



認定 NPO 法人

日本システム監査人協会報

2016 年 10 月号

No 187

— No.187 (2016 年 10 月号) <9 月 25 日発行> —

今月のテーマは

「システム監査への期待」です。

今週の注目記事

【システム監査に関するアンケート結果と課題】

写真提供：高橋純一



巻頭言

『 IT アセスメント研究会について 』

会員番号 555 松枝憲司（副会長）

SAAJ の新たなビジョンに対する具体的な活動の一環として、IT アセスメント研究会を立ち上げていく予定です。現在想定している主な研究テーマは、以下のとおりです。

1. IT ガバナンス関連

(1) JISQ38500 : 2015 の活用の検討

IT ガバナンスを広く普及させ、企業等に有効に活用を図る方策を検討する。

その結果として IT ガバナンスに関するアセスメントへのニーズの高まりに繋げる。

(2) ISO38500 関連基準及び ISO38500 : 2015 の日本語化の検討

上記(1)の JISQ38500 の活用を図るうえでは、その関連基準である ISO38501,38502、38504,38505 等の理解は不可欠である。また現在の JISQ38500 は ISO38500 : 2008 を J I S 化したものであるが、既に ISO38500 : 2015 が発行されており、この日本語化も必要である。

(3) ISO38503 (Assessment of the governance of IT) の ISO 化の支援

IT ガバナンスのアセスメントに関する基準であり、過去数年に渡って行ってきた ISO 化の支援を継続する。

2. システム管理基準の改訂の検討

現行のシステム管理基準については、経済産業省に動きがなく、現状のままでは利用価値が低下するばかりである。このテーマに関しては、システム監査学会とのコラボレーションにより実現させていきたい。

以上について、進め方等を固め次第、会員の皆様に参加募集を予定しています。奮ってご参加ください。

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>

○ 巻頭言	1
【 I T アセスメント研究会について 】	
1. めだか	3
【 システム監査への期待 】	
2. 投稿	4
【 システム監査の活性化 】	
3. 本部報告	5
【「新個人情報保護法」が P M S に及ぼす影響 ～ P M S ハンドブック読者！必読！～ 第 6 回 】	
4. 支部報告	12
【 I T - B C P 体験セミナー 開催結果報告 】 近畿支部	
【 第 1 6 0 回定例研究会 】 近畿支部	
【 2016 年度 長野県例会・研究報告 】 北信越支部	
5. 注目情報	23
【 システム監査に関するアンケート結果と課題について 】 システム監査学会	
【 プレス発表 「平成 28 年度秋期情報処理技術者試験」の応募者数について 】	
6. セミナー開催案内	28
【 協会主催イベント・セミナーのご案内 】	
7. 協会からのお知らせ	30
【 2 0 1 6 年度秋期 公認システム監査人及びシステム監査人補の募集 】	
【 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	34

めだか 【 システム監査への期待 】

各企業では、活性化のため、ガバナンスの向上が進められている。2014年、金融庁は、機関投資家が投資先との間で対話を行い、経営を評価して、役員選任などを適正に行うように「スチュワードシップ・コード」を導入した。2015年、東京証券取引所は、「コーポレートガバナンス・コード」を制定し、東証1部2部上場会社に対し、複数の独立取締役を確保することを要請するとともに、経営トップや役員に関し報酬基準、選任基準、具体的決定理由などの事項について開示を要請した。

システム監査人は、ITや情報セキュリティに係るガバナンスに照らして、情報システムのリスクへのコントロールが適切かを監査し、マネジメントに報告することを職務としている。世の中の議論は下記(1)(2)(3)のように激しいものがあるが、システム監査人は、これらを心得つつ、ガバナンスや倫理規定のもとに、その職務を誠実にやり、システム監査への期待に応えていくことが大切であると思う。

(1)「21世紀の資本」(トマ・ピケティ著、みすず書房)は、資本主義の暴走による「格差拡大」のメカニズムを解き明かそうとした。

(2)「希望の資本論 私たちは資本主義の限界にどう向き合うか」では、賃金は、次に挙げる水準で維持されないと、「資本主義の再生産」ができなくなると論じている。

①1カ月働いて、次の1カ月働けるだけのエネルギーが出てくるように家を借りて、食べ物や服を買って、レジャーも少しする。

②家族を養い、次の世代の労働力を生産する。

③さまざまな技術革新が起きると、それに合わせて自分で学習しなければいけない。

(3) 2016年8月7日発行「朝日新聞グローブ」は、特別寄稿「EU離脱を望んだ英国」で英国の状況を伝えている。今後は、リスボン条約50条に基づく離脱手続きが、英国側からの「離脱通知」によって始まるが、英国の思惑は、移民の流入を抑えつつ市場への自由な参加を継続するよう上手く交渉を進めることであるという。「イギリス帝国の歴史 アジアから考える」によると、自由貿易や資本主義によって繁栄したイギリス帝国(the British Empire)は、1600年、イギリス東インド会社の設立に始まって、1973年、ヨーロッパ共同体(EC)への加盟、そして、1997年、香港返還により終焉している。



(空心菜)

参考:「希望の資本論 私たちは資本主義の限界にどう向き合うか」池上彰・佐藤優 著 朝日文庫

「イギリス帝国の歴史 アジアから考える」秋田茂 著 中公新書2167

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

<目次>

投稿 【 システム監査の活性化 】

会員番号 0557 仲厚吉 (会長)

「システム監査」とは、情報システムの信頼性、安全性、有効性について、独立した立場から監査し、当該システムの責任者に報告し、あわせて、報告書の公表により、システム責任者の社会的説明責任を果たすことを支援するものです。当協会では、システム監査の活性化に資するよう、「公認システム監査人」の皆様に意見交換や研修の場（フォーラム）を提供し、積極的なご参加をお願いしています。

公認システム監査人認定制度について

当協会認定「公認システム監査人」は、実務経験、小論文、倫理規定順守の心得を試験し認定されます。システム監査技術者試験（AU）の合格者をはじめ、情報セキュリティその他の高度情報処理技術者、中小企業診断士、公認会計士、技術士、CISA（米国に本部を置く ISACA の認定取得者）、ISMS 又はプライバシーマーク主任審査員に対し一定の要件を満たしていれば認定する制度になっています。

情報処理技術者試験について

独立行政法人情報処理推進機構（IPA）は、システム監査に係って、“システム監査技術者試験（AU）～独立した立場で IT を監査するご意見番～” を設けています。“情報システムを監視し、リスクとコントロールを評価することによって、組織体の情報システムの適切な活用を促進し、IT ガバナンス向上やコンプライアンス確保に貢献できる監査人や情報システム責任者などを目指す方に最適です。” としています。「期待する技術水準」は、次のように挙げられています。

- (1) 情報システムや組込みシステム及びそれらの企画・開発・運用・保守に関する幅広く深い知識をもち、その目的や機能の実現に関するリスクとコントロールに関する専門知識をもち。
- (2) 情報システムや組込みシステムが適用される業務プロセスや、企業戦略上のリスクを評価し、それに対するコントロールの問題点を洗い出し、問題点を分析・評価するための判断基準を自ら形成できる。
- (3) ITガバナンスの向上やコンプライアンスの確保に寄与するために、ビジネス要件や経営方針、情報セキュリティ・個人情報保護・内部統制などに関する関連法令・ガイドライン・契約・内部規定などに合致した監査計画を立案し、それに基づいて監査業務を適切に管理できる。
- (4) 情報システムや組込みシステムの企画・開発・運用段階において、有効かつ効率的な監査手続を実施するための監査技法を適時かつ的確に適用できる。
- (5) 監査結果を事実に基づく論理的な報告書にまとめ、有益で説得力のある改善勧告を行い、フォローアップを行うことができる。

<目次>

2016.10

【「新個人情報保護法」がPMSに及ぼす影響 ～PMSハンドブック読者！必読！～ 第6回】

会員番号 2589 林昭夫（個人情報保護監査研究会）

今月号では「第四章 第三節 監督」を解説します。

第40条～第42条、および第47条は、2016年1月1日から施行されています。

この連載の前回までの内容は、以下のサイトで閲覧できます。

目次 = <http://1.33.170.249/saajpmsHoritsu/000PIPHoritsu.html>

第四章 個人情報取扱事業者の義務等 （続き）**第三節 監督****第40条（報告及び立ち入り検査） （旧三十二条）**

個人情報保護委員会は、**前二節及びこの節の規定の施行に必要な限度において、個人情報取扱事業者又は匿名加工情報取扱事業者（以下「個人情報取扱事業者等」という。）**に対し、個人情報又は匿名加工情報（以下「個人情報等」という。）の取扱いに関し、必要な報告若しくは資料の提出を求め、又はその職員に、当該個人情報取扱事業者等の事務所その他必要な場所に立ち入らせ、個人情報等の取扱いに関し質問させ、若しくは帳簿書類その他の物件を検査させる。

- 2 前項の規定により立入検査をする職員は、その身分を示す証明書を携帯し、関係人の請求があったときは、これを提示しなければならない。
- 3 第一項の規定による立入検査の権限は、犯罪捜査のために認められたものと解釈してはならない。

