認定 NPO 法人
日本システム監査人協会報
2015 年 10 月号
No 175
No. 175（2015 年 10 月号）＜9 月 25 日発行＞

2015.9.5
西日本支部合同
研究会 In GIFU
交流会

長良川鵜飼

写真提供：松井秀雄
（近畿支部）

巻頭言

テーマ：「ＰＭＳハンドブック」番号法に対応した様式を公開

（「西日本支部合同研究会 In GIFU」で発表）

会員番号 1760　斎藤由紀子
（副会長　事務局長　個人情報保護監査研究会主査）

2015 年 9 月 3 日第 189 回通常国会で「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案」が制定された。民間事業者は、10 月 5 日以降に従業者等から個人番号を収集し、2016 年度から個人番号の利用、提供が始まる。

個人情報保護監査研究会では、9 月 1 日付で、「6か月で構築する個人情報保護マネジメント実施ハンドブック（以下、PMS ハンドブック）」の購読者向けダウンロードサイトで、番号法に対応した各種様式を公開した。「個人番号関係事務規程」、「個人情報保護体制」、「個人情報管理台帳」、「リスク分析表」「個人番号取扱記録簿」「委託先調査表」等の様式において、番号法でいう、「個人番号関係事務」というキーワードで統一したことで、既存のPMSによく馴染んだものとなった。

2015 年 9 月 6 日に開催された、「西日本支部合同研究会 In GIFU」でも、「個人番号関係事務」関連様式の一部をご紹介。 鵜飼船での交流会では、松明の灯りの観覧の中、事業者のための「PMSハンドブック」の更なる様式の充実を誓い、この名残惜しさをいかにせむとの思いであった。

・・・・・　おもしろうてやがて悲しき鵜舟かな（芭蕉）　・・・・・　＞関連記事

各行から Ctrl キー+クリックで
該当記事にジャンプできます。
（各記事末尾には目次へ戻るリンク有）

＜目次＞

2015.10

めだか 【 システム監査人の喜び ① 】

現在のIT社会では、情報資産や個人情報の保護と利活用が大きな課題になっている。JIS Q 27001:2014規格（情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要求事項）やJIS Q 15001:2006規格（個人情報保護マネジメントシステム-要求事項）は、それぞれのリスクをいかにマネジメントするかを規定している。

リスクマネジメントは、JIS Q 31000:2010規格（リスクマネジメント-原則及び指針）が基本であり、同規格ではリスクマネジメントを効果的なものにするために、組織は、次の原則をすべての階層で順守することが望ましいとしている。

a) リスクマネジメントは、価値を創造し、保護する。
b) リスクマネジメントは、組織のすべてのプロセスにおいて不可欠な部分である。
c) リスクマネジメントは、意思決定の一部である。
d) リスクマネジメントは、不確かさに明確に対処する。
e) リスクマネジメントは、体系的かつ組織的で、時宜を得たものである。
f) リスクマネジメントは、最も利用可能な情報に基づくものである。
g) リスクマネジメントは、組織に合わせて作られる。
h) リスクマネジメントは、人的及び文化的要素を考慮に入れる。
i) リスクマネジメントは、透明性があり、かつ、包含的である。
j) リスクマネジメントは、動的で、繰り返し行われ、変化に対応する。
k) リスクマネジメントは、組織の継続的改善を促進する。

リスクマネジメントの枠組みは、PDCAサイクルを回して継続的改善を図ることである。リスクマネジメントプロセスは、組織の状況を確かめ、リスクアセスメント（リスク特定、リスク分析、リスク評価）、及びリスク対応から、モニタリング及びレビュー、並びにコミュニケーション及び協議を行っていくことである。

リスクマネジメントは、すでに多くの企業で実践されているが、コミュニケーション及び協議を行っていくプロセスは、様々な利害関係者が存在するため、難しいプロセスである。このプロセスに関して養老孟司先生の「文系の壁」を読んでみて、文系と理系の違いとは、文系は言葉で対話し、理系は設計図や数式で対話するところにあると思った。また、文系と理系に分けるのではなく、実験室とフィールドに分ける仕分け方もあると書かれている。コミュニケーション及び協議を上手く行っていくためには、言葉や設計図、数式など多様なメディアの利用、及びフィールド感覚を持つことが重要になる。

システム監査人は、ITガバナンスにおいてリスクに応じたコントロールが適切に整備・運用されているか、また情報システムがその目的に照らして有効であるかを監査し、代表者に報告を行うことが職務である。その職務を果たすことにシステム監査人の喜びがあると思う。

（空心菜）

参考:「文系の壁」 理系の対話で人間社会をとらえなおす 養老孟司 著 PHP新書994

（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。）

2015.10

めだか　【　システム監査人の喜び　② 】

のっけから意外なことを申し上げるようですが、実は言葉の本来の意味で「システム監査人」として、業務を担った経験はありません。特に組織の内部監査の一翼を担ったことはないのです。このため、内部監査の部門でシステム監査人の役割を担う方のご苦労を知らないのです。

内部監査の場合は、監査を受け入れてもらうための努力が不断に必要です。被監査部署にとって、システム監査の意義についてよほど理解がなければ、受検の負担がありますし、監査の指摘をありがたい、と思うのは、経費がかかるのでなかなか実現しなかった事項が監査指摘のせいで予算化されたとき、くらいでしょうか。

その意味で経験を積んだのは、外部監査的な立ち位置からのアプローチです。広い意味で国民から負託を受けた機関として、第三者の視点から、システムの統合や更改プロジェクト、あるいは情報セキュリティ対策を検証する業務に長年従事しました。

監査対象になった組織がきちんと対応することで、利害関係者の安心を得ることができる、という意味で、監査そのものが社会インフラ的な役割を担っていました。そのなかでいつも心がけていたのは、監査を受ける組織の体力を考え、組織が持つ特性をきちんと踏まえたうえで、「なるほど、そういうことならもうひと頑張りしてみよう」「気が付かなかった視点を示唆してもらった」と思ってもらえるか、ということでした。

ただ、ともすると、監査でたくさん指摘事項をリストアップすることが、仕事の成果として見えやすいきらいがなかったとは言えません。その意味で、「なんだ、何の指摘もしてこなかったのか」、本当にシステム監査は必要なのか、などと周囲から揶揄（やゆ）されることもありました。それでも「当たり前のことをきちんとできているか」に重点を置いて、それができていれば敢えて指摘事項を挙げないことも多かったように思います。

そんななかで、監査終了後少し時間が立って、監査先の経営陣が自分の上席者と会った際、「先日のシステム監査では、いろいろ気づかない視点を示唆してもらい、大変感謝している」と、意外な反応を漏らし、それが伝わってくることがままありました。つまり監査を通じた議論のプロセスから、被監査先が学んだことが相応にあったようなのです。

こうした対話型で臨むシステム監査の姿勢は在職中変わりませんでした。議論は丁寧にする、しかし敢えて指摘するまでもないことは大きな視点に溶け込ませて伝達する。ああそうか、これで良いんだ、と何度となく思い直して仕事をしてきました。

昨春でこの仕事場を後にしました。こうした接点はもうなくなった、もう縁が切れたかと思っていました。

そんなある日、協会の月例研究会が終わると、声をかけてこられた会員がいらっしゃいます。「その節はお世話になりました。大変勉強になりました」。協会の活動を通じて、業務上の接点を持った方とも繋がっていることを、実感した瞬間でした。

今後もSAAJの活動の中で、変わらない立ち位置で皆さんとコミュニケーションしていければと思いました考えています。

（拡張子）

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

＜目次＞

2015.10

投稿【　システム監査人の魅力　】

会員番号　0557　仲　厚吉　（会長）

当協会では、2015 年 8 月 21 日（金）18 時 20 分より第 27 回 CSA/ASA フォーラム（日立システムズ本社・大崎）で、CSA 利用推進グループ主査　力利則　氏により IT ガバナンスについて講演会を開催し、多数の CSA/ASA の皆様が参加しました。

JIS Q 38500:2015 規格（情報技術-IT ガバナンス）は、日本規格協会より 2015 年 7 月 21 日付で発行されています。IT ガバナンスのモデルは、「IT ガバナンス（（評価（Evaluate）、指示（Direct）、モニタ（Monitor））」と、「事業プロセス（IT プロジェクト、IT 運用）」の二つに分けられています。「IT ガバナンス」は、「事業プロセス」との間で、「計画・方針」を指示し、「プロトコル」を評価し、「パフォーマンス＆適合」をモニタするという構図になっています。なお、「プロトコル」は、現在の ISO では「プロポーザル」と言っています。

良好な IT ガバナンスのための六つの原則は、責任（Responsibility）、戦略（Strategy）、取得（Acquisition）、パフォーマンス（Performance）、適合（Conformance）、人間行動（Human Behavior）を規定しています。それぞれの IT ガバナンスのための原則に、評価（Evaluate）、指示（Direct）、モニタ（Monitor）のサイクルを回し、良好な IT ガバナンスを構築していきます。

