



認定 NPO 法人

## 日本システム監査人協会報

2018年4月号

No.205

No.205 (2018年4月号) &lt;3月25日発行&gt;

## 今月号は話題満載です。

1. 総会特集
2. 創立 30 周年記念出版案内 → 割引特典の申込書も掲載
3. 経済産業省「システム監査基準」「システム管理基準」の改訂案が公表 → 関連記事を掲載



写真提供：0557 仲厚吉

## 巻頭言

## 『システム監査基準』、『システム管理基準』が改訂されます

会員番号 6027 小野修一 (会長)

この度、仲前会長の後任として会長に就任致しました小野修一です。微力ながら、理事および会員の皆様と協力して、当協会の発展、システム監査の普及に努めます。どうぞよろしくお願い致します。

さて、皆様もご存知だと思いますが、10年ぶりに、『システム監査基準』および『システム管理基準』が改訂されます。前回の改訂が行われた平成16年から今日までの間のITの進展、IT利活用環境の多様化、ITを取り巻く社会情勢の変化などを踏まえ、改訂されることになりました。

経済産業省の強力なリーダーシップの下、システム監査に係わりをもつ4団体、日本システム監査人協会、システム監査学会、情報システムコントロール協会 (ISACA)、ITガバナンス協会からの代表メンバーによって、『システム監査基準・システム管理基準検討委員会』および『システム監査基準・システム管理基準検討ワーキンググループ』を組織し、平成29年夏から、定期的に会合をもちながら改訂作業を進めてきました。平成30年3月の時点でパブリックコメントの募集を行う段階に至っており、寄せられたご意見等を反映して4月に経済産業省から両基準の改訂版が公表される予定になっています。

平成16年版の基準に比べて、両基準ともかなり具体的な内容になっており、官民を問わず広範なIT環境やITへの取組みに対してシステム監査を実施し、健全なIT環境の構築・維持に繋げることが期待されています。

SAAJ会員の皆様には、2つの改訂版基準を有効に活用し、時代のニーズに則したシステム監査を実施するようお願いいたします。

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>

○ 巻頭言 .....	1
【『システム監査基準』、『システム管理基準』が改訂されます】	
1. めだか .....	3
【システム監査基準（案）／システム管理基準（案）について】	
2. 投稿 .....	4
【エッセイ「鉄鼠」】	
3. 総会特集 .....	5
【第 17 期通常総会を終えて】	
【第 17 期通常総会特別講演録】	
【第 17 期通常総会報告】	
【新役員体制】	
【新任理事・新任監事のご紹介】	
【2017 年度会報アワード】	
4. 本部報告 .....	20
【第 229 回月例研究会講演録】	
【システム監査基準・管理基準の改訂作業について】	
【PMS 要求事項 JIS Q 15001:2017 と「個人情報取扱規程」の事例 連載 2】	
【「発注者のプロジェクトマネジメントと監査」を刊行】	
5. 支部報告 .....	30
【北信越支部 2018 年度 支部総会・研究会報告】	
【近畿支部 第 172 回定例研究会】	
6. 注目情報 .....	37
【「システム監査基準」「システム管理基準」の改訂案に対する意見公募（経済産業省）】	
【サイバーセキュリティに関するガイドラインを公開（JASA）】	
7. セミナー開催案内 .....	38
【協会主催イベント・セミナーのご案内】	
【外部主催イベント・セミナーのご案内】	
8. 協会からのお知らせ .....	40
【新たに会員になられた方へ】	
【協会行事一覧】	
9. 会報編集部からのお知らせ .....	42

注目：基準改訂

注目：基準改訂

注目：記念出版

**めだか 【 システム監査基準（案）／システム管理基準（案）について 】**

システム監査人は、監査テーマに関して被監査部門の人たちとコミュニケーションをとって監査を行っていくが、コミュニケーションにおいてお互いに相手の言葉を100%理解できているかということ、それは難しい。しかし、監査テーマを限って行えば、相互理解はその範囲で大きく乖離しないものである。ただし、範囲を限定しすぎると全体的な問題が見えなくなるため、監査テーマの範囲を決める匙加減が大切である。

SAAJの「システム監査人倫理規定」では、第4条（監査基準・手続き）に、“システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。”とある。システム監査人は、「システム監査基準」、及び「システム管理基準」を参考に、被監査部門に対して、監査テーマの範囲を決め、システム監査の基準、手続きを明らかにして、システム監査を行う必要がある。

このたび、経済産業省商務情報政策局サイバーセキュリティ課より、「システム監査基準（案）」、「システム管理基準骨子（案）」及び「システム管理基準（案）」が公表され、パブリックコメントが求められている。「意見公募の趣旨・目的・背景」には、次のように述べられている。

“経済産業省では、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るシステム監査制度について、「システム監査に関する検討会」を開催し、制度に関する見直しを進めて参りました。このうち、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」、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」について、昨今の社会情勢の変化や技術の進展等を踏まえ、改訂をいたしました。両基準について、広く国民の皆様から御意見をいただきたく、以下の要領で意見の募集をいたします。忌憚のないご意見を下さいますようお願い申し上げます。”

システム監査人は、今後、「改訂システム監査基準」、及び「改訂システム管理基準」の制定により、それらを熟読、理解し、昨今の社会情勢の変化や技術の進展等を踏まえたシステム監査業務にあたることが求められる。

参考：「システム監査人倫理規定」平成14年2月25日制定 日本システム監査人協会



(空芯菜)

(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。)

**【エッセイ】 鉄鼠**

会員番号 0707 神尾博

多数のマシンから、大量のパケットやサービス要求を特定のサーバに送り付け、パフォーマンスの低下や機能停止に追い込む DDoS (Distributed Denial of Service) 攻撃。防御が極めて困難であるため、セキュリティ技術者にとって、至って頭の痛い厄災だ。たとえば ISP による、ターゲットへのパケットを消滅させるブラックホールルーティングのようなやり方では、正当なものまで届かなくなるという、とてつもない代償を払う必要がある。おまけに攻撃側からすれば、マルウェアに感染させた他人の機器のリソースを使うので、原価が激安なことも、被害者側にとって腹立たしい限りだ。

従来の DDoS 攻撃は、数多くのパソコンに感染したマルウェアによるボットネットを、指令者が遠隔操作するものが中心だった。他には DNS を利用するものもある。ところが 2016 年に発見された Mirai は、Linux 系のネットワークカメラやプリンタ等を踏み台にする。2017 年には、IoT デバイスのストレージを破壊し再起不能にする、極めて悪辣な PDoS (Permanent Denial of Service) 攻撃の被害拡大も報告されている。また単にサービス妨害だけでなく、攻撃停止と引き換えに金銭を要求する DDoS 脅迫 (DDoS Extortion) まで登場する始末だ。

平安時代には、白河天皇の「皇子が誕生したら何なりと褒美を与える」との命を受け、それを祈祷で果たした頼豪という僧侶がいた。ところが、横槍を入れた延暦寺により「三井寺に戒壇院建立」という天皇との約束を反故にされた。彼は「鉄鼠 (てっそ)」となり、皇子を呪い殺したばかりか、84,000 匹もの鼠を率い比叡山の経典を食いちぎったという。物量作戦による妨害や破壊行為は、この時世から存在したようだ。

現代では、鼠は IT、特に有線伝送路の大敵だ。経典ならぬネットワークケーブルを噛んで、いとも簡単に断線させる。これには、被覆に唐辛子成分を練りこむ等の対策がなされている。大量の鼠といえば、築地市場移転の際に、500 匹とも 5,000 匹ともいわれる鼠が、銀座方面に移動するのではないかと危惧されている。そういえば著者も、会社に近接する施設や、実家の近所の民家の解体の際には、思い当たる節があった。

システム監査では、頼豪のような恨みを持つ者による人的リスク、DDoS 攻撃のような技術的リスク、そして電線や機器への物理的リスクへの備えのチェックについて、もれなく実施しなければならないのは言うまでもない。

(このエッセイは、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。画像は Wiki により著作権保護期間満了後のものを引用しています。)



&lt;目次&gt;

**総会特集 【 第 17 期通常総会を終えて 】**

会員番号 0557 仲厚吉 (会長\*)

\*本ページ以下の「総会特集」において、役職名の記載は総会開催時の役職名としています。

第 17 期通常総会が、2018 年 2 月 23 日に開催され、定款変更、2017 年度事業報告及び決算、2018 年度事業計画及び予算、並びに理事・監事の選任をご承認いただき、会員の皆様には篤く御礼を申し上げます。

2018 年度は、1 年を通して、創立 30 周年記念行事が行われます。その端緒として、通常総会当日、特別講演「人工知能研究の最新情報－インタラクティブな人工知能を目指して－」と題し、人工知能学会山田誠二会長をお招きして特別講演を開催、また、会場において、創立 30 周年記念出版「発注者のプロジェクトマネジメントと監査」(同文館出版)をお披露目し好評を得ました。

2 期 4 年、会長を務めてまいりましたが、このたび、新メンバーの登用を図る趣旨から、会長を退任することに致しました。会員の皆様にご利用を心より感謝いたします。在任中のトピックスのひとつに、協会活動の公益性を認定 NPO 法人として所轄庁の東京都より認定されたことがあります。これは担当された役員の皆様のご協力があった実現できました。認定 NPO 法人として協会活動の公益性をアピールしていくとともに、認定を維持するため会員の皆様にご寄附のご協力をお願い申し上げます。

2018 年 3 月 8 日の理事会において新会長は小野修一会長に決まりました。今後は小野修一会長のもと、協力して当協会の発展に努めてほしいと思います。2018 年は、経済産業省より「システム監査基準」、「システム管理基準」の改訂版が発行されます。また、「IT ガバナンスのアセスメント」の ISO 化、等々、協会に求められる活動が目白押しの 1 年になります。微力ながら引き続き協会活動に協力してまいりたいと思います。

&lt;目次&gt;



**総会特集****第 17 期通常総会特別講演録 【人工知能研究の最新情報－インタラクティブな人工知能を目指して－】**

会員番号 0557 仲厚吉（会長）

第 17 期通常総会で SAAJ 創立 30 周年を記念して特別講演が開催されました。

第 17 期通常総会特別講演 会場：機械振興会館 日時：2018 年 2 月 23 日 15 時 30 分～17 時

演題：「人工知能研究の最新情報－インタラクティブな人工知能を目指して－」

講師：人工知能学会会長 国立情報学研究所 総合研究大学院大学 東京工業大学 山田誠二教授

講演の要約

○AI を取り巻く状況、人工知能 AI とは何か

・現在の第 3 次 AI ブームは、「過度な期待」のピーク期にあたる。人工知能 AI とは、(人間並みの) 知的な処理をコンピュータ上に実現するもので、ダートマス会議 (1956) に始まる第 1 次 AI ブームから約 60 年が経過した。人工知能 AI には、「強い AI」即ち単独で人間と同等の AI を目指す研究と「弱い AI」即ちあくまで人間をサポートする知的システムを目指す研究がある。

○AI ここ数年のトピック－第三次 AI ブーム－

・1980 年代の第 2 次 AI ブーム (記号処理・論理、エキスパートシステム) の後、2010 年代の第 3 次ブームの AI は何が違うのかというと、「統計的機械学習」と「ニューラルネットワークの復権－ディープラーニング」である。第 3 次ブームの AI 実用化ブレイクの背景にあるのは、ビッグデータと計算機パワーである。

