



認定 NPO 法

日本システム監査人協会報

2018年2月号

No.203

No.203 (2018年2月号) <1月25日発行>

2018年の会報年間テーマは、
「システム監査人の新たな活躍」に
決定しました。



2月は総会がありますのでご出席ください。

写真提供：仲会長

巻頭言

「～新年度のスタートについて～」

会員番号：0281 カ利則（副会長）

当協会にとっては1月から新年度が始まり総会が2月23日（金）に開催されます。昨年度の振り返りと新年度のスタートを踏まえて、次の2点について述べたいと思います。

（1）システム監査基準／管理基準の改定作業が進んでいます。

13年振りにシステム監査基準／管理基準の改定作業が進んでいます。両基準とも会員の皆様にとっては大いに関連する事項と思います。一昨年から準備の会合がスタートして昨年、正式に経済産業省の委員会が編成され、両基準の改定作業が進んでいます。この作業にはSAAJでは主にITアセスメント研究会のメンバーが関わっています。SAAJ以外にも関連団体や大学の先生方が関わっています。13年間更新されていなかったのだからかなりの見直しも必要でしたが、この1年でできることに多少絞って検討を進めています。まもなくパブリックコメントの案内が出ると思いますのでもうしばらくお待ちください。

（2）ISO/IEC38500シリーズ&ISO/IEC38503の取組みも進んでいます。

ISO/IEC38500シリーズは、ISO/IEC JTC1/SC40/WG1というワーキンググループにおいて数年前からIT Governanceの国際標準化に取り組んできました。昨年6月のSAAJ特別月例会でもご紹介しましたが、ITガバナンスについて各国での標準化の関心が高く、38500（第2版）、38501、38502、38504、38505が規格化されています。昨年はその国際会議が日本の岡山で開かれ、SAAJからも数名のメンバーが参加しています。また特に38503（Assessment of Governance of IT）については以前にもご紹介していますが、日本からの発案でSAAJのITアセスメント研究会のメンバーが案作りに大いに関わっています。38503案については各国との議論もだいぶ進んできており、今年中にはほぼ形は見えてくると思います。ぜひ関心を持って頂ければと思います。

両テーマについて詳しいことはITアセスメント研究会にお尋ねください。

以上

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

○ 巻頭言	1
【新年度のスタートについて】	
1. めだか	3
【システム監査人に求められる能力】	
2. 投稿	4
【システム監査人の新たな活躍】	
【ICT部門におけるBCPへの取り組みと課題】	
【エッセイ】陰陽師	
3. 支部報告	15
【近畿支部 第170回定例研究会】	
4. 注目情報	17
【情報セキュリティ対策支援サイトの公開（IPA）】	
【平成30年度春期情報処理技術者試験・情報処理安全確保支援士試験受験申込み開始（IPA）】	
【第四次産業革命スキル習得講座認定制度（経済産業省）】	
【IoT国際競争力指標(2016年実績)の公表（総務省）】	
【プライバシーマーク新審査基準を公表（JIPDEC）】	
5. 協会からのお知らせ	18
【第17期通常総会の開催（予告）】	
【協会行事一覧】	
【会報掲載「論文」募集要項の改定について】	
【新たに会員になられた方へ】	
6. 会報編集部からのお知らせ	23
【会報編集部からのお知らせ】	
【会員限定記事】	

めだか 【 システム監査人に求められる能力 】

システム監査人に求められる能力は、情報システムへの知見、監査技法の習熟、そして、コミュニケーション能力である。当協会は、「システム監査人倫理規定」を設けており、倫理規定の項目に、「使命」、「責務」、「監査基準・手続き」、「監査報告」、「守秘義務」、「独立性」、「公正不偏」、「社会的信頼の保持」、「名誉と信義」、「システム監査人間の規律」、「自己研鑽」などを定めている。倫理規定は、システム監査人が順守すべきことであり、言い換えれば、システム監査人が身につけるべき能力ともいえる。

