認定 NPO 法人
日本システム監査人協会報
2018 年 10 月号
No 211
No.211（2018 年 10 月号）<9 月 25 日発行>

秋の夜長の過ごし方は？

ぜひ SAAJ の会報を
じっくり読んでみてください

会報バックナンバーはこちらから

写真提供：0557 仲厚吉　（秋田　寒風山）

巻頭言

～勉学の秋です～関心を持って具体的に行動しましょう！

会員番号：0281　カ　利則（副会長　月例研担当）

早いもので年末まであと３ヶ月になりました。暑い夏から少し涼しい秋にもなってきました。今回の巻頭言では次の２つのことをお伝えしたいと思います。２つともご存知のこととは思いますが、勉学の秋です。ぜひ時間を取って関心を持って具体的に取り組んでみてください。

（１）「発注者のプロジェクトマネジメントと監査」～ＳＡＡＪより出版！～もう読みましたか？

ＳＡＡＪからこの本が出版されたことは会員の皆様には総会や会報記事や先日の月例研での講演等でお聞きになっていると思います。この本は主査の原田憲幸氏を中心にプロジェクトマネジメント研究会のメンバー計９名が多くの時間を費やして制作した本です。トラブルプロジェクトにならないように発注者（委託元）が何をすれば良いのかを、企画・要件定義・調達、プロジェクト計画、外部設計、実装設計、プログラミング・テスト、総合テスト、受入検査・検収、運用試験、移行、品質管理等の各フェーズについて具体的な項目とその説明を記述しています。さらにシステム監査人としてプロジェクトをどういうタイミングでどういう監査観点で監査したら良いかを説明しています。システム監査人にとってとても役に立つ書籍であると思います。ご購入がまだの方はＳＡＡＪのＨＰに詳しい案内があるのでぜひ会員価格でご購入ください。

https://www.saaj.or.jp/shuppan/index.html

https://www.saaj.or.jp/shibu/130801PRJM2018Chirashi.pdf

（２）システム監査・管理基準の改定～経産省から 2018/4 月に公表～読み込んで使っていますか？

こちらも月例研や会報でご紹介しましたが、13 年振りにシステム監査・管理基準が改定されました。会員の皆様にはぜひ使って頂いてその事例の紹介や疑問点、改善点があれば、ＩＴアセスメント研究会までお寄せいただければと思います。システム監査関連の複数団体とも情報を共有して今後の取り組みを進めようとしています。　https://www.saaj.or.jp/shibu/kijun.html

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
【～勉学の秋です～関心を持って具体的に行動しましょう！】

1．めだか ……3
【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】

2．投稿 ……4
【エッセイ　仙境異聞】

3．本部報告 ……5
【PMS 要求事項【JIS Q 15001:2017】と「個人情報取扱規程」の事例　管理策 7】

4．支部報告 ……12
【近畿支部 30 周年記念シンポジウム　新システム監査基準／管理基準のポイント】
【近畿支部 30 周年記念シンポジウム　地方自治体のＩＣＴ監査に求められる役割と課題について】

5．注目情報 ……18
【ISMS-AC が IAF（国際認定フォーラム）の ISMS MLA（国際相互承認協定）に加盟】
【ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）】
【デジタルトランスフォーメーションに向けた研究会の報告書】

6．セミナー開催案内 ……19
【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】

7．協会からのお知らせ ……22
【新たに会員になられた方へ】
【協会行事一覧】

8．会報編集部からのお知らせ ……24

2018.9

めだか　【　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　】

2018 年 7 月 26 日の月例研究会は、「第 24 回企業 IT 動向調査 2018（2017 年度調査）～データで探るユーザー企業の IT 動向～」をテーマにしている。本調査の重点テーマは、「ビジネスのデジタル化に向けて動き出した IT 部門の実像」というものである。

アンケート有効回答 1078 社、インタビュー調査 50 社によると、ユーザー企業の IT 動向は、増収増益企業が大幅に増加し、この 10 年で 2 番目の好業績であることから、IT 投資が増え、業務プロセスの効率化（省力化、業務コスト削減）、迅速な業績把握、情報把握（リアルタイム経営）、営業力の強化、ビジネスモデルの変革を図るなどである。IT 重点トレンドは、AI、IOT、クラウド、ビッグデータ、RPA（Robotics Process Automation）とともに、MDM（Master Data Management）がとりあげられている。業務プロセスの効率化などでマスタデータを見直し情報システムを再構築するという動向がわかる。情報システムの再構築に当たっては、システム開発トラブルの未然防止のため、SAAJ 監修「発注者のプロジェクトマネジメントと監査」（同文舘出版）を参考にするようにお勧めしたい。2018 年 9 月 7 日の月例研究会は、この本の解説をテーマに開催される。

AI・ビッグデータでは、米国で 2016 年に「あなたを支配し、社会を破壊する、AI・ビッグデータの罠」（原題 WEAPONS OF MATH DESTRUCTION：数学破壊兵器）が出版されている。サービスプロバイダーは、ビッグデータを集め AI で数学的モデルを当てはめて予測するサービスを提供しているが、データの質や数学的モデルに問題があっても不透明で個人を不当に層別するなどの重篤な影響を与えていると警告し、監査による透明化などの今後の方向を提案している。一方、欧州では、2018 年 5 月 25 日より一般データ保護規則（GDPR）が適用され、基本原則に、「適法性、公正性及び透明性」、「目的の限定」、「データの最小化」、「正確性」、「記録保存の制限」、「完全性及び機密性」、「アカウンタビリティ」の 7 原則を挙げ、個人データ侵害は違法であるとし高額の罰則を設けている。システム監査人は、改訂システム監査基準・管理基準を参考に情報システムの光の部分とともに影の部分に留意することが大切である。

改訂システム監査基準は、留意事項に、“組織体の内部監査人がシステム監査を実施する場合には、日本内部監査協会の「内部監査基準」又は内部監査人の国際組織 IIA の「専門職的実施の国際フレームワーク」を、また情報セキュリティ監査制度に基づく監査を実施する場合においては、「情報セキュリティ監査基準」をあわせて参照することが望ましい。”としている。情報システムは、内部監査および情報セキュリティ監査でも重要であり、これからのシステム監査人の新たな活躍が期待される。（空心菜）

参考：「あなたを支配し、社会を破壊する、AI・ビッグデータの罠」キャシー・オニール著　久保尚子訳　インターシフト

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

<目次>

2018.9

【エッセイ】仙境異聞

会員番号　0707 神尾博

江戸後期の国学者・平田篤胤は、仙童寅吉という不思議な少年に出会った。寅吉は 7 歳から 5 年間、杉山僧正という天狗の化身である丸薬売りの老人の壺を経由して、常陸国の岩間山に赴き仙術の修行をした。その後も 15 歳まで江戸と仙界とを行き来したという。興味を持った篤胤は、寅吉を自宅に寄宿させた上で細部にわたってヒアリングを実施し、彼の異界での生活を著書「仙境異聞（せんきょういぶん）」にまとめた。徹底した精査の姿勢は、システム監査人から見ても称賛に値するほどだ。