・AI 研究の主流は、論理・記号・可読な知識を扱う AI である。機械学習 (ML) は、AI のごく一部、さらに、ニューラルネットワーク (NN) は、ML の一部、さらに、ディープラーニングは、NN の一部である。

○AI の得手／不得手、AI で変わる社会－今後有望な応用分野－

・ディープラーニングの成功例として、一般物体認識、テレビゲームの学習、Google の猫、AlphaGO がある。しかし、ディープラーニングは万能ではない。上手くいく／いかないが予測不能のため応用分野選定のノウハウが蓄積されないという弱点がある。

・AI で変わる社会－今後有望な応用分野－は、賢い情報検索、高度なパターン認識、会計関連、ネット利用の様々なサービスの AI 化が挙げられる。

○人工知能学会 (JSAI) 倫理指針

・人工知能学会 (JSAI) では、2017 年 2 月 28 日、人工知能学会会員に向けて「倫理指針」を掲げ、「1. 人類への貢献」「2. 法規制の遵守」「3. 他者のプライバシーの尊重」「4. 公正性」「5. 安全性」「6. 誠実な振る舞い」「7. 社会に対する責任」「8. 社会との対話と自己研鑽」「9. 人工知能への倫理遵守の要請」を挙げている。

○これからの AI－インタラクティブ AI－

・これからの AI は、人間と AI が得意分野を補い合い協調して問題解決にあたるインタラクティブ AI である。

感想

人工知能研究の権威である人工知能学会会長山田誠二教授による特別講演は人工知能研究を俯瞰し未来を展望するすばらしい講演で受講者の皆様は大満足だったと思います。

&lt;目次&gt;

**総会特集 【 第17期通常総会報告 】**

会員番号 1581 齊藤茂雄（事務局）

第17期通常総会は以下のとおり行われました。

1. 日 時 2018年2月23日（金） 13:30～14:30
2. 場 所 東京都港区芝公園3丁目5番8号  
機械振興会館 地下3階 第1研修室
3. 出席者数 136名（委任状65名を含む）
4. 審議事項
  - （1）定款一部変更の件
  - （2）2017年度事業報告の件
  - （3）2018年度事業計画の件
  - （4）2018年度予算の件
  - （5）役員選任の件
5. 議事の経過の概要および議決の結果  
互選により、館岡副会長を議長に選任し、続いて上記5議案の審議を行った。  
議長より本日の議事録をまとめるにあたり、議事録署名人2名を選任することを諮り、互選により齋藤由紀子副会長、齊藤茂雄理事の2名を選任した。  
第17期通常総会資料に基づき、以下の通り審議及び議決が行われた。
  - （1）定款一部変更の件  
仲会長より定款の一部変更について説明を行い、審議を諮ったところ、全員異議なくこれを可決した。
  - （2）2017年度事業報告の件
    - 1) 事業概要報告  
仲会長より2017年度事業報告について説明を行った。
    - 2) 会計報告及び監査報告  
安部会計担当副会長より2017年度の会計決算報告について説明を行い、続いて木村監事より監査報告が行われた。  
上記について審議を諮ったところ、全員異議なくこれを可決した。
  - （3）2018年度事業計画の件  
仲会長より2018年度事業計画（案）について説明を行い、審議を諮ったところ、全員異議なくこれを可決した。
  - （4）2018年度予算の件  
安部副会長より2018年度予算（案）について説明を行い、審議を諮ったところ、全員異議なくこれを可決した。
  - （5）役員選任の件  
齋藤事務局長より役員選任（案）について説明を行い、審議を諮ったところ、全員異議なくこれを可決した。

以上により本日の議事を終了し、議長は会員各位の今後の協力を要請して閉会を宣言した。

&lt;目次&gt;

総会風景



仲厚吉会長



斎藤由紀子事務局長



司会：松尾正行理事



議長：館岡均副会長



会計報告：安部晃生副会長



監査報告：木村祐一監事



総会風景



出版報告：原田理事 (PJM 監査研)



特別講演講師 人工知能学会会長 国立情報学研究所教授 山田誠二 氏





【各支部長の紹介】



宮崎雅年 北海道支部長



横倉正教 東北支部長



宮本茂明 北信越支部長



久保田秀男 中部支部長



荒町弘 近畿支部長



廣末浩之 中四国支部長

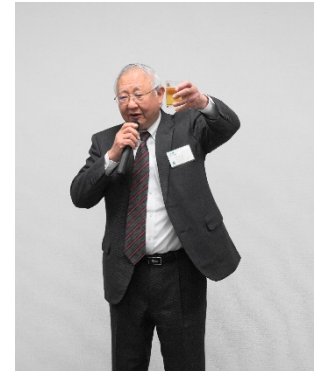


船津宏 九州支部長

総会終了後の懇親会模様



司会：野田正勝理事



乾杯：小野修一副会長

同日開催された本部・支部慰労会風景



<目次>

総会特集 【 新役員体制 】
----------------

会員番号 1581 齊藤茂雄 (事務局)

第17期は役員改選期にあたるため、総会において、以下のとおり役員が選任されました。

	役員	氏名	備考	
本部	1	理事	安部 晃生	
	2	理事	大石 正人	
	3	理事	小野 修一	
	4	理事	加佐見 明夫	
	5	理事	越野 雅晴	
	6	理事	齊藤 茂雄	
	7	理事	斎藤 由紀子	
	8	理事	櫻井 俊裕	
	9	理事	櫻井 由美子	
	10	理事	佐々野 未知	
	11	理事	清水 恵子	
	12	理事	鈴木 信夫	
	13	理事	竹原 豊和	新任
	14	理事	舘岡 均	
	15	理事	力 利則	
	16	理事	戸室 佳代子	
	17	理事	豊田 諭	新任
	18	理事	中山 孝明	
	19	理事	仲 厚吉	
	20	理事	野田 正勝	
	21	理事	原 純江	
	22	理事	原田 憲幸	
	23	理事	林 昭夫	
	24	理事	福田 敏博	新任
	25	理事	松枝 憲司	
	26	理事	松尾 正行	
	27	理事	三谷 慶一郎	
	28	理事	三輪 智哉	
	29	理事	柳田 正	
	30	理事	山口 達也	新任
北海道	31	理事	宮崎 雅年	
東北	32	理事	横倉 正教	
北信越	33	理事	宮本 茂明	
中部	34	理事	久保田 秀男	新任
	35	理事	安井 秀樹	新任
近畿	36	理事	荒町 弘	
	37	理事	福本 洋一	
	38	理事	荒牧 裕一	新任
中四国	39	理事	廣末 浩之	
九州	40	理事	船津 宏	新任
監事	41	監事	木村 裕一	
	42	監事	大西 智	新任

<目次>

<b>総会特集 【 新任理事・新任監事のご紹介 】</b>
-------------------------------

今年度から新たに理事・監事になられた方は、以下の9名（本部4名、支部4名、監事1名）です。

本部理事	竹原豊和
本部理事	豊田 諭
本部理事	福田敏博
本部理事	山口達也
中部支部理事	久保田秀男
中部支部理事	安井秀樹
近畿支部理事	荒牧裕一
九州支部理事	船津 宏
監事	大西 智

上記9名の方に、それぞれの自己紹介をお願いいたしました。

=====

#### 会員番号 2574 竹原豊和（本部理事）

このたび、理事に就任させていただきました竹原豊和と申します。私は現在、株式会社スクウェア・エニックスという、主にゲームアプリケーション関連事業及び出版事業を展開している企業にて、システム監査の手法を使用したアプリケーションの通信品質試験を実施しております。この試験は、付随する仕組みも含めて問題が無いかの試験とフォローアップを実施しておりますので、システム面に特化した内部システム監査と言ったほうがわかりやすいかもしれません。日本システム監査人協会の会員の方の中には、情報通信や情報セキュリティに強い方が多数いらっしゃいますので、今後も御教授及び御指導いただき、スキルアップに努めさせていただきたいと考えております。御教授及び御指導いただきたく、宜しくお願い致します。



また、私自身、至らない点が多々あるかと思いますが、これまでの経験を活かして今後の日本システム監査人協会及びシステム監査の発展に寄与させていただきたいと考えておりますので、重ねて御教授及び御指導いただきたく、宜しくお願い致します。

**会員番号 1200 豊田 諭 (本部理事)**

この度、新たに理事に就任いたしました、豊田 諭と申します。

私は、商社の情報システム部門に所属し、子会社を含む国内外システムの開発、運用、保守と各種管理業務に携わった後、2年前に退職いたしました。当協会には2002年に入会いたしましたが、退職前に情報セキュリティとITガバナンスの基準・規程等の整備とその運用確認などの業務に関わっていたこともあり、現在はITアセスメント研究会と情報セキュリティ監査研究会に所属して活動しております。



昨今の情報技術の発展は凄まじいものがあり、システム監査が対象とするシステム自体が高度化、複雑化し、システムの範囲も拡大し続けていますので、これに合わせ、システム監査の拠り所である各種基準・規程類も常に見直し進化させる必要があります。また、システムが抱える情報セキュリティなどのリスクも同じく高度化、複雑化し、対象範囲が拡大し続けていますので、今や情報セキュリティはシステム監査から外せないものと捉えています。

皆様のご指導ご鞭撻をいただきながら、両研究会の活動等を通じて協会や会員の皆様に少しでも貢献できるように努めてまいりたいと思います。どうぞ宜しくお願いいたします。

**会員番号 2422 福田敏博 (本部理事)**

このたび新たに理事に就任しました福田敏博です。私はエンジニアリング会社に勤務し、現在は産業オートメーションのサイバーセキュリティを専門にコンサルティングをしています。手前味噌ながら、この業界の第一人者として「工場・プラントのサイバー攻撃への対策と課題がよ〜くわかる本」を書いています。

<http://www.amazon.co.jp/dp/4798044466/> (Kindle版もあります)

一般的な情報システムでは、IT (Information Technology) という用語を使います。一方、産業オートメーションでは、OT (Operational Technology) という用語が使われるのを、皆さんご存知でしょうか。昨年あたりから、産業系のシステム (制御システム等) をOTシステムと呼ぶことが増えてきました。

近年OTでは、ITと同じようなサーバやパソコン、ネットワークなどが活用されています。しかしながら、OTのセキュリティリスクが十分認識されていなく、大手企業でもセキュリティ対策が進んでいないのが現状です。個人的には、そもそもOTでガバナンスの観点が欠落しているのが問題だと感じています。

今後は協会の活動を通して、OTガバナンスといった新たな分野を開拓したいと思っています。何卒よろしくお願いたします。



**会員番号 2063 山口達也（本部理事）**

この度、新たに理事に就任しました山口と申します。IT に関しては、約 9 年間、大手銀行のシステム開発業務を担当した後、監査法人に転職し、以降約 18 年間、主に金融機関を中心に IT 内部統制に関する外部監査（財務諸表監査）、システムリスク管理、情報セキュリティ、個人情報保護、大型プロジェクトマネジメント、内部監査品質評価等の外部評価や態勢構築支援等に従事してきました。昨今では、従来のシステム監査における安全性・信頼性・効率性の観点に加え、有効性の観点から評価する IT ガバナンスに関する外部評価等にも従事しております。