- ※ 第一節（個人情報取扱事業者の義務）、第二節（匿名加工情報取扱事業者等の義務）を含め、その取扱いに関して、個人情報保護委員会に監督権限があることを規定しています。
- ※ 第一項により、旧三十二条に規定されていた主務大臣における“報告の徴収”に加えて、立ち入り検査の権限が個人情報保護委員会に与えられました。
- ※ この節で記述されることは、罰則の対象となります。
- ※ 第40条は、2016年1月1日から施行されています。

第41条（指導及び助言） （旧三十三条）

個人情報保護委員会は、**前二節の規定の施行に必要な限度において、個人情報取扱事業者等に対し、個人情報等の取扱いに関し必要な指導及び助言を**することができる。

- ※ 旧三十三条にはなかった「指導」の権限が個人情報保護委員会において新たに加えられました。

※ 第41条は、施行期日が明確ではありませんが、2016年1月1日から施行されていると思われます。

第42条（勧告及び命令）（旧三十四条）

個人情報保護委員会は、個人情報取扱事業者が第十六条から第十八条まで、第二十条から第二十二條まで、第二十三条（第四項を除く。）、第24条、第25条、第26条（第二項を除く。）、第27条、第28条（第一項を除く。）、第29条第二項若しくは第三項、第30条第二項、第四項若しくは第五項、第33条第二項若しくは第36条（第六項を除く。）の規定に違反した場合又は匿名加工情報取扱事業者が第37条若しくは第38条の規定に違反した場合において個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者等に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる。

- 2 個人情報保護委員会は、前項の規定による勧告を受けた個人情報取扱事業者等が正当な理由がなくてその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときは、当該個人情報取扱事業者等に対し、その勧告に係る措置をとるべきことを命ずることができる。
- 3 個人情報保護委員会は、前二項の規定にかかわらず、個人情報取扱事業者が第十六条、第十七条、第二十条から第二十二條まで又は第二十三条第一項、第24条若しくは第36条第一項、第二項若しくは第五項の規定に違反した場合又は匿名加工情報取扱事業者が第38条の規定に違反した場合において個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該個人情報取扱事業者等に対し、当該違反行為の中止その他違反を是正するために必要な措置をとるべきことを命ずることができる。

※ 第1項で、違反行為の中止、違反是正措置を取るべき旨の勧告の対象となるのは、以下のとおりです。

- 第十六条（利用目的による制限）
- 第十七条（適正な取得）
- 第十八条（取得に際しての利用目的の通知等）
- 第二十条（安全管理措置）
- 第二十一条（従業員の監督）、第二十二条（委託先の監督）
- 第二十三条（第三者提供の制限）
- 第24条（新設：外国にある第三者への提供の制限）
- 第25条（新設：第三者提供に係る記録の作成等）
- 第26条（新設：第三者提供を受ける際の確認等）
- 第27条（保有個人データに関する事項の公表等）
- 第28条（開示）、第29条（訂正等）、第30条（利用停止等）、第33条（手数料）
- 第37条（匿名加工情報の提供）
- 第38条（識別行為の禁止）

通常、是正命令は勧告に従わない場合に出されます。しかし、勧告を経ずに是正命令を出することができる場合として、個人の重大な権利利益を害する事実があるため緊急に措置を

とる必要がある場合を想定して、第3項に以下を規定しています。

- 第24条（外国にある第三者への提供の制限（適切な外国への提供、本人の同意取得）に違反、若しくは、
- 第36条（匿名加工情報の作成等）第一項（規則に従った加工）、第二項（安全管理）若しくは第五項（照合禁止）に違反した場合、又は
- 第38条（識別行為の禁止）の規定に違反した場合

※ 第42条は、2016年1月1日から施行されています。

第43条（個人情報保護委員会の権限の行使の制限）

（旧三十五条）

個人情報保護委員会は、前三条の規定により個人情報取扱事業者等に対し報告若しくは資料の提出の要求、立入検査、指導、助言、勧告又は命令を行うに当たっては、表現の自由、学問の自由、信教の自由及び政治活動の自由を妨げてはならない。

- 2 前項の規定の趣旨に照らし、個人情報保護委員会は、個人情報取扱事業者等が第76条第一項各号に掲げる者（それぞれ当該各号に定める目的で個人情報等を取り扱う場合に限る。）に対して個人情報等を提供する行為については、その権限を行使しないものとする。

- ※ 第43条第一項では、個人情報保護委員会が権限を行使する場合に、事業者の表現、学問、信教、政治の各分野に対する自由を妨げないことを規定していますが、これは、憲法第21条の、表現の自由、検閲の禁止に基づく概念です。
- ※ 第二項の規定は、第76条（適用除外）第一項各号に掲げる者（報道、著述、大学その他の研究機関の研究、宗教活動、政治活動の各活動の用に供する目的である場合）には、第4章（個人情報取扱事業者の義務等）の規定は適用されないことに基づいています。
- ※ 第43条は施行期日が附則に記述されていないため、未施行となります。

第44条（権限の委任） （新設）

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、個人情報取扱事業者等に対し、第四十二条の規定による勧告又は命令を効果的に行う上で必要があると認めるときは、政令で定めるところにより、第四十条第一項の規定による権限を事業所管大臣に委任することができる。

- 2 事業所管大臣は、前項の規定により委任された権限を行使したときは、政令で定めるところにより、その結果について個人情報保護委員会に報告するものとする。

つづき

- 3 事業所管大臣は、政令で定めるところにより、第一項の規定により委任された権限及び前項の規定による権限について、その全部又は一部を内閣府設置法（平成十一年法律第八十九号）第四十三条の地方支分部局その他の政令で定める部局又は機関の長に委任することができる。
- 4 内閣総理大臣は、第一項の規定により委任された権限及び第二項の規定による権限（金融庁の所掌に係るものに限り、政令で定めるものを除く。）を金融庁長官に委任する。
- 5 金融庁長官は、政令で定めるところにより、前項の規定により委任された権限について、その一部を証券取引等監視委員会に委任することができる。
- 6 金融庁長官は、政令で定めるところにより、第四項の規定により委任された権限（前項の規定により証券取引等監視委員会に委任されたものを除く。）の一部を財務局長又は財務支局長に委任することができる。
- 7 証券取引等監視委員会は、政令で定めるところにより、第五項の規定により委任された権限の一部を財務局長又は財務支局長に委任することができる。
- 8 前項の規定により財務局長又は財務支局長に委任された権限に係る事務に関しては、証券取引等監視委員会が財務局長又は財務支局長を指揮監督する。
- 9 第五項の場合において、証券取引等監視委員会が行う報告又は資料の提出の要求（第七項の規定により財務局長又は財務支局長が行う場合を含む。）についての審査請求は、証券取引等監視委員会に対してのみ行うことができる。

- ※ 個人情報保護委員会は、必要な報告、若しくは資料の提出を求めることを事業所管大臣に委任することができます。さらに事業所管大臣は、地方支分部局その他の政令で定める部局又は機関の長に委任することができるため、結局、個人情報取扱事業者等は、地方の関連機関に報告することとなるようです。
- ※ 第四項以降、金融庁長官への委任、金融庁長官から証券取引等監視委員会への委任、さらに、財務局長又は財務支局長への委任と金融業界におけるエスカレーションルールが特別に規定されています。
- ※ この条項における「権限の委任」には第41条の「指導及び助言」の権限は含まれていません。
- ※ 第44条は未施行です。

第45条（事業所管大臣の請求）（新設）

事業所管大臣は、個人情報取扱事業者等に前二節の規定に違反する行為があると認めるときその他個人情報取扱事業者等による個人情報等の適正な取扱いを確保するために必要があると認めるときは、個人情報保護委員会に対し、この法律の規定に従い適当な措置をとるべきことを求めることができる。

- ※ 第44条において、地方の機関や財務支局長が受け付けた、個人情報取扱事業者等からの報告書は、事業所管大臣がそれを判断して、個人情報保護委員会に、“適当な措置を取るべきことを求める”という手続きとなります。
- ※ 第45条は未施行です。

第46条（事業所管大臣）**（旧三十六条）**

この節の規定における**事業所管大臣**は、次のとおりとする。

- 一 個人情報取扱事業者等が行う個人情報等の取扱いのうち雇用管理に関するものについては、厚生労働大臣（船員の雇用管理に関するものについては、国土交通大臣）及び当該個人情報取扱事業者が行う事業を所管する大臣又は国家公安委員会（次号において「大臣等」という。）
- 二 個人情報取扱事業者等が行う個人情報等の取扱いのうち前号に掲げるもの以外のものについては、当該個人情報取扱事業者が行う事業を所管する大臣等

※ 第46条は未施行です。

第四節 民間団体による個人情報の保護の推進**第47条（認定）****（旧三十七条）**

個人情報取扱事業者等の個人情報者等の適正な取扱いの確保を目的として次に掲げる業務を行おうとする法人（法人でない団体で代表者又は管理人の定めのあるものを含む。次条第三号ロにおいて同じ。）は、**個人情報保護委員会**の認定を受けることができる。

- 一 業務の対象となる個人情報取扱事業者等（以下「対象事業者」という。）の個人情報等の取扱いに関する第52条の規定による苦情の処理
 - 二 個人情報等の適正な取扱いの確保に寄与する事項についての対象事業者に対する情報の提供
 - 三 前二号に掲げるもののほか、対象事業者の個人情報等の適正な取扱いの確保に関し必要な業務
- 2 前項の認定を受けようとする者は、政令で定めるところにより、個人情報保護委員会に申請しなければならない。
 - 3 個人情報保護委員会は、第一項の認定をしたときは、その旨を公示しなければならない。