JIS Q 27014:2015 規格（情報技術-セキュリティ技術-情報セキュリティガバナンス）も、日本規格協会より 2015 年 7 月 21 日付で発行されています。この規格は、情報セキュリティガバナンスについての概念及び原則に基づくガイダンスを示します。同規格を適用することによって、組織が情報セキュリティに関連した活動を、評価、指示、モニタ及びコミュニケーションできるようになるとしています。また、同規格は、JIS Q 27001:2014 規格（情報技術-セキュリティ技術-情報セキュリティマネジメントシステム-要求事項）を引用しています。

情報セキュリティガバナンスのための六つの原則は、原則1（組織全体の情報セキュリティを確立する。）、原則2（リスクに基づく取組みを採用する。）、原則3（投資決定の方向性を設定する。）、原則4（内部及び外部の要求事項との適合性を確実にする。）、原則5（セキュリティに積極的な環境を醸成する。）、原則6（事業の結果に関するパフォーマンスをレビューする。）を規定しています。また、経営陣は、情報セキュリティを統治するために、“評価”、“指示”、“モニタ”、及び“コミュニケーション”の各プロセスを実行すると規定しています。

情報セキュリティは国を挙げて論じられ、情報セキュリティガバナンスの重要性は、社会一般に認められていくと思われます。一方、IT ガバナンスの重要性は、今後、IT の利活用を図る経営陣、及び IT 利用者に理解を求めていく活動が必要です。当協会では、2015 年 12 月 14 日（月）18 時 30 分より第 209 回月例研究会（機械振興会館地下 2 階ホール・神谷町）で、IT ガバナンスをテーマにしたセミナーを開催します。同セミナーを受講し、所属組織の経営陣や IT 利用者に IT ガバナンスの重要性を広めるようお願いしたく思います。今後、システム監査人の魅力は、IT ガバナンスの普及を通じて、IT 監査人として健全な IT 社会の発展に資する活動のなかに育まれていくと思います。

以上

＜目次＞

2015.10

投稿【「ＰＭＳハンドブック」購読者向けダウンロードサイトに番号法対応様式公開　】

会員番号 1760 斎藤由紀子（個人情報保護監査研究会主査）

「６か月で構築する個人情報保護マネジメントシステム実施ハンドブック」（以下、ＰＭＳハンドブック）の購読者向けのダウンロードサイトで、2015 年 9 月 1 日に、番号法対応様式を公開しました。

日本システム監査人協会

TOP | 6か月で構築するPMS様式集 | 会員専用

6か月で構築するPMS様式集

SAAJPMS改定履歴 20150901

6か月で構築するPMS様式集

HOME ＞ 6か月で構築するPMS様式集

次回改定：お知らせonの方にメールでお知らせします。（お知らせのON/OFFはユーザーセンター＞プロフィー
できます。

2015年9月1日　番号法対応様式Upload

6ケ月で構築する　「個人情報保護マネジメントシステム実施ハンドブック」様式集

PMS文書体系 ← 2015/9/1版

- 3301個人情報取扱規程は、JIS Q15001:2006の規格および解説を規定化しました。
- Topics！2015/9/1　3305個人番号関係事務規程　を追加しました。あわせて関係様式を改定、追加しました。
- 3430安全管理規程は、個人情報の取扱のリスクに応じ、適宜変更してお使いください。
- 初めての方はZIPファイルのみダウンロードしてください。
- 逐次Updateします。改定したファイルのみダウンロードできます。

	PMS規程・様式	制定日	直近の改
A：	ダウンロード：3200～3307.zip（226KB）　20150901		
1	3200個人情報保護方針	2014年12月10日	2015年9月１日
2	3210個人情報の取扱について	〃	2015年9月１日
3	3301個人情報取扱規程	〃	2015年9月１日
4	3302PMARK認証取得スケジュール	〃	
5	3303ＰＭＳ年間計画書(兼点検表)	〃	2015年9月１日
6	3305個人番号関係事務規程　New!	2015年9月１日	
7	3306特定個人情報記録　New!	2015年9月１日	
8	3307個人番号マスター　New!	2015年9月１日	

【番号法対応：新様式】

3305 個人番号関係事務規程

3306 特定個人情報記録

3307 個人番号マスター

3422-02「個人番号」の取扱いについて（通達）

3434-09 委託先調査票（C：個人番号関係事務）

3434-10 業務委託契約書（C：個人番号関係事務）

以下は、新様式の一部

個人番号関係事務規程

PMS3300

株式会社○○○○

制定：　2015 年 9 月 1 日

所管：個人情報保護事務局

第３条　個人番号関係事務の範囲

当社の、個人番号関係事務の範囲は以下のとおりとする。

対象者	識別	個人番号関係事務
役職員（扶養家族含む）に係るもの	A1	給与所得・退職所得の源泉徴収票作成事務
	A2	雇用保険届出事務
	A3	労働者災害補償保険法に基づく請求に関する事務
	A4	健康保険・厚生年金保険届出事務
役職員の配偶者に係るもの	B4	国民年金の第３号被保険者の届出事務
役職員以外の個人に係るもの	C1	報酬・料金等の支払調書作成事務
	C2	配当、剰余金の分配及び基金利息の支払調書作成事務
	C3	不動産の使用料等の支払調書作成事務
	C4	不動産等の譲受けの対価の支払調書作成事務

第４条　個人番号関係事務に係る組織体制

個人番号関係事務に係る組織体制は、「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」に、以下について権限と責任を定める。

（１）個人番号関係事務責任者　（個人情報保護管理者が兼務）

（２）個人番号関係事務部門管理者

（３）個人番号関係事務担当者

PMS3306 個人番号取扱記録簿　【２０

業務名	個人番号関係事務　（サンプル）
★保管、廃棄方法の取扱いは「個人情報管理台帳」記載に従う。 ★個人番号を削除した場合は、行単位でグレー網掛けをする。 ★毎年データを受け継いで新規ファイルを作成し、⑧～⑪を記録する。 ★★次年度のファイルは、グレーの行は削除する。	A1：給与所得・退職所得の源泉徴 A2：雇用保険届出事務 A3：労働者災害補償保険法に基づ A4:健康保険・厚生年金保険届出事 B4：国民年金の第３号被保険者の C1:報酬・料金等の支払調書作成事 C2：配当、剰余金の分配及び基金 C3:不動産の使用料等の支払調書作 C4:不動産等の譲受けの対価の支払

点検:毎月

【個人番号】取得状況（２０１６年度は2015年末取得を含む）								【２０１６年度】 の利用　（1）				
NO	① 氏名	②社員番号/種類	③個人番号取得日	④取得担当者	⑤手段	⑥確認資料	⑦確認資料取扱	⑧対象業務	⑨ 提出日	⑩控	⑪担当者	点検印
例	青井春夫	W297401	2015/12/5	斎藤由紀子	手渡し	a雇用契約有	コピー保存	A1：源泉徴収票/税務署	1/9	控個人番号なし	斎藤由紀子	
例	青井冬子	配偶者	2015/12/5	柴田幸一	代理人手渡し	c通知カード＋運転免許	コピー保存	A1：源泉徴収票/税務署	1/9	控個人番号なし	藤澤博	
例	赤井夏子	講師	2016/1/10	斎藤由紀子	郵送	e住民票＋運転免許証	シュレッダー	C1：報酬支払/税務署	3/5	控個人番号なし	藤澤博	

【番号法対応のため改定:既存様式】

3200 個人情報保護方針
3210 個人情報の取扱について
3301 個人情報取扱規程
3303PMS年間計画表(兼点検表)
3311 業務フロー
3312 個人情報管理台帳
3313-01 リスク分析表(従業者情報)
3341-01 個人情報保護体制
3341-02PMS に関する責任と権限一覧表
3424-02 通知と同意書(従業者)
3433-01 機密保持誓約書
3510PMS 文書体系

以下に、一部をご紹介します。

制定：２０１○年○月１日
最終改定：２０１○年○月１日

個人情報保護方針

株式会社　○○○○
代表取締役社長　○○○○

株式会社○○○は、△△△（例：広告代理店、人材派遣、印刷、情報システム開発）事業者として取扱う個人情報の重要性と社会的責任についてよく認識し、当社における個人情報保護マネジメントシステム（ＰＭＳ）定着への活動を日々推進しています。当社は「行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、番号法と呼ぶ）」、「個人情報の保護に関する法律（以下、個人情報保護法と呼ぶ）」および、「JIS Q15001:2006　個人情報保護マネジメントシステム－要求事項」を遵守し個人情報を取り扱う組織として次の方針を掲げます。