上記の通り、これまでではどちらかといえば現場における実践的な対応が中心であり、「システム監査はどうあるべきか」等の理論的な話は相対的にあまり関与してきておりませんでした。今回協会の理事に就任したことを契機に、こちらの方面についても皆様と一緒に知見を深めていきたいと考えております。

また、逆にあるべき論とは別に、現実がどうなっているのかといった情報のフィードバック等、これまでの自身の経験や本業としてシステム監査に携わっている事を活かしつつ協会に貢献していきたいと思っております。

どうぞよろしくお願い致します。

**会員番号 1112 久保田秀男（中部支部理事・支部長）**

この度、新たに理事（中部支部長）に就任いたしました久保田と申します。私は 1982 年に地銀に入学し、営業店で 2 年の内務事務全般、3 年の渉外係を経験した後、システム部門に異動となり、主に情報系システムの企画・開発を担当しました。また、当時本店ビル内にあったシステムを更改し、併せて新設のセンターに移行することにも携わりました。システム部門には 7 年余り所属し、その後、東京事務所、営業開発部門、内部監査部門、及び企画部門を経て、約 4 年前に連結子会社のリース会社に転籍となり、システムを含む業務全般を所管しています。システム更改に関しては、前述した更改以外に所属した各部門で携わり、銀行で計 3 度経験いたしました。現在のリース会社においても、リースの基幹システムのパッケージシステムへの更改を担当し、2 年ほど前に移行を完了いたしました。また、内部監査部門に所属したときには、主に本部各部に対する業務監査、及びシステム監査を担当し、IT 統制、オペレーショナルリスク管理の高度化に対する監査が必要となった際は、監査法人、コンサルなどと協議し監査の企画も行いました。



システム監査技術者試験は、東京事務所での勤務の中で銀行協会、関係省庁などとの会議、打合せなどのなかで、異動前のポジションでは、ユーザ部門と打合せ、システムを企画、開発、リリースまでを一貫して行う、建築で例えると大工のような仕事を行ってききましたが、システムを施工主の立場で管理する、建設会社の管理者のような視点での仕事を経験したことから、そういった能力を整理する意味で受験し合格しました。合格後、2014 年に当協会に入会し、以来、なかなか研究会に参加できない幽霊会員のような状態の時もありましたが、現在まで協会活動に参加してきております。

今後、中部支部長として、支部活動のより一層の活性化に努め、「経営に役にたつシステム監査とは」など各種のテーマについて研究会を通して考えていきたいと思っております。

### 会員番号 1694 安井秀樹（中部支部理事・副支部長）

安井秀樹、と申します。愛知県生まれの愛知県育ちで54歳です。所属は富士通株式会社です。大学（文系）卒業後に入社し、30数年経ちました。入社した頃は「SE30歳定年説」と言われていましたので、この年までSEをやっているとは想像していませんでした。現在は、社内のシステム開発プロジェクトの健全性やリスクの監査や若手向けに品質管理の教育などを担当しています。協会へは2008年に入会し、中部支部所属です。



実家は愛知県にありますが、2012年より大阪勤務のため、普段は大阪暮らしです。

関西にいますので、冬季（新酒）限定で、灘五郷、京都伏見、奈良の日本酒の蔵めぐりをしています。春から夏にかけては、ビール工場や日本ワインの醸造所などを訪ねています。秋はサントリー山崎蒸留所の有料ツアーに参加するのが恒例になりつつあります。という訳で、拘りなく、何でも呑む、普通の酒好きのおっさんです。どうぞ、よろしくお願ひします。

### 会員番号 0655 荒牧裕一（近畿支部理事・副支部長）

このたび理事及び近畿支部副支部長に就任いたしました、荒牧裕一と申します。よろしくお願ひいたします。

私が「情報処理システム監査技術者試験」に合格したのは25年前の平成5年でした。当時は27歳以上でなければ受験資格が無かったのですが、その27歳を迎えた記念のつもりで受験したところ、たまたま午後Ⅱの論述のテーマが自分の得意のテーマだったこともあり合格してしまい、かえって戸惑ったことを憶えています。すぐに協会に入会して例会に参加したのですが、もちろん私が最年少で周囲の方はベテラン揃い、話の内容も高度で付いていくのが大変でした。



それから私も、監査法人で実務を経験するなど少しずつですが経験を重ね、年下の会員も徐々に増え、今では年長組の一員として活動しております。たまたま合格したことがコンプレックスだった試験についても、試験名称が「システム監査技術者試験」に変わった後の平成21年に再度受験して、今度は実力で合格しました。

私の経験がどの程度お役に立てるかは判りませんが、出来る限りのことをしたいと思っております。

**会員番号 0811 船津 宏 (九州支部理事・支部長)**

この度九州支部長になりました船津 宏です。こんにちは。

私は NEC グループのシステムエンジニア出身で、平成 9 年に SAAJ に入り、21 年目ということになります。九州支部は、ビデオ視聴や情報交換を中心に月例会を開催しており、ずっと啓発を受けており、プライバシーマークの審査員になることができたなど実利も経験しています。

私は先人が維持してきたこの活動をこれからも世話役として支えて行きたいと思っています。

個人的には、趣味は旅好き、新しいもの好きです。審査員の仕事は、出張や新しい事業プロセスに接するという意味で、趣味と一致しています。

SAAJ の活動としては、本部との連携の強化などで新たな活動を模索したいと思いますので、ご指導ご鞭撻の程よろしくお願い申し上げます。

**会員番号 1697 大西 智 (監事)**

この度、金子監事の退任の後を受け、新たに監事に就任しました大西智です。

当協会には、2008 年 4 月に入会し、システム監査の実務経験がないため、システム監査事例研究会に同年 10 月より参加させて頂きました。事例研究会では、「事例に学ぶ課題解決セミナー」の立上げに参加し、システム監査について色々勉強させて頂きました。システム監査実務・実践セミナーにも参画させて頂き、先輩の方々より、セミナー教材の作成・改訂、セミナー事務局運営並びにセミナー講師の心構え・ノウハウ等をご伝授頂きました。

2014 年より、理事を 2 期 4 年務めさせて頂きました。2014~2015 年は事例研究会の主査を務め、システム監査普及サービスの受託もさせて頂きました。2016~2017 年は、システム監査活性化委員会・情報セキュリティ監査研究会の担当理事をさせて頂きました。

2 期 4 年務めたため、理事を退任することにしましたが、理事退任の代わりに、監事の役を仰せつかりました。よろしくお願いいたします。



<目次>

**総会特集 【 2017年度 会報アワード 】**

会員番号 1795 藤澤 博 (会報主査)

## 【 2017年度 会報アワードの表彰について 】

2017年1月から12月までの会報記事の投稿の中から、以下のとおり表彰者を選定しました。

「めだか」の部	:	空心菜
「本部報告」の部	:	ホームページ運営委員会
「支部からの優良報告」の部	:	近畿支部、北海道支部



会報アワードの発表 (藤澤主査)

## \*参考【 会報アワード制度について 】

会報アワード制度は、2010年度会報記事の投稿から「めだか」、「投稿記事、エッセイ」、「部会や支部からの優良報告」の3分野に分けてスタートし、優秀作品に対し、総会時に表彰することとしました。今回で8回目の表彰です。以前は会報記事の投稿者に薄謝として図書券を配布していた制度に変わるものです。これからも、会報への積極的な投稿をお願いします。

以上

&lt;目次&gt;



**本部報告****第229回月例研究会講演録 【 IT ガバナンスの国際標準化の最新動向とその取り組み 】**

会員番号 2574 竹原豊和

【講師】 SAAJ ITアセスメント研究会 有志

松尾正行氏 (ISO/IEC JTC1/SC40 WG1 メンバー)

カ 利則氏 (ISO/IEC JTC1/SC40 専門委員&amp;WG1 メンバー)

【日時・場所】 2018年1月29日(月) 18時30分~20時30分 機械振興会館 B2F ホール

【テーマ】 「IT ガバナンスの国際標準化 (ISO/IEC38500 シリーズ) の最新動向とその取り組み」

**【要旨】**

企業経営における IT 戦略として、IT 効果の最大化、IT リスクの最小化、コンプライアンス実現のために IT ガバナンスの導入と確立が重要かつ効果的と考えられている。IT ガバナンスに関しては、日本では 2015 年 7 月に「JIS Q 38500:2015」として JIS 化されたが、グローバルな取り組みとしては、ISO/IEC38500 として 2008 年に初版ができ、その後 38501、502、504、505 等が発行され、ISO/IEC38500 も 2016 版として改訂も進み、諸外国ではその重要性を理解して 取組みも本格化している。

今回の月例研では、SAAJ の IT アセスメント研究会 (松枝主査) の有志で、「ISO/IEC SC40 専門委員会 (IT サービスマネジメントと IT ガバナンス)」の日本の WG1 メンバーであるお二人が、IT ガバナンスの国際標準化 (ISO/IEC 38500 シリーズ) の最新動向と日本での取組みと課題について、解説する。

**【講演録】**

第一部 : 38500、501、502、504、505 の説明 (カ氏)

IT ガバナンスは ISO/IEC38500 となっており、38500、501、502、504、505、それと 503 が存在する。503 については日本主体で進めている ISO 規格であり、その辺りについては第二部で松尾氏に解説いただく。

IT ガバナンスに関して、日本では 2015 年 7 月に「JISQ1 38500:2015」として JIS 化されている。なお、38500 シリーズにおいて JIS 化されているのは、38500 のみであり、その他については現状で JIS 化及び日本語化されていない。IT ガバナンスの国際標準化については、2013 年 11 月の ISO/IEC の JTC1 (第 1 合同技術委員会) の総会で、専門委員会設立が承認され、2014 年 2 月より活動を開始した「SC40 専門委員会」にて検討が進められている。システム監査と IT ガバナンスは、本来密接な関係である内容だが、この委員会に SAAJ のメンバーも参加しており、その意味からも双方にとって有意義な関係性を構築している。

今現在 IT を企業経営に活用していない企業など皆無であるため、IT は一般的に「企業経営と密接な関係」である状況だが、その企業経営において重要となる「コーポレートガバナンス」の一部を担うものが「IT ガバナンス」となっている。

SC40 には様々な WG が存在しているが、その中の WG1 が IT ガバナンスとなっている。なお、WG2 が IT サービスマネジメント、WG3 が IT を使ったビジネスプロセスアウトソーシング、WG4 が IT サービスマネジメントインフラストラクチャとなっている。

WG1 は様々な国から構成されており、英国を含む EU の多数の国々、豪州、北米、中国、韓国、そして日本が参加している。Expert 登録者名も 100 名以上となっており、日本国内における WG1 のリエゾン日本 IT ガバナンス協会と SAAJ となっている。

38500 シリーズの中で 38500 は JIS 化されているため、日本語化が行われているが、その他については SAAJ の IT アセスメント研究会にて和訳している状況となっている。38500 シリーズにおいては、IT ガバナンスと事業プロセスに分けて考えている状況だが、この中の事業プロセスにおいては「P→D→C→A (PDCA)」というサイクルとなっているが、IT ガバナンスは「Evaluate→Direct→Monitor (EDM)」というサイクルとなっている。