※ 認定個人情報保護団体の認可主体は、主務大臣から個人情報保護委員会に変更されました。

※ 上記以外に「認定個人情報保護団体」に、個人情報取扱事業者等として匿名加工情報取扱事業者が含まれることになったことがポイントです。

※ 第47条は、2016年1月1日から施行されています。

※ 第48条～第52条までは、大きな改定はありませんので省略します。

第53条（個人情報保護指針）（旧四十三条）

認定個人情報保護団体は、対象事業者の個人情報等の適正な取扱いの確保のために、個人情報に係る利用目的の特定、安全管理のための措置、開示等の請求等に応じる手続その他の事項又は匿名加工情報に係る作成の方法、その情報の安全管理のための措置その他の事項に関し、消費者の意見を代表する者その他の関係者の意見を聴いてこの法律の規定の趣旨に沿った指針（以下「個人情報保護指針」という。）を作成するよう努めなければならない。

- 2 認定個人情報保護団体は、前項の規定により個人情報保護指針を作成したときは、個人情報保護委員会規則で定めるところにより、遅滞なく、当該個人情報保護指針を個人情報保護委員会に届け出なければならない。これを変更したときも、同様とする。
- 3 個人情報保護委員会は、前項の規定による個人情報保護指針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、当該個人情報保護指針を公表しなければならない。

- ※ 法改正により、認定個人情報保護団体の「個人情報保護指針」作成にあたって、法律の規定の趣旨に沿った指針を見直すこととなりました。
- ※ 個人情報保護委員会は、認定個人情報保護団体から届出のあった個人情報保護指針を公表します。
- ※ 第53条は未施行です。

※施行規則（案）は、青緑字で記載します。

【施行規則（案）】第24条

法第53条第二項の規定による届出は、別記様式第三による届出書によるものとする。

- ※ 施行規則案では、認定個人情報保護団体が作成する「別記様式第三による届出書」には以下を記載することとなっています。
- 1. 届け出をする認定個人情報保護団体名称等、
- 2. 届け出る個人情報保護指針にかかわる事項、
- 3. 個人情報保護委員会による個人情報保護指針の公表に関する希望の有無等、
- 4. 添付書類（個人情報保護指針（必須）その他）

【施行規則（案）】第25条

法第53条第三項の規定による公表は、インターネットの利用その他の適切な方法により行うものとする。

- ※ 現在も、個人情報保護委員会のサイトでは「認定個人情報保護団体一覧」に、指針の名称が公表されていますが、内容については一部非公開となっている業界があります。今後見直されていくことと思われます。

http://www.ppc.go.jp/files/pdf/personal_ninteidantai.pdf

- 4 認定個人情報保護団体は、前項の規定により個人情報保護指針が公表されたときは、対象事業者に対し、当該個人情報保護指針を遵守させるため必要な指導、勧告その他の措置をとらなければならない。

※ 旧四十三条の“努力義務”から、改定された第53条では“義務”へと変わりました。

【施行規則（案）】第26条

認定個人情報保護団体は、法第53条第三項の規定による公表がされた後、遅滞なく、インターネットの利用その他の適切な方法により、同条第二項の規定により届け出た個人情報保護指針を公表するものとする。

※ このように「新個人情報保護法」の改定を順次見ていくと、民間事業者に対してできる限り解りやすく配慮されていることがわかります。

.....

次回は、「第五章 個人情報保護委員会（第59条～第74条）」から解説します。

バックナンバー目次 = <http://1.33.170.249/saajpmsHoritsu/000IPHoritsu.html>

「PMSハンドブック」の読者専用ダウンロードサイトでは、新個人情報保護法、番号利用法の改正を反映した規程・様式集を公開しています。！！

SAAJ「PMSハンドブック」ご紹介サイト：<http://www.saaj.or.jp/shibu/kojin.html>

認定NPO法人日本システム監査人協会 個人情報保護監査研究会 ■

<目次>

支部報告 【 IT-BCP体験セミナー 開催結果報告 】

会員番号 1709 荒町 弘 (近畿支部)

1. セミナー名称 : IT-BCP体験セミナー
2. 開催日時 : 2016年7月30日(土) 13:00~17:00
3. 開催場所 : 大阪市ICT戦略室内 研修室
4. 当日参加者 : 受講者 16名
スタッフ 荒町、尾浦、金子、松井、伊藤 (BCP研究プロジェクト)
福本、三橋

**5. 開催報告**

本セミナーは大阪市ICT戦略室からの実施依頼に基づき開催しました。大阪市ではICT-BCPの策定を今年度実施するにあたり、幹部職員を中心とするメンバーに対して意識付けを行うための研修を行いたい、という意向から当協会のセミナーグループに相談を頂戴しました。近畿支部BCP研究プロジェクトでは、今回、「個別セミナー」でのBCP体験セミナー実施を検討し、開催の運びとなりました。

受講者にはあらかじめ当日の演習で用いるA社に関する情報を事前配布資料として提供し、事前学習のうえ、体験セミナーに臨んでいただきました。

カリキュラムは3つの講義と演習2題から成っており、オリエンテーションの後に講義1、続いて演習2題を実施した後、講義2講義3を行っていただきました。演習課題では大規模災害発生時の企業IT部門担当者の立場で初動対応について検討いただきました。16名の受講者は3つのグループに分かれてグループ討議を行いリーダーが検討結果を発表するという流れで、8つの課題を限られた時間の中で検討し、結果をチームごとに発表するというものであり、緊張感のある体験演習を行っていただきました。チーム単位での検討結果の発表後は、講師講評を踏まえて受講者全員で成果の共有を図りました。

5.1 オリエンテーション (担当: 荒町氏)

セミナー開催にあたり、オリエンテーションとして以下の説明からスタートしました。

- ・ SAAJ近畿支部BCP研究プロジェクトの活動概要
- ・ IT-BCPの普及状況や東日本大震災の教訓としての災害時における初動の重要性
- ・ 当セミナーの目的とするところについて

5. 2 講義 1 : 「自治体ICT-BCPの現状と想定外への対応」 (担当 : 松井氏)

1つ目の講義として、と題した講義を行いました。講師自らが経験してきたBCPの実効性を高めるための取組みの紹介に続き、ISOや各種ガイドラインが推奨している事項について触れました。ISO22301では、策定したBCPの実効性を検証する要求事項として「演習およびテスト」を、実効性を高める取組みとして「意識・能力の向上、および訓練プログラム」が推奨されています。経済産業省ガイドラインにおいては、BCPの有効性を確認する手段として「テスト」を、BCPの維持を確認する手段として「監査」が言及されており、総務省のガイドラインでは「簡易訓練」「定期的な訓練」の実施が必要不可欠であると述べられています。

BCP訓練の必要性が述べられている一方で、実際にはBCP訓練が行えない組織が多い。「負担の少ない訓練・演習の方法」「本番環境に影響を与えない訓練・演習の方法」を周知することで、訓練・演習を実施する組織を増やすことができるのではないか、そのための取組みとして「実機訓練」と「机上訓練」がある。

「実機訓練」と「机上訓練」の双方から得られた気付きと成果や注意点に関すること、それぞれの比較について解説を行いました。比較の結果、本番環境への影響が少ない「机上訓練」からの取り組みを行い、予備機を用いた訓練、本番機を用いた訓練へと段階的に取り組みを進めることで訓練の限界を広げていくのが良いのではないか、という提案もありました。

最後に、想定外への備えについてICT部門としてどのように認識し、どのような準備が必要で、どのような対応がとれるのか、という問題提起とともに、訓練を段階的にステップアップする方法の紹介をもって講義を終了しました。



5. 3 グループ演習 (担当 : 金子氏/尾浦氏 (講評担当))

受講者には、近畿圏で30店舗の運営を行う中堅流通業を営む企業A社のIT部門担当者の立場で、大規模災害が発生した直後に起こる8つのシーンに対してどのような初動対応を行うのかということについて検討し、グループで共有・討議のうえリーダーに発表してもらうという流れで演習に取り組んでもらいました。

- ①8つの課題を10分間自分自身で考え、対応内容を記した付箋を貼り付ける (所要時間 10分)
- ②グループメンバー全員の付箋を模造紙に貼り・共有・討議し、意見をまとめる (所要時間 20分)

③グループごとに検討結果を発表する（所要時間 5 分）

演習では、検討課題に対して意図的にタイトな時間設定とし、限られた時間内で多数の案件を一度に迅速に意思決定する重要性に気付いていただく狙いで、インバスケット研修の手法を採用しました。

(1)演習 1（災害発生直後の初動対応）

災害発生直後に起こる社内各部署からの問い合わせ等に対して、IT 部門としてどのように判断・対応すべきかを検討していただきました。

- ・優先順位付け、どの部署の誰にどのように指示を行うか等

(2)演習 2（IT-BCPのポイント検討）

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

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

(3)講師講評／演習の解説（担当：尾浦氏・金子氏）

各チームの発表内容に対し、講師側から実務体験も踏まえて講評を行いました。また、8つのシーンの設定の背景と初動対応、及びIT-BCP策定のポイントについて解説しました。



