとしている。

(3)監査計画の策定にあたっては、監査対象が情報システムのガバナンスに関するものか、情報システムのマネジメントに関するものか、あるいは情報システムのコントロールに関するものかを考慮して監査計画を立案することとしている。

【基準７】リスクの評価に基づく監査計画の策定

システム監査人は、システム監査を行う場合、情報システムリスク及びシステム監査業務の実施に係るリスクを考慮するリスクアプローチに基づいて、監査計画を策定し、監査を実施しなければならない。

解釈指針として、ここでいうリスクアプローチには２つの考え方があり、リスクの影響が大きい監査対象に重点的に監査資源を配分するというアプローチと、監査の結論を誤る可能性としての監査リスクを合理的に低い水準に抑えるというアプローチであるとしている。

【基準８】監査証拠の入手と評価

システム監査人は、システム監査を行う場合、適切かつ慎重に監査手続を実施し、監査の結論を裏付けるための監査証拠を入手しなければならない。

解釈指針として、１．システム監査においてシステム監査人は、個別監査計画に基づいて、監査手続を実施することによって、監査証拠を入手する。２．監査手続は、監査対象の実態を把握するための予備調査（事前調査ともいう。）、 及び予備調査で得た情報を踏まえて、十分かつ適切な監査証拠を入手するための本調査に分けて実施される、として予備調査、本調査について言及している。

監査手続の適用に際しては、チェックリスト法、ドキュメントレビュー法インタビュー法、ウォークスルー法、突合・照合法、現地調査法、コンピュータ支援監査技法などが利用できるとし、なかでもコンピュータ支援監査技法については、監査対象ファイルの検索、抽出、計算等、システム監査上使用頻度の高い機能に特化した、非常に簡単な操作で利用できるシステム監査を支援する専用のソフトウェアや表計算ソフトウェア等の利用等の技法を紹介している。

またアジャイル手法を用いたシステム開発プロジェクトなどでは、アジャイル手法を用いる開発現場に、監査対応のためだけのドキュメント作成に追加的な負荷をかけないような考慮が望ましい、としている。

また監査手続は、それぞれ単独で実施される場合もあるが、通常は、一つの 監査目的に対して複数の監査手続の組み合わせによって構成される、として複数の監査手続きが例示されている。

【基準９】監査調書の作成と保管

システム監査人は、監査の結論に至った過程を明らかにし、監査の結論を支える合理的な根拠とするために、監査調書を作成し、適切に保管しなければならない。

【基準１０】監査の結論の形成

システム監査人は、監査報告に先立って、監査調書の内容を詳細に検討し、合理的な根拠に基づき、監査の結論を導かなければならない。

監査報告書における指摘事項とすべきと判断した場合であっても、監査調書に記録されたシステム監査人の所見、当該事実を裏づける監査証拠等について、監査対象部門との間で意見交換会や監査講評会を通じて事実確認を行う必要がある。

【基準１１】監査報告書の作成と提出

システム監査人は、監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。

システム監査報告書の作成に際しては、正確性、客観性、簡潔性、明瞭性、理解容易性、適時性に留意する。さらに、表現が敵対的になることを避け、建設的なものとすることを心掛ける必要がある。

留意事項として、(1)システム監査報告書は、システム監査の依頼者が当該報告書の主要読者となる点に留意し、経営陣を宛先とする場合には、詳細監査報告書とは別に、要約監査報告書を作成するなどの工夫が望ましい。なお、要約監査報告書では、監査の専門用語及び実施した監査の詳細な記載はできる限り避けることが望ましい。(2)システム監査報告書の作成に際して、業務監査に関する監査報告書と一体のものとして作成することが効果的な場合がある。(3)システム監査報告は、文書で作成することを原則とするが、緊急を要する場合には口頭で報告を行うこととし、後日、監査報告書を提出することができる。(4)ペーパレス化を行っている組織の場合は、プレゼンテーションソフトを利する等、組織体の状況に応じて工夫する必要がある。

情報システムのガバナンスを対象としたシステム監査報告書等、監査報告の内容が組織体の経営に直結するとか、経営を脅かす重要なリスクとなりうるような場合には、ガバナンス機能を担う機関に対してシステム監査報告書を提出することが望ましい、としている。

