認定NPO法人

日本システム監査人協会報

2016年8月号
No 185

― No.185（2016年8月号）<7月25日発行>―

会報四半期(８月～10月号)のテーマは

「システム監査への期待」です。

システム監査には、情報システムのリスクに対するコントロールを検証・評価することが期待されている。(ＳＡＡＪ小冊子より)

写真提供：仲会長

巻頭言

会員番号　1750　舘岡均（副会長）

『昨年の日本年金機構・個人情報流出の教訓』

2015年5月の日本年金機構における個人情報流出は、その甚大な被害に皆が衝撃を受け、このようなサイバー攻撃を根絶するために官民あげて原因究明、再発防止を図りました。具体的には、「日本年金機構における個人情報流出事案に関する原因究明調査結果」等の調査報告書が2015年8月に報告され、さらに「サイバーセキュリティ戦略」が9月に定められました。これらを踏まえて、各省庁、自治体、独立行政法人、特殊法人等にては、サイバー攻撃犯罪を防ぐよう、本格的に防御対策等が着手され始めた経緯がありました。

さて、約1年を過ぎて振り返ってみますと、日本年金機構の事案は、やはりサイバー攻撃対策のエポックメイキングな取組みの契機として位置づけられており、最近の各研究団体における講演、あるいは研究成果報告を拝見しますと、日本年金機構の事案を踏まえて、それぞれの研究を展開しています。

しかし最近でも、「JTBにおける個人情報の流出」等のインシデントが相変わらず発生しています。これまで示されている対策などを確実に実施していると、未然防止、あるいは早期発見により被害を最小限に出来たとも言われています。

このような状況下で、さらに2020年東京オリンピック・パラリンピックに向けて各組織にて防御策が進められていることから、システム監査人は、システム監査の一環として情報セキュリティの監査、あるいはコンサルティングにおいて、その力量の発揮が益々求められています。

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＞

2016.7

めだか　【　システム監査への期待　】

会報7月号では、IoTとは「つながる」インフラストラクチャであるということからシステム監査の多様性について考えてみた。そうしたところ、英国では、国民投票の過半数によりEUから「離脱」するよう決まったことでキャメロン首相が想定外の結果を受け辞任表明、また、スコットランドがEUに「残留」するため英国から独立する動きが始まったことや、株価の下落、ポンド安、円高などの状況が報じられている。英国では、若い層は、「残留」に、高齢層は、「離脱」に投票したという。

情報学最前線という市民講座を受講し、インターネットで目的サイトに到着するのに、到着までのサイト数は、4.74であると、解析されたと聞いて驚いた。世界は、英国のEU離脱騒ぎのように、政治、経済、宗教など、あちこちで異文化がぶつかりあって、たいそう広いと思うが、サイバー空間は、あっという間にサーバ同士がつながるスモールワールドで、悪意のある人間も多く、例えば、戦後の闇市を思わせる。コンピュータが汎用機の時代、プログラマーは、システムエンジニアの設計のとおりコーディングする職種を言っていたが、IoTの時代、プログラマーは、アルゴリズムを考案し、プログラムを自由自在に書く能力のある人を言っていて、今は、官民を挙げて優秀なプログラマーを育成しようとしている。

さて、東京国立博物館特別展「ほほえみの御仏―二つの半跏思惟像―」を見学した。奈良県の中宮寺門跡に伝わる国宝の半跏思惟像は、木造の飛鳥時代（7世紀）の仏さまで、優しく微笑むお姿は教科書で良く知られている。韓国の国宝金銅仏は、三国時代（6世紀）の仏さまで、ふっくらとした頬に、かわいい微笑を浮かべている。展示室では、二つの仏さまが相対して展示されていて、会話しているように見えた。

IoTの時代、システム監査人は、お互いに会話しながら、情報システムに関わる経営責任、戦略性、調達、有効性、準拠性、人間行動、及びサイバーセキュリティの課題を洗い出して、経営層に助言するなど、システム監査への期待にこたえていきたいと思う。

（空心菜）

参考１：「情報学最前線 平成28年度市民講座 第1回 つながりのビッグデータ解析人間関係ネットワークの科学と活用」国立情報学研究所

参考２：「日韓国交正常化50周年記念 特別展「ほほえみの御仏―二つの半跏思惟像―」」 東京国立博物館

（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>

2016.7

投稿　【　システム監査の活性化　】

会員番号　0557 仲厚吉　（会長）

サイバーセキュリティ経営ガイドライン

経済産業省と独立行政法人情報処理推進機構は、「サイバーセキュリティ経営ガイドライン」を策定し、経営者のリーダーシップの下でサイバーセキュリティ対策が推進されることを期待するとしています。

http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

当協会は、システム監査の普及、及びシステム監査人の活動促進のため、システム監査を核として、「ITアセスメント」を行っていくように取り組んでいて、当ガイドラインは、システム監査人が、経営面で「ITアセスメント」を行う際に重要なガイドラインのひとつになると考えています。概要は、次の通りです。