我々も閲覧中のサイトやメール本文内の URL のクリックで、予期せぬ場所へ誘導されることがある。鬱陶しい広告くらいは序の口で、ネット取引に似せたデザインでパスワードを詐取されたりすると、悲惨な状況に陥ることも少なくない。目当てのサイト以外への転送の手口としては、DNS キャッシュポイゾニングのような正しい情報を書き換えてしまうもの、あるいは Web ミドルウェアや独自に開発した Web アプリの脆弱性を突いて、不正なサイトへリダイレクトするように細工をしてしまうもの等がある。

歴史的に Web サイト改竄の著名なところでは、2000 年の我が国の複数の官公庁に対するものが挙げられるが、当時のハクティビズムや技術力誇示から、近年は金銭や重要情報を目的としたマルウエアのダウンロードサイトへの誘導等に移ってきた。最近では 2017 年に WordPress（Content Management System の一種）の脆弱性を狙った攻撃で、全世界で 150 万以上のサイトが被害に遭った。テロ組織まがいの画面に書き換えられた日本の大学の例もある。

被害防止には修正プログラム適用はもとより、ハッシュ値で内容変更を検知して管理者にメールを送信したり、ログを Web サーバとは別の場所に保管したりといった多面的な対策も必要だ。では、自分の運営サイト以外の改竄を見つけた時にはどうするか？一般には JP-CERT への報告が推奨されている。刑事ドラマでは「第一発見者を疑え！」が常套句だが、セーフブラウジング中の警告はよくある話なので。よもや容疑がかかることはあるまい。

さて一説によると、その後の寅吉は超能力が失せながらも、天狗に教わったという秘薬を子孫に伝え、末代まで好評を博したという。一方で、現代のサイバーセキュリティでは、マルウエアの分析や駆除のために「ハニーポット」や「サンドボックス」という異界を利用するケースがあるが、これぞまさに IT の妙薬と呼べるだろう。

（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 により著作権保護期間満了後のものを引用しています。）

<目次>

2018.9

本部報告　PMS 要求事項【JIS Q 15001:2017】と「個人情報取扱規程」の事例　　管理策 7

会員番号　1760 斎藤由紀子　（個人情報保護監査研究会）

新個人情報保護法では、個人情報の保護とともに有用性の確保が必要とされ、個人情報保護法第四章第二節に、匿名加工情報取扱事業者等の義務（36 条～39 条）が新設されました。
http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/viewContents?lawId=415AC0000000057_20170530_428AC0000000051
関連して、個人情報保護法施行規則、個人情報保護法ガイドライン（匿名加工情報編）等が整備されています。
今回も、附属書 A（規定）および附属書 B（参考）の要求事項を確認しつつ、できるかぎりシンプルな規程として「3300 個人情報取扱規程」のサンプルをご紹介したいと思います。

※ この連載を基にした HTML 版を公開しています。
規格本文＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/000JISQ15001_2017.html
管理策 1＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/001JISQ15001_2017.html
管理策 2＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/002JISQ15001_2017.html
管理策 3＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/003JISQ15001_2017.html
管理策 4＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/004JISQ15001_2017.html
管理策 5＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/005JISQ15001_2017.html
管理策 6＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/006JISQ15001_2017.html
管理策 7＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/007JISQ15001_2017.html

引用：日本規格協会「日本工業規格 JIS Q 15001:2017 個人情報保護マネジメントシステム要求事項」

赤字：【2006 年版 JIS】から追加、変更となった規格

青字：PMS 監査研究会のコメント

A.3.4.2.9	匿名加工情報 法 36～39 条 施行規則 20～23 条 法 GL（匿名加工編）	組織は、匿名加工情報の取扱いを行うか否かの方針を定めなければならない。 組織は、匿名加工情報を取扱う場合には、本人の権利利益に配慮し、かつ法令等の定めるところによって適切な取扱いを行う手順を確立し、維持しなければならない。
	附属書 B.3.4.2.9	個人情報保護リスク軽減の観点から、組織は、匿名加工情報を安易に個人情報保護マネジメントシステムの対象外と捉えることなく、匿名加工情報の取扱いの各局面において復元のリスクがないかなどについてリスクアセスメント及びリスク対策を行うことが望ましい。 “匿名加工情報の取扱いを行うか否かの方針”とは、このリスクアセスメント及びリスク対策の結果である。したがって、当該方針の文書化及び外部への公表の要否についても、リスクアセスメント及びリスク対策を踏まえた運用となる。匿名加工情報取扱いのリスクアセスメント及びリスク対策は、A.3.3.3 を参考に行うことが望ましい。 “適切な取り扱いを行う手順”は、法令等の遵守の観点から、文書化した情報として管理し、A.3.5 を参考に内部規程の作成、記録の管理などを行うことが望ましい。 また、A.3.5 に基づく教育の実施など、匿名加工情報を取り扱う担当者を踏まえた管理を行うことも有効であるといえる。組織が、付属書 A に示す管理策を参考に匿名加工情報を管理することが、“確立し、かつ、維持”につながる。
	【P マーク審査のポイント】 ・匿名加工情報の取扱いを行うか否かの方針を定める。ただし、外部への公表は必須ではない。 ・匿名加工情報とすることで、本人の同意を得ずに目的外利用、第三者提供が可能となる。 ・個人情報保護法施行規則第 19 条（個人情報保護委員会規則で定める基準・・要約）	

1.個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）。
2.個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）。
3.個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む）。
4.特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む）。
5.前各号に掲げる措置のほか、個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し、その結果を踏まえて適切な措置を講ずること。
6.匿名加工情報についても「個人情報管理台帳」で管理し「リスク分析」を実施することが PMS として有効である。

・匿名化しても、流通が規制される情報
1.カルテなどの医療情報
2.電話など通信情報
3.クレジットカードなどの信用情報

・**法第 36 条～39 条**「匿名加工情報取扱事業者」等の義務　・・・・要約
1.個人情報保護委員会規則で定める基準に従い、個人情報を加工しなければならない。
2.匿名加工情報の作成に用いた個人情報から削除した記述等及び加工の方法について、安全管理のための措置を講じなければならない。
3.匿名加工情報を作成したときは、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならない。
4.匿名加工情報を第三者に提供するときは、匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表し、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示しなければならない。
5.匿名加工情報を作成して自ら当該匿名加工情報を取り扱うに当たっては、当該匿名加工情報を他の情報と照合してはならない。
6.匿名加工情報を作成したときは、苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。