ａ．個人情報の適切な取得・利用及び提供

当社は、△△△に関する事業で取扱う○○に関するお客様の個人情報、及び□□□に関する事業、並びに雇用等において取扱う特定個人情報を含む個人情報について、あらかじめ特定された利用目的の範囲の中で個人情報の適切な取得・利用を行い、利用目的の達成に必要な範囲を超えた個人情報の取扱(目的外利用）を行わないこと及びそのための措置を講じます。

ｂ．法令及び規範の遵守

当社は、個人情報の取り扱いに関して、「番号法」「個人情報保護法」など各種法令、国が定める指針その他の規範を遵守いたします。

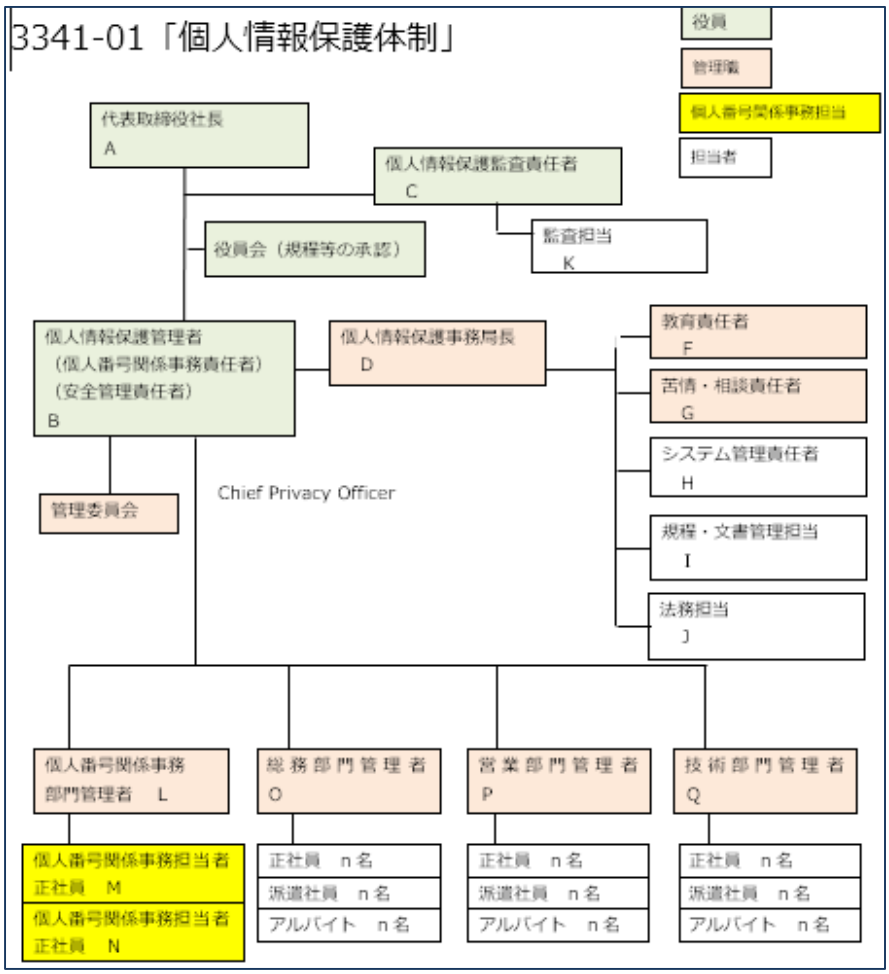
3312 個人情報管理台帳　「個人番号関係事務」

①種類	②媒体	③個人情報の項目	⑮機微他	④利用目的	⑤取得入力	⑥取得時期	⑦件数	⑧コピー	⑨開示	⑩アクセス権限	⑪保管場所保管方法
同意書	紙	氏名、個人番号取得の同意	－	人事管理	人事担当より	入社手続き時 変更申請時	200件／累積	－	開示	人事課長 人事担当	人事担当 常時施錠CAB
住民票	紙	氏名、住所、世帯情報	－	住民税処理 基本情報	人事担当より	入社手続き時 変更申請時	200件／累積	－	開示	役員 人事課長 人事担当	人事担当 常時施錠CAB
人事管理データ	電子	氏名、住所、入社年月日、生年月日、電話番号、役職、給与、資格、退職金	－	人事管理	担当が入力	－	200件／累積	－	開示	人事課長 人事担当	共有ファイルサーバー¥人事部¥人事管理
イントラネット登録情報	WORD	氏名、社員番号、メールアドレス	－	社内コミュニケーション	人事担当が入力	入社手続き時	200件／累積	全社共有	開示	人事課長 人事担当	イントラネットサーバー
個人番号確認資料 (従業者、扶養家族)	紙	氏名、住所、性別、生年月日、社員番号、個人番号	個人番号	個人番号関係事務	本人および代理人	2015年12月(全従業者)、入社手続き時	250件／累積	－	開示	個人番号関係事務担当者	個人番号関係事務専用CAB 常時施錠
個人番号確認資料(外部)	紙	氏名、住所、性別、生年月日、個人番号	個人番号	個人番号関係事務	本人	源泉手続き時	250件／累積	－	開示	個人番号関係事務担当者	個人番号関係事務専用CAB 常時施錠
個人番号マスタ(従業者、扶養家族)	Excel	社員番号、姓カナ、個人番号(2分割)	個人番号	個人番号関係事務	人事担当が入力	－	250件／累積	－	開示	個人番号関係事務担当者	共有ファイルサーバー¥人事部¥個人番号関係事務

3313-01 リスク分析表　「個人番号関係事務」

取得	入社手続	1～23	入社時取得書類 従業者現況表 住民票 同意書	本人・直接手渡し	紙	禁止	利用目的の通知漏れ	入社手続キット「同意書(従業者用」
							書面による同意の取得漏れ	授受記録(明細)
							個人番号の不適正取得	「3306特定個人情報記録」に記録
保管	従業者管理						目的外利用(期限を超える保管)	台帳見直し時の点検
							漏えい(紛失)	保管管理者の限定
								施錠管理

3341-01 個人情報保護体制



3424-02 通知と同意書（従業者）

入社時および入社後に提出いただく個人情報については、漏えい，滅失又はき損の防止に努め適切な安全管理体制のもとに、下記の通り取り扱います。

1．提出された個人情報の利用目的は下記に限定して取り扱います。
①人事管理：就業規則等に定める人事諸施策に関する管理
②勤務管理：就業規則等に定める労働時間および勤務状況の管理
③税務管理：法令等で定められた労務･税務処理
④業務管理：業務施策の企画立案、業務実施状況の把握
⑤経理精算：必要経費の精算
⑥給与情報：給与計算、指定金融機関への振込
⑦福利厚生：福利厚生事務・管理処理
⑧教育研修：社内外における教育・研修
⑨安全管理：施設の入退出、情報システム等の監視および点検
⑩個人番号関係事務：番号法に基づく個人番号関係事務

6ヶ月で構築する「**個人情報保護マネジメントシステム実施ハンドブック**」購入者用ダウンロードサイトでは、今後も、法律の施行等にあわせて、様式の改定、追加を致します。
「PMSハンドブック」のご購入は　個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html から、「書籍注文書.PDF」をダウンロードし、FAXでお申込みください。（特別価格、送料込み2500円）

＜目次＞

2015.10

【エッセイ】稲生物怪録

会員番号 0707 神尾博

2015年6月に公表された日本年金機構の事件を初めとして、外部からの攻撃による情報漏洩は、標的型メールに端を発する場合が多い。添付ファイルのクリックが契機となり、高機能マルウェアは数ヶ月から数年に渡り、段階的に活動を継続する。たとえばIT環境の調査、脆弱性への攻撃、権限の乗っ取り、感染拡大、重要情報の奪取等だ。

江戸時代にはたたり石での肝試しがきっかけとなり、三次藩（現在の広島県の一部）の自宅で30日間に渡り、夜な夜な幾多の妖怪の襲撃を受け続けた16歳の少年がいた。藩士で名を稲生平太郎という。剛毛の一つ目巨人、空中を徘徊する女の生首、走り回る蟹のような大石、等々。幼い弟と二人暮らしの彼は恐怖に立ち向かい、折れない心で妖怪を次々と撃退していった。その体験記は「稲生物怪録（いのうもののけろく、いのうぶっかいろく）」という物語にまとめられ、後世に残されている。この例に限らず、惰弱な人心に付け入る妖怪も、肝が据わっているつわものの前では、妖力を存分に発揮できないことがあるという。

サイバーセキュリティにおいても、高度な脅威には胆力と知力を兼ね備えたHRO（High Reliability Organization：高信頼性組織）化というアプローチがあるのではないか。実際、航空管制や救急救命は、使命感や強靭な意思を備えた精鋭が、社会的要請に応え十分に機能している。重要情報を取り扱う組織では、要員を相応の力量を備えた者に限定し、教育を施しても中途半端に留まる連中を排していった方が、効率的で事故のリスクも激減するだろう。そもそも「教育」は、ISOのマネジメントシステムにおいても「力量（competence）」確保のサブセット、手段に過ぎないとされており、選別という「他の方法」の採用を否定していない。