情報システムへの知見であるが、2018年の旬な話題と言え、インタラクティブな人工知能と並んで、ビットコインとブロックチェーンの利用の本格化がある。「池上彰のこれが「世界のルール」だ！」では、“ビットコインとは何か—無政府主義のおカネの危険と魅力”と書かれている。ビットコインは、2008年ごろに「サトシ・ナカモト」という日本人のような名前の人物がネットで公表した理論がもとになっている。ビットコインの発行は上限が定められており、使いたい人はビットコイン取引所で現金とコインを交換し、ビットコインを欲しがると多くいたら値上がりする。これまでの通貨は、発行した中央銀行が存在するが、そんなものは存在しない。信用の後ろ盾になる政府もないという仮想通貨であり、投機の対象にもなっているということである。

「入門 ビットコインとブロックチェーン」には、ビットコインとともにブロックチェーンとは何かの解説がわかりやすく書かれている。“ブロックチェーンの利用が本格化するの、いつ頃ですか？”という質問への回答が気になるが、著者は次のように回答している。

“ブロックチェーンの登場は、「メインフレームコンピュータ（大型コンピュータ）からPCへの変革」「電話からインターネットへの変革」に続く「ITにおける第3の革命」と考えることができます。・・・インターネットの普及を振り返ると、多くの人々が一般的に使うようになるまでに、導入から10年以上の時間がかかりました。そうなった大きな理由は、電話回線からインターネット回線へと通信回線を変える必要があったことです。しかし、現在はすでに、通信インフラは整っています。したがって、ブロックチェーンは、インターネットの普及よりもっと短い時間で実用化される可能性があります。”

経済産業省「ブロックチェーン技術を利用したサービスに関する国内外動向調査」は、基本的な解説が参考になるので参照しておきたい。

<http://www.meti.go.jp/press/2016/04/20160428003/20160428003.html>

参考：「池上彰のこれが「世界のルール」だ！」池上彰著 文春文庫

「入門 ビットコインとブロックチェーン」野口悠紀雄著 PHP ビジネス新書



(空心菜)

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

<目次>

投稿 【 システム監査人の新たな活躍 】

会員番号 0557 仲厚吉（会長）

第 17 期通常総会は、2 月 23 日（金）に開催されますので会員の皆様のご出席をお願い申し上げます。2018 年度の本部計画（案）は、システム監査人の新たな活躍を目指して、次のように致します。

1.本部・計画**1. 1. 全般概要・計画**

2018 年度は、協会創立から 30 周年を経て、30 年間の実績を踏まえながら、新たな歴史を作っていく端緒の年にしたい。

（1）活動方針

2018 年度協会事業の活動方針は次の 3 点とする。また、年間を通して 30 周年記念行事を計画・実施する。

1) システム監査人の社会的評価の向上

「認定 NPO 法人」の認定する資格として「公認システム監査人」への評価を向上させる。

2) システム監査の活性化

○社会の多様な要請に対応し、信頼性・安全性が高くかつ有効な IT 活用を実現することを目標として、IT サービスの提供者と利用者双方における適切な統制を維持・向上させる活動を、既存のシステム監査を核にした「IT アセスメント」としてとらえる。そのうえで、SAAJ の活動を「IT アセスメント」の定着に焦点を当てて取り組む。

○これにより、会員を含むシステム監査人のビジネス機会の増大を図り、SAAJ の知名度向上、会員の拡大に繋げる。

3) 協会組織の充実

協会組織体制を充実整備し、新メンバーの登用などにより活性化に取り組む。

（2）活動計画

システム監査の活性化の一環として、次の活動を行う。

- 1) 「Assessment of the governance of IT」の ISO 化を推進する。
- 2) 「システム監査基準・システム管理基準」改訂版の啓発活動を行う。
- 3) システム監査に関連する他団体との交流を進める。
- 4) コミュニケーション向上のため、ホームページ、会報を充実する。

（3）2018 年度の予算編成

予算編成は協会事業の方向性に沿って予算を編成する。

1) 編成方針

予算編成方針は、収益性ととも活動性を重要とする。

2) 事業活動

事業活動は、収支バランスを原則とする。収支は公認システム監査人等認定事業収支が隔年上下変動することを考え 2 年タームで取り組む。

3) 事務局

事務局業務の効率化を図り、会員サービスの向上に取り組むとともに、会計と協力し、協会の健全運営に努める。

<目次>

投稿 【 「ICT部門におけるBCPへの取り組みと課題」 】

(SAAJ 近畿支部 BCP 研究プロジェクト)