5. 4 講義 2：「自治体のための演習補講」～地防計・全庁BCPとIT-BCP～（尾浦氏）

2つ目の講義は、グループ演習の補講として、そして地域防災計画・全庁BCPとIT-BCPという視点での講義を行いました。グループ演習の補講としては、演習課題のいくつかのシーンをモデルに、その状況が発災に関して「覚知」の段階なのか、「情報収取・分析」あるいは「災害対策本部設置 BCP 発動」のどの段階にあると想定されるか、といった課題提起からはじまり、タイムラインを意識した BCP 対策の必要性等について事例を交えての講義を行いました。

発災後の経過時間ごとにフェーズを4段階で分け、部局ごとに異なる BCP 対象業務があり、応急対策を要する業務と通常業務との区分に応じた対応の考え方などについて、講師ご本人の経験も踏まえ



て解説しました。

5. 5 講義3：「組織のBCPを確実に動かすために必要なもう一つの準備」

～職員の参集率と家族の危機管理～（伊藤氏）

大規模災害発生直後には職員の安否確認や参集可否などの確認が行われ、組織の復旧への行動や市民の生命・財産を守るための行動が行われます。この際、職員自身がいち早く職務に専念できるためには、自らの家族の安否確認ができていないことが前提になると考えられます。このように、危機管理に必要な要素として、家族の危機管理も大きな部分を占めると考えられ、家族の危機管理が（事前準備と災害直後の対応）ができてこそ、組織の危機管理・地域への貢献ができるものと考えられ、「公助の限界」を大きく広がられるヒントがあるものと思われます。

本講義では家族の危機管理に対する考えや、災害発生直後の行動基準を定め公表している自治体の事例紹介、民間企業でのBCP策定・実践例などの紹介を行いました。

講義後、勤務時間中に巨大地震発生によりインフラサービス停止（停電発生）した場合、何に困るか、その事象は事前対策可能なものか、その後の判断により対応を取らなければならない事象なのか、についてグループでディスカッションいただき、グループ発表を行っていただきました。



6. 受講された皆様の感想

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

- ・これまでに総務省の資料を読むなどしてわかったつもりになっていても、制約された時間の中で発想すると、わかっていなかったことに気づくことができた
- ・今日の目的がBCPの早期作成であるため・発災時にしなくてははいけない事／判断しなくてはいけないことの気づきがありました。

最後の自組織の課題検討は課題が少しバクッとしていて取り組みにくかった

- ・普段はあまり考えない状況について検討する機会となった。
- ・テンションが上がった
- ・時間がない中で判断していく難しさと重要性が実感できた。
- ・BCPを作成するための気づきになり有意義でした。
- ・IT-BCP策定に向けて基礎的な知識を得ることができた。

- ・ 初動対応時にすべき行動を考えると なかなか思いつかず、事前の対応が必要であることに気づいた。
- ・ ICT-BCPの着眼点が明確に解説していただいている。

7. 感想

今回は BCP 研究プロジェクトとしても初めての「出前セミナー」でありました。受講者も政令指定都市の ICT-BCP の策定と運用を担う方々ということもあり、スタッフ一同もいつも以上に緊張して臨んだセミナーでありました。受講いただきました皆様には、グループ演習を通じて、ICT-BCP 策定のために役立つ「気づき」を幾分か得ていただけたのではないかと思います。

大阪市 ICT 戦略室として、災害発生時の初動の判断や、災害が発生した際に被害を最小限にするための備えは何なのか、事前に決めておくべきルール・計画は何なのか、ということについて整理する機会を持たれる際に本セミナーでの「気づき」がお役に立てれば幸いです。

受講者の皆様、スタッフ／関係者の皆様、ご協力ありがとうございました。

以上

<目次>

支部報告 【 近畿支部 第160回定例研究会 】

会員番号 0645 是松 徹

1. テーマ 「医療情報システム監査の意義と今後の情報部門の役割について」
～病院間相互監査&ワークショップセミナーの取り組みを通して～
2. 講師 池田市地域活性課 課長 藤本 智裕 氏
(前：市立池田病院経営企画室 室長)
3. 開催日時 2016年7月15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、今年の春まで市立病院の経営企画室長の立場で、長年、経営企画から診療支援、診療情報管理、情報システム等に至るまで、幅広く病院運営に携わってこられてきた。その中で医療情報システムの監査にも取り組まれており、これらのご経験を踏まえ、今回の講演では、医療情報システム（電子カルテ等）の動向、医療情報システムの安全対策と監査及び課題、病院相互監査の取組み、監査ワークショップセミナーの取組み等についてお話しいただいた。

<講演内容>

(1) 医療情報システム（電子カルテ等）

医療情報システムは、医事会計システムを皮切りにオーダリングシステム、電子カルテシステム、地域電子カルテシステムと進化してきており、ゲノム・再生医療、診断支援DSS、臨床研究、ビッグデータ、地域SNSとの関わり等の高度化が期待されている。昨今、他医療機関からの電子カルテ参照が可能となり、他施設・他職種連携の時代へと向かっている。医師と患者間の「情報の非対称性」が言われる中で、医療情報システムには高度な専門性を背景とした多様な要求への対応と安全性が求められている。

(2) 医療情報システムの安全管理

診療録の記載・電子保存の面では、「医師法24条」「歯科医師法23条」「e-文書法」に準拠し、真正性、見読性、保存性確保への留意が必要である。加えて、医療に関わる情報を扱うすべての情報システムとそれらの導入、運用、利用、保守及び廃棄に関わるすべての組織を対象とした「医療情報システム安全管理ガイドライン」が厚労省から公表されており、電子的な医療情報を扱う際の責任のあり方や情報の相互利用と標準化、情報システムの基本的な安全管理、電子保存の要求事項、運用管理についての指針が示されている。

(3) 医療情報システム安全管理評価制度（PREMISs）

「医療情報システム安全管理ガイドライン」を適用指針として、（財）医療情報システム開発センター（MEDIS-DC）が技術面、運用面の観点から客観的にその安全性を評価する制度である。本制度は、安全性の担保力を客観的に評価する事、及び安全性と利便性・効率性、経済性とのバランスをとる事を目的としている。受審側は、自己評価をした上で書類審査と現地審査を受け、合否判定と合格レベルとして3段階評価が下され、認定証を受領する運びとなる。本制度の活用としては、外部監査としての利用（シ

システム導入済)と導入時の検収ツールとして利用(システム導入予定)が考えられる。

(4) 病院情報部門が抱える課題

講師の所属組織が加入している某ベンダのユーザ会で、情報部門が抱える課題の把握のためにアンケート等から課題を抽出し分析を行った。課題を以下の7分野に分類し、それぞれに①機能改善、②運用ノウハウ、③教育・セミナー、④営業支援、の優先度から解決策を検討した。

【課題】：1. 経営、2. 企画導入・レベルアップ、3. 調達、4. 運用管理、5. データ分析・活用
6. ガバナンス、7. コンピテンシー

結果、運用管理に関する課題が全体の約6割を占め、その解決策としてはコンテンツの拡充が多数提示された。開発⇒導入⇒運用⇒改善のサイクルにおいて、運用⇒改善から開発にフィードバックして機能改善につなげる流れが必要であり、運用管理ノウハウとして職人技から仕組みへ、暗黙知から形式知へと移行する「運用管理規定」の重要性が改めて認識された。

(5) 病院間相互監査(内部監査)の取り組み

公的認定を受けた専門知識や経験を有する監査員等が、互いの病院をPREMISsに準拠した共通の仕組みの下に内部監査を行い、継続的改善を図る取り組みである。監査結果は病院長に報告し、組織を巻き込むことに留意している。公的認定資格には、講師が保有する公認医療情報システム監査人(MISCA)、上級医療情報技師等がある。「医療情報システム安全管理ガイドライン」を根拠指針とし、医療情報安全管理監査人協会が公表している「監査実践ガイド」を参考とした内部監査の手順に則り、監査計画書の作成、監査の実施と講評会開催、監査報告書の作成・提出、監査対象部門から提出される改善報告書等を踏まえたフォローアップ監査を実施する。

(6) 医療情報システム監査ワークショップの取り組み

近年のパッケージ化・ネットワーク化により運用管理に関する課題が多様化し、運用管理規定の重要性が高まっていることを背景に、「医療情報システム監査ワークショッププログラム」を開発し、継続的改善を図ることとした。複数病院(2施設)でグループとなり、監査対象側と監査側を交代して持参した運用管理規定を相互監査する進め方で実施した。ワークショップは、2013年度の福岡での試行を皮切りに、2014年度に東京(11施設17名)、名古屋(11施設19名)、札幌(10施設14名)と計3回開催した。

受講後のアンケートからは、単に知識の習得だけでなく、多様なワークショップの実践により実際の改善行動につなげることができたとの結果が読み取れた。課題が複雑化する中、人財教育の在り方として、座学だけではないワークショップの有効性が示唆されたと考えている。

6. 所感

重要性を認識しつつも接点のなかった医療情報システムの動向と運用側の医療機関の取り組み実態を改めて知ることができた。また、医療情報システムに求められる3原則(真正性・見読性・保存性)と利便性のバランスは所謂攻めと守りの話であり、医療分野に限らずセキュリティ面での共通の課題と考える。今回のご講演では、説明の合間に随所でなされた講師の勤務先・池田市の紹介が効果的であった。その中で「呉春」が池田市の地酒と知ったことは、左党の私にとってこれまた有益であった。 以上