- 経営者が認識する必要のある「３原則」
  - ① 経営者は、IT活用を推進する中で、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、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めた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、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要
- 経営者が担当幹部に指示すべき重要10項目
  - ① サイバーセキュリティリスクの認識、組織全体での対応の策定
  - ② サイバーセキュリティリスク管理体制の構築
  - ③ サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
  - ④ サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
  - ⑤ 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
  - ⑥ 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
  - ⑦ ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
  - ⑧ 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のための環境整備
  - ⑨ 緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
  - ⑩ 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

会員の皆様には、システム監査活性化の一環として、当ガイドライン利活用へのご検討をお願いしたく思います。

以上

<目次>

2016. 7

第 214 回月例研究会：講演録

【　実践的なセキュリティと監査の役割　】

会員番号　148　木村　裕一

【講師】内閣サイバーセキュリティセンター　　基本戦略グループ（分析担当）

企画官　結城　則尚　氏

【日時・場所】2016年6月21日（火）18：30～20：30

【テーマ】「実践的なセキュリティと監査の役割」

【要旨】

セキュリティは組織全体で取り組む組織力が必要であり、組織を指揮して管理するマネジメントシステムが重要です。
その組織に最適化されたマネジメントシステムを構築・維持し、適切なセルフアセスメント、内部監査、マネジメントレビューを実施し、改善に結び付けるサイクルを継続的に行っていくことが求められています。
こうしたサイクルにおいて、客観的に組織内の課題を指摘する外部監査の活用は、とりわけ重要です。
一方、システム認証をとることに専念して、マネジメントシステムが形骸化している例も多く見受けられます。
監査は組織のパフォーマンスを向上させる重要なものと位置づけ、現場で見られる課題と方策を説明します。

【講師自己紹介】

現在内閣サイバーセキュリティセンター基本戦略グループ（分析担当企画官）、地方公務員としてスタートののち、トラブルシューティング、審査機関の認定委員、原子力関連の検査などセキュリティに関して30年の経験を重ねてきた。最初の監査は米国で経験し3年間苦労してプロセスアプローチを身に着けた。プロセスアプローチのほうが要素型より効率が良いと考える。セキュリティに問題がある職場は環境も良くないが、信頼性を高めることで良くなる。不安全な職場は何か人間環境がおかしい。健全な職場に安全が宿ると認識している。

【講演概要】

はじめに　　セキュリティ対策への取り組みについて

結城氏は、セキュリティに関する上原哲太郎氏（立命館大学教授）の次のツイッターメッセージにうなずいたことから、話を始めた。

『セキュリティって全分野ひとりで出来るスーパーマンなんていないんだからどうやったってチーム戦。いい選手集めるのは重要だけどそれ以上にいいコーチや監督がいないと勝てない。他部門には常に疎まれる立場なのでオーナーがその価値を認めて支えてあげないと簡単にチーム全体の士気が下がる。

・　想定外を想定して、アドリブをも必要とするすそ野の広い総力戦(チーム戦)

・　これまで各自が経験してきた知見を遺憾なく発揮できるようにすることが重要

・　組織内のマネジメントシステムに、適切なセキュリティが組み込まれていることが重要』

当日の要約ともいえるこの導入から始められて、次の内容で講演をされた。

（以下、当日の資料を引用して概要を記述する（木村））

１．セキュリティ監査の重要性

(1) マネジメントシステムの役割

・セキュリティは組織全体で対応する必要がある

・組織を指揮して管理するマネジメントシステムが自律的に回ることが期待される

（2）マネジメントシステムがうまく回るための仕組み

・セルフアセスメント、内部監査、マネジメントレビューは必須

反面、どの組織でも、自分自身のことを客観的に見ることはできない

・外部評価をうまく活用し、ありのままの姿を映し出してもらうことが有益

しかし、自分の弱点を知りたがらない傾向があり、監査側、被監査側で遠慮しあっている面もみられる

・付加価値のある外部監査がわが国のサイバーセキュリティ確保には不可欠

・自組織の弱さを客観的に把握できていることは、何よりの強み

・監査においては、なぜそう指摘するのか、被監査側にわからせることが必要

・特に、次の言は最もよくない。

「規格がそう言っている」という説明は逆効果

２．　セキュリティに対する素朴な疑問

(1) 情報セキュリティ、サイバーセキュリティ、セキュリティの混同？

・情報セキュリティとは？

情報の「機密性(C)」「完全性(I)」「可用性(A)」を維持すること(ISO/IEC27000 2.33)

・IAEA(国際原子力機関)のセキュリティの定義は以下の通り

予防、検知、対処／盗難、妨害、破壊行為、不正アクセス、不正移送、その他不正行為

この定義の方がわかり易いのでは？

・米国では、予防、検知、対処で語られる場合が多い

(2) セキュリティ＝機密性と受け止められている場合が多い

・完全性(Integrity),可用性(Availability)が忘れられている？

・セキュリティを高めたので、使いにくいということを聞いたことありませんか？

（これはおかしい）

・CIのバランスをどう取っていくかが重要ではありませんか？

・制御系ではCIAではなく、AICの順と聞くが、みなさんはどう思いますか？

(3) ISMSやCSMSといったMS(マネジメントシステム)の目的は？

・「セキュリティは、組織全体で対応する」もの

・ やらされ感がしばしば見える、だれのためのものなのか？（自分のものである）

・ そもそもの定義まで遡ってみているのか？

・ アリバイでやっているなら意味がないのでは？

３．マネジメントシステムの課題

(1) **組織をうまく導き、運営する**には、**体系的で透明性**のある方法によって**指揮及び管理する**ことが必要である。**すべての利害関係者のニーズに取り組む**とともに、**パフォーマンスを継続的に改善**するように**設計**された**マネジメントシステムを実行し、維持することで成功をおさめる**ことが出来る。