荒町弘、伊藤聖子、尾浦俊行
尾崎正彦、金子力造、松井秀雄**はじめに**

1995年の阪神淡路大震災では、震災にあった企業の殆どが業務停止の状態に陥り企業の信用に大打撃を与え、この教訓をもとにBCPに関心がもたれた。

さらに、新潟県中越沖地震におけるリケン・ショックや東日本大震災における計画停電では、被災地以外の企業もが業務停止を余儀なくさせられる事態を全国の企業が目の当たりにし、さらにBCPへの関心が深まった。

当BCP研究プロジェクトは、東日本大震災の前年である2010年よりBCPの中でも特にITを重点におき、研究活動を行ってきた。2011年には、事業者向けの取り組みとして、某社IT部門に対するBCP策定を支援した。2013年からは、IT部門の初動対応について検討を行い、その成果を基にIT部門向け初動対応演習カリキュラムを構築し演習を実施した。2016年には某自治体のICT部門職員向けに同演習を実施した。

これらの活動にあたって参照したのが、各機関から公表されているガイドラインである。

本稿では、これらのBCP作成ガイドラインを踏まえ、民間企業、医療機関や自治体における取り組み事例を紹介しながら、実効性あるIT-BCPの普及に向けた考察を行う。

なお、各ガイドラインは、対象とする組織や目的により表現が異なっている。例えば、BCPは一般には「事業継続計画」と訳されるが、総務省から各自治体向けに公表されるガイドラインでは「業務継続計画」となり、情報処理技術(IT)は通信技術を含むことを強調してICT(Information Communication Technology)と呼ばれることが多い。

以下では、都度、紹介するガイドラインに合わせた表記を使用する。

第1章 既存のBCPガイドライン

BCPガイドラインとして以下のものが公開されている。

1. IT部門向けBCPに特化されたもの

(1)「地方公共団体におけるICT部門の業務継続計画(BCP)策定に関するガイドライン」 総務省 (平成20年8月)

地方公共団体において、ICT部門の業務継続が自治体自身の業務継続において重要であることから、地方公共団体のICT-BCP策定の助けとなる資料として総務省から提供された。

(2)「ICT部門の業務継続計画<初動版サンプル>」 総務省 (平成25年5月)

事業継続計画の局面の中で、初動が重要であるとの認識にたち、「初動版」が公開されたが、その内容には東日本大震災の教訓が盛り込まれた。

被災直後の情報収集連絡体制の確立と災害対策本部の立ち上げ当初から72時間の救急・救命、避難対策、生活支援が重視されており、この時間帯における業務継続計画は特に求められるといえる。

(3) 「IT サービス継続ガイドライン改定版」 経済産業省 (平成 24 年 12 月)
業種を特定せず、IT サービスに関して、災害時などに事業継続するための方法を提示したものの。

(4) 「IT サービス継続ガイドライン 改定版」 情報サービス産業協会 (2014 年 9 月)
経済産業省「事業継続計画 (BCP) 策定ガイドライン」及び内閣府の「事業継続ガイドライン (第 2 版)」の IT にかかる部分について、組織における実施策等を具体化したものである。本ガイドラインはその性格上、「事業継続計画 (BCP) 策定ガイドライン」と一対をなすものである。

2. 全社 B C P もしくは事業別 B C P 向け

(1) 「市町村のための業務継続計画作成ガイド」 内閣府 (平成 27 年 5 月)
地方自治体において BCP は法定計画ではないため自治体ごとに記載内容が異なる事を踏まえ、「特に重要な 6 要素」として以下の項目を掲げている。

- ① 首長不在時の明確な代替準備及び職員の参集体制
- ② 本庁舎が使用できなくなった場合の代替庁舎の特定
- ③ 電気・水・食料等の確保
- ④ 災害時にもつながりやすい多様な通信手段の確保
- ⑤ 重要な行政データのバックアップ
- ⑥ 非常時優先業務の整理