この EDM の詳細を説明すると E が「現在と将来の IT の利用についての評価」、D が「ビジネス目標に合致するように、計画とポリシーを策定し、実施」、M が「ポリシーへの準拠と計画に対する達成度をモニター」となっている。IT ガバナンスを考える際、良質な IT ガバナンスのために、「責任」「戦略」「取得」「パフォーマンス」「適合」「人間行動」という 6 つの原則がある。この 6 つの原則は IT ガバナンスにおいて経営者に必要な条件ともいえる。

38500 シリーズのそれぞれの内容を簡単に説明すると 38501 が「導入ガイド」となっており、IT ガバナンスをどのように導入するのか、といった内容となっている。38502 については「フレームワークとモデル」となっており、ガバナンスとマネジメントの関連と、それぞれに伴う責任を明確にするモデルを規定するといった内容となっている。38504 については「原則基盤の標準ガイド」、「原則ベースの基準ガイダンス」となっており、一般的な推奨指針をそれらの形式、内容と記述レベルに関して提示するといった内容となっている。38505-1 については、新規格であるが、データガバナンスという位置づけとなっている。データガバナンスを規格化することにより、経営者が IT についてきちんとした説明責任が要求されるという意味で「IT ガバナンス」が重要視される状況となる。また、データガバナンスの応用として 38505-2 がある。

38500 については、JIS 化されているとおり、適用範囲は「組織のディレクタ（この場合、経営者）のために、その組織内で IT の効果的、効率的で受容可能な使用に関するガイドとなる原則を提供すること」となっている。また、対象となる組織はあらゆる大きさであり、公的、私的の区別なく NGO も含めた組織となっている。

なお、日本語化においては、特に用語の翻訳に苦心した。例えば、IT ガバナンスを意味する英語は「corporate governance of IT」となっているが、この場合だと「企業のみ」と勘違いされてしまう可能性があり、実際には企業だけではなくその他の組織も含んでいるため、corporate（企業）は訳さずに IT ガバナンスとしている。

38500 シリーズの特徴である「EDM モデル」については、日本国内において特に経営者に伝わっておらず、どのようにして伝えていくべきかという部分は現状の課題と考える。

38501 に関しては IT ガバナンスの導入ガイドであり、国の政策としての位置づけも大きいと考える。したがって、この 38501 の JIS 化（日本語化）を進めることで、「IT ガバナンスをどのように導入したらいいのか」、「経営者が IT に対してどのように取り組めばいいのか」、「グローバルな競争の中でどのように取り組んでいけばいいのか」を知ってもらうことが可能となる。また、同様に 38502、38504、38505-1 についても積極的な JIS 化（日本語化）が必要と考える。

## 第二部：38503 の説明（松尾氏）

ISO/IEC 38503 は、日本主導で導入が進められており、2018 年 1 月末までに 38503 の NWIP (New Work Item Proposal) を提出できるよう原案を作成中である。38503 は過去のプロジェクト期限切れにより、2017 年 5 月の岡山会議後から再スタートした準備中のプロジェクトである。

38503 が正式にプロジェクトとして認められるのは最短で 2018 年 6 月で、それまでに提案（NWIP とドラフト文書の作成）と投票を完了する必要がある。この作業を有志 6 カ国で行っている状況である。

38503 は、IT ガバナンスのアセスメントに関する国際規格であるが、その範囲はガバナンスレイヤーから

マネジメントレイヤーとのインターフェースまでをカバーしており、内容として「目的と範囲 (Scope and Objective)」、「アセスメント手法と実施(The Approach for Assessment, Implement Assessment Programme)」、「成熟度評価モデル (Maturity Assessment Model)」、「便益成果と成功証拠 (Beneficial Outcomes and Evidence of Success)」の4つに大別されるが、その背景として「ガバナンス行動 (Governance Behavior)」なども検討している。

38503 の適用範囲は、「経営陣、上級マネジャ、スキルのある評価者に対して IT ガバナンスのアセスメントの計画と実行を支援」「(IT 利用の程度に関係なく) すべての形態、規模の組織に適用」となっている。また、38503 の目的は、「組織における IT ガバナンスのアプローチと手法のガイダンスの提供」「経営陣に、組織における IT ガバナンスが適切に行われているかの評価を提供」「組織における IT ガバナンスの改善点と手法の提示」となっている。

さらに「IT ガバナンス環境の評価」「ガバナンスフレームワークの評価」「組織背景の明確化の評価」「IT 利用に関する現状及びあるべき状態の明確化の評価」「変革プログラムの評価」「モニター能力の評価」といった6つの主要局面の評価も重要となっている。

ガバナンスには「ソフト」と「ハード」があり、ソフト面においては非共通的なもの、反対にハード面においては共通的なものが多い。ガバナンス行動においては、HOW と WHAT に分けすることが可能であり、「HOW」はマネジメント層、「WHAT」はガバナンス層中心となっている。また、ガバナンスの評価はアセスメントの範囲だけではないことにも留意する。評価の形態を主観性と客観性に区分した場合、経営陣による自己評価は主観的、内部/外部のアセッサによる評価は客観的と考えられる。その中間に位置するファシリテータ方式はハイブリッド的なものとなっており、バランスが良い形と考えられる。

今後の開発スケジュールは、2017年2月初旬にNWIP,CD/WDの提出、2018年2月～4月がNWIPに関する投票、2018年5月がNWIP,CD/WDに対するコメント期間、2018年6月にSC40WG1全体会議での方向決定、2018年6月以降に38503のドラフト標準の開発となる。NWIPの投票においては、5か国の賛成を得られれば承認される。

近い将来改訂が予定されている日本の「システム監査基準」「システム管理基準」において、第一章にITガバナンスが記載される予定となっており、その意味でもITガバナンスは今後システム監査と密接な関係を持つことが予測される。その際に対応が行えるようにするためには、38500シリーズを理解しておくことが大事である。

#### 【所感】

今回、御講演いただいた「ITガバナンスのアセスメントの国際標準化」を聞かせていただいた率直な感想として、今後のシステム監査においては、ITガバナンス分野を無視できない状況になっていることを実感した。

近い将来更新される、システム監査基準やシステム管理基準にITガバナンスに関する規定が追加されるため、ITガバナンスは今まで以上にシステム監査業務に意味を持つこととなるが、規定の有無に関わらずこれだけITが一般化している現在、やはりITガバナンスという視点からシステム監査を行っていくことは、これからの時代において、ある意味で当たり前なこととなっていく、そしてシステム監査という行為そのものが更に重要視されていくのではないだろうか、と感じた。

<目次>

**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 】**

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・管理基準改訂作業の目的

システム監査基準及び管理基準は公表から10年以上経過しており、社会情勢の変化(ITガバナンスが重視され、情報システムの構築・運用管理方法も多岐にわたるようになった等)に十分な対応ができていないと難しいことから、企業等の情報システムの戦略的な構築・運用管理の実現を支援し得る、質の高いシステム監査制度の基盤を構築することを目的として改訂されました。原案は3月中旬にパブリックコメントを募集しており、この会報が出るタイミングでは、パブコメを受けた後の新基準が提示されていると思われます。

以下はパブコメ案で示された新システム監査基準と管理基準の目次です。

## ○システム監査基準 (案)

前文 (システム監査基準の活用にあたって)

I. システム監査の体制整備に係る基準	IV. システム監査実施に係る基準
【基準1】システム監査人の権限と責任等の明確化	【基準8】監査証拠の入手と評価
【基準2】監査能力の保持と向上	【基準9】監査調書の作成と保管
【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	【基準10】監査の結論の形成
II. システム監査人の独立性・客観性及び慎重な姿勢に係る基準	V. システム監査報告とフォローアップに係る基準
【基準4】監査人としての独立性と客観性の保持	【基準11】監査報告書の作成と提出
【基準5】慎重な姿勢と倫理の保持	【基準12】改善提案のフォローアップ
III. システム監査計画策定に係る基準	
【基準6】監査計画策定の全般的留意事項	
【基準7】リスクの評価に基づく監査計画の策定	

## ○システム管理基準 (案)

前文 (システム管理基準の活用にあたって)

I. ITガバナンス	III. 開発フェーズ
1. 情報システム戦略の方針及び目標設定	1. 開発ルール管理
2. 情報システム戦略遂行のための組織体制	2. 基本設計管理
3. 情報システム部門の役割と体制	3. 詳細設計管理
4. 情報システム戦略の策定の評価・指示・モニタ	4. 実装管理
5. 情報システム投資の評価・指示・モニタ	5. システムテスト (総合テスト) の管理
6. 情報システムの資源管理の評価・指示・モニタ	6. ユーザ受入テスト管理
7. コンプライアンスの評価・指示・モニタ	7. 移行管理
8. 情報セキュリティの評価・指示・モニタ	8. プロジェクト管理
9. リスクマネジメントの評価・指示・モニタ	9. 品質管理
10. 事業継続管理の評価・指示・モニタ	
II. 企画フェーズ	IV. アジャイル開発
1. プロジェクト計画管理	1. アジャイル開発の概要
2. 要件定義管理	2. アジャイル開発に係る人材の役割
3. 調達管理	3. アジャイル開発のプロセス (反復開発)

V. 運用・利用フェーズ	VII. 外部サービス管理
1.運用管理ルール 2.運用管理 3.情報セキュリティ管理 4.データ管理 5.ログ管理 6.構成管理 7.ファシリティ管理 8.サービスレベル管理 9.インシデント管理 10.サービスデスク管理	1.外部サービス利用計画 2.委託先選定 3.契約と管理 4.サービスレベル管理
	VIII. 事業継続管理
	1.リスクアセスメント 2.業務継続計画の管理 3.システム復旧計画の管理 4.訓練の管理 5.計画の見直しの管理
VI. 保守フェーズ	IX. 人的資源管理
1.保守ルール 2.保守計画 3.情報セキュリティ管理 4.変更管理 5.保守の実施 6.ソフトウェア構成管理 7.ライフサイクル管理	1.責任と権限の管理 2.業務遂行の管理 3.教育・訓練の管理 4.健康管理
	X. ドキュメント管理
	1.ドキュメントの作成 2.ドキュメントの管理

## 2. システム監査制度に関する継続的な改善について

新基準の普及や継続的な改善を行うための枠組みについては、基準の見直しについて中心的に担当してきたシステム監査関連4団体（システム監査学会、日本システム監査人協会、ISACA 東京支部、IT ガバナンス協会）で、2018年の活動を検討しています。決定しているイベントは以下の通りです。

### ○「4団体共同 システム監査制度カンファレンス」

- ・日時：2018年5月19日(土) 13時~16時(カンファレンス)、16時30分~18時(懇親会)
- ・場所：イイノホール(定員500名) 東京都千代田区内幸町2-1-1 飯野ビルディング4階
- ・主催：ISACA 東京支部 共催：システム監査学会、日本システム監査人協会、ITGI  
(プログラム案)

1. 基調講演「システム監査制度改訂の意義」
2. パネルディスカッション「システム監査基準、システム管理基準の改訂のポイント」
3. 講演「システム監査制度の普及と継続的改善」等