これらには、**組織が継続的な成功を達成するのを支援するねらいがある。**

（これは、ISO9000:2000の0.2で品質マネジメントの原則として記述されているが、読み飛ばされることが多い。しかし、重要なことでありしっかりと理解する必要がある。）

（２）年金事案におけるCSIRTの運用等の調査結果

年金事案を調査した結果、次のような状況があった。

書いてあるからやっている、書いていないからやっていない

そこには、ＭＳに必要な主体性、目的が見えない。アリバイがあっても、事案発生によって被害が出た際に役に立たないのでは？

４．年金機構情報漏えい事案報告書について

（１）昨年の日本年金機構による事案を次の報告書を作成し公表した。

「日本年金機構における個人情報流出に関する原因究明調査結果」

（平成27年8月20日　　サイバーセキュリティ戦略本部）

作成にあたって次を考慮事項とした。

策定方針（＝いわば監査方針）：「失敗から得られた教訓をもって、サイバーセキュリティ体制の改善に資する」報告書を作る

読み手：政府職員全員及び一般国民の方々とし、複雑な事案を単純化し記載する

事実関係を把握し、教訓を全省庁長に展開できるよう、教訓を一般化した（書くのは難しかった）。

この事案を、「組織事故」ととらえ組織としての問題点を提起した。

（２）内容の紹介

内容については、次のような項目による紹介があった。

・本部及びＮＩＳＣがとるべき再発防止対策

・原因究明報告書　おわりに

当報告書は、サイバーセキュリティ基本法に基づくものとして、厚労省、警察庁、防衛省の関係省庁の連携によって調査、解明がされた。その点は意味がある報告書である。

・年金事案の原因究明

原因究明のための「年金事案感染端末と不審な通信の図」を公開している。この図は、公開するかどうか、内部で議論があった。これまでこのような情報は公開されておらず、世界でもまれである。

・予防、検知、対処の観点からのアプローチ

完璧な予防は非現実的。侵入検知はできているか。対処体制はどうか。

（注）講師から、皆さんにぜひ「この報告書を読んでみてほしい」とのコメントがあった。

5．実践的セキュリティマネジメント

（1）認証制度が伴うような○○MSで一般的にみられる傾向

・ 認証を取るための手段となってしまう傾向がみられる

（2） ○○ MSに嫌悪感を感じているのでは？

・ MSは組織全体で十全なセキュリティをもたらす方法を一般化したもの

→**ABC**と理解せよ　**A：**当たり前のことを、**B：**馬鹿にせず、**C：**ちゃんとする

・ MSは的確に運用すれば、効果が期待できる

・ 反面、無理解、曲解は、悲惨な結果をもたらす

・ 効果的な活用には、座学も現場も精通が不可欠

・ 円滑な業務遂行に支障をきたしているのでれば、やり方を疑え

6．セキュリティは組織運営の一部

(1) 経営者の責任は重要だが、（経営者だけではできないことである）

係長セキュリティの反省から、「経営者の責任」の強調をよく耳にする

経営者の責任だけ明確にすればセキュリティは本当に高まるのか？

2006年改正の会社法で組織統治は一般化している

セキュリティはその一つとして組み入れてもらえばよいのではないか

(2) セキュリティは、全分野ひとりで出来ないチーム戦

・ 優秀な選手集めるのは重要

・ それ以上に優秀なコーチ、監督がいないと勝てない

・ セキュリティは、他部門には常に疎まれる立場

リーダーがその価値を認め、チームを支えないとチーム全体の士気は下がる

・ 一人ですべてできないことを知る

トップ、ミドル、ローがそれぞれ適切な役割分担がなされて全員参加

各人の役割、これまで歩んできたキャリアパスで得た経験を総動員する

・ チームワークをもって全力を尽くすのではないか？

（3）トップマネジメント自身が直接実施しなければならない事項

ISO/IEC 27001:2013　　5.1 リーダシップ及びコミットメント

これらの実施について、形式的にならないよう要求事項の趣旨を組んで自ら指揮して取り組む必要がある

（4）管理者に必要とされる管理能力

専門的能力　　対人関係能力　　概念化能力

”組織の諸階層で必要とされる管理能力”はそれぞれ異なる。たとえば、経営幹部は、さぎょうじっしそうのすべての具体的作業に通じる必要は無い

7．組織のセキュリティマネジメントのパフォーマンスアップのヒント

文書化の量は適切か？

・品質を保証するのに必要な範囲

・「文書化したものの性質」

文書化の量は適切か？業務が問題なく実施でき、作業者が代わっても業務の質を低下させない程度の内容を確保。時間の経過とともに、「文書化した内容」と「実態」にずれが生じる。