また改善勧告の記載に際しては、重要改善事項と通常改善事項、あるいは緊急改善事項と中長期改善事項等、その重要度や緊急度に区別して記載すること。あわせて、改善に責任を有する担当部署を明確にする必要がある。(1)改善勧告の記載に際しては、改善事項のみならず、改善によって期待される効果等を記載することが望ましい。(2)監査対象について保証の付与と助言をあわせて行う場合、助言については、別途「助言報告書」等の表題を付した個別の報告書を作成することが望ましい、としている。

【基準１２】改善提案のフォローアップ

システム監査人は、監査報告書に改善提案を記載した場合、適切な措置が、適時に講じられているかどうかを確認するために、改善計画及びその実施状況に関する情報を収集し、改善状況をモニタリングしなければならない。

監査報告書に改善提案を記載した場合には、当該改善事項が適切かつ適時に実施されているかどうかを確かめておく必要がある。なお、システム監査人は、改善の実施そのものに責任をもつことはなく、改善の実施が適切であるかどうかをフォローアップし、システム監査の依頼者たる経営陣に報告することになる点に留意する。フォローアップは、発見された不備の重要性、改善対応に要する期間を含む改善の難易度、その他監査対象部門の状況に応じて弾力的に実施することが望ましい。監査対象部門は、改善提案のもととなった指摘事項の重要性に鑑み、当該指摘事項に関するリスクを受容すること、すなわち改善提案の趣旨を踏まえた追加的な措置を実施しないという意思決定が含まれる場合もある、としている。そしてシステム監査人による改善計画の策定及びその実行への関与は、独立性と客観性を損なうことに留意すべきである、としている。

以上

<目次>

2018.5

支部報告 【 近畿支部 第１７２回定例研究会 】

会員番号 0655 荒牧 裕一（近畿支部）

１．テーマ 「【JIS Q 15001:2017】～SAAJ 個人情報保護監査研究会の考察～」

２．講師 認定 NPO 日本システム監査人協会 副会長
個人情報保護監査研究会主査、プライバシーマーク主任審査員
斎藤 由紀子 氏

３．開催日時 2018 年 3 月 16 日（金） 18:30～20:30

４．開催場所 大阪大学中之島センター ２階 講義室 201

５．講演概要

講師は SAAJ 個人情報保護監査研究会の主査をされていますが、研究会では、2014 年 12 月の「６ヶ月で構築する個人情報保護マネジメントシステムハンドブック」（以下 PMS ハンドブック）の上梓後、2013 年 5 月 31 日の番号利用法制定、2015 年 9 月 9 日の個人情報保護法の改定を研究テーマとし、これら法令等の個人情報保護マネジメントシステム（以下、「PMS」という。）への影響を考察して、PMS ハンドブックの読書会員向けに、改定した規定、および様式を提供されてきました。

2017 年 12 月 20 日、日本規格協会から「個人情報保護マネジメントシステム－要求事項【JIS Q 15001:2017】」が発表されました。2018 年 3 月 1 日現在、その審査基準は十分に示されてはいませんが、研究会ではそれに基づいてできる限り客観的に、普遍的に、事業者が構築できる PMS を提案していこうと活動を行っています。

今回は、その成果の一部をご紹介いただきました。なお、講演の際に配布された資料は SAAJ 会報４月号の原稿であり、続きについても順次連載される予定です。

＜講演内容＞

（１） はじめに

【JIS Q 15001:2017】の附属書Ａ（規定）には、旧版（2006 年版）の本文に存在していた、「～すること」等の管理策が示されており、2018 年 8 月 1 日より、プライバシーマーク付与適格性審査においては附属書Ａが基準となる。また、附属書（参考）には、附属書Ａの管理策に関する補足が記載されている。これは 2006 年版規格解説に当たるもので、「～することが望ましい」ことが示されている。PMS をより効率的に確実に運用するために、附属書Ｂは大いに参考になる。

今回は、これらを踏まえた個人情報取扱規定のサンプルを見ながら、プライバシーマーク（以下、「Ｐマーク」という。）審査において事業者が勘違いしやすいポイントを説明していきたい。

（２） 適用範囲、用語の定義

PMS の適用範囲は、2006 年版と変更なく、事業者単位である。

用語の定義については、「個人情報保護法による」とされたことにより、PMS としての用語が省略された。

（３） 一般要求事項、個人情報保護方針

トップマネジメントへのインタビュー項目として、①個人情報保護目的を説明できること、②内部向け個人情報保護方針を文書化した情報を、組織内に伝達し、必要に応じて、利害関係者が入手可能にするための措置を講じていること、③外部向け個人情報保護方針を文書化した情報について、一般の人が入手可能な措置を講じていること、等が挙げられる。