(2) 「中小企業 BCP 策定運用指針」 中小企業庁 (平成 20 年 4 月)
この指針は、中小企業への BCP(緊急時企業存続計画または事業継続計画)の普及を促進することを目的として、中小企業関係者や有識者の意見を踏まえ、中小企業庁が作成したものである。

(3) 「BCP の考え方 に基づいた病院災害対応計画 作成の手引き」 厚労省 (平成 25 年 9 月)
従来の病院の災害マニュアルは、主として「災害急性期における医療活動マニュアル」であったが、阪神淡路大震災以降の大規模災害発生時には「想定外のインフラ破壊」により計画どおりの活動が行えなかった。この教訓を踏まえ、上記「手引き」では、ライフラインに係る設備の事前点検などを通じて自らの施設の脆弱な点を洗い出し、それらを補うための補強・備蓄やマスコミ対応計画をも含めた準備を行うよう求めている。

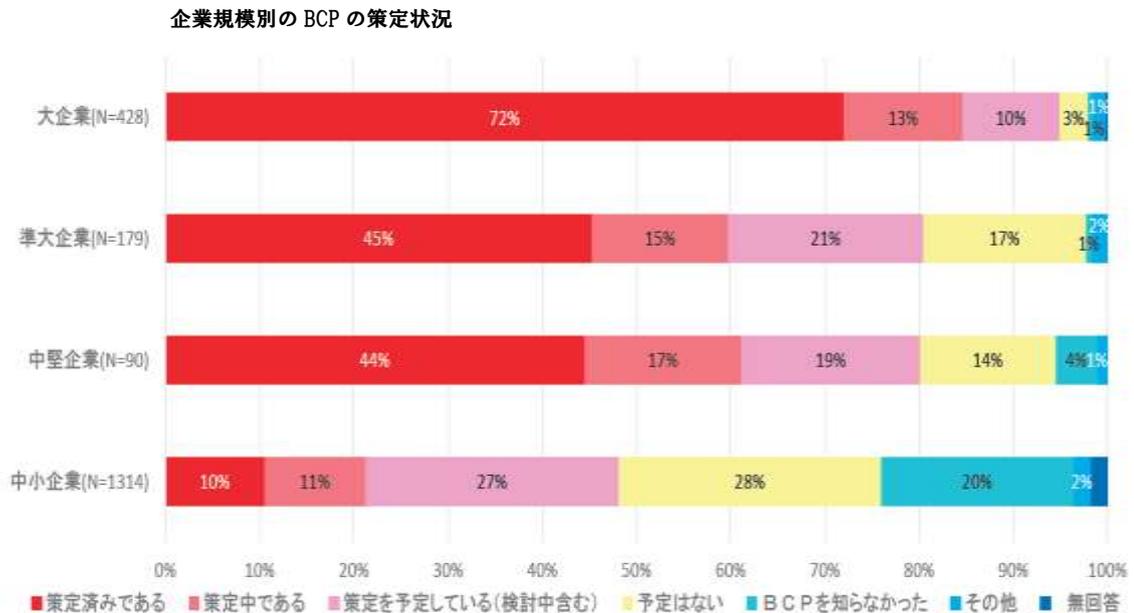
第 2 章. 全国の B C P 取り組み状況

(1) 自治体における取り組み状況

「地方公共団体における業務継続計画策定状況の調査結果」(平成 28 年 10 月 28 日 消防庁)によると、災害を対象とした業務継続計画の策定状況は
都道府県 100% [47 団体 (平成 27 年 12 月比 +5 団体)],
市区町村 41.9% [730 団体 (平成 27 年 12 月比 +95 団体)]
市区町村の策定状況は増加傾向にあるものの、未だ半分に満たない状況である。