・**施行規則第 20 条**（加工方法等情報に係る安全管理措置の基準）・・・・要約
1.加工方法等情報（削除した記述、加工方法に関する情報等）を取り扱う者の権限及び責任を明確に定めること。
2.加工方法等情報の取扱いに関する規程類を整備し、当該規程類に従って加工方法等情報を適切に取り扱うとともに、その取扱いの状況について評価を行い、その結果に基づき改善を図るために必要な措置を講ずること。
3.加工方法等情報を取り扱う正当な権限を有しない者による加工方法等情報の取扱いを防止するために必要かつ適切な措置を講ずること。

・**施行規則第 21 条**（個人情報取扱事業者による匿名加工情報の作成時における公表）・・・・要約
1.法第 36 条第三項の規定による公表は、匿名加工情報を作成した後、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行うものとする。
2.他の個人情報取扱事業者の委託を受けて匿名加工情報を作成した場合は、当該他の個人情報取扱事業者が当該匿名加工情報に含まれる個人に関する情報の項目を前項に規定する方法により公表するものとする。この場合においては、当該公表をもって当該個人情報取扱事業者が当該項目を公表したものとみなす。

・**施行規則第 22 条**（個人情報取扱事業者による匿名加工情報の第三者提供時における公表等）
1.法第 36 条第四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。
2.法第 36 条第四項の規定による明示は、電子メールを送信する方法又は書面を交付する方法その他の適切な方法により行うものとする。

※「個人情報取扱規程」のサンプルでは、「匿名加工情報の取扱いを行わない」とし、最小限の規定としています。

※「匿名加工情報取扱事業者」は、別途「匿名加工情報取扱規程」の策定が必要です。

【3300 個人情報取扱規程】サンプル

3.4.2.9　匿名加工情報

当社は、匿名加工情報の取扱いを行わない。

2　匿名加工情報の取扱いを開始する際は、事前に規程を定め、本人の権利利益に配慮し、かつ法令等の定めるところによって適切な取り扱いを行う手順を確立し、維持する。

■

A.3.4.3　適正管理　（2006：3.4.3）		
A.3.4.3.1	正確性の確保 2006：3.4.3.1 法第 19 条	組織は、利用目的の達成に必要な範囲内において、個人データを、正確、かつ、最新の状態で管理しなければならない。 組織は、個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。
	附属書 B 3.4.3.1	正確性の確保とは、例えば、誤入力チェック、誤りなどを発見した場合の訂正、内容の更新、保存期間の設定、データのバックアップなどの手順を確立することである。 なお、取得した個人データを一律に又は常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保することが望ましい。 個人データの消去にあたり、組織は、法令の定めによる保存期間などに留意することが望ましい。
	【P マーク審査のポイント】 ・個人データだけでなく、個人情報についても同様に正確性の確保が計られなければならない。 ・誤入力チェックは、画面と印刷物との照合、他者による再チェック、複数担当者の封入確認印の押印など、取扱う個人情報に応じて、安全管理規程や業務手順書に明確に定めておくこと。 ・データのバックアップは、情報システム単位で個別に手順書を定めておくこと。バックアップを取らないと判断した場合は、業務手順書等に「紙情報からの復元が可能」など、理由を記述すること。 ・毎年「個人情報管理台帳」の見直し時期に、保存期間を経過した個人情報について、廃棄・消去等について件数を見直すこと。 ・「個人情報管理台帳」の件数を更新した日を、消去記録とみなすことができる。 ・「特定個人情報」、「要配慮個人情報」、「受託した個人情報」、「提供を受けた個人情報」については、個別に消去記録、返却記録を取っておくこと。	

【3300 個人情報取扱規程】サンプル

3.4.3　適正管理

3.4.3.1　正確性の確保

当社は個人情報を正確かつ最新の状態で管理するため、「3430 安全管理規程」を定め、これを維持する。

2　当社は、個人データ等を利用する必要がなくなったときは、「3430 安全管理規程」6(個人情報の返却・廃棄・消去)の手順に従い、当該個人データまたは個人情報を遅滞なく消去するよう努めるものとする。

■

A.3.4.3.2	安全管理措置 2006：3.4.3.2 法第 20 条	組織は、その取扱う個人情報の個人情報保護リスクに応じて、漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならない。 安全管理措置に関する管理目的及び管理策は、付属書 C を参照
	附属書 B 3.4.3.2 保護法 GL8-3 保護法 GL8-4 保護法 GL8-5 保護法 GL8-6	安全管理措置は、緊急事態が発生した場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人情報の取扱状況などに起因する個人情報保護リスクに応じた必要かつ適切な措置を講じることが求められているのであって、全ての個人情報についての一律な措置を講じる必要がない。 安全管理措置とは、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、及び技術的安全管理措置をいう。

		“組織的安全簡易措置”とは、安全管理について従業者（法第 21 条参照）の責任及び権限を明確に定め、安全管理に対する規程及び手順書を整備運用し、その実施状況を確認することをいう。 “人的安全管理措置”とは、従業者（個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員など）だけでなく、取締役、執行役、理事、監査役、監事、派遣社員なども含まれる。）に対する、業務上秘密と指定された個人データの非開示契約の締結、教育・訓練などを行うことをいう。 “物理的安全管理措置”とは、入退館（室）の管理、個人データの盗難の防止などの措置をいう。 “技術的安全管理措置”とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視など、個人データに対する技術的な安全管理措置をいう。 "必要かつ適切"とは、経済的に実行可能な最良の技術の適用に配慮することをいう。 "経済的に実行可能な最良の技術"は、組織の事業内容及び規模によって異なっても差し支えない。 個人情報の漏えい事例には、廃棄時の漏えいが多く見られることから、廃棄に当たっても、電子ファイルの消去、個人情報が打ち出された紙の破砕処理などによって、廃棄された個人情報が他者に流出することのないよう留意することが望ましい。 なお、安全管理措置については、個人情報保護リスク軽減の観点から、個人情報を対象としている。
	【P マーク審査のポイント】 ・特定個人情報は、法定保存期間を経過した場合には、できるだけ速やかに、復元不可能な手段で廃棄又は削除しなければならない。そのため、「個人情報管理台帳」の年 1 回の見直し時期に、件数も見直されるはずである。 ・個人データの取扱いの運用に関する手法として、以下の事例が示されている。 ・個人データのアクセスの記録：システムログ、利用記録、業務日誌 ・個人データの持ち運び状況：授受記録、持出記録、返却記録 ・個人情報データベース等の削除・廃棄記録 ・個人番号関係事務担当者の、特定個人情報へのアクセス記録 ・個人データを取扱う区域の管理：入退室管理 ※サンプル「個人情報取扱規程」においては、個別の措置については記述せず、「3430 安全管理規程」を定めると規定するにとどめています。	