おわりに

・セキュリティは、組織全体の業務の一部であり、特殊なものではない

・すべての利害関係者のニーズに取り組むとともに、パフォーマンスを継続的に改善するように設計されたマネジメントシステムを実行し、維持することで成功を収めることができる

・自分たちのためとして、自発的な取り組みが大前提

・ＡＢＣ（Ａ：あたりまえのことを、Ｂ：ばかにせず、Ｃ：ちゃんとやる）

・セキュリティは、組織全体で取り組むべきものであり、マネジメントシステムが不可欠

・適合性に気を取られて形骸化する対策には、有効性を高めてゆくことが重要

・千里の道も一歩から、どう進めていくか、焦らず、じっくり、継続して取り組む

（講演ここまで）

【質疑応答】

今回の月例研究会は、以上の講演で前半部分を終了した。後半は、引き続いて、公開しない前提でビデオ撮影をせず、講師のフリーなお話をいただき、その後会場の参加者との質疑応答を行った。今回は、会報の記録としては、後半は省略させていただきます。

【記録者感想】

監査の役割について、日頃考えていることは、本当に被監査側にとって役に立つ有効な監査を行っているの

であろうか、ということである。これはシステム監査に限定しない、一般的な審査や、検査などにも共通する疑問と懸念であって、実態は監査人、検査者に誤解や誤りがあるように思われる。

そのことに、結城講師の幅広い経験に基づく話を聞くことができて、大変有効であった。その意味で特に、意識に残った言葉として、次がある。

・マネジメントシステムがうまく回るための仕組み
　監査においては、なぜそう指摘するのか、被監査側にわからせることが必要
　「規格がそう言っている」という説明は逆効果
・自分たちのためとして、自発的な取り組みが大前提
・「セキュリティは、組織全体で対応する」もの。組織業務の一部である。
・セキュリティは全分野ひとりで出来ないチーム戦
・マネジメントシステムの狙い
　マネジメントシステムは組織が継続的な成功を達成するのを支援することが狙い

これらのことは、頭では分かっているはずのことであるが、明確に言葉で表現して意識しないと、普段の業務においてなおざりになり行動に結びついていないことになりがちでもある。

様々な経験に基づく講師の重みのある言葉により、考え方が整理され、再確認できた、貴重な時間であった。

有難うございました。

以上

<目次>

2016.7

「新個人情報保護法]がＰＭＳに及ぼす影響　～ＰＭＳハンドブック読者！必読！～　　第４回

会員番号　2581　斉藤茂雄（個人情報保護監査研究会）

今月号では「第四章　第27条から第34条」まで解説します。そのうち第34条以外は、すでに2016年1月1日から施行されていますので、事業者は、PMSを再度確認する必要があります。

この連載の前回までの内容は、以下のサイトで閲覧できます。

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

第四章　個人情報取扱事業者の義務等　第一節　個人情報取扱事業者の義務　（続き）

第27条（保有個人データに関する事項の公表等）　　（旧二十四条）

個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

一 当該個人情報取扱事業者の氏名又は名称

二 全ての保有個人データの利用目的(第十八条第四項第一号から第三号までに該当する場合を除く。)

三 次項の規定による求め又は次条第一項、**第29条**第一項若しくは**第30条**第一項若しくは第三項の規定による請求に応じる手続（**第33条**第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四 前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

（以下省略）

現在公表されている法律は、旧番号のままであるため、条文中の条項番号を、新法に従い変更し、アラビア数字で記述しました。　例：第二十六条（旧法）　→第29条（新法）

第一項三の改正部分は第28条以下の条項追加による参照条項番号の変更であり、旧法と内容的には変わりません。

第28条（開示）　　（旧二十五条）

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの開示を請求することができる。

2　個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

三　他の法令に違反することとなる場合

3　個人情報取扱事業者は、第一項の規定による請求に係る保有個人データの全部又は一部について開示しない旨の決定をしたとき又は当該保有個人データが存在しないときは、本人に対し、遅滞なく、その旨を通知しなければならない。

4　（以下略）

※　今回の改正では「本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人デー

タの開示を請求することができる。」と、本人の権利が明示的に示されました。旧法では、“個人情報取扱事業者は、（中略）、当該保有個人データを開示しなければならない。”　と事業者の義務として記述されていたことから180度の転換です。

※　今回の個人情報保護法改正の背景に、「新EUデータ保護指令」の採択への対応があると言われています。旧個人情報保護法は「新EUデータ保護指令」よりもいくつかの点で規定が緩やかであるとの指摘があり、その一つに「開示・訂正・消去請求権が本人の権利として明示的には認められていない。」という点がありました。今回の改正において、ようやく本人が開示等の請求を行う権利を有することが明確化されたものです。

※　「新EUデータ保護指令」は、2016年4月14日、欧州議会本会議において「EU一般データ保護規則（General Data Protection Regulation、以下GDPR）として正式に可決されました。施行は2018年が予定されており、それまでの2年間に、規則内容の具体化や各国政府・企業の対応作業が進められていくことになります。