<目次>

支部報告【北信越支部 2016 年度 長野県例会・研究報告】

会員番号 1281 宮本 茂明（北信越支部）

以下のとおり2016年度 北信越支部 長野県例会を開催しました。

- ・日時：2016年9月10日（土） 13:00-17:00 参加者：7名
- ・会場：長野市生涯学習センター
- ・議題：1.研究報告

「金融機関における開発プロジェクト検査の事例紹介」

長谷部 久夫 様

「情報セキュリティポリシーの構築 ～総合的な情報セキュリティ対策～」

梶川 明美 様

2. 西日本支部合同研究会 北信越支部報告検討

- ・環境変化に対応するシステム開発管理態勢の整備とその監査について

◇研究報告

「金融機関における開発プロジェクト検査の事例紹介」

報告者（会員番号 1766 長谷部 久夫）

報告者が関与した金融機関の開発プロジェクト検査の取組事例を紹介し、ご意見・ご質問をいただいた。

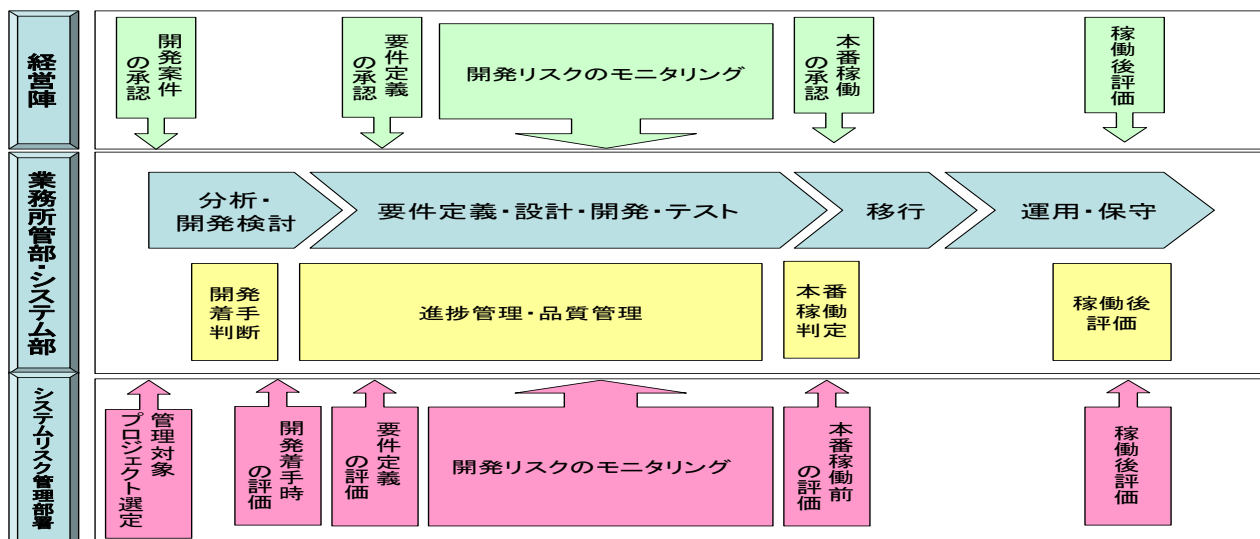
1. 前提となる開発工程・開発管理体制等

（1）開発工程

ウォーターフォール型による開発方式を採用。開発工程として、①受付、②調査・検討、③要件定義、④外部設計、⑤内部設計、⑥プログラム開発・単体テスト、⑦結合テスト、⑧総合テスト・ユーザーテスト、⑨登録・引継、⑩移行、⑪試行・稼働検証、⑫実績・効果検証の全 12 工程を設定。

（2）経営陣及び業務所管部（ユーザー部門）等の参画

システム開発に係る経営陣・業務所管部（ユーザー部門）の役割を規定し、下図の参画を求めている。



2. 開発プロジェクト検査の概要

(1) 実施目的

ア. システム開発リスクの低減

システムの大規模化・複雑化に伴い、システム開発では稼働時期の遅延、予算の超過、システム停止や誤作動及び情報漏えい等リスクが増大している。システム部の検査者が開発プロジェクト検査を実施（内部監査部門によるシステム監査は別途実施）し、開発プロジェクト運営・管理、及びシステムリスク管理の手続等の実施状況を検証することにより、上記のリスクを低減させる。

イ. システム品質の確保

本検査により、①有効性（経営方針または経営戦略を実現するために、システムが有用な情報や業務処理機能を提供すること）、②信頼性、③安全性、④効率性、⑤遵守性といったシステム品質を確保する。

ウ. システム開発文書の品質向上

検査者が、検査対象案件に係る開発文書を査読し、発見した不備を被検査者である開発プロジェクト担当者へフィードバックすることにより、開発文書の品質を向上させる。

(2) 実施要領

ア. 実施タイミング

本検査の実施タイミングは、「要件定義レビュー前」「総合テスト前」及び「稼働判定レビュー前」。

イ. システム重要度・情報重要度の把握

検査者は、本検査の実施にあたり、対象案件の「システム重要度」及び「情報重要度」を把握する。

ウ. 点検方法

各点検項目の評価は、被検査者による自己評価をベースとする。検査者は、点検項目について適切な評価判定をするために、本検査の実施タイミングに応じたシステム開発文書を査読したうえで、被検査者にインタビューする。

(3) 検査結果、指示事項への改善対応の記録、検査完了の報告

検査報告書に点検結果、改善指示事項、改善状況、および検査完了を記録。また、要件定義レビュー／稼働判定レビュー会議において検査実施状況を報告。

3. 開発プロジェクト検査の点検項目

(1) 点検項目の体系

ア. プロジェクト運営・管理の状況

イ. システムリスク管理の状況（金融検査マニュアルの確認項目ほか）

（ア）情報セキュリティ対策の状況

（イ）システム開発・運用管理の状況

（ウ）防犯・防災・バックアップ・不正利用防止

（エ）外部委託管理の状況

(2) 具体的な点検項目

開発プロジェクト検査における具体的な点検項目については、前提となる開発管理態勢の整備状況と併せて詳細に説明した。本報告では、特に注意して確認している点検項目を抜粋して以下に示す。

ア. プロジェクト運営・管理の状況

各開発工程の開始基準・終了基準を明確にし、マスタースケジュールやWBSに基づき適切に進捗管理を行っているか。業務所管部との連携（特に業務要件の変更対応やユーザー検証等）は十分か。アーキテクチャーレビュー（技術標準の遵守・新技術リスク評価の確認）での指摘事項は対応済か。

イ. システムリスク管理の状況

(ア) 情報セキュリティ対策の状況

システム重要度・情報重要度評価が適切か。各重要度に応じた安全対策を計画・実装しているか。

(イ) システム開発・運用管理の状況

本番と開発環境との差異分析、運用管理部門との連携、パッケージ性能・拡張性・セキュリティ等。

(ウ) 防犯・防災・バックアップ・不正利用防止

総合テストにおいてコンティンジェンシープラン策定と、その教育・訓練を計画・実施しているか。

(エ) 外部委託管理の状況

システム開発・運用業務に係る外部委託先との契約が適切か、当該委託先における安全対策の整備状況に問題はないか。

4. 開発プロジェクト検査の成果と課題

(1) 成果

ア. 開発プロジェクト管理の支援

被検査者による自己点検をベースとする検査により、プロジェクト管理上の考慮漏れ防止や、リスク事象の未然発生防止など、経験の浅い開発担当者を支援する仕組みとして機能している。

イ. 開発管理態勢の実効性向上

開発プロジェクト管理の有効性を高めるために導入した仕組みや手続が適切に実施されているか検証することで仕組み等の定着を図り、開発管理態勢の実効性を高めている。

(2) 課題

ア. システム品質の「有効性」評価

要件定義レビュー前の検査においては、「業務要件」と「システム要件」との整合性を確認しているが、当該システムが経営や業務に役立つかを判断することは難しい。経営陣を含めた所定手続が適切に実施されているか確認するのが限界。

金融分野においては、Fintech（Financial と Technology を組み合わせた造語、IT を駆使して新たな金融サービスを生み出したり、顧客の目線でサービスを見直したりする動きのこと）の動向が注目を集めている。その取組において、システム開発管理態勢の在り方も変わっていくことが想定される。今後も、有効な検査を実施していくため、当支部での研究活動をはじめとして、広く情報収集に努め、研究を深めていく所存です。

「情報セキュリティポリシーの構築 ～総合的な情報セキュリティ対策～」

報告者 (会員番号 0947 梶川 明美)

1 はじめに

2016年3月に富山県警を退職し、情報関係の個人事務所を開業した。何件かの業務を受託させていたが、その中から情報セキュリティポリシーの構築業務について発表する。

2 受託の経緯

開業の挨拶回りをする中で、A社の経営者から社内の情報セキュリティや経営全般に関する思いを聞く機会を得た。2時間に及ぶ懇談を要約すると、会社として成長を続ける中で情報セキュリティ対策は必須であり情報セキュリティポリシーを作りたいというものであった。だが、ポリシー以外にも整備したい規程がいくつもあり、どれから手を付けていくか迷っておられるようであった。

A社は急成長の途上にあり、ポリシーは今作らなくてもいずれ必要になると感じたので、社内で作成する際の参考となるサイトを、軽易なものからプロ仕様のものまでいくつか紹介した。程無く情報セキュリティポリシーの構築業務を発注したいとの連絡をいただいた。