【3300 個人情報取扱規程】サンプル

3.4.3.2　安全管理措置

当社は取扱う個人情報の漏えい、滅失又はき損の防止その他の個人情報を安全管理のために、必要、かつ適切な措置を講じるため「3430 安全管理規程」を定め、これを維持する。

■

A.3.4.3.3	従業者の監督 2006： 3.4.3.3 法第 21 条	組織は、その従業者に個人情報を取扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。
	附属書 B 3.4.3.3	監査役に対する監督を実施する場合には、例えば、株主総会による選任権及び解任権を通じた監督が考えられ、取締役など業務執行者による監督は、内部監査の独立性が害されるため監督したことにならない。 なお、A.3.4.5 の認識の管理策は、従業者に、個人情報保護マネジメントシステムの運用を確実に実施できる力量を備えさせるための管理策であり、従業者の監督とは意味合いが異なる。 また、組織が従業者に個人情報を取り扱わせる場合、個人データと同様に取り扱わせなければならないことについては、B.3.3.1 参照。

	【P マーク審査のポイント】 ・従業者との「機密保持誓約書」の締結が主眼である。 ・「機密保持誓約書」と「個人情報の取扱いに関する通知及び同意文書」を混同しないこと。同じ文書として、署名欄を一つにしているケースがあるが、不適合である。 ・派遣社員については、派遣元と受け入れ派遣社員との間で取り交わすことが望ましい。 ・監視カメラについて 欧州では、企業が従業員に黙って社内に監視カメラを設置し、制裁金が科された事例が複数見られる。さらに GDPR によって、従業員との雇用契約とは別に同意の手続きが必要という認識となってきている。カメラの角度などによっては、同意を拒否する機会を与えるという認識が必要である。

【3300 個人情報取扱規程】サンプル

3.4.3.3　従業者の監督

当社は従業者に個人情報を取扱わせるに当たって、必要、かつ適切な監督を行う。そのため「3430 安全管理規程」を定めこれを維持する。

2　従業者との雇用契約時に、個人情報を含む機密保持義務遵守のため「3433-01 機密保持誓約書」を締結する。

3　「3433-01 機密保持誓約書」記載の機密保持義務は、雇用契約終了後も一定期間有効とする。

■

A.3.4.3.4	委託先の監督 2006： 3.4.3.4 法第 22 条	組織は、個人データの取扱いの全部又は一部を委託する場合、特定した利用目的の範囲で委託契約を締結しなければならない。 組織は、個人データの取扱いの全部又は一部を委託する場合は、十分な個人データの保護水準を満たしている者を選定しなければならない。このため、事業者は、委託を受ける者を選定する基準を確立しなければならない。委託を受ける者を選定する基準には、少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認できることを含めなければならない。 組織は、個人データの取扱いの全部又は一部を委託する場合は，委託する個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。 組織は、次に示す事項を契約によって規定し、十分な個人データの保護水準を担保しなければならない。 a)委託者及び受託者の責任の明確化 b)個人データの安全管理に関する事項 c)再委託に関する事項 d)個人データの取扱状況に関する委託者への報告の内容及び頻度 e)契約内容が遵守されていることを委託者が、定期的に、及び適宜に確認できる事項 f)契約内容が遵守されなかった場合の措置 g)事件・事故が発生した場合の報告・連絡に関する事項 h)契約終了後の措置 組織は、当該契約書などの書面を少なくとも個人データの保有期間にわたって保存しなければならない。
	附属書 B 3.4.3.3	委託を行う場合においては、委託者は、消費者など、本人の権利利益保護の観点から、事業内容の特性、規模及び実態に応じ、委託の有無、委託する事務の内容を明らかにするなど、委託処理の透明化を進めることが望ましい。A.3.4.3.4 における委託先には、個人も含まれる。 “必要かつ適切な監督”には、組織が、A.3.4.3.2 に基づき安全管理措置を講じることが含まれる。例えば、委託者が委託する業務内容に対して必要のない個人データを提供しないよう安全管理措置を講じることは A.3.4.3.2 に適合する。一方、委託者が必要のない個人データを委託先に提供した結果、委託先が個人データを漏えいした場合には、委託者についても、A.3.4.3.2 に適合しない。 また、個人データの取扱いの全部又は一部を委託する場合に限らず、委託先への個人情報の提供又は委託先との間での個人情報の授受が発生する場合は、B.3.3.1 参照。 委託先が倉庫業、運送業、データセンター（ハウジング、ホスティング）などの事業者であって、当該事業者に取り扱わせる情報に個人データが含まれるかを知らせること

		なく預ける場合であっても、委託者は委託するものが個人データであることを知っているわけであるから、A.3.4.3.4 における監督の対象に含まれる。ただし、“個人データ”に関する条項を契約書に盛り込まなくてもよい。 A.3.4.3.4 の　a) ～g)の事項は、いかなる場合にも契約によって規定することを要求するものではなく、取り扱う個人データのリスクに応じて規定する内容が変わっても差し支えない。 A.3.4.3.4b)個人データの安全管理に関する事項には、次の事項が含まれる。 －個人データの漏えい防止及び盗用禁止に関する事項 －委託範囲外の加工及び利用の禁止 －委託先契約範囲外の複写及び複製の禁止 －委託契約期間 －委託契約終了後の個人情報の返還・消去・廃棄に関する事項 A.3.4.3.4c)再委託に関する事項には、次の事項が含まれる。 －再委託を行うに当たっての委託者への文書による報告 個人データの取り扱いを再委託する場合、委託元との契約に、再委託を行うに当たっての委託元への文書による事前報告又は承認について盛り込むことが望ましい。 委託元が委託先について“必要かつ適切な監督”を行っていない場合で、委託先が再委託をした際に、再委託先が適切といえない取り扱いを行ったことによって、何らかの問題が生じたときは、元の委託元がその責めを負うことがあり得るので、再委託する場合は注意をすることが望ましい。 このため、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、再委託先に対し、A.3.4.3.2 に基づき少なくとも委託する当該業務に関しては、自社と同等以上の個人情報保護の水準にあることを客観的に確認することが望ましい。確認の例としては、委託先が再委託する相手方、再委託する業務内容、再委託先の個人データの取扱方法などについて、委託先から事前報告又は承認を求めること、委託先を通じて又は必要に応じて自らが、定期的に、及び適宜に監督を実施することなどがある。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とすることが望ましい。 【必要かつ適切な監督を行っていない場合】 事例 1)再委託の条件に関する指示を委託先に行わず、かつ、委託先の個人データの取扱状況の確認を怠り、委託先が個人データの処理を再委託し、再委託先が個人データを漏えいした場合。 事例 2)契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにも関わらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を講じなかった結果、委託元の認知しない再委託が行われ、その再委託先が個人データを漏えいした場合。 なお、人材派遣事業者との人材派遣契約、清掃事業者との契約、オフィスの賃貸借契約などは、個人データの取扱いを含まない限り、A.3.4.3.4 の対象外として差し支えない。これらは広く A.3.4.3.2 に含まれるものであり、このような事業者とは、守秘義務に関する事項を盛り込んだ契約を締結することが望ましい。
	【P マーク審査のポイント】 ・委託先選定基準に基づいて委託先を選定し、定期的に再評価を実施していること。 ・「個人情報委託先リスト」等で、全ての委託先が漏れなく特定されていることが確認できること。 ・再委託先がある場合は、「個人情報委託先リスト」等で、確認できること。 ・特定個人情報の再委託については、最初の委託者の許諾が必要である。 ・委託先とは、A.3.4.3.4 の a)～h)の内容が盛り込まれた契約を締結していること。 ・委託契約書が個人情報の保有期間にわたって保存されていること。 ・委託先に渡した個人情報について、返却記録、消去・廃棄記録があること。	