また、高機能ウイルスにはSIEM（Security Information and Event Management）と呼ばれるツールが有効であるとされている。SIEMはセキュリティ関連のログを幅広く収集して分析を行い、不審なふるまいを自動検出して、システム管理者に通報したり、通信を遮断したりするツールだ。異常の例を挙げると、入退室カードでは退社しているはずの社員のIDで社内からサーバへのアクセスがある、データベースへのアクセス直後に決まって縁遠い国へのパケット量が増える等がある。さらに最近では、技術者がマルウェアの行動パターンを定義するだけではなく、過去に累積された膨大なデータを機械学習させ、怪しい挙動の検出の精度向上に生かすといった、AI（Artificial Intelligence）技術の導入も進んでいる。

平太郎に降伏した妖怪の首領は、その豪胆を讃えて「もう一人の妖怪大将が現れたら、これを叩けば私が駆けつける」と、木槌を授けたと伝えられている。タフな精神力と高性能なツールの組み合わせは、まさに鬼に金棒だ。今後のサイバーセキュリティに関する議論や対策には、HROやAIの視点が不可欠になってくるだろう。

（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 より著作権保護期間満了後のものを引用しています。）

以上

＜目次＞

2015.10

第 205 回月例研究会講演録【 CSMS（サイバーセキュリティマネジメントシステム）認証と ISMS 認証の現状と今後 】

会員番号 0557 仲 厚吉

講師 ： 一般財団法人 日本情報経済社会推進協会（JIPDEC）
情報マネジメント推進センター 参事 高取 敏夫 氏

日時、場所 ： 2015 年 8 月 24 日（月）18:30 - 20:30、機械振興会館 地下 2 階ホール （神谷町）

講演テーマ ：「CSMS（サイバーセキュリティマネジメントシステム）認証と ISMS 認証の現状と今後」

要旨 ：

我が国の政府機関や重要インフラ事業者等に対して高度な技術によるサイバー攻撃が集中することが懸念されており、サイバーセキュリティ対策の強化が喫緊の課題となっている。

このような背景から、CSMS 認証と ISMS 認証への期待が高まっており、これらの認証についての現状と今後の展開について概説する。

講演録 ：

1．CSMS（サイバーセキュリティマネジメントシステム）認証

(1) 制御システムセキュリティの必要性

CSMS 認証は、エネルギー分野（電力、ガス等）や石油・化学、鉄鋼等のプラント、鉄道等の交通インフラ、機械、食品等の生産・加工ラインなどの重要インフラの操業中断が無いように、重要インフラを支える制御システムへのセキュリティの必要性から求められています。

IACS（Industrial Automation and Control System）は、エネルギー分野（電力、ガス等）や石油・化学、鉄鋼等のプラント、鉄道等の交通インフラ、機械、食品等の生産・加工ラインなど社会・産業基盤を支える産業用オートメーション及び制御システムである。
IACS は、従来、専用システムで構成され、外部ネットワークとは接続されていないことから、セキュリティ上の脅威は殆ど意識されていなかった。しかし、近年、業務システム向けに開発された汎用技術（PC やサーバの基盤環境、TCP/IP 等のプロトコル等）、ネットワーク（遠隔操作、遠隔保守等）、メディア（データ抽出、パラメータ変更）の活用が進んだ結果、いわゆるサイバー攻撃の対象となっている。
IACS がサイバー攻撃を受けて停止した場合、社会インフラやビジネスの継続に深刻な影響を及ぼすだけでなく、HSE（Health、Safety and Environment）に対する深刻な影響が生じる可能性もある。

(2) 制御システムセキュリティを実現するための基準

制御システムセキュリティを実現するため、制御システムセキュリティ標準として、制御システム分野で、制御システムの利用者、装置製造者のそれぞれが活用できる IEC 62443 シリーズがあります。

IEC 62443-1 シリーズ	この規格全体の用語・概念等の定義
IEC 62443-2 シリーズ	組織に対するセキュリティマネジメントシステム
IEC 62443-3 シリーズ	システムのセキュリティ要件や技術概説
IEC 62443-4 シリーズ	部品（装置デバイス）層におけるセキュリティ機能や開発プロセス要件

制御システムのサイバーセキュリティマネジメントシステム（CSMS）は、制御システム関連組織向けに特化した要求事項を規定しています。CSMS の主要なカテゴリーは、リスク分析、CSMS によるリスクへの対処、並びに CSMS の監視及び改善の3つで構成されており、リスク分析をベースとしたセキュリティマネジメントシステムの構築が可能になっています。

(3) CSMS の対象者

CSMS 構築は、制御システムの保有事業者（アセットオーナー）、及び運用・保守事業者（オペレーター）、制御システムの構築事業者（システムインテグレーター）の三位一体で取り組むことが必要不可欠です。各事業者が単独で取り組むのではなく、連携して関係プレイヤーが CSMS 構築に取り組む必要があります。

制御システムを保有する事業者：アセットオーナー
制御システムの構築事業者：システムインテグレーター
制御システムの保守・運用事業者：オペレーター

(4) CSMS 適合性評価制度の目的

CSMS 適合性評価制度は、IACS を対象としたサイバーセキュリティマネジメントシステムに対する第三者認証制度です。CSMS 適合性評価制度は、わが国の制御システムセキュリティの向上に貢献するとともに、利害関係者からも信頼を得られるセキュリティ対策を確保し、維持することを目的としています。

(5) CSMS 認証基準の構成

CSMS 認証基準（IEC 62443-2-1:2010）は、4.2 リスク分析、4.3 CSMS によるリスクへの対処、4.4 CSMS の監視及び改善、から構成されています。

4.2 リスク分析	4.2.2 事業上の根拠：IACS のサイバーリスクに対処するため組織の固有のニーズを識別及び文書化する。
	4.2.3 リスクの識別、分類及びアセスメント：組織が直面している一連の IACS のサイバーリスクを識別し、これらのリスクの可能性及び重大度のアセスメントを行う。
4.3 CSMS によるリスクへの対処	4.3.2 セキュリティポリシー、組織及び意識向上
	4.3.3 選ばれたセキュリティ対抗策
	4.3.4 導入
4.4 CSMS の監視及び改善	4.4.2 適合：組織向けに開発された CSMS に従っていることを確実にする。
	4.4.3 CSMS のレビュー、改善及び維持管理：時間の経過に合わせて CSMS がその目標に合致し続けることを確実にする。

(6) CSMS 認証基準（IEC 62443-2-1:2010）

CSMS 認証基準（IEC 62443-2-1:2010）は、事業上の根拠、リスクの識別、分類及びアセスメント、リスクの優先順位のアセスメント、関連するリスクの識別及び優先付け、リスク許容度の確立、CSMS によるリスクへの対処、リスクマネジメント及び管理策の導入、上位レベル及び詳細なリスクアセスメントの更新、CSMS の監視及び改善などを、要求しています。

4.2.2 事業上の根拠	組織は、IACS のサイバーセキュリティを管理するための組織の取り組みの基礎として、IACS に対する組織の固有の依存性に対処する、上位レベルの事業上の根拠を策定しなければならない。
4.2.3 リスクの識別、分類及びアセスメント	4.2.3.1 リスクアセスメント方法の選択
	4.2.3.2 リスクアセスメントの背景情報の提供
	4.2.3.3 上位レベルのリスクアセスメントの実行
	4.2.3.8 詳細なリスクアセスメントの方法の識別
	4.2.3.9 詳細なリスクアセスメントの実行
	4.2.3.11 物理的リスクのアセスメントの結果と HSE 上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合
	4.2.3.12 IACS のライフサイクル全体にわたるリスクアセスメントの実行
4.3.2 セキュリティポリシー、組織及び意識向上	システム又は組織がその資産を保護するためにサイバーセキュリティサービスをどのように提供するかを規定または統制する一種の規則である。
	4.3.2.6.5 リスクに対する組織の許容度の決定
4.3.3 選ばれたセキュリティ対抗策	「4.3 CSMS によるリスクへの対処」に規定する CSMS のプロセスの一部として「5.詳細管理策」より管理策を選択しなければならない。選択した管理策及びそれらを選択した理由、並びに管理策の中で適用除外とした管理策及びそれらを適用除外とすることが正当である理由を示した「適用宣言書」を作成しなければならない。
4.3.4 導入	4.3.4.2.1 IACS リスクの継続的管理 組織は、設備の使用期間全体にわたって、受け入れられるレベルになるようにリスクを管理するために、IACS 装置及び対抗策の選択及び導入を含んだリスクマネジメントの枠組みを採用しなければならない。 4.3.3 で選択した管理策を導入する。リスクの対処は、組織が許容できる期間内に行う必要があるため、その期間を念頭に置いた管理策の適切な導入計画の策定が求められる。ただ、新たなプロセスや基準を持ち込むのではなく、従来から行っていた活動をブラッシュアップし、PDCA サイクルを適用する方向で整理し、CSMS の管理策へと発展させる方法も有効である。