第29条（訂正等）　　**（旧二十六条）**

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの内容が事実でないときは、当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を請求することができる。

2　（以下略）

第29条についても、本人は、で始まる文に改定され、（事業者は）開示しなければならない。から、（本人は）請求することができる。となりました。

第30条（利用停止等）　　**（旧二十七条）**

本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの内容が事実でないときは、当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を請求することができる。

2　個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

3　本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第23条第一項又は第24条の規定に違反して第三者に提供されているときは、当該保有個人データの第三者への提供の停止を請求することができる。

4　（以下略）

第30条についても、本人は、で始まる文に改定されました。なお、JIS規格では、事業者は、で始まってはいますが、個人情報に関する本人の権利（3.4.4.1）としています。

※　この後、第31条（理由の説明）、第32条（開示等の請求等に応じる手続）、第33条（手

数料）と続き、条文中の用語として、開示等の求め　→　開示等の請求　と改められています。JIS規格3.4.4.2の、”開示等の求め”　の用語も今後検討されると思われます。

第34条（事前の請求）　　　　　　（新設）

本人は、第28条第一項、第29条第一項又は第30条第一項若しくは第三項の規定による**請求に係る訴え**を提起しようとするときは、その訴えの被告となるべき者に対し、あらかじめ、当該請求を行い、かつ、その到達した日から二週間を経過した後でなければ、その訴えを提起することができない。ただし、当該訴えの被告となるべき者がその請求を拒んだときは、この限りでない。

2　前項の請求は、その請求が通常到達すべきであった時に、到達したものとみなす。

3　前二項の規定は、第28条条第一項、第29条第一項又は第30条第一項若しくは第三項の規定による請求に係る仮処分命令の申立てについて準用する。

※　第34条は未施行です。

※　“請求に係る訴えを提起”　とは、裁判による開示・訂正等の訴えが可能だということです。しかし、むやみやたらな訴訟や十分な理由もない訴えが多発することを避けるために、事前の請求を行うこと、請求した後2週間を経過していること、または事業者から請求を拒まれたときでなければ、提訴できないとしています。

※　上記の詳細な手続きは、現時点で明確になっていません。認定個人情報保護団体および個人情報保護委員会では、苦情の受付や、苦情の申し出について必要なあっせんを行いますが、”苦情”と、裁判所への“訴え”とは異なりますので、今後“訴え”の取り扱いについて、規則や条例等で明確にされると思われます。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

次回は、「第四章第二節　匿名加工情報取扱事業者等の義務(第36条～第39条)」から解説します。

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

「ＰＭＳハンドブック」の読者専用ダウンロードサイトでは、

新個人情報保護法、番号利用法の改正を反映した規程・様式集を公開しています。　！！

6月1日の改定では、「3725a 適合性監査チェック リスト」（JIS規格適合性）に、個人番号関係事務関連の監査項目を追加しています。

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

認定NPO法人日本システム監査人協会　個人情報保護監査研究会　■

<目次>

2016.7

第 29 回ＣＳＡフォーラム開催

【ＩｏＴ時代のサイバーセキュリティ対策～サイバー攻撃から工場・プラントを守るには～】

会員番号　2581 斉藤 茂雄（CSA 利用推進 G）

今回は、ジェイティ エンジニアリング株式会社 シニアコンサルタントの福田敏博様を講師にお迎えしました。福田様は多くの「制御システム」「生産管理システム」の構築を手がけて来られ、昨年『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』（秀和システム）を上梓されました。

情報セキュリティというと個人情報漏えいやオフィスやデータセンタのセキュリティ対策が思い浮かぶのですが、今やサイバー攻撃の激化などにより、工場やプラントといった社会の重要インフラのセキュリティ対策が、重要な課題になっています。

今回のお話では、工場・プラントにおける情報システムの状況、セキュリティ対策の現状などの基本的な知識を得ることが出来ました。また生産現場の情報セキュリティ意識はまだまだ低いといった生々しいお話もあり、CSAとしてさらに理解を深め、セキュリティ対策に寄与する活動が必要だと思いました。

開催の概要は以下です。終了後講師を囲んで短時間ですが懇親会を実施しました。

タイトル：「ＩｏＴ時代のサイバーセキュリティ対策～サイバー攻撃から工場・プラントを守るには～」

概要；（当日使用スライドのコンテンツより抜粋）：

① **はじめに**

② **ビジネス環境の変化**

経済成長長期低迷/需要が増えないことから市場ニーズ、価値観の変化/必需→贅沢→社会貢献へ

③ **セキュリティ環境の変化**

制御システムのセキュリティの要素は「可用性（A)」→「完全性（I)」→「機密性（C)」の順/
これに「健康（Health)」「安全（Safety)」「環境（Environment)」要素が加わる