【3300 個人情報取扱規程】サンプル

3.4.3.4　委託先の監督

当社は個人情報の取扱いの全部又は一部を委託する場合、十分な個人情報の保護水準を満たしている者を選定し、全社の委託先について「3434-01 委託先管理台帳」を作成し管理する。

2　委託先選定基準として以下を定める。

A	3434-02 委託先調査票　　（A：シンプル）
B	3434-03 委託先調査票　　（B：詳細）
C	3434-09 委託先調査票　　（C：個人番号関係事務）
D	3434-08 委託先自己評価票（D：再評価用）

3　各部門長は、個人情報を委託する前に、「3421 個人情報取得・変更申請書」および、前項に規定する A～D のいずれかに必要事項を記載し、個人情報保護管理者の承認を得る。

4　部門長は、委託先と下記の内容を含めた「3434-04 業務委託契約書」又は、「3434-10 業務委託契約書（個人番号関係事務）」を締結し、原本を個人情報保護管理者宛に提出する。個人情報保護管理者は、委託契約に係る個人情報の保有期間にわたって、当該契約書を保管する。

a)	委託者および受託者の責任の明確化
b)	個人情報の安全管理に関する事項
	漏えい・盗用防止
	範囲外加工・利用禁止
	範囲外複写禁止
	委託契約期間
	契約終了後の返還・消去・廃棄
c)	再委託に関する事項
d)	個人情報の取扱状況に関する委託者への報告の内容及び頻度
e)	契約内容が遵守されていることを委託者が定期的に、及び適宜に確認できる事項
f)	契約内容が遵守されなかった場合の措置
g)	事件・事故が発生した場合の報告・連絡に関する事項

5　部門長は、「3303PMS 年間計画書（兼点検表）」に従い、委託先について毎年 1 回以上および、委託先について安全管理上の懸念があった場合に再調査を実施し、個人情報保護管理者へ提出する。再評価は状況に応じて、第 2 項に規定する A)～D)のいずれかの委託先選定基準を使用する。

6　部門長は、個人情報を委託する都度、「3434-06 委託業務指示書」および「3434-07 委託業務指示書管理台帳」もしくはそれにかわる個人情報の授受記録によって個人情報の所在を管理しなければならない。

7　部門長は、「3434-07 委託業務指示書管理台帳」を毎月点検する。

8　個人情報保護管理者は、第 2 項に規定した委託先選定基準の内容が社会情勢や環境の変化に適合しているかどうか、毎年 1 回以上点検しなければならない。

■

次回は、3.4.4　個人情報に関する本人の権利　から考察します。

以上　■■

<目次>

2018.9

支部報告　【　近畿支部　30 周年記念シンポジウム　】

会員番号　2508 藤原敏宏

1．テーマ　　「新システム監査基準／管理基準のポイント」

2．講師　　SAAJ 副会長

（株）ビジネスソリューション　代表取締役

松枝 憲司 氏

3．開催日時　２０１８年6月３０日（土）　１３：１０～１４：００

4．開催場所　エル・おおさか(大阪府立労働センター)　６階 大会議室

5．講演概要

日本システム監査人協会副会長、ＩＴアセスメント研究会主査で、平成３０年４月に改訂されたシステム監査に関する検討会に委員として携わった講師から、システム監査基準／管理基準の改定にどういう視点で取り組んだかという観点でご紹介頂いた。

＜講演内容＞

(ア)新システム監査基準・管理基準の公開と目的

今回の基準改定の目的として、①現在の技術環境に従来の管理基準が適合していない、②監査と管理の基礎知識、経験がない人による利用が若干困難である事(従来のものは管理項目が並んでいるだけで、別途ある分厚い解説書で理解する必要がある。)、③必ずしも監査や管理の行為規範・基準としての観点からの記述が徹底されていない(プログラマー、SE が行う事が書かれている場面がある)、④セキュリティ管理基準との補完性が明確でない、⑤情報システムの IT の定義・使い分けがいまひとつはっきりしていない、⑥IT ガバナンスの定義がはっきりしないまま言葉が使われている。といった点に問題意識を持ち、記述形式の改定が図られた。

改定内容として、従来の管理基準には主語がなかった為、『誰が』を明確にした。「すべきこと」と「することが望ましいこと」を明確に区別した。基準の構成として、監査基準は各基準→主旨→解釈指針の 3 段階、管理基準は各項目→主旨→着眼点の 3 段階で記述し、管理基準の方は従来の解説書がなくても、使える事を願った構成にしている。

(イ)システム監査基準の改定のポイント

監査の実施の手順に従って、大きく 5 つにグループ分けされている。個々で記述されている内容はそれほど大きく変化はしていないが、前文にシステム監査の定義を記載している。

前文には、システム監査の目的、意義と適用上の留意事項、システム監査上の判断尺度、改定の背景と主要な改定内容について記述されている。

(ウ)システム管理基準の改定のポイント

情報技術環境の劇的な変化への対応(システムの開発・保有からサービスの利用へ)、情報システム設

計方法論の変容（従来のウォーターフォール型からアジャイル等へ開発方法が変わってきている）、情報システムと情報技術の関係、ＩＴガバナンスへの貢献を操作化（IT ガバナンスとしての行動を具体的に見えるように）といったポイントで改定されている。

管理基準は、グローバルスタンダードのＩＳＯ等を参照しているが、参照しているだけで、この管理基準を使えば、それぞれの ISO 等を満たすというものでは決してないので、それぞれの該当するものを確認する必要がある。