(7) 上位レベル及び詳細なリスクアセスメントの更新

4.2.3.10(再アセスメントの頻度及びトリガーになる基準の識別)では、組織は、技術、組織又は産業活動の変化に基づいた、再アセスメントのトリガーになるあらゆる基準を識別するだけではなく、リスク及びぜい弱性の再アセスメントの頻度も識別しなければなりません。組織は、適切なタイミングで上位レベル及び詳細なリスクアセスメントを更新する必要があります。更新のトリガーとしては、たとえば以下のケースが挙げられます。

- IACS の新規システム導入時
- IACS のシステム更新時
- IACS のシステムの変更
- 法律・規制の変更
- IACS に対するリスクの変化

(8) CSMS の監視及び改善

組織は、4.4(CSMS の監視及び改善)のため、4.4.3(CSMS のレビュー、改善及び維持管理)を図ります。

4.4.3 CSMS のレビュー、改善及び維持管理	4.4.3.1 CSMS に対する変更を管理及び導入するための組織の割り当て
	4.4.3.2 CSMS の定期的な評価
	4.4.3.3 CSMS の評価のトリガーの確立 組織は、CSMS の関連要素のレビュー及び場合によって変更を行うきっかけとなる、設定されたしきい値を持つトリガーのリストを確立しなければならない。これらのトリガーには、少なくとも、重大なセキュリティインシデントの発生、法律及び規制の変更、リスクの変化及び IACS に対する大きな変更が含まれる。しきい値は、組織のリスク許容度に基づかなければならない。
	4.4.3.5 リスク許容度のレビュー

(9) CSMS と ISMS の関係

CSMS(IEC 62443-2-1)の構成は、本文と手引書から成り立っています。本文は、「マネジメントシステム(MS)」と「管理策」、及び「附属書 A(参考)CSMS の要素の開発に関する手引き」で構成されます。「管理策」には、「手引書」が IEC 62443-2-2 として提案中です。CSMS と ISMS の関係では、両者の共通要件と固有要件を特定し、CSMS の構築には CSMS 固有の要件の適用が求められます。

(10) CSMS 固有の要件の概要

ISO/IEC 27001:2014 になく CSMS 認証基準(IEC 62443-2-1)にだけある要求事項(固有の要件)の一部を記載します。全体は、「CSMS ユーザーズガイド-CSMS 認証基準(IEC 62443-2-1)対応-Ver.1.2 平成 27 年 5 月 JIPDEC」の付録 3 で参照できます。本ユーザーズガイドは、次の Web サイトで入手できます。

http://www.isms.jipdec.or.jp/csms/doc/JIP-CSMS111-12.pdf

CSMS 認証基準(Ver.1.0)	IEC 62443-2-1	
	項番	要件
4. サイバーセキュリティマネジメントシステム		
4.2 リスク分析		
4.2.3 リスクの識別、分類及びアセスメント		
4.2.3.3 上位レベルのリスクアセスメントの実行	4.2.3.3	IACS の可用性、完全性又は機密性が損なわれた場合の財務的結果及び HSE(Health, Safety and environment)に対する結果を理解するために、上位レベルのシステムリスクアセスメントが実行されなければならない。
4.2.3.5 単純なネットワーク図の策定	4.2.3.5	組織は、論理的に統合されたシステムのそれぞれについて、主要装置、ネットワークの種類及び機器の一般的な場所を示す単純なネットワーク図を策定しなければならない。
4.2.3.11 物理的リスクのアセスメントの	4.2.3.11	資産のリスク全体を理解するために、物理的リスクのアセスメン

結果と HSE 上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果の統合		トの結果と HSE 上のリスクのアセスメントの結果とサイバーセキュリティリスクのアセスメントの結果が統合されなければならない。
4.3 CSMS によるリスクへの対処		
4.3.2 セキュリティポリシー、組織及び意識向上		
4.3.2.4.5 訓練プログラムの経時的な改訂	4.3.2.4.5	新たな又は変化する脅威及びぜい弱性を説明するために、サイバーセキュリティの訓練プログラムが必要に応じて改訂されなければならない。
4.3.2.6.3 リスクマネジメントシステム間の一貫性の維持	4.3.2.6.3	IACS のリスクに対処するサイバーセキュリティのポリシー及び手順は、他のリスクマネジメントシステムによって作成されたポリシーに対して一貫性があるか、又はそれらを拡張したものでなければならない。
4.4 CSMS の監視及び改善		
4.4.3 CSMS のレビュー、改善及び維持管理		
4.4.3.6 業界の CSMS 戦略の監視及び評価	4.4.3.6	マネジメントシステムの所有者は、リスクアセスメント及びリスク軽減のための CSMS のベストプラクティスに関して業界を監視し、それらの適用可能性を評価しなければならない。
4.4.3.8 セキュリティ上の提案に関する従業員のフィードバックの要求及び報告	4.4.3.8	セキュリティ上の提案に関する従業員のフィードバックが、積極的に求められ、パフォーマンス上の欠点及び機会の点から経営幹部に必要に応じて報告が戻されなければならない。
5.詳細管理策		
5.2 要員のセキュリティ		
5.2.3 要員の継続的な選別	4.3.3.2.3	要員に対しては、利害の対立又は適切な方法で職務を実行することに対する懸念を示唆する可能性がある変化を確認するために、継続的な調査も行われなければならない。
5.3 物理的及び環境的セキュリティ		
（以下、省略）		

(11) CSMS 適合性評価制度の普及、及び今後

重要インフラ事業者はセキュアな制御システムを構築・保守及び運用する責務があり CSMS 認証が重要となります。

政府機関や重要インフラ等に対するサイバー攻撃が増加傾向にあり、サイバー攻撃が安全保障上の大きな脅威となりつつある。
重要インフラ等に対するサイバー攻撃は、社会全体に重大な影響を及ぼす可能性が高い。
2020 年の東京オリンピック/パラリンピックでは、わが国の政府機関や企業等に対してサイバー攻撃が集中することが懸念されており、サイバーセキュリティ対策の強化が急務である。

2. ISMS 認証の現状と今後

(1) ISMS 認証とは

ISMS 認証とはなにかの説明があり、また、ISMS 認証取得組織の年度別推移と海外における ISMS 認証状況の紹介がありました。日本の認証登録数は、2013 年に 7,084 件で、インドの 1,931 件、英国の 1,923 件をおさえて第一位となっています。

ISMS 認証基準は、JIS Q 27001:2014(ISO/IEC 27001:2013)である。
ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることである。
そのためには、ISMS を組織のプロセス及びマネジメント構造全体の一部として、かつ、その中に組み込むことが重要である。

(2) ISO/IEC 27000 ファミリー

ISO/IEC 27000 ファミリーの各規格について説明がありました。

ISO/IEC27000:2014 JIS Q 27000:2014	ISMS ファミリー規格の概要、ISMS ファミリー規格において使用される用語等について規定した規格。
ISO/IEC27001:2013 JIS Q 27001:2014	組織の事業リスク全般を考慮して、文書化した ISMS を確立、実施、維持及び継続的に改善するための要求事項を規定した規格。
ISO/IEC27002:2013 JIS Q 27002:2014	情報セキュリティマネジメントの確立、実施、維持及び改善に関するベストプラクティスをまとめた規格。ISO/IEC 27001 の「附属書 A 管理目的及び管理策」と整合がとられている。
ISO/IEC FDIS 27017:2015	クラウドサービスの提供者及びクラウドサービス利用に適用される情報セキュリティ管理策をまとめた規格。構成は、ISO/IEC 27002 の管理策との整合がとられている。附属書 A には、追加の管理策及び実施の手引きが規定されている。
ISO/IEC 27011:2008	電気通信業界内の組織に適用される情報セキュリティ管理策をまとめた規格。構成は、ISO/IEC 27002 の管理策との整合がとられている。SC27 と ITU-T の共同で発行された。

(3) ISMS ユーザーズガイド

「ISMS ユーザーズガイド-JIS Q 27001:2014(ISO/IEC 27001:2013)対応」発行のお知らせが、2014 年 4 月 14 日に JIPDEC 情報マネジメント推進センターより公表されました。本ガイド(PDF 版)は無料で配布され、入手を希望する場合は、次の Web サイトで申込みができます。

http://www.isms.jipdec.or.jp/JIP-ISMS111-30.html

ISMS 適合性評価制度に適用される認証基準が改訂され JIS Q 27001:2014 となったことに伴い、2008 年に発行した ISMS ユーザーズガイドが改訂されました。本ガイドの主な読者として想定しているのは、ISMS 認証取得を検討若しくは着手している組織において実際に ISMS の構築に携わっている方及びその責任者です。本ガイドでは、JIS Q 27001:2014 に記述された主要な条項を紹介し、要求する内容、要求の意図、コンセプト等について解説しています。