3 業務の経過

(1) やりたいことを明確化

訪問時の懇談内容をベースに、ポリシー構築の目的、概要、体制作り、構築方法、社内教養からPDCAサイクルまでのスケジュールを、業務の進め方（案）として文書化した。

(2) 業務の進め方に関する合意

上記案を説明し、経営者の方向性に一致しており問題がないことの確認をいただいた。

(3) 本当の希望

更に、経営者の事業展望、気になっている問題、現状における情報セキュリティレベル、競合他社の状況など、A社の事業に関するさまざまな事柄についてじっくり傾聴した。その結果、運用面や技術面を含めた総合的な情報セキュリティを目指したいという真の希望が見えてきた。

技術的な対策は経費がかさむため、まずはポリシー構築による内部統制でしっかりと運用し、優先順位を付けて技術的対策を行っていくことを提案した。

(4) その他業務

現在構築済みの技術的なセキュリティ対策を全社に展開したいとの希望があり、そこから発展して県外支店における通信環境の改善や外出先での電子メール等の安全な使用方法についても相談を受けることとなった。

4 おわりに

情報セキュリティ関係ではA社以外からも相談をいただいているが、外部監査による情報セキュリティ監査を依頼したいというものである。個人事業者でも問題無いかと確認したが、日本システム監査人協会に継続して所属しているので大丈夫とのことであった。協会の信用度は極めて高いのだと認識した。

以上

<目次>

注目情報（2016.8～2016.10）**【 システム監査に関するアンケート結果と課題 】 システム監査学会****システム監査に関するアンケートの結果と課題について***"The result of the questionnaire on system audits, and the issues which should be discussed"*

システム監査学会

システム監査に関するアンケート 分析・評価ワーキンググループ 報告

2016 年8月

はじめに

システム監査学会では、**2015** 年秋に、システム監査に関するシンポジウム等の参加者に対し、システム監査の実施状況、利用する基準、規程類、現行基準の見直しの必要性について意識調査を実施した。そして「システム監査に関するアンケート 分析・評価ワーキンググループ」を組成し、アンケートデータの詳細分析を踏まえ、監査役の視点等の日本独自の経営との関係についての考察、サイバーセキュリティ戦略の観点でのポイントとプロセスフロー等の課題検討を行った。ワーキンググループがとりまとめた分析結果について報告する。

1. アンケートの結果**(1) 調査の目的と方法**

「実践研究に資するため、システム監査に関わる者に対し、システム監査の実施状況、利用する基準、規程類、現行基準の見直しの必要性について、意識調査を行う」ことを目的に、以下の3 回のイベントで無記名のアンケートを配布、回収する方式で実施した。

●対象：情報システム・ユーザ会連盟主催「システム監査講演会」

実施日：2015 年10 月22 日

回答件数：98 件（回収率24.5%）

●対象：NPO 法人日本システム監査人協会主催「月例研究会」

実施日：2015 年11 月19 日

回答件数：63 件（回収率：60.6%）

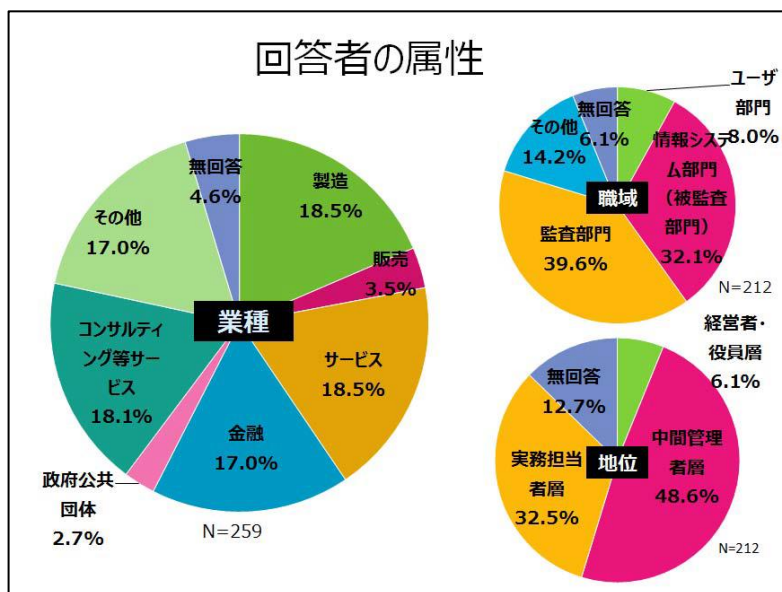
●対象：システム監査学会主催「第28 回公開シンポジウム」

実施日：2015 年11 月20 日

回答件数：98 件（回収率：62.4%）

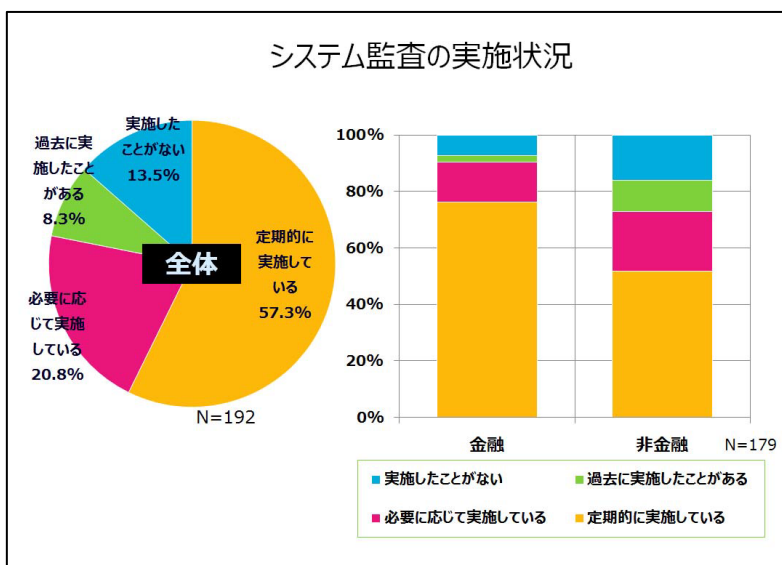
(2) 回答者の属性

回答者の所属する組織の業種は、コンサルティング等サービスが18.1%を占める他、販売が3.5%と少ないものの、製造、サービス、金融はそれぞれ17%から18.5%と偏りはみられなかった。回答者自身の職域としては、監査部門が39.6%と最も多く、次いで被監査部門である情報システム部門が32.1%であった。地位では中間管理者層が48.6%、実務担当者が32.5%を占めていて、「システム監査に関わる者に対して調査を行う」という目的に適合していることが裏づけられた。



(3) システム監査の実施状況

「システム監査に関心がある者」を対象とした調査であり、国内平均とは一致しない可能性はあるが、今回のアンケートでは、78.1%の組織で「定期的に」または「必要に応じて」システム監査が実施されていた。業種別にみると、やはり金融業では実施率が高く、90.5%で実施されていた。金融以外の業種でも73.0%で「定期的に」または「必要に応じて」実施されていた。

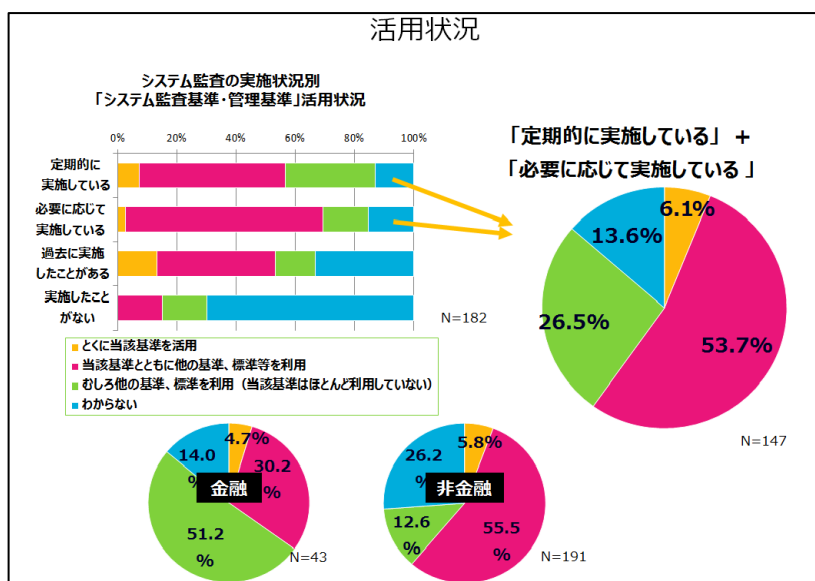


(4) 「システム監査基準／システム管理基準」の活用状況

監査の実施において、経済産業省の「システム監査基準／システム管理基準」を活用しているか尋ねたところ、「定期的に」または「必要に応じて」監査を実施している組織では、59.8%が利用していた。逆にほとんど利用していないとの回答は26.5%であった。

金融業では、「金融検査マニュアル」「金融庁監査指針」「FISC システム監査指針、安全対策基準」など、他の基準・標準を利用しており、経済産業省の「システム監査基準／システム管理基準」は、ほとんど利用していないと回答した組織が51.2%と多かった。一方、金融以外の業種では61.3%で広く活用されて