(エ) システム管理基準枠組みのポイント

今まではなかったシステム管理基準の枠組みについて記載している。大きな目的としては、今回管理基準に取り込んだ IT ガバナンスについて多くページを割いて説明している。

- IT ガバナンスのモデルについて JIS38500:2015 で採用されているものは ISO38500:2008 をベースとしており、ISO38500:2015 はまだ JIS 化されていない。
- 経営陣から指示している内容が ISO38500:2008 では計画と方針だったが、ISO38500:2015 では戦略と方針となっており、評価する対象が ISO38500:2008 ではプロトコルだったが、ISO38500:2015 では、提案と計画となっている。
- 新しい管理基準では、ISO38500:2015 を意識したものとなっている。
- ＩＴガバナンス層はＣＩＯ、C×O、CIO や各部門長を入れた委員会等を含めた経営陣とし、IT マネジメント層は各部門の部門長以下という整理で管理基準は作られており、組織に合わせた読み替えが必要となる。

(オ) フェーズ別改定概要とポイント

第 1 章のポイントとして、情報戦略といっているものを IT ガバナンスに置き換えており、同じような項目もあるが、構成として IT ガバナンス層で戦略・方針を決めるとマネジメント層がその次のレベルのものを実行していくという建て付けになっており、2 章以降のものと連携をとっていく形になる。

従来と大きく変わった点として、全体最適化という言葉が何か所にもでてきたが、今回は使っておらず、IT ガバナンスに変えている。個人的な理解としては、全体最適という言葉は全体の範囲が曖昧であり、また、ある時点で全体最適が図れたとしても、環境が変わる中で最適であり続ける事は考えられない為、全体最適の解は分からないという事で、正解のないものに悩ますよりは、EDM サイクルを回す方が、より実態に合うのではないかという考えである。

- 企画フェーズ以降ではドラスティックな点はない。
- やる人の事を書いていたもの（開発計画、分析、調達）を監査・管理する側の視点（プロジェクト計画の管理、要件定義の管理、調達の管理）に名称を変更した。
- アジャイル開発は、最後まで色々な意見もあったが、開発のフェーズの一部ではなく新設とした。
- 運用・利用フェーズは旧管理基準の運用業務がベースだが、当然ながら利用するだけのユーザーの視点も必要である事から、運用・利用フェーズとしている。
- 新しい管理基準では、保守フェーズはソフトウェアを対象としている。

- 外部サービス管理における外部サービスは、外部のリソースを活用して企業内の業務の遂行を外部に委託する事を指す。（クラウド etc）
- 事業継続管理のフェーズにおける事業継続は IT ガバナンスレベルでの方針、業務継続は個々の業務、情報システムの継続を指す形で使い分けている。

(カ)ISO38500 関連基準の動向

ISO38500 シリーズの各項目についてご紹介頂いた。

現状では、ISO38500:2008 だけが JIS 化されており、IT アセスメント研究会では、1～5 までを独自で翻訳し、学習している。6 月上旬に ISO38503 が次のステップに進む。

6．所感

本講演では管理基準を定める上での背景等をご説明頂いた。個人的には、JIS 規格等についても同様であるが、そのものだけを読んでも理解する事が難しく、そこに至る経緯等を把握する事で理解がしやすくなるケースが多いように感じる。今後、自分自身がシステム監査基準/管理基準を学習する上で、役立つ講演であったと思う。

以上

<目次>

2018.9

支部報告　【　近畿支部　30 周年記念シンポジウム　】

会員番号　1497 尾浦俊行

１．テーマ「地方自治体のＩＣＴ監査に求められる役割と課題について」

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6月３０日（土）　１４：０５～１４：５５

４．開催場所　エル・おおさか(大阪府立労働センター)　６階 大会議室

５．講演概要

講師は民間企業の内部監査部門、監査法人での外部監査業務、会計検査院調査官の経験を経て、大阪市でＩＣＴ監査を率いておられる片岡氏。　地方自治体でのＩＣＴ監査のあるべき姿、現状並びに課題への対応についてお話しいただきました。

Ⅰ．地方自治体における監査制度

一般企業における会計監査と比較した場合の地方自治体における監査制度の特徴として、

・自治体の監査制度は監査委員により行われる

・監査報告は監査委員名で出され、監査委員事務局は予備調査・本調査を通じて監査委員監査の材料を提供する

・地方公共団体における事務等が最少の経費で最大の効果をあげているか否かについて特に意を用いて行われる

の３点が挙げられる。

また、監査委員監査には常に住民目線に立脚して行うことが求められており、さらに昨今は

・法令重視は当たり前であり、従来のコンプライアンス重視の監査から、本当に効果的にやっているかという観点の３Ｅ（経済性、効率性、有効性）へと変わってきている。

・国の会計検査院検査も同様の流れであり、受検側も意識改革が求められている。

Ⅱ．地方自治体におけるＩＣＴ監査の役割

今や、ＩＣＴは行政サービスおよび自治体運営における重要な基盤であり、自治体においてはＩＣＴの適正利用が強く求められている。このような時代の要請に基づき、総務省から「電子自治体の取組を加速するための１０の指針」が示されており、ＩＣＴ監査もこれらの実現に寄与することが期待されている。これらを踏まえた地方自治体におけるＩＣＴ監査のミッションは

「地方自治体が、ＩＣＴの適正利用を阻害するリスクに対するコントロールを適切に整備・運用するよう助言・勧告すること」である。

一方、ＩＣＴの適正利用を阻害するリスクを醸成してしまう地方自治体の一般的問題として

・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

・電子自治体の取組は、特定の職員の能力・努力に依存している

の３点が以前からも言われているが、今も変わっていない

Ⅲ．大阪市におけるＩＣＴ監査

１．大阪市におけるＩＣＴ監査取組みの経緯

地方自治体の監査委員監査においては、ＩＣＴが事務の簡素化・効率化並びに市民の利便性の向上に合致した形で構築・運用されているか等の観点からＩＣＴ監査に取り組む必要があるが、大阪市の監査委員監査は過去、必ずしも十分な取り組みができていなかった。

このようななか、ＩＣＴリスクの増大に伴い「**ＩＣＴの課題に突っ込んでいける監査委員（監査委員事務局職員）がいない**」ために「**継続的・体系的なＩＣＴ監査の実施ができていない**」ことに対する大阪市の監査委員や監査委員事務局内での問題意識と危機感の高まりがあり、監査部にＩＣＴ監査の専門家を活用することが検討され、ＩＣＴ監査担当課長の設置とＩＣＴ監査実施担当者の育成が始まった。