本カンファレンスは当協会の5月の月例会を兼ねていますので、会員の皆様も積極的にご参加ください。

<目次>

**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 連載 2 】**

会員番号 1760 齋藤由紀子 (個人情報保護監査研究会)

個人情報保護マネジメントシステム－要求事項【JIS Q 15001:2017】の附属書 A (規定) 管理目的及び管理策には、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 (規定) が基準となります。

参考：2018 年 1 月 12 日発表「プライバシーマーク付与適格性審査基準」

[https://privacymark.jp/system/operation/jis\\_kaisei/index.html](https://privacymark.jp/system/operation/jis_kaisei/index.html)

また、附属書 B (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ます。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」ことが示されています。個人情報保護マネジメントシステム (以下附属書 B において PMS と呼ぶ) をより効率的に確実に運用するため、附属書 B はおおいに参考になります。

今回から、ページの許す限り、本文、附属書 A (規定) 及び附属書 B (参考) を考察し、併せて JIS 適合性を満たす PMS 文書の事例として「3300 個人情報取扱規程」のサンプルを見ていきます。

※ この連載を基にした HTML 版に「連載 1」から公開を開始しました。

規格本文 > [https://www.saaj.jp/03Kaiho/saajpmsJISQ15001\\_2017/000JISQ15001\\_2017.html](https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/000JISQ15001_2017.html)

管理策 1 > [https://www.saaj.jp/03Kaiho/saajpmsJISQ15001\\_2017/001JISQ15001\\_2017.html](https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/001JISQ15001_2017.html)

PMS 監査研究会のコメントは、事業者が「具体的にどうすればよいか」を判りやすく伝えるため、やや断定的な表現にしていますが、事業者の状況によっては、必ずしも必要でない場合もあることをご了承ください。又、2018 年 5 月からスタートする欧州連合 (EU) 一般データ保護規則 (GDPR) の影響もあり、「具体的にどうすればよいか」も大きく変化していくことが考えられます。

今後プライバシーマーク審査基準の確定及び変化によって、HTML 版で訂正していきます。

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

個人情報保護マネジメントシステム－要求事項 JIS Q 15001 : 2017		
1.	本文 適用範囲	この規格は、 <b>組織が、自らの</b> 事業の用に供している個人情報に関する、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善するための要求事項について規定する。この規格が規定する要求事項は、種類または規模を問わず、全ての組織に適用できることを意図している。 <b>この組織は、個人情報の保護に関する法律 (平成 15 年法律第 57 号) (以下、個人情報保護法という。)</b> に定める <b>個人情報取扱事業者を意味する。</b>
		<b>【P マーク審査のポイント】</b> ・PMS の適用範囲は、2006 年版 JIS 規格と変更なく、事業者単位である。 ・“事業の用に供している”の“事業”とは、一般社会通念上事業と認められるものをいい、営利事業だけを対象とするものではない。 ・従業員の個人情報は、事業の用に供している個人情報である。 ・承認は、電子承認でもよい。

【JIS Q 15001 : 2017】規格を元に、規程のサンプルを見ていきます。

## 個人情報取扱規程

PMS3300

## 【3300 個人情報取扱規程】 サンプル

### 1. 本規程の目的

本規程は、「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」(以下、JIS Q 15001:2017、又は規格と呼ぶ)に基づき、個人情報保護マネジメントシステム (以下 PMS と呼ぶ) 運用の具体的な手順を定める。

#### 1.1 適用範囲

PMS は、当社の全従業者 (正社員、契約社員、嘱託社員、パート社員、アルバイト社員、取締役、執行役、理事、監査役、監事、派遣社員、受入出向社員) に適用する。

#### 1.2 適用対象

PMS は、当社の事業の用に供しているすべての個人情報を適用対象とする。

個人情報保護マネジメントシステム－要求事項 JIS Q 15001 : 2017		
2. 引用規格 ……省略		
3.	本文 用語及び定義	この規格で用いる主な用語及び定義は、個人情報保護法による。その他の主な用語及び定義は、次による。 (以下省略)
	<b>【P マーク審査のポイント】</b> ・用語は個人情報保護法による。とされたことで【JIS Q 15001:2017】では、PMS としての用語が省略された。	

## 【3300 個人情報取扱規程】 サンプル

### 2. 用語の定義

PMS において使用する用語は、個人情報の保護に関する法律 (2003 年 5 月 30 日法律第 57 号、2016 年 5 月 27 日第 51 号改定)、および JIS Q 15001:2017 の 3 (用語及び定義) に準じ次の通りとする。

#### 2.1 個人情報 (法)

個人に関する情報であって、特定の個人を識別できるもの。他の情報と容易に照合することによって特定の個人を識別することができることとなる情報、および個人識別符号を含む。

#### 2.2 個人識別符号 (法)

政令で定めるものであって、顔認識・指紋データ等の生体情報等、特定の個人を識別することができるもの。もしくは、個人に発行されるカード等に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、特定の本人を識別することができるものをいう。

#### 2.3 要配慮個人情報 (法)

次に示す事項のいずれかの種類を含む個人情報をいう。

a)	人種、信条、社会的身分
b)	病歴
c)	犯罪の経歴
d)	犯罪により害を被った事実
e)	次に掲げる事項のいずれかを内容とする記述等 (本人の病歴又は犯罪の経歴に該当するものを除く。) とする。 ・身体障害、知的障害、精神障害 (発達障害を含む。) その他の個人情報保護委員会規則で定める心身の機能の障害があること。 ・本人に対して医師等により行われた疾病の予防及び早期発見のための健康診断等の結果

	<ul style="list-style-type: none"> <li>・健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと。</li> <li>・本人を被疑者又は被告人として、逮捕、搜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと。</li> <li>・本人を少年法第三条第一項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。</li> </ul>
e)	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

## 2.4 個人情報データベース等（法）

個人情報を含む情報の集合物であって、検索することができるように体系的に構成したものをいう。

## 2.5 個人データ（法）

個人情報データベースを構成する個人情報をいう。

## 2.6 組織（JIS 3.1）

責任及び権限をもつトップマネジメントが存在し、自らの目的を達成するため、責任、権限及び相互関係を伴う独自の機能をもつ、個人又は人々の集まり。

## 2.7 本人（法、JIS 3.4）

個人情報によって識別される特定の個人。PMS では個人情報は「本人のもの」と認識する。

## 2.8 本人の同意

本人が、個人情報の取扱いに関する情報を与えられたうえで、自己に関する個人情報の取扱いについて承諾する意思表示のこと。子ども又は事理を弁識する能力を欠く者の場合は、代理人の同意も得なければならない。

## 2.9 代理人

法律で定められた親権者、又は家庭裁判所で認められた後見人、本人が選定した任意代理人などをいう。

## 2.10 トップマネジメント（JIS 3.5）

当社のトップマネジメントは、代表取締役社長とする。ただし、“代表者”もしくは“社長”と言い換えることができる。

## 2.11 個人情報保護管理者（JIS 3.41）

トップマネジメントによって組織の内部に属する者の中から指名された者で、PMS の計画・実施及び運用に関する責任及び権限をもつ者。トップマネジメントに PMS の見直し及び改善の基礎として、PMS の運用状況を報告する。なお、略称として“PMS 管理者”を用いることができる。

## 2.12 個人情報保護監査責任者（JIS 3.42）

トップマネジメントによって組織の内部に属する者の中から指名された者で、公平、かつ客観的な立場で監査の実施及び報告を行う責任と権限をもつ者。なお、監査役は監査責任者を兼ねることはできない。

## 2.13 個人情報保護マネジメントシステム

組織が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。

## 2.14 不適合

個人情報保護法をはじめとする法令、規範および、JIS Q 15001:2017 規格の要求を満たしていないこと。



## 2.15 提供

提供には以下の概念がある。

a)	委託	自社と同等の安全管理措置が講じられている組織に個人情報を受け渡す。個人情報の管理責任は委託元にある。
b)	第三者提供	個人情報を渡したあとの管理責任が第三者に渡る。あらかじめ本人の同意を得ないで第三者提供を行うことは個人情報保護法に違反する。
c)	共同利用	個人情報を複数の組織と共同で利用する。本人の同意を得た後に共同利用者を追加する場合は、再度本人の同意が必要。

## 2.16 保有個人データ（法）

開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう。なお、6か月以内に消去することとなるものについても、当社は保有個人データとして取り扱う。なお受託した個人情報については、当社に開示権限は無い。

## 2.17 雇用管理情報

当社の全従業員、従業員になろうとした者、並びに過去において従業員であった者の、雇用管理のために取得、保管、利用等する個人情報をいい、病歴、収入、家族関係等の情報を含む、従業員等の個人に関するすべての情報をいう。

## 2.18 個人番号関係事務

個人番号関係事務に係る用語は、「3305 個人番号関係事務規程」第2条に定める。

## 2.19 匿名加工情報（法）

個人情報に含まれる記述等の一部を、個人情報委員会規則に従って、復元することのできない方法により削除、あるいは他の記述等に置き換え、もしくは、個人識別符号の全部を削除することにより、特定の本人を識別することができないようにしたものをいう。

## 2.20 匿名加工情報取扱事業者（法）

匿名加工情報を事業の用に供している者をいう。

当社は、匿名加工情報取扱事業者ではない。

表 A.1 – 管理目的及び管理策		
A.3 管理目的及び管理策		
A.3.1 一般 (2006 : 3.1)		
目的 個人情報保護マネジメントシステムの運用を行うため		
A.3.1.1	附属書 A 一般	この管理策に規定する A.3.2 から A.3.8 は、トップマネジメントによって権限を与えられた者によって、組織が定めた手順に従って承認されなければならない。
	附属書 B	“トップマネジメントによって権限を与えられた者”とは、原則として個人情報保護管理者を指す。ただし、承認する案件の軽重は、経営判断を要するものから現場の担当者の判断に任せるものまでさまざまであり、個人情報保護管理者以外のものが承認する場合もあり得る。 “組織が定めた手段”についても、承認する案件の軽重によって、経営層の決議を要するものから部署内の決済までさまざまであると考えられる。
【P マーク審査のポイント】		
・トップマネジメントへのインタビュー項目		
a) 個人情報保護目的を説明できること。(A.3.2.1) (2016 : 理念を明確にしていること)		
b) 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。(A.3.2.1)		
c) 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。(A.3.2.2)		
d) 個人情報保護のための人的資源を説明できること (A.3.3.4)		

	<p>e)マネジメントレビューのアウトプットには、継続的改善の機会及び PMS のあらゆる変更の必要性に関する決定を含んでいること。(A.3.7.3) (2016 : リスク認識とその対応)</p> <p>f)PMS を継続的に改善していること。(A.3.8)</p> <ul style="list-style-type: none"> <li>・文書審査では、包括的に個人情報保護管理者等による承認手順を確認する。</li> <li>・現地審査では、A.3.2 から A.3.8 の管理策について、承認を得たことが確認できる記録を確認する。</li> <li>・承認は、電子承認でもよい。</li> </ul>
--	---

【3300 個人情報取扱規程】 サンプル

3. 個人情報保護マネジメントシステム (PMS)