(2) 民間企業における取り組み状況

平成 29 年防災白書では大企業については 72%、中堅企業で 44%、中小企業に至っては、わずか 10%である。



出典：「企業の事業継続に関する熊本地震の影響調査（平成29年6月）」より内閣府作成

(2) 医療機関における取り組み状況

平成 28 年の熊本地震をきっかけに、平成 29 年 3 月 31 日厚生労働省医政局長発信には、災害拠点病院の指定要件に「事業継続計画の整備を行っていること」さらには、この事業継続計画に基づき「被災した状況を想定した研修、訓練」を実施することなどが追加された。この要件は平成 31 年 3 月までに整備しなければ災害拠点病院の「指定」を解除されることとなっている。

これらの状況を踏まえ、実効性ある事業継続に向けた取組を行っている医療機関の事例を紹介する。

第3章. IT部門のBCP策定における課題

当ワーキンググループでは、入手できた複数の自治体の「ICT部門におけるBCP」について検討を行ってきた。その中で、比較的人口規模が近い、北海道K町（人口は約2万人）と新潟県M市（人口は約4万人）のICT-BCPについて、第1章1項（3）で紹介した重要6要素を中心とした比較を示す。

	北海道K町	新潟県M市
CIOまたはIT統括責任者不在時の明確な代替準備及び職員の参集体制	△ 首長不在に関する記述はないが、職員の自動参集基準の記述はある。	○ 首長不在の代替基準、職員の参集体制について明確に記述されている
代替IT拠点の設定	×	○
代替IT資源（サーバー、ネットワーク）の確保	×	○
電気・水・食料等の確保	△ 水・食料の「確保」に関する記述がない。	△ 水・食料の「確保」に関する記述がない。
IT関連備品の確保	△（LANケーブル）	○（プリンタ、トナー）
LAN仮設作業	○	×
重要な行政データのバックアップ	○ 「外部データ保管媒体」を前提とした記述があるので、外部保管が行われていると判断した。	○ 「外部保管しているバックアップデータ」を前提とした記述があるので、外部保管が行われていると判断した
重要情報システムの整理	×	○
外部事業者への協力要請	○	○
被災者支援システム	×	○
災害対策本部設置にあたっての行動計画	○	×
訓練計画	○ 毎年7月	○ 毎年9月

同一規模、同一業種であっても網羅されている項目にかなりの差異があるが、このうち代替拠点や代替サーバーおよび消耗品（トナー等）については 前述のICT部門の業務継続計画<初動版サンプル>で詳しく示された部分である。K町については同サンプル公表前に作成されたため その時点では検討に至っていなかったものと思われる。

このように、IT-BCP策定を推進するうえで、指針・ガイドラインではなく具体的サンプルを示すことの意義は大きいと思われる。

ただし、同サンプルは被害拡大防止が主眼となる被災初動期に限定したものであるうえ、自治体向けであるために情報システムの点検・再稼働に先んじて災害対策本部の運営や避難所等への情報提供を重視する設定である点など 民間企業が参照するには十分ではない。よって、当研究プロジェクトとして民間企業用に小

康期、復旧期を含めた IT-BCP サンプルの公表を目指していく。

第4章. IT-BCPの更新と定着における課題

IT-BCPを組織に定着するためには、訓練を重ねながら訓練で得られた気付きを元に更新を繰り返すことが必要となる。当研究プロジェクトでも、気付きを与えることに主眼をおいた机上訓練を過去3回開催し好評を博してきた。これらについては会報等で報告済みであるため割愛し、本稿では某医療機関におけるBCP訓練の事例を報告する。

この訓練では、

- ・何を優先させ、何を切り捨てるか
 - ・情報共有に伴うタイムロスが初動活動の妨げとならないか
 - ・情報共有を行うことがロスタイム以上のベネフィットを生むか
 - ・あらかじめ計画した体制、使用ツールが予定通り機能するか
 - ・頭で考えていたことが実際の行動にスムーズに結びつくのか。
 - ・発災期の混乱の中で、安全を確保しつつ上記活動が実行できるか
- を確認し、結果について意識共有することを目標として実施された。

このように具体的な問題意識に基づいて、訓練シナリオを作成してこそ気付きを生む訓練が可能となる。当研究プロジェクトが行ってきた机上訓練でも、教材開発時点でどのような気付きを得てもらいたいかを明確に設定したうえで状況設定、状況付与および演習課題を設定している。