3. 情報セキュリティ、サイバーセキュリティの今後の展開

(1) 情報セキュリティ管理基準(平成 27 年改正版)

情報セキュリティ管理基準(平成 27 年改正版)は、JIS Q 27001:2014 及び JIQ 27002:2014 と整合性を取り、組織体が効率的に情報セキュリティマネジメント体制の構築と適切な管理策の整備と運用を行えるように規定しており、監査人が監査上の判断の尺度として用いるべき基準になっています。また、日本における ISMS 認証制度である「ISMS 適合性評価制度」において用いられる、適合性評価の尺度にも整合するよう配慮されています。

(2) サイバーセキュリティリスクと企業経営に関する研究会

サイバー攻撃の高度化により、サイバーリスクが企業経営にとって大きなリスクとなっている状況に加え、個人情報保護法改正及びマイナンバー法施行といった状況を踏まえ、IPA 及び経済産業省はリスクの見える化やセキュリティ強化のための有効な経営的・技術的対策を検討しています。

研究会の検討事項は、サイバー攻撃の早期検知・対処や事前対策に有効な経営的・技術的対策の検討、企業におけるセキュリティ経営を妨げている制度的課題等の抽出、セキュリティ経営を促進するような社会システムの在り方の検討、わが国企業のセキュリティ経営の促進のため、今後、政府及び関係機関が負うべき役割、講じるべき政策などが挙げられています。

4. 質疑応答、及び受講した感想

講演後の質疑応答では、CSMS 認証取得組織について質問があり、三菱化学エンジニアリング株式会社と、横河ソリューションサービス株式会社の 2 社が CSMS 認証を受けているとの説明があった。CSMS 構築は、制御システムの保有事業者(アセットオーナー)、及び運用・保守事業者(オペレーター)、制御システムの構築事業者(システムインテグレーター)の三位一体で取り組むことが必要不可欠であるので、今後は、制御システムの保有事業者(アセットオーナー)の認証取得が重要であるとの説明がありました。

我が国の政府機関や重要インフラ事業者等に対して高度な技術によるサイバー攻撃が集中することが懸念されており、サイバーセキュリティ対策の強化が喫緊の課題となっています。このような背景から、CSMS 認証と ISMS 認証への期待が高まっていますが、両者の違いは、前者で最も避けるべき事態は、操業の中断であり、IACS の可用性の維持とともに HSE 上のリスクへのアセスメントであるのに対し、後者は、情報資産を対象に、情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)の喪失へのリスク対策を求めているという点にあります。

本講演を受講して、両者のマネジメントシステムや管理策には共通する部分が多く、両者の共通要件と固有要件を特定し、CSMS を構築する際、CSMS 固有要件の適用を考えていくと良いことが理解できました。

以上

＜目次＞

2015.10

支部報告　【　近畿支部　第１５３回定例研究会　】

会員番号 1709 荒町 弘 （近畿支部）

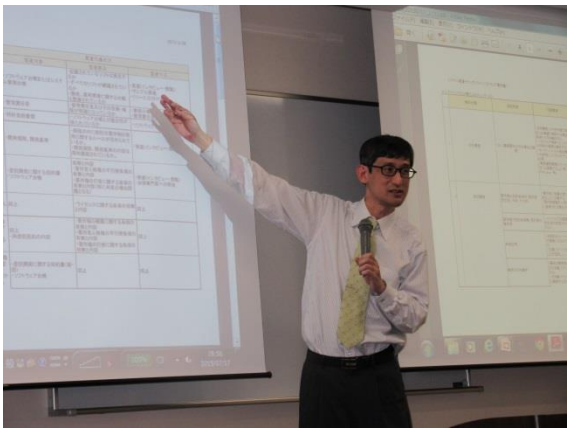
１．テーマ　（1）「ソフトウェア著作権研究プロジェクト最終報告」
（2）「システム監査の多様性研究プロジェクト（システム監査学会）報告」

２．講師　京都聖母女学院短期大学 生活科学科 准教授 荒牧裕一 氏
（本協会近畿支部会員、システム監査学会理事）

３．開催日時　2015年7月17日（金） 18:30～20:30

４．開催場所　大阪大学中之島センター 7階 講義室703

５．講演概要（１）



「ソフトウェア著作権研究プロジェクト最終報告」

ソフトウェア著作権研究プロジェクトはもともと、
「コンプライアンスのシステム監査研究会」の活動成果を受け、
分野別により深い研究を行うために発足した。
「ソフトウェア著作権」を研究対象に選んだ理由は、以下のとおり。
①昔から存在し、頻繁に改正がある。
②どの企業や業種にも共通して問題になる。
③違反には刑事罰があり、リスクが高い。
④内容が複雑でシステム監査学会との共同研究に適している。

本プロジェクトでは最終成果物として「システム監査チェックリスト」を作成した。これは、ソフトウェア著作権に関する注意事項を導入形態別に分類したものである。監査の進め方として、「監査対象」「監査要点」「監査手法」についてまとめてきた。

（ア）ライセンス契約の問題点

ライセンス契約はパッケージ業者とユーザー間の直接契約であり、第三者に対する対抗要件を備えないということが問題である。このため、パッケージ業者がソフトウェアの著作権を含めて別会社に事業譲渡を行った場合、ユーザーのライセンス契約を含んだ移転がなされるか否かにより、ユーザーのソフトウェア利用権が失効してしまうことがあるため注意が必要である。

（イ）ソフトウェア管理台帳

ソフトウェアおよびライセンスの適切な管理を行うための台帳として、JIPDECから公開されているSAMユーザーズガイドの内容をたたき台とし、ソフトウェア管理台帳の項目等を検討してきた。本台帳は、開発したソフトウェアおよび購入したソフトウェアの双方を管理できるように工夫してある。また、媒体などの情報も合わせて管理できるように配慮してある。本台帳の管理で注意が必要なのは、業務システムとして完成したソフトを管理する場合、システムのモジュールごとのライセンス形態についても確認して記載しておくという点である。

（ウ）ソフトウェア著作権管理の成熟度モデル

上記、SAMユーザーズガイドを参考とし、ソフトウェア著作権の管理レベルを0～5の6段階に分類し成熟度モデルを作成した。それぞれの段階において可能な監査の種類を示してあるので、ソフトウェア著作権に関するシステム監査を行う際に、予備調査段階で管理レベルについての評価を行う必要がある。

５．講演概要（２）

「システム監査の多様性研究プロジェクト（システム監査学会）報告」

システム監査学会では、多様化するシステムとそれに対応するシステム監査実務のあり方について研究してきた。多様性に関する視点はいくつかあり、これらの視点で研究発表や意見交換を行ってきた。

＜多様性に関する視点＞

- 監査を実施する組織の多様性・・・「民間企業」を対象とする監査が中心であったが、住基ネットや個人情報保護法施行などの流れも受け、「公共団体」「非営利団体」にもその対象が広がり、ついには大学等の「教育機関」「研究室」や「教員」までもその対象となってきている。従来の「聖域」がなくなりつつある。
- 技術の進歩とリスクの多様性・・・「ビッグデータ」「ネットバンキング」「SNS」スマホ利用の拡大など、ICT活用社会の広がりを受け、多様化したリスクに対する「適切なリスク分析」や「監査手法の検討」の必要性が高まっている。
- 管理状況（成熟度）の多様性・・・監査が可能な組織なのか、コンサルティングから行い監査可能な成熟度までレベルを上げていく必要のある組織なのか、成熟度からみた監査対象組織も多様化している。
- 監査業務の多様性・・・監査の形態は「直接監査」や「間接監査」そしてこれらを組み合わせてものも増えつつあり、手続きも「監査」「レビュー」「合意された手続き」による場合とで監査業務自体が多様化している。
- 監査目的の多様性・・・監査目的については、システムの信頼性／安全性／効率性が中心であったが、コンプライアンス／利便性／経営戦略適合性という目的も加わってきている。
- 情報提供先の多様性・・・監査報告についても従来は、経営者への情報提供（内部目的）が中心であったが、昨今はステークホルダーへの説明責任（外部目的）が増えてきている。
- アプリ・認証形態・機器の多様性・・・クラウドコンピューティングの普及や認証方式の多様化、タブレットやスマートフォンなど端末機器が多様化しており監査対象業務や範囲の絞込みも難しくなってきている。
- 監査の活用場面の多様性・・・経営のPDCAサイクル全体での監査の利用が増えてきている。