内部向け個人情報保護方針には、方針の内容についての問い合わせ先掲載については問わない。

外部向け個人情報保護方針については、組織のトップページから、外部向け個人情報保護方針へのリンクがあることが必要である。

（４） 計画

個人情報の特定にあたっては、台帳の件数は、概数でもよいが、できるだけ人数を記したほうが良い。また、要配慮個人情報を取り扱っている部門では、台帳に「本人同意の有無」の項目が必要となる。個人情報保護法では個人情報と個人データを区別しているが、JIS では同様に取り扱うこととなる。

リスクアセスメント及びリスク対策については、特定したリスクに対する対策については、「運用の確認の記録」により、リスクが顕在化していないかを点検する必要がある。

計画策定においては、計画に含まれるべき項目はあまり変わっていない。ただし、PDCA のすべてのフェーズで是正措置に繋げることが必要である。

（５） 実施及び運用

2016 年の個人情報保護法改正により、要配慮個人情報の概念が加わり、これを取得、利用又は提供する場合は、あらかじめ書面による本人の同意を得ていることが求められる。この概念は、JIS2006 で既に規定されており、その範囲も実質的には同じだと考えられる。この面では、法律が JIS に追いついて来たともいえる。

個人情報を取得した場合の措置については、公表文書「個人情報の取り扱いについて」に特定された利用目的が公表されていることが必要である。受託によって取得した個人情報についても、その利用目的を公表する。

共同利用する者から個人情報を取得する場合でも、その共同利用者が共同利用に関する公表の措置を講じていない場合は、本人に連絡又は接触する際に本人同意が必要となる。

新規追加された外国にある第三者への提供の制限は、EU の一般データ保護規則（GDPR）の動向次第の面がある。また、匿名加工情報も法改正で新たに加わったが、実際にこれを利用する事業者は少なく、審査基準も明確にはされていない状況である。

委託先の監督については、「委託先の選定記録」に、委託する個人データの内容が記されている必要があるが、何を委託しているのかを把握していない事業者も未だ多い。

（６） 文書化した情報、苦情及び相談への対応

文書化した情報については、「記録を除く情報」と「記録」とに分けて管理の規定を行う。

苦情と開示は別個に規定する必要があるが、これを一緒に規定してしまう事業者が多い。

（7） パフォーマンス評価、マネジメントレビュー、是正措置

パフォーマンス評価のうち「運用の確認」は、残存リスクが顕在化していないか、リスク対策が実施できているかなど、日常業務において気づいた点があれば、それを是正及び予防していくものであるため、小規模な組織であっても、「運用の確認」を行うことが望ましい。

内部監査においては、「JIS との適合性監査」の後、「運用監査」を実施していることが必要である。

トップマネジメントは、マネジメントレビューを実施するために、少なくとも年一回、適宜に PMS の状況について個人情報保護管理者からの報告を受けて PMS を見直さなければならない。

不適合に対する是正措置に含めなければならない事項とその実施者は次のとおりである。

①不適合の内容を確認する（代表者）

②不適合の原因を特定し、是正措置を立案する（個人情報保護管理者）

③期限を定め、立案された措置を実施する（代表者）

④実施された是正措置の結果を記録する（不適合があった部門の長）

⑤実施された是正措置の有効性をレビューする（個人情報保護管理者、代表者）

（8） 質疑応答

講演の後に質疑応答がなされ、以下の質問を始め、多くの質問・感想が寄せられた。

Q：Tポイント等の共同ポイントにおいて、個人情報の利用に関する規約の改定が頻繁に行われることについてどう思われるか。

A：規約の改定ごとに同意をとっていない点に問題があると感じている。

6．所感

私のように、プライバシーマークの審査機関や取得企業での勤務経験のない者は、審査実務に関する知識も経験も乏しいですが、そのような者でも良く理解できるように具体例を挙げながらポイントを説明してくださり、非常に参考になりました。また、JIS の規定に沿って話を進めていただいたので、体系的の中での位置づけも良くわかりました。

講演でも触れられましたが、GDPR のスタートが 5 月に控えています。また、今年に入って Facebook からの個人情報漏洩が明らかになるなど、個人情報保護の要求レベルはますます高まってきていると感じます。企業にとって、JISQ15001 の基準を守ることは、必要条件ではあっても決して十分条件ではないことを認識しつつ、PMS の維持・改善のための不断の努力を行う必要性を改めて感じました。