２．ＩＣＴ監査取組みの基本スタンス

個別改善は勿論ながら、組織上の本質的な原因分析にもとづく再発防止について指摘し改善を促すことが最も重要との認識のもと

①個々の統制活動の不備指摘だけにとどまらず、ＩＴガバナンス上の課題についても十分な検証と問題指摘及び提言を行う

②リスクの顕在化を未然に防止するためのコントロールの有無を主眼に置く

③内部統制の構築・改善に貢献する

④ＩＣＴ関係者の教育と啓発に貢献する

の４点を基本スタンスとしている。

３．監査委員監査報告書の記載について

監査の結果、明らかになった事実や原因、改善事項を記載した課題事項確認書を作成し、受検局とやりとりする。場合によっては局長からのコメントを求めることもある。

監査委員監査報告書の指摘事項を書く際には、単に露わになった問題の発生原因を追求するのではなく「あるべき状況」を踏まえたうえでの本質的原因と改善勧告を書く。

３Ｅ監査になるほど本質的原因への合意をとることは難しくなるが、そこが大事であり外すことはできない。

４．過年度における監査実施後の所感

内部統制の不足と、外部業者への過度な依存が感じられる。その原因としてＩＣＴ統括部門、ＩＣＴ利用部門共にＩＣＴ監査を受けたことがなく、ＩＣＴに係るリスク認識が不足していることがあげられる。

自分たちが何をしたいか、優先順位はどうかを自治体側のＩＣＴ部門がしっかりと業者に伝えなければならないということがわかっていない。

５．改善勧告の効果の例

システムの導入・運用を組織的に管理する仕組みや基本的リスク管理ができていないことが明らかになったため、「抜本的にＩＣＴ管理体制を見直し、ＩＣＴ人材を養成・確保すべき」との改善勧告を行い、外部からのＩＣＴ専門人材の登用や、局内におけるＩＣＴ専門組織の新設にもつなげた。

Ⅳ．地方自治体におけるＩＣＴ監査の更なる普及に向けて

１．ＩＣＴ監査の普及を阻む原因

① 監査委員において、ＩＣＴ監査の重要性・必要性への認識が不十分である。

② 事務局職員のＩＣＴに係る知見が不足している。

③ ＩＴガバナンス上の指摘・提言が不足している。

２．対応策

① 監査委員の意識改革が必要である。また監査専門委員として、ＩＴ専門家を活用する方法もある。

② 事務局職員の教育や、庁内ＩＣＴ部門経験者の登用することが考えられる。

③ ＩＣＴ監査をツールとして経営的視点からの指摘や改善勧告を行う。

３．新システム監査基準／システム管理基準の活用

今回の改訂では、項目ごとに実施主体（実施者）、主旨、着眼点、モニタリング項目を明確にし、ＥＤＭモデルを盛り込んでいる。これらは、金融庁の検査基準には従来からある視点である。

特に、新システム管理基準　Ⅰ－４から１－１０のＩＣＴガバナンスに係る管理基準は今後ぜひとも活用すべきである。

＜所感＞

自治体ＩＣＴ監査においても３Ｅ監査への要請が高まっているというお話について、先進自治体においてＣＯＢＩＴで言うところのＩＴ統制成熟度が向上していることの現れであろうと感じました。

経営的視点を持ってＩＣＴの技術的負債を解消し、攻めのＩＣＴ投資に向けた余力を生み出すことは、ベンダーは勿論のことＩＣＴ統括部門、ＩＣＴ利用部門のいずれからも中立の立場から行わなければ困難であり、技量面からもシステム監査人でなくては難しいはずです。大阪市のように監査側に必要な人材を確保しＩＣＴの適正利用に関するＥＤＭを回している団体は急速に攻めのＩＣＴが進んでいき、そうでない団体との差が開いていくのでしょう。

外部業者への過度な依存というご指摘については、経済産業省のデジタルトランスフォーメーションに向けた公開資料の中でも「ベンダー側のリスクが高すぎて負いきれない」といった課題が提起されるなど危機的レベルに近づいているようであり、この面でも長期的ＥＤＭをツールとして監査側が果たすべき役割は大きいはずだと感じました。

ＩＣＴ監査について真正面から取り組まれ、着実な成果を上げている事例を知ることは、我々にとっては正しく働く勇気が沸いてくる貴重な機会だったと感じます。今後とも引き続きご指導をお願いするしだいです。

以上

<目次>

2018.9

注目情報（2018.8～2018.9）

■「IAF（国際認定フォーラム）のISMS MLA（国際相互承認協定）に加盟」報道発表【ISMS-AC】2018/8/24

一般社団法人情報マネジメントシステム認定センター(ISMS-AC)は、国際的な認定機関の協力組織であるIAF（国際認定フォーラム）において、ISMS の MLA(国際相互承認協定)への加盟が認められ、8 月 21 日付けで加盟の調印を行いました。

https://isms.jp/iaf/MLA/IAF_ISMS_MLA.html

■「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）」の公表【経済産業省】2018/9/3

経済産業省では、本年 2 月 28 日に第 1 回会合を開催した「産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）ビルサブワーキンググループ」において、ビルシステムに関するサイバーセキュリティ対策についての検討を行ってきました。この度、「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（β版）」を取りまとめました。

http://www.meti.go.jp/press/2018/09/20180903003/20180903003.html

■「デジタルトランスフォーメーションに向けた研究会の報告書『DX レポート～IT システム「2025 年の崖」の克服と DX の本格的な展開～』」を公表　【経済産業省】2018/9/7

経済産業省は、我が国企業がデジタルトランスフォーメーション（DX）を実現していく上での IT システムに関する現状の課題の整理とその対応策の検討を行い、『DX レポート～IT システム「2025 年の崖」の克服と DX の本格的な展開～』として報告書を取りまとめました。

http://www.meti.go.jp/press/2018/09/20180907010/20180907010.html

<目次>

2018.9

【 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236回	日時	2018 年 10 月 22 日(月)18:30～20:30
	場所	港区芝公園　3-5-8　機械振興会館 地下 2 階ホール http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
	テーマ	IoT・ビッグデータ時代のソフトウェア・AI に係る知的財産
	講師	平塚 三好 氏 東京理科大学ビジネススクール（大学院 経営学研究科 技術経営専攻） 教授博士（工学）
	講演骨子	ソフトウェア特許をはじめ、異業種間の標準必須特許のライセンス交渉の在り方、ビッグデータの不正競争防止法での保護等、近年の官庁の議論の紹介を通じ、IoT・ビッグデータ時代のソフトウェアやビッグデータ、OSS 等に関する知的財産の取り扱いについて、解説する。 また、AI についても、AI のからくりを紹介しつつ、AI の知財における保護の在り方に関する研究を紹介する。
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	下記 URL よりお申込みください。 https://www.saaj.or.jp/getsurei/getsurei_form236.html