3.1 一般要求事項

当社は、個人情報保護マネジメントシステム (PMS) を確立し、実施し、維持し、かつ、改善する。本規程の 3.2 (個人情報保護方針) から 3.8 (是正処置) の承認については、3.3.4 (資源、役割、責任及び権限) に定める。

<p>A.3.2 個人情報保護方針 (2006 : 3.2)</p> <p>目的 個人情報保護の理念を明確にし、公表するため。</p>		
A.3.2.1	<p><b>内部向け</b> 個人情報保護方針</p>	<p>トップマネジメントは、5.2.1e)に規定する内部向け個人情報保護方針を文書化した情報には次の事項を含めなければならない。</p> <p>a)事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること[特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い(以下、“目的外利用”という。)を行わないこと及びそのための措置を講じることを含む。]</p> <p>b)個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守すること。</p> <p>c)個人情報の漏えい、滅失又はき損の防止及び是正に関すること</p> <p>d)苦情及び相談への対応に関すること。</p> <p>e)個人情報保護マネジメントシステムの継続的改善に関すること。</p> <p>f) <b>トップマネジメントの氏名</b>  <b>トップマネジメントは、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なければならない。</b></p>
	<p>附属書 B</p>	<p>内部向け個人情報保護方針に、単に“事業内容及び規模を考慮して適切に取扱います”などと記載したり、本体 A.3.2.1 の a)~e)の各事項の文言をそのまま記載することは A.3.2.1 に適合しない。</p> <p>A.3.2.1 の a)においては、“特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い(以下、目的外利用という)を行わないこと及びそのための措置を講じることを含む”とされているが、これは本体の A.3.4.2.6 を遵守した対応を求めているものである。</p> <p>A.3.2.1b)の“法令、国が定める指針その他の規範”については、B.3.3.2 に示す。</p> <p>A.3.2.1 の“利害関係者”には、従業員のほか、例えば、委託先、協業相手などの取引先などが考えられる。</p>
<p>【P マーク審査のポイント】</p> <ul style="list-style-type: none"> <li>・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。</li> <li>・外部向け個人情報保護方針(A.3.5.1b)のみでも良いが、その場合は、A.3.1.1 を含むこと。</li> </ul>		

A.3.2.2	<p><b>外部向け</b> 個人情報保護方針</p>	<p>トップマネジメントは、外部向け個人情報保護方針を文書化した情報には、A.3.2.1 に規定する内部向け個人情報保護方針の事項に加えて、次の事項も明記しなければならない。</p> <p>a)制定年月日及び最終改訂年月日</p> <p>b)外部向け個人情報保護方針の内容についての問い合わせ先</p> <p><b>トップマネジメントは、外部向け個人情報保護方針を文書化した情報について、一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。</b></p>
	<p>附属書 B</p>	<p>外部向け個人情報保護方針は、A.3.2.2 に基づき一般の人が知り得るようにするための措置が求められるため、容易に理解できる表現であることが望ましい。</p> <p>A.3.2.2 の、“一般の人が知り得るようにするための措置”としては、例えば、ウェブサイトによる公開が考えられる。ウェブサイトをもたない場合は、例えば、会社パンフレットに記載し、受付カウンターに自由に持ち帰ることができるように用意しておくとともに、遠方からの問い合わせに対しては、要望があればすぐに送付する体制を整えておくといった手段で差し支えない。</p>

## 【3300 個人情報取扱規程】 サンプル

### 3.2 個人情報保護方針

トップマネジメントは個人情報保護の理念を明確にし、次の事項を含む「3200 個人情報保護方針」を定める。方針は従業員に教育および掲示によって周知し、また利害関係者や一般の人が入手できるように当社のホームページに掲載する。

a)	事業の内容および規模を考慮した適切な個人情報の取得、利用及び提供に関し、目的外利用を行わないことおよびそのための措置を講じること。
b)	個人情報の取扱いに関する法令、国が定める指針、その他の規範を遵守すること。
c)	個人情報の漏えい、滅失又はき損の防止および是正に関すること。
d)	苦情および相談への対応に関すること。
e)	PMS の継続的改善に関すること。
f)	トップマネジメントの氏名
g)	制定日および最終改定日
h)	個人情報保護方針の内容についての問合せ先

次回は、A.3.3 計画 から考察します。

「3300 個人情報取扱規程」の 3300 とは、A.3.3 の規格番号に起因し、A.3.3.1(個人情報の特定)、A.3.3.3 (リスクアセスメント及びリスク対策) など、規格要求事項に対応する、PMS の規程となります。

発表した会報をベースに、HTML 版を公開しています。

規格本文> [https://www.saa-j.jp/03Kaiho/saa-jpmsJISQ15001\\_2017/000JISQ15001\\_2017.html](https://www.saa-j.jp/03Kaiho/saa-jpmsJISQ15001_2017/000JISQ15001_2017.html)

管理策 1> [https://www.saa-j.jp/03Kaiho/saa-jpmsJISQ15001\\_2017/001JISQ15001\\_2017.html](https://www.saa-j.jp/03Kaiho/saa-jpmsJISQ15001_2017/001JISQ15001_2017.html)

以上 ■ ■



<目次>

## 本部報告 【 「発注者のプロジェクトマネジメントと監査」を刊行 】

会員番号 1604 原田憲幸 (プロジェクトマネジメントのシステム監査研究会)

### 1. 開発トラブルを未然防止する「プロジェクトマネジメントと監査」を3年かけて本にしました！

システム開発で大トラブルとなる例は少なくないですが、どのプロジェクトも必死に取り組んでいて、それでも大トラブルになっています。なぜそうなるのか？何とかしたい……というのが、当研究会のテーマです。その成果を3年かけてまとめ、ようやく本にしました。

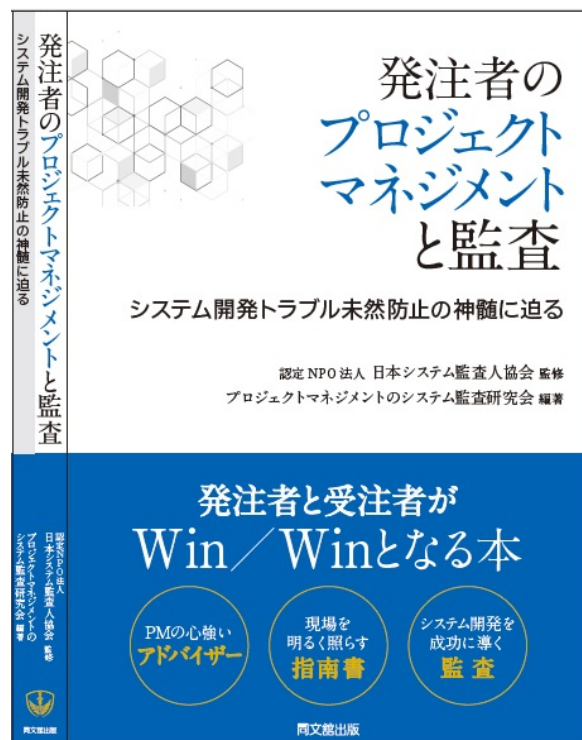
### 2. 内容

- ・1章～3章では、トラブル事例の紹介とトラブル未然防止の基本、発注者/受注者の役割について述べます。
- ・4章～10章では、発注者のプロジェクトマネジメントと要点を述べ、11章では、それをPMBOK®で解説します。
- ・12章～15章では、開発を成功に導くプロジェクト監査について具体的に述べます。

執筆：プロジェクトマネジメントのシステム監査研究会

監修：NPO日本システム監査人協会

出版社：同文館出版株式会社 A5版 220ページ



### 3. 特徴

#### 発注者と受注者が Win/Win となる本

開発を成功に導くために発注者は何をすべきか？を発注者視点で具体的に示します。本書では、ユーザ企業だけでなく、再発注における発注者（SI会社等）も発注者として扱います。

#### PMの心強いアドバイザー

詳細な項目表、絶対に外せないPoint、豊富な事例等で、PMが何をしたらよいかを具体的に述べ、アドバイスします。

#### 現場を明るく照らす指南書

すぐ活用できるチェック表、分析法などを満載し、プロジェクトの現場ですぐ実践できる指南書です。

#### システム開発を成功に導く監査

具体的な監査観点表を豊富に掲載し、開発を成功に導くプロジェクト監査の実践にすぐ役立ちます。

### 4. 購入方法

- ・書店、Amazon等 : 定価 ¥3,456 (本体 ¥3,200 + 税)
- ・SAAJ会員の安価な購入 : ¥2,900 (税込み、送料込み) SAAJホームページから「書籍注文書.PDF」(次ページ様式)をダウンロードして、出版社にFAXで直接申し込み下さい。

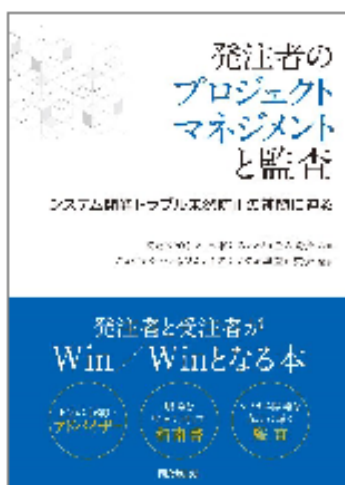
<https://www.saaaj.or.jp/shibu/130801PRJM2018Chirashi.pdf>

認定NPO法人日本システム監査人協会30周年記念出版

# 発注者の プロジェクトマネジメントと監査

—システム開発トラブル未然防止の神髄に迫る—

認定NPO法人日本システム監査人協会【監修】  
プロジェクトマネジメントのシステム監査研究会【編著】



A5判・238頁・並製  
本体価格3,200円（税抜）

発注側の視点で、トラブル防止のための  
プロジェクトマネジメントのポイントが  
わかる！

【目次】

第1章 システム開発の トラブル事例と教訓	第10章 実践的品質管理
第2章 トラブル未然防止の基本	第11章 (発注者視点)のプロ ジェクトマネジメントの 基本
第3章 受/発注それぞれの役 割	第12章 トラブルを未然防止す るプロジェクト監査
第4章 企画・要件定義・調達	第13章 プロジェクト監査 (企画フェーズ)
第5章 プロジェクト計画の作成、 キックオフ	第14章 プロジェクト監査 (設計開発フェーズ)
第6章 外部設計	第15章 プロジェクト監査 (サービス開始フェーズ と効果検証フェーズ)
第7章 実装設計	
第8章 プログラミング、単体テス ト、結合テスト	
第9章 総合テスト、受入試験・ 検収、業務運用試験、移 行、サービス開始判定	

PMの心強い  
アドバイザー

現場を明るく照らす  
指南書

システム開発を成功に導く  
監査

- ◆申込方法 同文館出版宛てに、FAXまたは郵送で以下の申込書を使ってお申し込みください。  
同文館出版株式会社 〒101-0051 東京都千代田区神田神保町1-41  
TEL 03-3294-1801 FAX 03-3294-1807
- ◆支払方法 現品到着後、同封の請求書によりお支払い願います。  
※特別頒布価格は、以下申込書利用者限定で、書店ではお申し込みできません。

お申込みはFAXで 同文館出版 03-3294-1807

同文館出版(担当:福井)行き

平成 年 月 日

書名	特別価格	ご注文冊数
発注者のプロジェクトマネジメントと監査 —システム開発トラブル未然防止の神髄に迫る— (ISBN:978-4-495-20711-3)	定価3,456円+送料を →2,900円 (税・送料込)	