④ **今なぜ制御システムセキュリティ？**

「サイバーセキュリティ基本法」の成立、第 14 条：重要インフラ事業者におけるサイバーセキュリティ確保の促進/サイバーセキュリティは経営問題

⑤ **Industrie4.0 や IoT で今後どう変わる？**

取り巻く技術の変遷→クラウド、ビッグデータ・AI、IoT、製造業のサービス化/
制御システムオープン化→工場そのもののオープン化⇒「よりつながる工場へ」

⑥ **セキュリティ対策（CSMS）の重要性**

⑦ **CSMS（Cyber Security Managiment System）認証の概要**

認証基準：国際標準 IEC62443-2-1:2010 がベースで一部追加変更/JIPDEC が認証機関

開催日時： 2016 年 7 月 4 日（月） 18 時 30 分～20 時 30 分

開催場所： 中央区日本橋兜町 12-7 兜町第 3 ビル　NATULUCK 茅場町新館 3 階大会議室

■■■■■■■■■■――――――――■■■■■■■■■■

ＣＳＡフォーラムはＣＳＡ・ＡＳＡの皆様が、「システム監査に関する実務や事例研究、理論研究等」を通して、システム監査業務に役に立つ研究を行う場です。ＣＳＡ・ＡＳＡ同士のフェイスｔｏフェイスの交流を図ることにより、相互啓発や情報交換を行い、ＣＳＡ・ＡＳＡのスキルを高め、よってＣＳＡ・ＡＳＡのステータス向上を図ります。ご参加のお問い合わせはＣＳＡフォーラム事務局：csa@saaj.jp まで（@は小文字変換要）

■■■■■■■■■■――――――――■■■■■■■■■■

ＣＳＡ利用推進Ｇのキャッチフレーズ

＊＊ＣＳＡ・ＡＳＡを取得してさらに良かったと思ってもらえる資格にしましょう！！

<目次>

2016.7

支部報告【北信越支部 2016 年度 福井県例会・研究報告】

会員番号　1281 宮本　茂明（北信越支部）

以下のとおり2016年度 北信越支部 福井県例会を開催しました.

・日時：2016年6月11日（土） 13:00-17:00　　参加者：８名

・会場：福井市総合ボランティアセンター　研修室Ａ

・議題：１.研究報告

「システム監査におけるリスクベース監査の実践」

小嶋　潔　様

２．西日本支部合同研究会 北信越支部報告検討

・北信越支部報告テーマ：システム開発/構築に関わるシステム監査

◇研究報告

「システム監査におけるリスクベース監査の実践」

～　システムリスク評価とシステム監査の対象システム選定について　～

報告者 (会員番号　1739　小嶋　潔)

１．はじめに

私が勤務している銀行の監査部門において、昨年監査法人に依頼して内部監査の品質評価を行いました。その際に、システム監査の対象システムの選定方法に関して「システム単位でのリスク評価が為されていない」との指摘がありました。システム単位でのリスクアセスメントを実施し、リスクが高いと判断した重要なシステムについては、部署別監査の一部としてではなく、当該システムを対象として別途監査を行うべきであるというものです。実際には、監査担当者の経験に基づきリスク評価を行い、監査対象を決定しているのですが、明文化した選定方式に関する規程や、選定結果に至った経緯を記録していなかったことについて改善すべきであるとされました。

そこで本日は、今期から当行において実践しようということとなった、システム単位でのリスクアセスメントの内容と、システム監査対象の選定に関する考え方と方式についてご紹介すると共に、未だ最終的な結論に達していない部分について、出席の皆様からヒントを得ることができればと考えています。

２．内部監査の品質評価について

米国内部監査人協会の「内部監査の専門的実施の国際基準および倫理綱要」では、５年に１度の外部評価が要求されており、日本内部監査協会でも少なくとも５年毎に実施することを求めています。金融庁のアンケートでも、外部評価を実施している地方銀行が増加してきているという結果が出ており、当局も注目していることが窺われます。

当行でも、かねがね内部監査の高度化を標榜していることから、外部専門家の評価やアドバイスを通じて内部監査を充実・高度化することを目的に、監査法人による品質評価を受けることになりました。

３．当行における従来の監査対象の選定

近年の当行のシステム監査は、部署別業務監査における監査項目の一つとしてシステム監査を行ってきました。もちろん大規模案件については、プロジェクト監査として通常の監査とは別にシステム監査を実施していますし、重要なシステムの外部委託先である、勘定系の共同センターや多数のサブシステムを稼働しているデータセンターについても個別の監査を行ってきました。しかしながらそれ以外は、例えばシステム部門の業務監査の際に、ついでにシステム監査を実施するという方式でやってきました。内容的には、J－SOXのＩＴ全社・全般統制の評価項目や、ＦＩＳＣ（金融情報システムセンター）のシステム監査項目にしたがって監査を実施しています。

当行では細かいものも含めると１００を超えるサブシステムが稼働していますが、それぞれのシステムとその重要度に着目した切り口では監査を行っていませんでした。情報セキュリティ、開発、運用･･･といった監査項目を個別のサブシステムに当てはめて監査するという発想はなく、各担当部署毎に監査項目について対応状況を検証するという考え方が中心でした。

４．システム監査におけるリスクアセスメントの考え方

１００を超えるサブシステムをシステム単位にリスク評価することで、監査対象を絞り込み、限りある監査資源を重点的に配分することで効率的な監査を実施しようというのが、現状当行で考えているリスクベース監査の実践方法です。