６．所感

ソフトウェア著作権に関する紛争は年を経るごとに多くなっている。国際的な著作権保護団体であるBSA（ビジネス・ソフトウェア・アライアンス）では、組織内での不正コピーに関する内部告発を促しており、不正コピーが解決されたときには、情報提供者に謝礼金を払うという対応も行っている。著作権違反は組織にとって大きな経営リスクとなってきていることを再認識した。

また、昨今は企業間での事業譲渡等も盛んに行われており、パッケージソフトウェアの製品名の変更や、ソフトウェア自体のバージョンアップによる製品構成の変更が生じるなど、ソフトウェアのライセンス管理は今後ますます複雑化していくと考えられる。SAM台帳に代表されるようなソフトウェアおよびライセンス管理の強化は喫緊の課題であり、そもそも企業や団体におけるソフトウェア管理に関する一層の意識向上が必要であると感じた。

監査の多様性という視点においては、多様化する経営課題を解決していくために、システム監査に対する期待や監査自体の責任は、今後一層重くなると考える。

情報システムの多様化や変化する経営環境に合わせたシステム監査の必要性について、今後さらに理解を深めて、経営に役立つシステム監査とは、という問いへの解を私自身も見出していきたい。

本日は、コンプライアンスとシステム監査、多様化するシステム監査につき貴重な講演を頂戴しました。

以上

＜目次＞

2015.10

注目情報（2015.9～2015.10）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■【SECセミナー　3500プロジェクトの開発データで実証された品質マネジメントのヒントと現場事例】

2015年9月16日　独立行政法人情報処理推進機構

IPA/SEC では、エンタプライズ系分野における国内の多様なソフトウェア開発のプロジェクトデータを収集・分析した「ソフトウェアデータ白書」を発行しており、その最新版である、「ソフトウェア開発データ白書 2014-2015」において、29 社 3,541 プロジェクトのデータを分析した統計情報を公開しています。

本セミナーでは、それらのデータに対して行った新たな信頼性向上等に向けた興味深い分析結果に加え、その分析内容に関連する先駆的企業のレビュープロセス改善に関する現場事例も紹介します。

（2015 年 10 月 16 日　開催）

http://sec.ipa.go.jp/seminar/20151016.html

■【職場の情報セキュリティ管理者の育成のためのガイドとハンドブックを公開しました】

2015年9月16日　独立行政法人情報処理推進機構

情報セキュリティ対策は近年ますます重要になっており、IT サービスを提供する側だけではなく、IT を利用するあらゆる部門において、組織のセキュリティポリシーやルールを徹底する等の取組みが必要です。 IPA では、IT を利用する組織において情報セキュリティ対策を実施する際の実施体制や、各部門で情報セキュリティ対策を担う人材の役割とその育成について解説する 2 種類の資料を公開しました。

（2015 年 9 月 16 日）

http://www.ipa.go.jp/jinzai/hrd/security/index.html#section13

＜目次＞

2015.10

【協会主催イベント・セミナーのご案内】

■月例研究会（東京）

第207回	日時:2015 年 10 月 23 日(金)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「失敗した IT プロジェクトの真の原因に迫るマンダラ図の紹介」
	講師	認定 NPO 法人　日本システム監査人協会　近畿支部 公認システム監査人　　松井　秀雄　氏
	講演骨子	IT プロジェクトで失敗を経験した時、何を学び、何を語り継ぐべきでしょうか？ ここ数十年の間、IT 部門では IT プロジェクト・マネジメントの手法を踏まえて、失敗プロジェクトから得た知見を蓄積し再発防止に努めてきたにもかかわらず、多くの IT プロジェクトが失敗しています。ある IT 業界誌に IT プロジェクトの7割が失敗しているという記事が出た程です。それほど多くのプロジェクトが失敗に終わる原因は、失敗プロジェクトの失敗原因を検討する際、検討メンバーの思いつきに頼った狭い範囲の検討に終始し、真の原因を究明できていないため、有効な「再発防止策」が打ち出せていない可能性があります。 当発表では、失敗原因を検討する際に網羅性のある視座・視点を検討メンバーに提供するツールとして「IT プロジェクト版・失敗原因検討マンダラ図」を紹介します。 これは、失敗学会の失敗原因マンダラ図をベースに開発したもので、4 月 5 日に NHK-TV で全国放送された番組「サキどり 『さよなら、失敗するワタシ～失敗学最新事情～』」の中でも紹介されました。 さらに特性要因図やなぜなぜ分析との共存を含めたマンダラ図の活用法や、システム監査における使用例も紹介します。システム監査では、「なぜその問題事象が起こったかを検討し、その原因をコントロール(仕組み)の欠点(弱点)としてとらえて指摘するスタンスが問題事象の再発防止に寄与すると考え、マンダラ図で原因分析を行い、「真の原因」を踏まえた改善提言をした事例を紹介します。
	お申込み	日本システム監査人協会ホームページ
第208回	日時:2015 年 11月19日(木)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「リスクマネジメントと危機管理　～想定内と想定外原点に戻って考える～」(仮題)
	講師	東京海上日動リスクコンサルティング株式会社 上席主席研究員　指田　朝久　氏
	講演骨子	詳細確定次第、HPでご案内いたします。
第209回	日時:2015 年12月14日(月曜日)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「IT ガバナンスの JIS 化」(仮題)
	講師	日本 IT ガバナンス協会(ITGI Japan)　　副理事長　梶本 政利 氏 認定 NPO 法人 日本システム監査人協会　副会長　　力 利則 氏
	講演骨子	詳細確定次第、HPでご案内いたします。
第210回	日時:2016年1月21日(木曜日)　18:30～20:30　場所:機械振興会館　　地下 2 階　ホール	
	テーマ	「最近のインターネットバンキングに係る不正送金事犯の現状と対策」(仮題)
	講師	警察庁 生活安全局 情報技術犯罪対策課 指導第一係 課長補佐　小竹 一則 氏
	講演骨子	詳細確定次第、HPでご案内いたします。

■システム監査体験セミナー（実践編）（大阪：近畿支部主催） 再掲

	システム監査体験セミナー（実践編）	
	日時：2015 年 10 月 24 日（土）13:00～20:00 /25 日（日）10:00～17:00	
	概要	・本セミナーは、システム監査を実際に行う機会が少ない現状において、システム監査技術者や公認システム監査人を目指される方、内部監査ご担当者やシステム監査にご興味をお持ちの方々に、模擬体験を通したシステム監査能力向上の機会をご提供することを目的としております。特に内部監査人養成は企業の内部統制整備に欠かせない要件となっており、この機会を利用した監査実務の体験は短期間での養成に最適と考えます。今回の監査テーマは昨年度と同様に「現行システムとユーザニーズの適合性、経営戦略と情報システムとの適合性」という、経営者の視点に立ったテーマと致しました。
お申し込み		HPでご案内中です。 （http://www.saaj.or.jp/shibu/kinki/taiken20151024.html）

【外部主催イベント・セミナーのご案内】

■ＩＳＡＣＡ東京支部 2015 年　月例会予定（東京）

日時： 2015 年 10 月例会 10/27（火）開催予定 19:00-20:40(受付開始：18:30) 2015 年 11 月例会 11/25（水）開催予定 18:30-20:10(受付開始：18:00) 2015 年 12 月例会 12/22（火）開催予定 19:00-20:40(受付開始：18:30)	
詳細	http://www.isaca.gr.jp/education/index.html

■ＩＴＣ協会　2015 年度主催セミナー

名称	自治体ビジネス研修「新入門編」【2015 年度版】
日時	2015/10/23(金） 東京開催は申込み受付中です。
名称	マイナンバー導入支援者育成研修 ー中小企業・小規模事業者への導入実務演習付きー
日時	2015/09/28（月） 大阪開催は申込み受付中です。 2015/09/29（火） 東京開催は申込み受付中です。
詳細	http://www.itc.or.jp/foritc/seminar/

＜目次＞

2015.10

新たに会員になられた方々へ

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

ご確認ください

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

特典

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

ぜひ参加を

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

ご意見募集中

・皆様からのご意見などの投稿を募集しております。
ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

出版物

・協会出版物が会員割引価格で購入できます。 http://www.saaj.or.jp/shuppan/index.html
システム監査の現場などで広く用いられています。