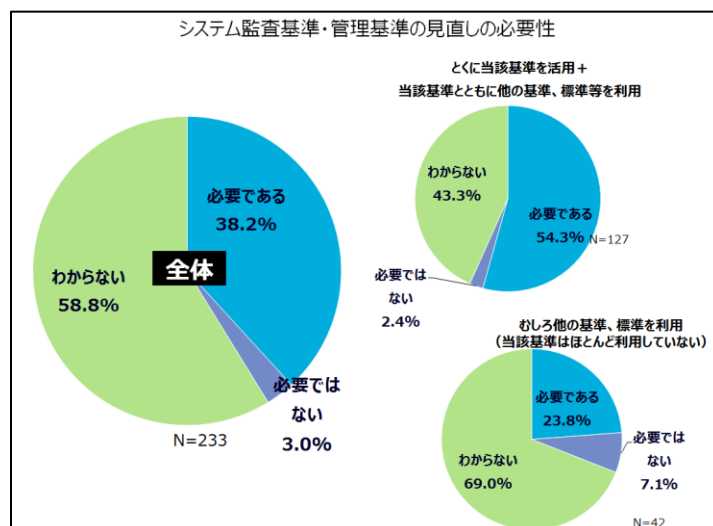
いた。



(5) 見直しの必要性とその理由

経済産業省の「システム監査基準／システム管理基準」の見直しが必要と思うかどうかの問いに対しては、38.2%が必要であると回答した。金融以外の業種を中心とした当該基準を利用しているグループでは、54.3%が必要であると回答し、さらに金融を中心とした、利用していないグループでも23.8%が見直しは必要であると回答した。理由としては、次のような意見が多く挙げられた。

- ・現状のIT に合っておらず、新技術・IT 環境への対応が必要
- ・10 年間改訂されておらず、古い
- ・サイバーセキュリティを含むセキュリティ環境の変化への対応が必要



2.まとめ

少ない標本数ながらも、システム監査に知見のある、いわば「有識者」を対象とした意識調査を実施し、有用な結果を得ることができた。

そして、経済産業省の「システム監査基準／システム管理基準」は現在でも幅広く、多くの組織で活用されているが、同時に、時代に合わせた改訂が必要であり、学会として検討を進める、との結論に達した。

<アンケート様式>

※質問1 の①には数値を、それ以外の質問については該当する番号に○印をつけください。

[質問1] あなたの組織・個人特性をお教えてください。

①組織規模 従業員数 約 人／資本金 約 円

②業種 1. 製造 2. 販売 3. サービス 4. 金融 5. 政府公共団体 6. コンサルティング等
サービス 7. その他

・・・6を選択された方は、質問4 に進んでください。

③職域 1. ユーザ部門 2. 情報システム部門（被監査部門） 3. 監査部門 4. その他

④地位 1. 経営者・役員層 2. 中間管理者層 3. 実務担当者層

[質問2] システム監査の実施状況（頻度）をお教えてください。

1. 定期的に実施している
2. 必要に応じて実施している
3. 過去に実施したことがある
4. 実施したことがない
5. わからない

[質問3] 貴組織では独自のシステム監査基準・管理基準等を定めて、活用していますか？

1. はい 2. いいえ 3. わからない

[質問4] 監査の実施において経済産業省の「システム監査基準／管理基準」を活用していますか？

1. とくに当該基準を活用している
2. 当該基準とともに他の基準、標準等を参考にしている
3. むしろ他の基準、標準を利用して実施している（システム監査・管理基準はほとんど利用していない）
（利用基準、標準等の名称： ）
4. わからない

[質問5] 平成16 年改訂の経済産業省「システム監査基準／管理基準」の見直しが必要と思いますか？

1. 必要である
・理由：
・見直しの留意点：
2. 必要ではない
理由：
3. わからない

以上

<目次>

【 プレス発表 「平成28年度秋期情報処理技術者試験」の応募者数について 】

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）情報処理技術者試験センターは、2016年10月16日（日）に実施する「平成28年度秋期情報処理技術者試験（経済産業省所管）」の応募者数を公表しました。

平成28年度秋期情報処理技術者試験の応募者数は、前年同期比115.3%の220,826人（平成28年度から開始した情報セキュリティマネジメント試験を除くと198,640人（前年同期比103.7%））となりました。

各試験区分の応募者数は以下のとおりです。

	応募者数	前年同期 応募者数	前年同期比
総数	220,826	191,596	115.3%
情報セキュリティマネジメント試験	22,186	—	—
基本情報技術者試験	75,095	73,221	102.6%
応用情報技術者試験	52,845	50,594	104.4%
高度試験	70,700	67,781	104.3%
ITストラテジスト試験	6,676	6,663	100.2%
システムアーキテクト試験	8,157	8,181	99.7%
ネットワークスペシャリスト試験	18,096	18,990	95.3%
情報セキュリティスペシャリスト試験	32,492	28,274	114.9%
ITサービスマネージャ試験	5,279	5,673	93.1%

出展：IPA ホームページ

応募者の詳細については、次のURL（統計情報）をご覧ください。

URL：http://www.jitec.ipa.go.jp/1_07toukei/_index_toukei.html

<目次>

【協会主催イベント・セミナーのご案内】

■SAAJ「(2016年度)関東地区主催新会員向けSAAJ活動説明会」(東京・茅場町)

参 加 申 込 受 付 中	日時	2016年10月22日(土曜日) 13時30分～19時00分 (交流会(懇親) 1.5Hを含む。)
	場所	NATULUCK茅場町 新館 3階大会議室 〒103-0026 東京都中央区日本橋兜町12-7兜町第3ビル
	趣旨	関東地区において 2013～2016年度に新規ご入会 いただいた 会員の皆様 に、SAAJの各研究会・部会活動にご参加頂けるよう、オリエンテーションを兼ね、開催することになりましたので、ご案内いたします。 2科目の 無料セミナー とともに、 交流会 も予定しております。会員同士のコミュニケーションの場になりますので、ぜひご参加ください。なお、終了時、 受講証明書(4CPE) をお渡しします。 ※【関東地区】主催イベントですが、支部会員の皆様のご参加も歓迎いたします。
	内容	1. SAAJの研究会及び部会からの活動内容説明：1時間 各研究会・部会の活動内容・現状・参加メリット等について、主査等が説明を行います。 2. セミナー：3時間 (資料は、当日配布します。) (1) 事例に学ぶ課題解決セミナー 簡易演習「大手銀行の基幹システム障害」(2時間) 講師：システム監査事例研究会主査 野田正勝氏 (2)「個人情報保護マネジメントシステム実施ハンドブック出版の経緯」(1時間) 講師：個人情報保護監査研究会主査 斎藤由紀子氏 3. 交流会：1.5時間 引き続き、同会場で行います。お飲み物と簡単なおつまみをご用意します。
	参加費用	・活動内容説明・セミナー： 無料。 ・交流会： 1,000円。 (当日、受付でお支払い下さい。)
	定員	40名 ◇定員になり次第締切りますので、お早目にお申し込み下さい！◇
	参加申込方法	・SAAJ活動説明会受付窓口宛 (mailto:welcome@saaj.jp) に、 以下をメール本文に貼り付けて、必要事項をご記入の上、メールでお申込み下さい。 ----- メールタイトル：「2016年度関東地区SAAJ活動説明会参加申込み」 (2016年度)関東地区主催新会員向けSAAJ活動説明会 (10/22：NATULUCK茅場町新館3階大会議室) ●参加者氏名： ●SAAJ会員番号： ●SAAJ所属支部名： (関東地区会員の方は記入ご不要) ●交流会： 参加 OR 不参加 ●名簿へのメールアドレス記載の可否： 可 OR 不可 (お名前は全員記載します。) ----- ◇お問合せ先：SAAJ活動説明会受付窓口 大西智 E-mail： welcome@saaj.jp

■ SAAJ 月例研究会 (東京)

第 2 1 7 回	日時：2016年 10月7日 (金曜日) 18:30～20:30 場所：機械振興会館 地下2階ホール
	テーマ 「ITガバナンスとITリスク管理に対する経営者視点でのシステム監査の取組み」
	講師 プロティビティ LLC 牧 正人 様 (Managing Director)
	講演骨子 企業においては、単なる業務の効率化からビジネス変革の実現へとITの活用目的や範囲が拡大し、ITガバナンスやITリスク管理の重要性が益々高まっています。 これに伴いモニタリング機能としてその一端を担うシステム監査においては、これまでのITの信頼性・安全性・効率性の視点に加え、ビジネス変革を十分に支援できるITやアーキテクチャになっているのか、変革や変化のスピードに追従できるIT管理態勢になっているのか、といったより一層の経営者視点からの監査が求められています。 現代において、ITガバナンスやITリスク管理をどのように捉え評価していくべきか、個別のリスクテーマとして注目されているデジタルトランスフォーメーションやレガシーシステムの大規模更改プロジェクトの監査をどのように進めるべきか、監査実施のポイントや事例を紹介致します。

■ ISACA 月例会 (東京)