（１）リスクアセスメントの手法

ゼロからスタートして１００を超えるサブシステムのリスク評価をしようとしても監査部署では実施困難だし時間もかかるということで、システムリスク管理の所管部署であるシステム部門において行っている各サブシステムのリスク評価結果を活用することにしました。

（２）システム部門の実施するリスク評価

システム部門では、セキュリティチェックシートを使用して、毎年１回サブシステムのリスク評価を行っています。これは、「システムリスクの状況等のモニタリング」及び「システムリスクの認識・評価」を実施し、「システムリスクの削減（システムの安全性・安定稼働の確保）」につなげることを目的としています。このシステムリスクのモニタリングとリスクの認識・評価には、当局の「中小・地域金融機関向けの総合的な監督指針」や「金融検査マニュアル」、ＦＩＳＣの「安全対策基準」等の銀行にとってのスタンダードにおける変更点や改定内容を参考にして作成したチェックシートを用いています。

５．システム監査におけるリスクアセスメントの具体的な実施方法

（１）サブシステムのセキュリティチェック結果の確認

検証対象システムの網羅性を確認します。監査対象の絞り込みが目的ですので、当行のサブシステム一覧と対比して、網羅的にセキュリティチェックを行っているかを確認し、さらにチェックシートの内容の妥当性（改定状況の確認も含めて）を確認します。

（２）セキュリティチェック結果の評価

セキュリティチェックの結果として重要度が高いと評価されたサブシステムと、これにシステム改造や案件の発生を要因として年度中のリスクの変化が想定されるシステムを加えて、システム監査選定対

象のサブシステムの母集団とすることを予定しています。

（3）対象サブシステムの選定

上記（2）の対象サブシステムの母集団を選定した後、ここから先の具体的なサブシステムの選定に関しては、未だ決定していません。しかしながら、「結局、鉛筆舐め舐めの世界になった」ということにならないよう、例えば重要度の高いシステムに、開発案件数やシステム障害発生数を加味して、上位からいくつかを選定することを考えています。この選定過程を明確化して記録し、監査グループ内で協議し承認を受けて選定することになります。

6．システム別の監査の留意点について

ところで、監査の対象システムを選定して、限定したシステムに対して監査を行うということには、いくつかの問題点があると思われます。

すなわち、システム別に管理されていないような書類を閲覧するような場合は、対象システムを限定するのは逆に非効率ですし、内部統制的にはシステムを限定して監査することに意味がない監査項目もたくさんあると思われます。監査資源の有効活用を図るために行う対象システムの選定が、必ずしも効率的に監査を行うことに結び付かないということになってしまっては、本末転倒です。

したがって、システム別に監査する項目と、被監査部署の態勢的な問題に着目して監査する項目を分け、システム別の個別監査と部署別業務監査実施時に同時に行う態勢的システム監査の２種類のシステム監査を行う必要があります。しかしながら、この２タイプのシステム監査を行う余裕があるかも問題となるでしょう。通常の企業では内部監査においてシステム監査を行うこと自体に制約があることも多いでしょうし、当行でもシステム監査の要員は、他の本部等の内部監査や Ｊ－ SOX の評価作業との兼務で２名が精一杯といった状況です。（実質的にシステム監査に費やすマンパワーは、さらに限られます。）

このような現状のなかで、新たにシステム別の監査に取り組んでいくことには多少の無理はあるかもしれませんが、リスクベース監査という目標に対して少しでも近付いていけたらと考え、これから実行していこうと思っています。

また機会があれば、この取組の結果についてもご紹介できればと思っています。

以 上

<目次>

2016.7

注目情報（2016.6～2016.7）

■Microsoft 製品の脆弱性対策について(2016年7月)【IPA】

2016 年 7 月 13 日（日本時間）に Microsoft 製品に関する脆弱性の修正プログラムが 11 件公表されています。これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンを制御され、様々な被害が発生する可能性があります。

攻撃が行われた場合の影響が大きいため、できるだけ早急に修正プログラムを適用して下さい。

＜脆弱性の解消 - 修正プログラムの適用＞

Microsoft 社から提供されている修正プログラムを適用して下さい。Windows Update の利用方法については以下のサイトを参照してください。

Windows 10 の Windows Update については以下のサイトを参照してください。

Windows 10、Microsoft Edge、初めての月例セキュリティ リリース - 読み解き

https://blogs.technet.microsoft.com/jpsecurity/2015/08/11/windows-10microsoft-edge-3529/

Windows 10 以外の Windows Update の利用方法については以下のサイトを参照してください。

Windows 10 以外の Windows Update 利用の手順

https://www.microsoft.com/ja-jp/safety/pc-security/j_musteps.aspx

■攻撃の早期検知と的確な初動による深刻な被害からの回避を最終更新日：2016年6月23日

【注意喚起】IPA

～標的型攻撃メールに対しては リテラシの向上・適切な運用管理・セキュアなシステムの構築 の三位一体での対策を～

対象 ： 企業・組織の経営者、システム管理者、従業員（システムユーザー）

概要 ： 標的型攻撃メールに起因にした個人情報流出の事案が後を絶ちません。最近の事案(*1)では、主に以下のような要因があると考えられます。

要因 ： これらの要因は、昨年発生した大規模情報流出の事案と類似しています(*2)。企業・組織は以下のポイントを踏まえ、改めて標的型攻撃メール対策の確認・見直しを行ってください。