貴社名  
お届け先住所

〒

貴部門名  
TEL ( )

ご担当者名

※ご記入いただいた個人情報は、お申込みをいただいた書籍の発送目的のためにのみ使用させていただきます。

<目次>

**支部報告 【 北信越支部 2018 年度 支部総会・研究会報告 】**

会員番号 1281 宮本茂明 (北信越支部)

以下のとおり 2018 年度 北信越支部総会・研究会を開催しました。

- ・日時：2018 年 3 月 10 日 (土) 13:00-17:00 参加者：12 名 (会員 9 名, 他団体 3 名)
- ・会場：富山県民会館 (富山市)
- ・議題：1. 2018 年度北信越支部総会  
2. 本部総会参加報告  
3. 研究報告  
「サイバーセキュリティ経営ガイドライン」の改訂について 梶川 明美 氏  
「FISC 安全対策基準 第 9 版について」 長谷部 久夫 氏  
4. 意見交換：「データ利活用のシステム監査を考える」 コーディネータ：宮本 茂明

**◇2018 年度北信越支部活動計画について**

2018 年度北信越支部では、3 ヶ月毎に各県で研究会 (3 月支部総会[富山], 6 月福井県例会, 9 月長野県例会, 12 月石川県例会) を開催し、会員の研究報告及び他支部との合同研究会のテーマ検討等を実施していきます。他団体との支部研究会での交流等を通じ会員増強、システム監査の普及・啓発を推進していきます。また、西日本支部合同研究会を 11 月 17 日に福井市で「データ利活用に関するシステム監査」をテーマに開催することを計画中です。

**◇研究報告 1****「サイバーセキュリティ経営ガイドライン」の改訂について**

報告者 (会員番号 0947 梶川明美)

**1 はじめに**

経済産業省と独立行政法人情報処理推進機構 (IPA) は、IT に関するシステムやサービス等を供給する企業や経営戦略上 IT の利活用が不可欠な企業の経営者を対象に、経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定された。平成 27 年 12 月 28 日に Ver1.0 が公表され、平成 28 年 12 月 8 日に Ver1.1 として改訂、平成 29 年 11 月 16 日に Ver2.0 が改訂公表された。

このガイドラインには、経営者が認識する必要のある「3 原則」と経営者が CISO 等に指示すべき「重要 10 項目」がまとめられている。

**2 改訂概要**

昨今、サイバー攻撃が巧妙化しているため事前対策だけでは対処が困難となっており、米国のサイバーセキュリティフレームワークでは事前対策だけでなく、事後 (検知、対応、復旧) 対策を要求している。また、従来のガイドラインでは CSIRT の構築などの「対応」に関する項目はあるものの、「検知」や「復旧」に関

する内容が弱かった。このことから、米欧の取り組み状況も意識し、攻撃の検知や復旧に関する項目にもフォーカスした内容となっている。

### 3 企業経営と情報セキュリティに関する意識

企業の IT 利活用は、業務の効率化だけでなく、新しい製品やサービスを創造していく強い企業の必須条件となっている。一方サイバー攻撃は年々高度化、巧妙化しており、サイバー攻撃によって深刻な影響を引き起こす事件が発生するなど、その脅威は増大している。

そのため、セキュリティ投資は事業継続性の確保やサイバー攻撃に対する防衛力の向上だけでなく、IT 利活用によって企業の収益を生み出す上でも重要な要素となっている。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要である。このことから、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務であるといえる。

経営資源の配分として、セキュリティ投資を成長投資と認識している企業は 2 割弱であるが、コストとみる企業は 6 割強にのぼる。また、成長投資と考えている企業では 7 割以上の企業が必要なセキュリティ予算を確保できているのに対し、コストと考えている企業では 4 割程度に留まっている。

### 4 経営者が認識すべき 3 原則

経営者は、以下の 3 原則を認識し、対策を進めることが重要である。

- (1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
- (2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
- (3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

### 5 経営者が CISO 等に指示すべき 10 の重要事項

経営者は、CISO 等に対して、以下の 10 項目を指示し、着実に実施させるとともに、実施内容について CISO 等から定期的に報告を受けることが必要である。

下線を引いた指示は、今回の改訂で追加された指示または項目を含むものである。

#### <サイバーセキュリティリスクの管理体制構築>

指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

指示 2 サイバーセキュリティリスク管理体制の構築

指示 3 サイバーセキュリティ対策のための資源（予算、人材等）確保

#### <サイバーセキュリティリスクの特定と対策の実装>

指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

指示 5 サイバーセキュリティリスクに対応するための仕組みの構築

「攻撃の検知」に関する指示項目として追加された。

検知のための機器やシステムを導入しただけで満足せず、実際にログのチェックや職員の教育を行うなど、実効性のある運用が伴わなければならない。訓練を行っても巧みに仕組まれた標的型メー

ルを開いてしまうことがあり、サイバー攻撃がますます巧妙化していくことを理解しなければなら  
ない。

#### 指示6 サイバーセキュリティ対策におけるPDCAサイクルの実施

<インシデント発生に備えた体制構築>

#### 指示7 インシデント発生時の緊急対応体制の整備

#### 指示8 インシデントによる被害に備えた復旧体制の整備

「復旧」に関する指示項目として追加された。

企業ではBCPの策定・訓練の実施が進んでいるが、自然災害対策等を想定しており、サイバー攻  
撃についての復旧が意識されていないケースが多い。ランサムウェアのように、可用性に影響を与  
える攻撃も増加しているため、復旧に関する対策は重要である。

<サプライチェーンセキュリティ対策の推進>

#### 指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

委託先がSECURITY ACTIONを実施しているか。ISMS等の認証を取得していることが望ましい。

委託先におけるリスクマネーの確保として、委託先がサイバー保険に加入していることが望まし  
い。

<ステークホルダーを含めた関係者とのコミュニケーションの推進>

#### 指示10 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

## ◇研究報告 2

### 「FISC 安全対策基準 第9版について」

報告者 (会員番号 1766 長谷部 久夫)

平成30年3月末に改訂完了する予定の標記について情報交換したうえで、システム監査人の役割に  
ついて意見交換した。

#### 1. FISCとは

公益財団法人 金融情報システムセンター (FISC:The Center for Financial Industry Information  
Systems) の略。銀行、証券会社、保険会社、コンピュータメーカー、情報処理会社等の出捐により財団  
法人として1984年11月に設立し、2011年4月に公益財団法人へ移行。金融情報システムに関連する諸  
問題(技術、IT利活用、リスク管理、セキュリティ等)について総合的な調査研究を行い、安全対策基準  
等の各種ガイドライン・調査レポートの作成、セミナー等を通じて、その成果を還元している。

#### 2. 現行安全対策基準の概要

ガイドライン名は「金融機関等コンピュータシステムの安全対策基準・解説書」。金融機関等のよりど  
ころとなるべき共通基準として昭和60年12月初版刊行。現行版は、第8版(平成23年3月)、第8版  
版追補改訂(平成27年6月)。自然災害、機器障害、不正使用行為等から生ずる金融機関等コンピ  
ュータシステムの障害に対し、「障害発生未然防止」「障害影響の最小化」「障害からの早期回復」を  
図ることを目的とする。基準項目は、設備基準(138項目)、運用基準(120項目)、技術基準(53項目)で



構成され、合計 311 項目。近年は、「サイバー攻撃対応」「クラウド利用」「外部委託管理」をテーマとして基準項目を整備している。

### 3. 安全対策基準（第9版）の改訂概要

安全対策基準（第9版）は、近く発刊予定であり、その改訂内容については当協会の会報や研究会等で紹介されることが想定されるため、本稿では説明を割愛する。基準改訂の考え方は、公表されている『外部委託』『Fintech』に関する有識者検討会報告書での提言で示されているため、それらを紹介する。

#### (1) リスクベースアプローチを踏まえた基本原則の導入

多様化する基幹業務系以外のシステムに対し、安全対策を一律に実施するのではなく、リスクに応じて安全対策を策定する。安全対策基準の考え方は、ITガバナンスの下、金融情報システムに対しリスク評価を実施してリスク特性に応じた安全対策を適用するよう見直しする。

#### (2) 基本原則に基づいた安全対策基準の明確化

高い安全対策が必要なシステムは、金融情報システムのうち、重大な外部性を有するシステムや、機微情報（要配慮個人情報を含む）を有するシステム。金融機関等は最低限必要な対策を実施して、それ以外のシステムにおいても、金融機関等の判断により、高い安全対策を適用可能とする。

#### (3) 外部委託先の統制基準の拡充

外部委託やサービス利用への依存度が高まる中、安全対策基準は統制面の対策を拡充していくことが求められる。その要求に応じていくため、安全対策基準において、統制基準を明示的に示すことが有効。

### 4. システム監査人の役割

安全対策基準（第9版）改訂は、リスクベースアプローチによる安全対策実施を主眼とするものである。本改訂を踏まえると、システム監査人には、安全対策基準の基準項目に照らして管理策の不備を抽出するに止まらず、「組織が経営陣のITガバナンスの下、高度化するリスクをタイムリーに把握し、適切に対応する管理態勢を整備した上で、実際に成果を出しているか」検証すること、すなわちリスク管理PDCAに関与するシステム監査に取り組むことが、より一層重要になると考える。

特に、被監査者のリスクアセスメントをモニタリングし、それが不適切な場合は、当該事実及び監査人が自ら実施したリスクアセスメントの結果と、それに応じたマネジメント、又はコントロールの整備及び運用にかかる「助言」は重要な指摘事項となる。そのような有効な助言型監査を行うためには、被監査者と密接なコミュニケーションをとり、監査人自身の見識を高めることが必要になると思われる。

今後も3ヶ月ごとの支部例会・研究会等の「場」や、インターネットを活用したコミュニケーションにより、支部会員間で幅広く意見交換を行う本協会の活動を通じて、自己の見識をより高めることに努めていきたいと存じます。

以上

<目次>

**支部報告 【 近畿支部 第172回定例研究会 】**

会員番号 2520 松本拓也（近畿支部）

1. テーマ 「地方自治体における ICT 監査の現状と課題」
2. 講師 大阪市行政委員会事務局 監査部  
ICT 監査担当課長 片岡 学 氏
3. 開催日時 2018年1月19日（金） 19:00～20:30
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、企業の内部監査、監査法人、会計検査院でのご経験を経て、現在大阪市行政委員会事務局において ICT 監査をご担当されています。監査生活約 40 年の豊富なご経験の中から、今回は、ICT が高度化・多様化する中で、地方自治体における ICT 監査への取り組みと課題について、お話をいただきました。

**<講演内容>****(1) はじめに**

ICT が高度化・多様化する中、地方自治体では ICT を適正に利用し、住民への行政サービスの向上と行政コストや業務の効率化に資すること、また、住民情報の漏えい防止など情報セキュリティを確保することが命題となっており、それらを監査委員の立場から検証する ICT 監査の役割は非常に大きいものである。

現に、地方自治体の行政サービスや行政運営においては、ICT が重要な基盤として役割を果たしているが、これまで、この ICT 領域について監査委員による十分な監査が行われているとは言えない状況であり、ICT を管理・運営する部署においても受査経験が少ないものとなっている。