月 例 会	日時：2016年 9月 28日 (水曜日) 18時 30分～20時 10分 場所：(財)日本教育会館 一ツ橋ホール
	テーマ (1) データ活用最前線～技術要素とユース・ケース (2) 分析を基幹業務として実施するための、データ・ガバナンスの考え方
	講師 日本アイ・ビー・エム株式会社 アナリティクス事業部 (1) テクニカル・セールス 田中 裕一 様 (2) テクニカル・セールス 時光 さや香 様
	講演骨子 (1) IoT、機械学習、AIといったテクノロジーの発展とともに、日々生み出される膨大なデータを活用した新たなビジネスの実現が加速しています。今、どのような技術要素があり、それらをどのように組み合わせれば、何が実現可能なのか。オープンソースのテクノロジーを中心としたユース・ケースとともに、データ活用のための基盤構築について解説します。 (2) データ分析を基幹業務として実現するためには、分析基盤構築もさることながら、データそのものの活用シーンを意識したデータの流れをデザインすることも重要です。ハイブリッド・クラウド環境で、データはどのように貯められ、どのように流れて、ユーザーに活用されるのか。ユーザーに品質が良く、かつ、安全なデータを提供するにはどのような発想が必要なのか。データ・ガバナンスという考え方について解説します。
	詳細 http://www.isaca.gr.jp/education/annai.html

<目次>

【2016年度秋期 公認システム監査人及びシステム監査人補の募集】

2016年度秋期 公認システム監査人及びシステム監査人補の募集の〔公告〕が協会のホームページに掲載されています。資格取得を企図されている各位はご参照願います。〔公告〕の概略は下記の通りですが、申請書等の資料のダウンロードなども、ホームページからお願い致します。

<http://www.saa-j.or.jp/csa/csaboshu/csaboshu.html>

[補足]

システム監査技術者試験の合格者以外でも、情報セキュリティその他の高度情報処理技術者試験合格者、中小企業診断士、公認会計士、技術士、ITC、CISA、ISMS/プライバシーマーク主任審査員などの各位も、「特別認定講習」を修了することによって、システム監査人補の認定申請が出来ます。また、申請前直近6年間のシステム監査実務経験（実務経験みなし期間）が2年以上あれば、公認システム監査人の認定申請が出来ます。 (<http://www.saa-j.or.jp/csa/csaboshu/guide.pdf>)

----- 記 -----

2016年8月1日

認定特定非営利活動法人日本システム監査人協会

公認システム監査人認定委員会

2016年度秋期**公認システム監査人及びシステム監査人補の募集について****〔公告〕**

認定特定非営利活動法人日本システム監査人協会（以下、協会という）は、公認システム監査人認定制度（2002年2月25日制定）（以下、制度という）に基づき、「公認システム監査人(Certified Systems Auditor : CSA)」および「システム監査人補(Associate Systems Auditor : ASA)」を認定するため、2016年度秋期公認システム監査人およびシステム監査人補の募集を行います。募集の概要と申請書等の資料の入手方法は、以下のとおりです。

1. 認定資格

公認システム監査人およびシステム監査人補とする。

2. 申請条件

- (1) 認定申請者は、経済産業省が実施するシステム監査技術者（旧情報処理システム監査技術者）試験に合格していること。（制度2（5）特別認定制度に基づく特別認定講習の修了により、上記試験の合格者と同様に取り扱う者を含む）
- (2) 公認システム監査人の申請者は、申請前直近6年間のシステム監査実務経験（実務経験みなし期間）が2年以上あること。

3. 認定申請

- (1) 申請書類（記入方法は、募集要項参照）

公認システム監査人およびシステム監査人補の申請書類は、次表のとおりとする。

申請書類	公認システム監査人	システム監査人補	記事
(1)認定申請書	○	○	様式 1
(2)監査実務経歴書	○	—	様式 2
(3)小論文	○	—	様式 3
(4)宣誓書	○	○	様式 4
(5)資格証明 (写)	○	○	
(6)申請手数料振込書 (写)	○	○	
(7)面接試験	□	—	別途通知

(注 1) ○印の資料一式を申請書類として提出する。

(注 2) □印については、面接試験を実施する。

備考：公認システム監査人とシステム監査人補を同時申請する場合は、公認システム監査人用の申請書類を提出する。

(2) 面接試験

申請書類審査後、認定委員会が別途指定・通知する日時場所において、面接試験を受ける。

4. 募集期間

2016 年 8 月 1 日 (月) ～2016 年 9 月 30 日 (金) (同日消印まで有効)

5. 認定申請手数料 (消費税 8%を含む)

申請手数料	協会会員	非会員
(1) 公認システム監査人認定申請手数料 (注 1) システム監査人補と同時申請する場合も手数料は同じです。	21, 000 円	31, 500 円
(2) システム監査人補が申請する場合の公認システム監査人認定申請手数料	10, 500 円	15, 750 円
(3) システム監査人補認定申請手数料	10, 500 円	15, 750 円

6. 資料の入手方法

【個人情報の取り扱いについて】 同意

(1) 「公認システム監査人、システム監査人補 募集要項」

ダウンロード (PDF 形式)

(2) 申請書等様式一式

- ・ 認定申請書 (様式 1) : Word 形式
- ・ 監査実務経歴書 (様式 2) : Word 形式
- ・ 小論文 (様式 3) : Word 形式
- ・ 宣誓書 (様式 4) : Word 形式

(3) 公認システム監査人認定制度のダウンロード

- ・ PDF 形式

(4) 「公認システム監査人制度」創設のお知らせ (2002 年 7 月 1 日) のダウンロード

- ・ PDF 形式

(5) 特別認定講習に関する情報

(・ 特別認定講習機関認定については参照)

以上
<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。
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、見学也大歓迎です。

ご意見募集

- ・ 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

- ・ 会報のバックナンバー公開 http://www.saaj.or.jp/members/kaihou_dl.html
電子版では記事への意見、感想、コメントを投稿できます。
会報利用方法もご案内しています。 <http://www.saaj.or.jp/members/kaihouinfo.pdf>

お問い合わせ

- ・ 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				2016.9
2016	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事	
9 月	8：理事会	7：第 216 回月例研究会 15-16:第 28 回システム監査 実務セミナー（東京：晴海）	24-25：SAAJ 中部・北信越支部・JISTA 中部合同研究会 in Nagoya	
10 月	13：理事会	7：第 217 回月例研究会 22:(2016 年度)関東地区主催新会員向け SAAJ 活動説明会（東京：茅場町）	16：秋期情報処理技術者試験	
11 月	10：理事会 13：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/6〆切） 18：2017 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	中旬：秋期 CSA 面接 30：CSA 面接結果通知	5-6： 西日本支部合同研究会 in Matsue （開催場所：松江）	
12 月	1：2017 年度年会費請求書発送 8：理事会：2017 年度予算案 会費未納者除名承認 第 16 期総会審議事項確認 12：総会資料提出依頼（1/9〆切） 15：総会開催予告掲示 19：2016 年度経費提出期限	15：CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 16：秋期 CSA 認定証発送		
1 月	9：総会資料提出期限 16：00 12：理事会：総会資料原案審議 28：2016 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	1-31：CSA・ASA 更新申請受付 20：春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕	6：支部会計報告期限 25：SAAJ 創立記念日	
2 月	2：理事会：通常総会議案承認 27：法務局：資産登記、活動報告提出 理事変更登記 28：年会費納入期限	1～3/31：CSA・ASA 春期募集	24：第 16 期通常総会	
2015	過去に実施した行事一覧			
3 月	1：NPO 事業報告書、役員変更届東京都 へ提出 7：年会費未納者宛督促メール発信 10：理事会	2：第 211 回月例研究会 5-6：第 27 回システム監査 実務セミナー(前半) 上旬：CSA・ASA 更新認定書発送 19-20：第 27 回システム監査 実務セミナー(後半)		
4 月	14：理事会 30：法人住民税減免申請	初旬：新規 CSA・ASA 書類審査 中旬：新規 A S A 認定証発行 25：第 212 回月例研究会	17：春期情報技術者試験	
5 月	12：理事会 26：年会費未納者宛督促メール発信	中旬：新規 CSA 面接 26：第 213 回月例研究会 26～27：第 28 回システム監査 実践セミナー（2 日間コース）		
6 月	9：理事会 14：会費未納者督促状発送 15～：会費督促電話作業（役員） 30：支部会計報告依頼（〆切 7/14） 30：助成金配賦額決定（支部別会員数）	10：CSA 面接結果通知 21：第 214 回月例研究会	2015/6/3：認定 NPO 法人 東京都認定日	
7 月	5：支部助成金支給 14：理事会	20：秋期 CSA・ASA 募集案内 〔申請期間 8/1～9/30〕 20：認定委員会：CSA 認定証発送 26：第 215 回月例研究会	14：支部会計報告〆切	
8 月	（理事会休会） 27：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30		

<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

2016 年度の年間テーマは「システム監査の活性化」です。システム監査の活性化について、皆様といっしょに考えてみたいと思います。8 月号から 10 月号までの四半期テーマは「システム監査への期待」です。

経営者には、システム監査を経営に活かすという知見が必要ですし、システム監査人はこういった期待に応えることが重要です。会員各位の意見を募るべく、四半期テーマとしました。

システム監査人にとって、報告や発表の機会が多く、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。気に入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 : 「会報掲載論文募集要項」及び「会報掲載論文審査要綱」をご確認ください。

□ ■ 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。

会報記事への投稿の締切日は、毎月 15 日です。

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してください）。

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】（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

=====

■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。

■会員以外の方は、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。

【会員以外の方の送付停止】 <http://www.skansanin.com/saaj/register/>

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。

■ □ ■ S A A J 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

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）

Copyright(C)1997-2016、認定 NPO 法人 日本システム監査人協会

<目次>