<目次>

2016.7

【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216回	日時：2016年 9月7日（水曜日）18:30～20:30 場所：機械振興会館 地下2階ホール	
	テーマ	「日本のサイバーセキュリティ最前線」（仮題）
	講師	サイバーセキュリティ研究所 専務理事　名和 利男 様日本大学 商学部教授　堀江正之 先生
	講演骨子	近日公表予定

■SAAJ「関東地区会員向け SAAJ 活動説明会」(仮称)　NEW！

半日	日時：2016年 10月 22日（土曜日）14.:30から17:30(予定) 場所：NATULUCK茅場町 新館　3階大会議室
	SAAJの研究会及び部会からの活動状況説明　説明会終了後懇親会を予定（詳細は、別途公開）

<目次>

2016.7

【 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。

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

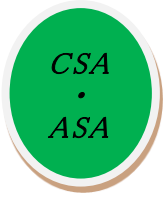
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・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。

・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。

・「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

・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。



・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

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

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

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2016.7
2016	**理事会・事務局・会計**	**認定委員会・部会・研究会**	**支部・特別催事**
7 月	5：支部助成金支給 14：理事会	1：秋期 CSA・ASA 募集案内 〔申請期間 8/1～9/30〕 20：認定委員会：CSA 認定証発送 26：第 215 回月例研究会	14：支部会計報告〆切
8 月	（理事会休会） 27：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
9 月	8：理事会	7：第 216 回月例研究会	
10 月	13：理事会		16：秋期情報処理技術者試験
11 月	10：　理事会 13：　予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/6〆切） 18：　2017 年度年会費請求書発送準備 25：　会費未納者除名予告通知発送 30：　本部・支部予算提出期限	中旬：秋期 CSA 面接 20：　CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 30：　CSA 面接結果通知	 5-6：西日本支部合同研究会 （開催場所：松江）
12 月	1：　2017 年度年会費請求書発送 2017 年度予算案策定開始 8：　理事会：2017 年度予算案 会費未納者除名承認 第 16 期総会審議事項確認 12：　総会資料提出依頼（1/9〆切） 15：　総会開催予告掲示 19：　2016 年度経費提出期限	9：　CSA/ASA 更新手続案内メール 16：秋期 CSA 認定証発送	
2015	**過去に実施した行事一覧**		
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 20：　2015 年度決算案 23：　2015 年度会計監査 28：　総会申込受付開始（資料公表） 31：　償却資産税・消費税	1-31：CSA・ASA 更新申請受付 20：　春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 21：　第 210 回月例研究会	 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 25：法務局：資産登記、活動報告提出 理事変更登記 29：年会費納入期限	1～3/31：CSA・ASA 春期募集	 22：第 15 期通常総会 特別講演 個人情報保護委員会 委員長　堀部　政男　氏
3 月	1：NPO 事業報告書、役員変更届東京都へ提出 7：年会費未納者宛督促メール発信 10：理事会	2：第 211 回月例研究会 5-6：第 27 回システム監査 実務セミナー(前半) 上旬：CSA・ASA 更新認定書発送 19-20：第 27 回システム監査 実務セミナー(後半)	
4 月	14：理事会 30：法人住民税減免申請	初旬：新規 CSA・ASA 書類審査 中旬：新規ＡＳＡ認定証発行 25：第 212 回月例研究会	 17：春期情報技術者試験
5 月	12：理事会 26：年会費未納者宛督促メール発信	中旬：新規 CSA 面接 26：第 213 回月例研究会 26～27：第 28 回システム監査 実務セミナー（2 日間コース）	
6 月	9：理事会 14：会費未納者督促状発送 15～：会費督促電話作業（役員） 30：支部会計報告依頼（〆切 7/14） 30：助成金配賦額決定（支部別会員数）	 10：　CSA 面接結果通知 21：第 214 回月例研究会	 2015/6/3：認定 NPO 法人 東京都認定日

<目次>

2016.6

【 会報編集部からのお知らせ 】

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

□■ 1． 会報テーマについて

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

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

システム監査人にとって、報告や発表の機会は多く、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。

□■ 2． 会報の記事に直接コメントを投稿できます。

会報の記事は、

1．PDF ファイルを、URL（ http://www.skansanin.com/saaj/ ）へアクセスして、画面で見る
2．PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
3．会報 URL（ http://www.skansanin.com/saaj/ ）の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気に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」をご確認ください。

□■ **会報投稿要項　（2015.3.12 理事会承認）**

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

会報記事への投稿の締切日は、毎月 15 日です。

バックナンバーは、会報サイトからダウンロードできます（電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にしてください）。

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

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

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

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

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

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

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

■会員以外の方は、購読申請・解除フォームに申請することで送付停止できます。
【会員以外の方の送付停止】　http://www.skansanin.com/saaj/register/

■□■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
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>