以上

<目次>

2018.5

注目情報（2018.4～2018.5）

■プレス発表 「IT人材白書2018」を発行【IPA】

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は2017年度IT人材動向調査を実施し、「IT人材白書2018」として発行しました。同調査はIT人材育成施策に必要となる基礎データの収集やIT人材の育成に関する動向や課題等について、とりまとめたものです。

IPAでは2008年から毎年、IT人材を取り巻く環境や動向などを把握することを目的として調査を実施し、「IT人材白書」として取りまとめています。

「IT人材白書2018」で、明らかになったのは以下の3点です。

（1） 第4次産業革命に求められる、価値創造型のIT人材の資質は、従来（課題解決型）のIT人材に求められる資質とは異なること。

（2） 人材の“質”不足の緩和（質向上）には、知識や経験を得やすい企業文化・風土が強く関係しており、効果があること。一方、企業文化・風土と人材の“量”不足の関係性は、“質”ほど明確ではないこと。

（3） 企業文化・風土を醸成させるにはモチベーション向上のための施策が有効であること。

URL：https://www.ipa.go.jp/about/press/20180424.html

以上

<目次>

2018.5

【 協会主催イベント・セミナーのご案内 】

■SAAJ 月例研究会（東京）

第233回	日時：2018年6月13日（水） 18時30分～20時30分 場所：機械振興会館 地下2階ホール	
	テーマ	ITシステム開発のトラブルはどこからくるのか？
	講師	細川 宣啓 氏 日本アイ・ビー・エム株式会社 東京基礎研究所 インダストリーソリューションサービス 品質エンジニアリング 部長
	講演骨子	企業にとってのITシステムの在り方やこれからの活用方法は様々ですが、実は近年発生したシステムトラブルは業態・業界を問わず同様の傾向を示しています。特に予想外・想定外のトラブル発生には、技術者のスキル・経験・勘所が深く関わっているようです。本講演では、システムトラブルの主原因の一つであるソフトウェア品質に焦点を充て、従来技術では補えない品質課題とトラブル解決・回避のコツを共有します。
	お申込み	下記URLよりお申込みください。 https://www.saaj.or.jp/getsurei/getsurei_form233.html

■近畿支部 30 周年記念シンポジウム

近畿支部30周年記念シンポジウム	日時：2018年 6月30日（土）大会 13:00～17:00 / 情報交換会 17:30～19:30 場所：エル・おおさか(大阪府立労働センター) 6階 大会議室	
	テーマ	システム監査@ニューフロンティア
	プログラム	1 来賓挨拶（経済産業省 近畿経済産業局 地域経済部 次世代産業・情報政策課様） 2 新システム監査基準／管理基準のポイント 3 地方自治体のICT監査に求められる役割と課題について 4 ブロックチェーン技術とシステム監査 5 次代を担うシステム監査のあり方について ---------- 6 情報交換会 ※都合により、講演内容・講師・時間等を変更する場合がありますのでご了承下さい。
	お申込み	https://www.saaj.or.jp/anniv_30th/anniv_kinki_30th_symposium.html

■監査実践セミナー（東京）

第32回	日時：2018年7月12日（木）～7月21日（金） 9時30分～17時（日帰り） 場所：晴海グランドホテル	
	教材	建設業におけるシステム運用に関する監査
	講師	事例研究会メンバー
	セミナー概要	企業にとってのITシステムの在り方やこれからの活用方法は様々ですが、実は近年発生したシステムトラブルは業態・業界を問わず同様の傾向を示しています。特に予想外・想定外のトラブル発生には、技術者のスキル・経験・勘所が深く関わっているようです。本講演では、システムトラブルの主原因の一つであるソフトウェア品質に焦点を充て、従来技術では補えない品質課題とトラブル解決・回避のコツを共有します。
	募集人員	定員10名（最小催行人員6名）
	応募締切日	2018年6月11日（月）
	お申込み	下記URLよりお申込みください。 https://www.saaj.or.jp/kenkyu/jissenseminar/jissenseminar32.html