セミナー

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

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

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

お問い合わせ

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

＜目次＞

2015.10

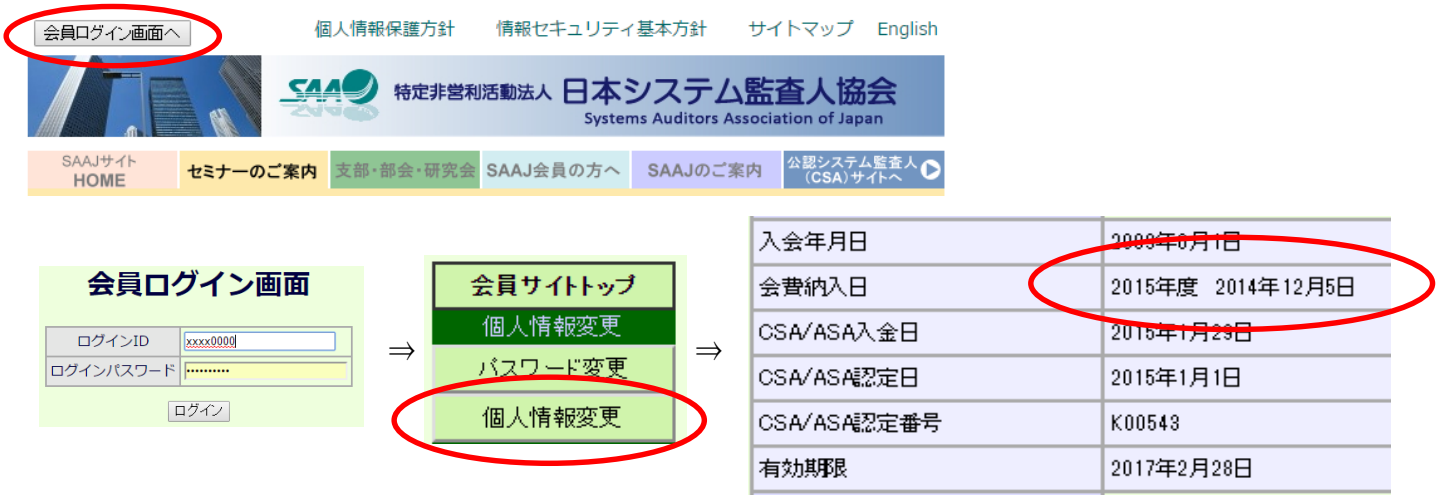
協会からのお知らせ　【年会費お支払状況をご確認ください】

会員番号　1760 斎藤由紀子　（事務局長）

会員各位

いつも、協会活動へのご協力を賜りありがとうございます。

会員の皆様からお支払いいただいた会費につきましては、協会ホームページ http://www.saaj.or.jp/kenkyu/index.html の「会員ログイン画面へ」から、会員ページにアクセスしていただきますと、会費のお支払状況をご確認いただくことができます。



年度をご確認ください。

2016年度の会費の請求書は、2015年12月に発送予定です。

既に、2016年度の会費をお支払いただいた方には、請求書はお送り致しませんが、二重振込のないよう、今一度お支払状況のご確認をお願い致します。

【2015年度会費未納の場合】

一部の会員の方について、2015年度の会費のお支払が未だ確認できません。2015年12月31日までに納付が確認できない場合は、除名処分となりますので、至急お手続きいただきますようお願い致します。

【ご寄附のお願い】

協会では、運営基盤のより一層の改善を図りたく、一口3,000円のご寄附をお願い申し上げます。

＜寄附金額＞￥3,000/一口　　ご寄附は、何口でも承ります。

＜振込先＞ご寄附は、協会会費に合算して、会費振込先にお振込みください。

＜東京都への個人情報の提供＞

法令に基づき、寄附者名簿（氏名、ご住所）を、所轄庁の東京都へ報告致します。

何卒ご了承賜りますようお願い致します。

＜会費・ご寄附についてのお問合せ＞：http://www.saaj.or.jp/toiawase/index.html　（事務局）

＜目次＞

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更・追加された予定			2015.10
2015 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
9 月	10：理事会	15：　第 206 回月例研究会	5-6:西日本支部合同研究会 （開催場所:岐阜）
10 月	8：　理事会	23：　第 207 回月例研究会	18：秋期情報処理技術者試験
11 月	12：理事会 13：予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/8〆切) 18：2016 年度年会費請求書発送準備 23：会費未納者除名予告通知発送 30：本部予算提出期限	中旬:秋期 CSA 面接 19：第 208 回月例研究会 20：CSA･ASA 更新手続案内 〔申請期間 1/1～1/31〕 27：CSA 面接結果通知	
12 月	1：2016 年度年会費請求書発送 2016 年度予算案策定 10：理事会:2016 年度予算案 会費未納者除名承認 第 15 期総会審議事項確認 11：総会資料提出依頼(1/8〆切) 15：総会開催予告掲示 18：2015 年度経費提出期限	10：CSA/ASA 更新手続案内メール 14：第 209 回月例研究会 18：秋期 CSA 認定証発送	
2016 年	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
1 月	8：総会資料(〆) 16:00 13：総会･役員改選の公示 14：理事会:通常総会資料原案審議 15：総会開催案内掲示･メール配信 20：2015 年度決算案 23：2015 年度会計監査 26：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 21：第 210 回月例研究会 20：春期 CSA･ASA 募集案内 〔申請期間 2/1～3/31〕	8：会計:支部会計報告期限 25：SAAJ 創立記念日
2 月	4：理事会:通常総会議案承認 22：第 15 期通常総会･特別講演 25：法務局:資産登記、活動報告提出 理事の変更登記 29：年会費納入期限	1～3/31:CSA･ASA 春期募集	
2015 年	**以下は、過去に実施した行事一覧**		
3 月	2 日　東京都への事業報告書提出 2 日　年会費未納者宛督促メール発信 12 日　理事会	4 日　第 200 回月例研究会 14-15 日　事例研:第 25 回システム監査実務セミナー(後半)	
4 月	9 日　理事会 末日　法人住民税減免申請	認定委員会:新規 CSA/ASA 書類審査 中旬　認定委員会:新規ASA認定証発行 28 日第 201 回月例研究会	19 日　2015 年春期情報技術者試験
5 月	14 日　理事会 29 日　年会費未納者宛督促メール発信	中旬　認定委員会:新規 CSA 面接 29 日第 202 回月例研究会	
6 月	3 日　認定 NPO 法人東京都認定！ 4 日　会費未納者督促状発送 11 日　理事会 12 日～会費督促電話作業(役員) 末日　支部会計報告依頼(〆切 7/14) 末日　助成金配賦額決定(支部別会員数)	10 日　認定委員会:CSA 面接結果通知 16 日　第 203 回月例研究会 18-19 日　事例研:第 27 回システム監査実践セミナー(日帰り 2 日間コース)	
7 月	8 日　支部助成金支給 9 日　理事会	1 日　秋期 CSA･ASA 募集案内 〔申請期間 8/1～9/30〕 14 日　第 204 回月例研究会 20 日　認定委員会:CSA 認定証発送	14 日　支部会計報告〆切
8 月	(理事会休会) 29：中間期会計監査	1：　秋期 CSA･ASA 募集開始～9/30 24：　第 205 回月例研究会	

＜目次＞

2015.10

会報編集部からのお知らせ

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

□■ 1. 会報テーマについて

2015 年度の年間テーマは、「システム監査人の魅力」です。これまでは「システム監査」に焦点を当ててきましたが、今年度は「システム監査人」に焦点を当てて考えてみたいと思います。8 月号から 11 月号までは、「システム監査人の喜び」をテーマといたします。皆様の幅広いご意見をお待ちしています。

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

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

1)PDF ファイルの全体を、URL(http://www.skansanin.com/saaj/)へアクセスして、画面で見る

2)PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る

3)会報 URL(http://www.skansanin.com/saaj/)の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

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

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

□■ 3. 会員の皆様からの投稿を募集しております。

分類は次の通りです。

1. めだか (Word の投稿用テンプレート(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (「会報掲載論文募集要項」及び「会報掲載論文審査要綱」があります)

□■ 会報投稿要項 （2015.3.12 理事会承認）

・投稿に際しては、Wordの投稿用フォーム（毎月メール配信）を利用し、会報部会（saajeditor@saaj.jp）宛に送付 して下さい。
・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
・特定非営利活動促進法第2条第2項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
・原稿の掲載、不掲載については会報部会が総合的に判断します。
・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。
バックナンバーは、会報サイトからダウンロードできます（電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にもなります）。
会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【本部・理事会議事録】（当協会ホームページ会員サイトから閲覧ください。パスワードが必要です）

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行： 認定 NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町2－8－8共同ビル6F

■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】 http://www.saaj.or.jp/toiawase/

■会報は会員への連絡事項を含みますので、会員期間中は、会員へ配布されます。
会員の所属や登録メールアドレス等の変更は、当協会ホームページ会員サイトより変更してください。
会員でない方は、購読申請・解除フォームに申請することで送付停止できます。
【会員でない方の送付停止】 http://www.skansanin.com/saaj/register/

■□■SAAJ会報担当
編集委員： 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子、西宮恵子、藤野明夫
編集支援： 仲厚吉 （会長）、各支部長
投稿用アドレス： saajeditor ☆ saaj.jp （☆は投稿時には＠に変換してください）

＜目次＞