しかし、最近では公的団体での ICT 問題（マイナンバーカードの管理システムに係るシステム障害、システム刷新の失敗事例など）がクローズアップされてきており、会計検査院も ICT に係る施策を注視している。また一般の事業会社等の ICT 監査の普及も徐々に進んでいるなかで、地方自治体における ICT 監査への取り組みは、更なる整備・充実が求められる段階にきている。

**(2) 地方自治体における監査制度**

大阪市の事例から見る監査委員監査の大きな特徴は、ICT 監査によって検出された個々の不備そのものの指摘のみならず、その不備の本質的な原因を追究することが重要とされている点である。これは、監査委員監査において、ICT 監査をいわばツールとして考え、監査委員が経営者目線で、大阪市の ICT の課題についての検証と改善勧告に取り組んでいるからであり、この点で、監査委員監査における ICT 監査には経営者に近い目線での監査が求められている。

### (3) 地方自治体における ICT と ICT 監査の重要性

地方自治体の活動において、ICT が果たす役割がさらに拡大していくなか、総務省も「電子自治体の取組みを加速するための 10 の指針」(平成 26 年 3 月)を提示している。しかし、こういった統一的な指針に対し、各地方自治体では従来からのローカルルールが複数存在する場合があります、これらを一つに取りまとめていくのはなかなか難しい。

地方自治体における ICT 監査は、ICT の適正利用の実現を阻害するリスクに対して、適切なコントロールが整備され、運用されているかを確認し、助言・勧告するものである。

地方自治体における ICT の問題としては、一般的に「ICT の適正利用が政策目標達成の手段として十分に位置づけられていない」、「情報システムの導入を、情報システムに精通していない各部署が実施している」、「電子自治体の取組みは、特定の職員の能力や努力に依存する」などが挙げられる。多くの地方自治体では、これまで ICT 監査を本格的・定期的実施してきておらず、実施している場合でもテーマ数が民間企業と比較して少ない状況である。これにより、地方自治体の ICT の担当者や情報システムの委託先は、適切な点検・評価を受けておらず、前述のような ICT の問題を引き起こしている可能性がある。

地方自治体における ICT の役割が拡大し、住民の関心も増していくなかで、今後、地方自治体の ICT に関する適切な税金の使い方についても、住民への説明が必要になってくるのではないかと考えられる。

### (4) 地方自治体における ICT 監査の取組みの方向性

地方自治体における ICT 監査では、個々の統制活動の不備指摘のみならず、本質的・共通的な問題(行財政運営組織における ICT の統制環境上の課題)をとらえ、十分な検証と問題指摘及び提言の実施、未然防止の重要性に念頭を置いた監査の実施、内部統制体制の構築への貢献、ICT リスクに関わる関係者のレベルアップへの貢献が重要である。

しかし、地方自治体で ICT 監査に取り組むには、様々な課題がある。

- ・システム調達においては、制度や仕組みは構築されているが、それらをモニターする能力が弱い。
- ・個別システムにおいて、管理者や担当者、システムエンジニアが、監査や点検を受けた経験が少ない。
- ・監査体制において、監査委員では ICT 監査の重要性や必要性への認識が不十分であったり、監査委員監査をサポートする事務局要員では ICT に係る知見が不足していたりということがあり、IT ガバナンス上の課題についての検証や問題指摘及び提言するためのスキルが不足している。

大阪市では、ICT や情報セキュリティのリテラシー向上に向け、監査事務局要員や局長級職員向けの研修などが実施されているとともに、ICT 部門においては、即戦力となる外部人材の採用などの対応も行われている。

地方自治体における ICT 監査の今後の取組みの方向性として、「監査委員自らが、ICT 監査に係る知見

を獲得し、その重要性を認識する」、「監査委員事務局スタッフが、ICTに係るリスクやコントロールについての基礎的な知識やスキルを修得することなどによって、ICT監査の実施環境を整備する」、「監査委員監査の実行部隊である監査委員事務局スタッフが、経営的視点から指摘や改善勧告につながる活動を行う」ことが重要である。

地方自治体におけるICTの活用はこれからであり、ICT監査も次の世代が継続できるように取り組んでいかなければならない。

## 6. 所感

監査委員監査については、なかなか直接触れる機会がなく、その仕組みや考え方を具体的に説明していただけのため、大変勉強になりました。

今回、講師が挙げられた地方自治体におけるICT監査の課題は、私自身がこれまでに担当した地方自治体向けの情報セキュリティ監査等でも、強く実感した部分です。特に人材育成について、職員が2~3年のサイクルで人事異動となることが多い地方自治体では、管理者や担当者のスキルレベルをなかなか維持できず、情報セキュリティ対策の導入は十分に行われていても、それを運用・管理していくことが難しいケースを目の当たりにしました。場合によっては、監査人の方が対象システムに詳しい、というような経験をしたこともあります。

これまで地方自治体では、マイナンバー制度の開始や総務省の指針に基づくネットワークの見直し等に取り組みされてきました。また今後も、総合窓口の導入やビッグデータの活用等でますますICT分野の利活用が注目されるなかでは、それらの導入後に絶対に必要となる維持・改善活動の存在を認識し、ICT監査へも積極的に投資していかなければならない時期に来ていると感じました。

以上

<目次>

**注目情報 (2018.2~2018.3)****■ 「システム監査基準」「システム管理基準」の改訂案に対する意見公募【経済産業省】**

経済産業省では、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るシステム監査制度について、「システム監査に関する検討会」を開催し、制度に関する見直しを進めてきた。

このうち、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」、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」について、昨今の社会情勢の変化や技術の進展等を踏まえて改訂が行われ、3月6日から20日までの間、改訂案に対する意見公募が行われた。

- \* 改訂案 : 「システム監査基準」 (案)
- 「システム管理基準骨子」 (案)
- 「システム管理基準」 (案)

**■ サイバーセキュリティに関するガイドラインを公開【JASA】**

特定非営利活動法人日本セキュリティ監査協会 (本部：東京都江東区、会長：慶應義塾大学名誉教授 土居範久) は、ISMSを適用している組織が、サイバーセキュリティ対策を行うための2つのマネジメントガイドラインを、3月2日に公開した。

公開したのは、「サイバーセキュリティ対策マネジメントガイドライン」とサプライヤーに求められる「管理された非格付け情報の保護対策マネジメントガイドライン」である。

サイバーセキュリティ対策については、米国政府が重要インフラ向けに策定した「重要インフラのサイバーセキュリティ対策向上のためのフレーム (Framework for Improving Critical Infrastructure Cybersecurity - NIST)」と、これに関連してサプライヤーが順守すべき管理された「非格付け情報の保護対策 (NIST SP800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations)」が世界的に用いられている。二つのガイドラインは、各々の基準と ISMS のための国際標準である ISO/IEC27001 及び ISO/IEC27002 とを各々比較し、ISMS に不足している、あるいはより明確にした方がいい内容を、ISO の規格に従って整理したものである。

サイバーセキュリティ対策マネジメントガイドラインについては、特に検知やインシデント対応、事業継続などについての記述が多く、予防が重点である ISMS に対して、初期被害を受けた後の対処の際に重要な内容が多く記載されている。管理された非格付け情報の保護対策マネジメントガイドラインにおいては、初期被害を受けた後の対処の際に重要な内容とともに、ベースラインとして最低限行うべき内容が明記されており、一定以上の強度をもつセキュリティ対策の具体例が分かる。

[http://www.jasa.jp/news/news\\_20180302.html](http://www.jasa.jp/news/news_20180302.html)

<目次>

## 【 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 2 3 1 回	日時：2018年 4月17日（火曜日）18:30～20:30 場所：機械振興会館 地下2階ホール	
	テーマ	「システムの不具合がもたらす社会的影響：ある損害賠償係争事件を巡って」
	講師	法政大学 理工学部 創生科学科 教授 玉井 哲雄 氏
	講演骨子	詳細確定次第、HPでご案内いたします。
	お申込み	近日、以下のHPでご案内いたします。 <a href="https://www.saa.or.jp/kenkyu/kenkyu/231.html">https://www.saa.or.jp/kenkyu/kenkyu/231.html</a>

## ■ 4 団体共同 システム監査制度カンファレンス（東京）

特別 月 例 研 究 会	日時：2018年 5月19日（土曜日）13:00～16:00 場所：イイノホール	
	共同開催団体	当協会のほか、ISACA東京支部、システム監査学会、ITGI
	プログラム案	1. 基調講演「システム監査制度改訂の意義」 2. パネルディスカッション「システム監査基準、システム管理基準の改訂のポイント」 3. 講演「システム監査制度の普及と継続的改善」等
	お申込み	詳細確定次第、HPでご案内いたします。

&lt;目次&gt;


## 【 外部主催イベント・セミナーのご案内 】

## ■ ISACA 月例会（東京）

2018年3月例会	日時：2018年 3月28日（水曜日） 18:30～20:10 場所：日本教育会館 一ツ橋ホール	
	テーマ	「FinTech 時代のリスク管理 ～ 銀行経営と監督のあり方を巡って ～」
	講師	日本銀行 金融機構局 国際課 企画役 山田 隆人 氏
	講演骨子	バーゼル銀行監督委員会は2016年4月、FinTechの発展が銀行業や銀行監督にもたらす含意について検討を行う作業部会を立ち上げた。今回は、同委員会が2018年2月19日に公表した最終提言書のポイントを紹介しつつ、今後FinTechが普及していく過程において浮上するであろうリスク管理や経営上の課題等について考察する。
お申込み	<a href="http://www.isaca.gr.jp/education/18_0305annai.html">http://www.isaca.gr.jp/education/18_0305annai.html</a>	

&lt;目次&gt;

## 【 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](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。

&lt;目次&gt;



【 SAAJ 協会行事一覧 】		赤字：前回から変更された予定	2018.3
2018	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
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
5月	10：理事会	中旬：春期 CSA 面接 19：システム監査制度カンファレンス	
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)	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)
7月	5：支部助成金支給 12：理事会	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) 24：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
前年度に実施した行事一覧			
9月	14：理事会	～ 秋期 CSA・ASA 募集中 ～9/30 迄 2：第 19 回「事例に学ぶ課題解決セミナー」 5：第 225 回月例研究会「IoT 時代のセキュリティを実現する 3 視点とシフトレフト」 14-15 & 28-29：第 30 回システム監査実務セ ミナー(日帰り4日間コース)	30：西日本支部合同研究会 in Fukuoka(福岡)
10月	12：理事会	21:SAAJ 活動説明会(東京茅場町) 30：第 226 回月例研究会	15：秋期情報処理技術者試験
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：総会開催予告揭示 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

&lt;目次&gt;

## 【 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。

今月号から 6 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	(決まり次第ご連絡します)	
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](mailto: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](mailto:saajeditor@saaj.jp)

**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.saa-j.or.jp/members\\_site/KaiinStart](https://www.saa-j.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.saa-j.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.saa-j.or.jp/members\\_site/KaiinStart](https://www.saa-j.or.jp/members_site/KaiinStart)

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： 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）

Copyright(C)1997-2018、認定 NPO 法人 日本システム監査人協会

<目次>