<目次>

2018.5

【 外部主催イベント・セミナーのご案内 】

■システム監査学会 研究大会

第32回	日時：2018年6月8日（金） 大会： 10:00～16:50／懇親会：17:10～19:00 場所：機械振興会館ホール他および地下３階B3-2 号室	
	主催/問合先	システム監査学会 事務局 〒106-0032 東京都港区六本木1-9-9 JIPDEC内 TEL03-5860-7556/Webからの問合せはこちらから
	統一論題	新システム監査制度とシステム監査
	開催趣旨	経済産業省は、2004 年の改訂後に生じた情報通信技術(ICT)環境と社会システムの大きな変化を踏まえて、システム監査基準およびシステム管理基準を改定しました。本大会では、この新しいシステム監査制度の改定経緯、特徴、目的、意図等について論じ、今後どのよう に展開を図り、新しいシステム監査制度を普及、浸透させていくかを考えていきます。 また、本学会 専門監査人部会および研究プロジェクトの成果報告と研究成果(一般公募)の発表を行い、多様なシステム監査の展開 について議論をさせていただきたいと思います。 会員および専門家ならびに関係者の厳しく真摯なご批判とご意見をいただければ幸いです。本学会会員ならびにシステム監査、情報セキュリ ティ、情報ソリューション、リスクマネジメント、BCP/BCMS 等に携わっている関係各方面の方々のご参加をお待ちしております。
	お申込み	下記URLよりお申込みください。 https://www.sysaudit.gr.jp/taikai/2018_taikai_32.html

<目次>

2018.5

【 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。
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

・ホームページでは協会活動全般をご案内　http://www.saaj.or.jp/index.html
・会員規程　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　http://www.saaj.or.jp/members/henkou.html

特典

・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

ぜひご参加を

・各支部・各部会・各研究会等の活動。　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。
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。
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

・「情報システム監査実践マニュアル」「６か月で構築する個人情報保護マネジメントシステム」などの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

セミナー

・月例研究会など、セミナー等のお知らせ　http://www.saaj.or.jp/kenkyu/index.html
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

・過去の会報を公開　https://www.saaj.jp/03Kaiho/0305kaihoIndex.html
会報に対するご意見は、下記のお問合せページをご利用ください。

お問い合わせ

・お問い合わせページをご利用ください。　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		2018.5
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
5 月	10：理事会	13,26：春期 CSA 面接 19：システム監査制度カンファレンス 「新システム監査／管理基準」 （第 232 回特別開催月例研究会） 28：CSAフォーラム（茅場町NATULUCK）	
6 月	1：年会費未納者宛督促メール発信 14：理事会 15：会費未納者督促状発送 16～：会費督促電話作業（役員） 29：支部会計報告依頼（〆切 7/13） 30：助成金配賦額決定（支部別会員数）	13：第 233 回月例研究会 中旬：春期 CSA 面接結果通知 下旬: 春期 CSA 認定証発送	認定 NPO 法人東京都認定日 （2015/6/3） 30：近畿支部 30 周年記念 シンポジウム
7 月	5：支部助成金支給 12：理事会	12：第 32 回システム監査実践セミナー (日帰り 2 日間コース) 下旬：秋期 CSA・ASA 募集案内	13：支部会計報告〆切
8 月	（理事会休会） 25：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
9 月	13：理事会	～ 秋期 CSA・ASA 募集中 ～9/30 迄	
10 月	11：理事会	27：会員向け活動説明会	21：秋期情報処理技術者試験
	前年度に実施した行事一覧		
11 月	9：理事会 9：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/9〆切） 18：2018 年度年会費請求書発送準備 25：会費未納者除名予告通知発送 30：本部・支部予算提出期限	11,18,25：秋期 CSA 面接 下旬：CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 30： CSA 面接結果通知	
12 月	1： 2018 年度年会費請求書発送 1： 個人番号関係事務教育 14：理事会：2018 年度予算案 会費未納者除名承認 第 17 期総会審議事項確認 15：総会資料提出依頼（1/9〆切） 15：総会開催予告掲示 19：2017 年度経費提出期限	15：第 228 回月例研究会 15： CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 26：秋期 CSA 認定証発送	12:協会創立記念日
1 月	9： 総会資料提出期限 16:00 10：役員改選公示（1/25 立候補締切） 11：理事会：総会資料原案審議 27：2017 年度会計監査 30：総会申込受付開始（資料公表） 31：償却資産税・消費税申告	1-31：CSA・ASA 更新申請受付 19： 春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 29：第 229 回月例研究会	6：支部会計報告期限
2 月	1：理事会：通常総会議案承認 28：2018 年度年会費納入期限	1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	23：第 17 期通常総会 役員改選
3 月	8：年会費未納者宛督促メール発信 8：理事会 27：法務局：資産登記、理事変更登記 活動報告書提出 東京都：NPO 事業報告書提出	1-31: 春期 CSA・ASA 書類審査 3-4 ＆17-18:「第 31 回システム監査実務 セミナー(日帰り 4 日間コース)」 会場：関東 IT ソフトウェア健保会館 14：第 230 回月例研究会 31：第 20 回「事例に学ぶ課題解決セミナー」 会場：市ヶ谷健保会館	
4 月	12：理事会	初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行 17：第 231 回月例研究会	15：春期情報技術者試験