■SAAJ 月例研究会（東京）		
第237回	日時	2018 年 11 月 21 日(水)18:30～20:30
	場所	港区芝公園　3-5-8　機械振興会館 地下 2 階ホール http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
	テーマ	信頼できるインターネット社会の実現に向けて －クラウドサービスの適合性評価の方向性－（仮称）－
	講師	山内 徹 氏 一般財団法人日本情報経済社会推進協会(JIPDEC) 常務理事 インターネットトラストセンター センター長 一般社団法人情報マネジメントシステム認定センター(ISMS-AC)代表理事
	講演骨子	クラウドサービスの適合性評価の方向性について（詳細準備中）
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	協会ホームページ https://www.saaj.or.jp/ でご案内準備中

■SAAJ「(2018 年度)関東地区主催会員向け SAAJ 活動説明会」(東京・茅場町)	
日時	2018年10月27日(土) 13時30分～17時30分 交流会 17時30分～19時00分
場所	NATULUCK茅場町新館　2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**会員の皆様**に、SAAJの各研究会・部会活動にご参加頂くための情報提供を目的に、昨年に引き続き、開催することになりましたので、ご案内いたします。 3つのテーマでの**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。 参加された方には、**受講証明書(4時間)**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・部会の活動内容や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：休憩含め3時間 （資料は、当日配布します。） (1)「監査基準、管理基準の改訂について（仮題）」（50分） 講師：ＩＴアセスメント研究会 (2)「JIS Q 15001改定内容について（仮題）」（50分） 講師：個人情報保護監査研究会 (3)「情報セキュリティ関連基準の動向（仮題）」（50分） 講師：情報セキュリティ監査研究会 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	下記URLよりお申込みください。 https://www.saaj.or.jp/kenkyu/Keizoku/keizoku_form.html

<目次>

2018.9

【 外部主催イベント・セミナーのご案内 】

■システム監査学会　第 31 回公開シンポジウム	
日時：2018 年 11 月 9 日（金）10 時～16 時 50 分	
主催	システム監査学会
場所	機械振興会館ホール（東京都港区芝公園 3-5-8）
テーマ	データ保護の動向とシステム監査
お申込み	https://www.sysaudit.gr.jp/sympo/2018_31_sympo_program.html

<目次>

2018.9

【 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　https://www.saaj.or.jp/index.html
・会員規程　https://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　https://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　https://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。　https://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

・「発注者のプロジェクトマネジメントと監査」「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。
https://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　https://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。　https://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。https://www.saaj.or.jp/toiawase/index.html
各サイトに連絡先がある場合はそちらでも問い合わせができます。

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2018.9
	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	13：理事会	～秋期 CSA・ASA 募集中　～9/30 迄 7：第 235 回月例研究会 13,14: 第 32 回システム監査実務セミナー(日帰り 4 日間コース)後半	
10 月	11：理事会	22：第 236 回月例研究会 27：会員向け活動説明会	21：秋期情報処理技術者試験
11 月	8：理事会 8：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/7〆切） 16：2019 年度年会費請求書発送準備 26：会費未納者除名予告通知発送 30：本部・支部予算提出期限	10,17,24：秋期 CSA 面接 21：第 237 回月例研究会 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	17：「2018 年度西日本支部合同研究会　in Fukui」
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 13：理事会：2019 年度予算案 会費未納者除名承認 第 18 期総会審議事項確認 14：総会資料提出依頼（1/7〆切） 14：総会開催予告掲示 19：2018 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〕 26：秋期 CSA 認定証発送	12:協会創立記念日
1 月	7： 総会資料提出期限 16:00 10：理事会：総会資料原案審議 26：2018 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 18： 春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕	7：支部会計報告期限
2 月	7：理事会：通常総会議案承認 28：2019 年度年会費納入期限	2/1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	22：第 18 期通常総会
	前年度に実施した行事一覧		
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)」 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」	
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	13,26：春期 CSA 面接 19：第 232 回特別開催月例研究会 「新システム監査／管理基準」 28：CSA フォーラム（茅場町 NATULUCK）	
6 月	1：年会費未納者宛督促メール発信 14：理事会 19：年会費未納者督促状発送 21～：会費督促電話作業（役員） 29：支部会計報告依頼（〆切 7/13） 30：助成金配賦額決定（支部別会員数）	13：第 233 回月例研究会 中旬：春期 CSA 面接結果通知 下旬: 春期 CSA 認定証発送	認定 NPO 法人東京都認定日 （2015/6/3） 30：近畿支部 30 周年記念シンポジウム
7 月	5：支部助成金支給 12：理事会	12：第 32 回システム監査実践セミナー(日帰り 2 日間コース) 26：第 234 回月例研究会 28：事例に学ぶ課題解決セミナー 下旬：秋期 CSA・ASA 募集案内	13：支部会計報告〆切
8 月	（理事会休会） 25：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30 30、31:第 32 回システム監査実務セミナー(日帰り 4 日間コース)前半	

<目次>

2018.9

【 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。
7 月号から 9 月号までの四半期に引き続き、10 月号から 12 月号までの四半期テーマも、「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。このテーマは、システムシステム監査人の皆様にとって、関心の高い重要なテーマであろうと思いますので、システム監査基準・管理基準の改訂に対して、システム監査人としてどう対応していくのか、皆様のご意見をお待ちしています。
システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。
会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

＊2018 年度会報テーマ

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

□■ 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。

■ 会報投稿要項

分類は次の通りです。

投稿要項が 2018 年 1 月 11 日に改定されました。ご確認の上、投稿をお願いします。

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 改定） 6,000 字以上。17,000 字程度。図表を含める。 システム監査の啓発、普及、理論深化、情報提供、実践、手法開発等に役立つ論文であること。 既発表論文は除く。

■投稿について

・投稿締切：15 日（発行日：25 日）

・投稿用フォーマット　※毎月メール配信を利用してください。

・投稿先：　saajeditor@saaj.jp　宛メール添付ファイル

・投稿メールには、以下を記載してください。

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

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

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

■注意事項

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

・編集担当の判断で、字体やレイアウトなどの変更をさせて戴くことがあります。

お問い合わせ先：　saajeditor@saaj.jp

2018.9

会員限定記事

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

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

ログイン ID（8 桁）は、年会費請求書に記載しています。

＝＝

■発行：認定 NPO 法人　日本システム監査人協会　会報編集部

〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F

■ご質問は、下記のお問い合わせフォームよりお願いします。

【お問い合わせ】　https://www.saaj.or.jp/toiawase/index.html

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

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

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。

■□■ＳＡＡＪ会報担当

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

編集支援：　小野修一（会長）、各副会長、各支部長

投稿用アドレス：　saajeditor ☆ saaj.jp　（☆は投稿時には@に変換してください）

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

<目次>