残念ながら、普段、防災・危機管理を意識することの少ないIT要員が問題意識をもってIT-BCPの訓練シナリオを作成することは困難であり、IT系のコンサルタントでも同様である。逆に、一般の防災・危機管理コンサルタントではITに関連する状況設定は困難である。

よって、当協会のようにITの専門知識と内部統制に関する知見を併せ持つ機関が訓練モデルを作成し公開することのニーズは高い。当研究プロジェクトではこれまでもIT版DIG(Disaster Imagination Game)の提案などを行ってきたが引き続き教材開発を進めていく。

【参考】医療機関でのBCP訓練

平成28年の熊本地震をきっかけに、平成29年3月31日厚生労働省医政局長発信には、災害拠点病院の指定要件に「事業継続計画の整備を行っていること」さらには、この事業継続計画に基づき「被災した状況を想定した研修、訓練」を実施することなどが追加された。

これらの状況から、災害拠点病院を中心として、実効性ある事業継続に向けた取組が広がりつつある。

【机上訓練概要】

実施時期：平成29年3月

被害想定：南海トラフ地震（垂水区：震度5強）

施設場所：神戸市垂水区（鈴木クリニック）

参加者：クリニックスタッフ14人

課題は8題（11問）がスクリーンに緊急地震速報の音とともに出題された。

最初の10分で自分の意見を考え、そのあとチームで意見を出し合い、意見のとりまとめに20分（訓練は、発災後1時間の行動を確認する）。

当医療機関では職員の参集率を高めるため職員の家族側も含めて「あらかじめの準備」「発災直後の行動」「生活復旧」の教育を進めている。また、クリニック専用の緊急時携帯カードや一斉メールサービス、LINEグループを安否確認のツールとしている。机上訓練では、これらのツールを予定通り活用できるかを検証した。



【実践的訓練概要】

実施時期：平成29年9月

被害想定：南海トラフ地震（垂水区：震度5弱）

施設場所：神戸市垂水区（鈴木クリニック）

参加者：クリニック全員、傷病者役（ボランティア7名）

傷病者役にはあらかじめシナリオを用意し、訓練の中で確認するチェックポイントを傷病者役にのみ伝え、訓練後のアンケートに記載されるチェック項目の結果をスタッフの勉強会で情報共有する。

今回は搬送先との連携を含めていないため、応急処置をして連携先への搬送を指示するところまでの確認となった。

第5章. 監査対象としてのBCP、BCM、BCMS

IT-BCP をシステム監査の視点からみた場合、IT-BCP は「いざという時には こうする計画です」と言っているに過ぎず、監査証跡でもなければ、被監査対象が「このとおり対策を行っている」と主張する言明書でもない。このことから、事業継続における情報システムの適正性をシステム監査可能な状況とするためには、BCP 策定を越え、BCP を実効性あるものとして定着、更新していくマネジメントプロセス (BCM) が経営活動の一部として組織的に行われるよう導く必要がある。

このような仕組み(事業継続マネジメントシステム:BCMS)の標準規格として ISO 22301 が 2012 年に発行された。

ISO 22301 の取得状況を、2006 年に初版が発行された ISO27001 (ISMS:情報セキュリティマネジメントシステム) と比較すると表のとおりであり、規格化からの年数が 2 分の 1 弱であることを差し引いても ISO 22301 の取得企業が極めて少ないことがわかる。

ISO 取得企業の内訳

	ISO27001 (ISMS)	ISO22301 (BCMS)
世界全体	33,290	3,853
日本国内	13,889	226

国際標準化機構: <https://www.iso.org/the-iso-survey.html>:2016 年

BCP、BCMS が進まない原因として、自社の進捗度・成熟度が定量的に把握できないことが大きいと思われる。このため、「完璧な BCP を作らなければ まったく手をつけていないと同じ」と思い込んで手を付けられず、とりあえず作ってしまえば「あります」「やっています」と言ってしまうため、そのまま放置されてしまい BCMS へと成熟しないという状況ではないだろうか。このような状況を改善するため、当研究プロジェクトでは 第3章、第4章で述べたサンプルをベンチマークとして IT-BCMS 成熟度を指標化する方法についても開発、公表していく予定である。