<目次>

2018.5

【 会報編集部からのお知らせ 】

1．会報テーマについて

2．会報バックナンバーについて

3．会員の皆様からの投稿を募集しております

□■ 1． 会報テーマについて

2018 年度の年間テーマは、「システム監査人の新たな活躍」とし、さらに四半期ごとに具体的なテーマを設定して、皆様からのご意見ご提案を募集いたします。

４月号から今月号までの四半期テーマは、「システム監査基準・管理基準改訂とこれからのシステム監査人」でした。システム監査人の皆様にとって、関心の高い重要なテーマであろうと思いますので、来月号から９月号までの四半期テーマも、引き続き「システム監査基準・管理基準改訂とこれからのシステム監査人」とします。システム監査基準・管理基準の改訂に対して、システム監査人としてどう対応していくのか、皆様のご意見をお待ちしています。

システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

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。

＊2018 年度会報テーマ

	四半期テーマ	年間テーマ
1 月号～3 月号	システム監査人に求められる能力	システム監査人の新たな活躍
4 月号～6 月号	システム監査基準・管理基準改訂と これからのシステム監査人	
7 月号～9 月号	システム監査基準・管理基準改訂と これからのシステム監査人	
10 月号～12 月号	（決まり次第ご連絡します）	

□■ 2． 会報のバックナンバーについて

協会設立からの会報第１号からのバックナンバーをダウンロードできます。

https://www.saaj.jp/03Kaiho/0305kaihoIndex.html

□■ 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。

投稿要項が変更になっておりますので、下記をご確認の上、投稿をお願いします。

□■ 会報投稿要項

1.	めだか	匿名（ペンネーム）による投稿 原則１ページ ※Word の投稿用フォーム（毎月メール配信）を利用してください。
2.	記名投稿	原則４ページ以内 ※Word の投稿用フォーム（毎月メール配信）を利用してください。
3.	会報掲載論文 (投稿は会員限定)	会報掲載「論文」募集要項（2018. 1.11 改訂） 6000 字以上。17,000 字程度。図表を含める。 システム監査の啓発、普及、理論深化、情報提供、実践、手法開発等に役立つ論文であること。 既発表論文は除く。

■投稿について

・投稿締切：15 日 (発行日：25 日)

・投稿用フォーマット　※毎月メール配信を利用してください。

・投稿先：　**saajeditor@saaj.jp**　宛メール添付ファイル

・投稿メールには、以下を記載してください。

- ✓ 会員番号
- ✓ 氏名
- ✓ メールアドレス
- ✓ 連絡が取れる電話番号

・めだか、記名投稿には、会員のほか、非会員 CSA/ASA、および SAAJ 関連団体の会員の方も投稿できます。

- ✓ 会員以外の方は、会員番号に代えて、CSA/ASA 番号、もしくは団体名を表記ください。

■注意事項

・投稿された記事については「会報編集委員会」から表現の訂正や削除を求めることがあります。又は、採用しないことがあります。

・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戴くことがあります。

お問い合わせ先：　saajeditor@saaj.jp

2018.5

会員限定記事

【本部・理事会議事録】（会員サイトから閲覧ください。会員パスワードが必要です）

https://www.saaj.or.jp/members_site/KaiinStart

ログイン ID（8 桁）は、年会費請求書に記載しています。

＝＝

■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、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。

https://www.saaj.or.jp/members_site/KaiinStart

■□■ＳＡＡＪ会報担当

編集委員： 桜井由美子、安部晃生、久保木孝明、越野雅晴、竹原豊和、豊田諭、福田敏博、藤澤博、柳田正、山口達也

編集支援： 小野修一（会長）、各副会長、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>