【参考】BCMS 取得企業の事例

知名度の高いショッピングセンターのイオングループでは小売業で初めて取得。取得理由として経営理念の「お客さまを原点に平和追及し、人間尊重地域社会貢献する。」を追求したとのことである。この BCMS を取得したことをきっかけとして、熊本地震では自衛隊や日本航空との連携により救援物資を運ぶなど、社会貢献につながる活動ができた。

NEC グループではお客様に対して事業継続を行い、サービスの提供することを重要視して取得している。NEC グループでは経営者層が、お客様の被害状況を考えながら経営判断を行う非常時の訓練を行っており、顧客満足の向上に努めている。これらのことが

むすび

日本の企業は中小企業が97%を占める。本来BCPは、事業基盤の弱い組織ほど策定の必要性が高いともいえる。しかしながら実際には中小企業のBCP策定率が極端に低いことは第2章でみてきたとおりである。

中小企業庁の調査ではBCP策定が進まない原因の中でスキル・ノウハウ不足が最も多く挙げられている。小規模な組織では人員も時間もそれほどかけられない。よって、3章から5章の各章で述べてきた対策を整備し、監査可能なレベルへと被監査人を導いていくことが必要と考える。

また、現在のIT-BCP対策は一旦最適化したはずのシステムにやみくもに鎧をかぶせる如き強靱化・二重化に走りがちであり、そのプロセスにおいて適切なITガバナンスが存在しているか否かは疑問である。我々システム監査人は、システムの企画・設計・開発段階においてリスク発生後の縮退運転等を想定し、事業継続に寄与すべくコントロールが働いているか否かを評価し、改善提案等を含めた報告を行えるよう監査基準・ポイントを拡充し、システム構築上の知見も高めていくべきではないか。

このようにして、被監査人とともに成長していくことがこれからのシステム監査人の社会的役割であろうと考える。

【参考文献】

- ・ 内閣府：「企業の事業継続及び防災の取り組みに関する実態調査」
http://www.bousai.go.jp/kyoiku/kigyuu/pdf/h27_bcp_report.pdf
- ・ 中小企業庁：「BCPに係る取組の現状」
http://www.chusho.meti.go.jp/pamflet/hakusyo/H28/h28/html/b2_4_2_2.html
- ・ 平成29年防災白書
内閣府 (<http://www.bousai.go.jp/kaigirep/hakusho/>)
- ・ 適合性評価制度
一般財団法人日本情報経済社会推進協会 (<https://isms.jp/furiwake-j.html>)
- ・ 事業継続計画策定ガイドライン
経済産業省 <http://www.meti.go.jp/report/downloadfiles/g50331d06j.pdf>
(http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000039.html)
- ・ イオン http://www.aeon.info/news/2017_1/pdf/170303R_1_1.pdf
- ・ NEC http://jpn.nec.com/press/201403/20140311_02.html

以上

<目次>

【エッセイ】 陰陽師

会員番号 0707 神尾博

1. 陰陽師

平安時代の京の都には、百鬼夜行が跳梁跋扈していた。より正確に言えば「その地で生活していた人々の心の中には」と言うべきか。疫病や落雷、火事等の厄災は、怨霊や鬼が引き起こしていると信じられていた。その化け物どもの前に立ち塞がったのは、安倍清明を始めとする「陰陽師」と呼ばれる、祈祷や占術を駆使するスペシャリストたちである。

一方、当世では、サイバー空間の様々な脅威を迎撃する、セキュリティの専門家たちが活躍している。彼らは不正アクセスやランサムウェア、DDoS 攻撃等から、組織や市民を守るべく日夜奮闘している。もちろん攻撃側である犯罪組織の、悪辣なミッションへの熱意も並々ならぬものであるが。

1000 年もの時を超えて、また形を変えて徘徊する物の怪ども。そして、中世と現代の、特殊な知識や実践力を備えたヒーローたちは、奴らに立ち向かう。2つの時代の闇と光である両者に、スポットを当ててみるのも一興だろう。

2. 陰陽道

陰陽師が利用するフレームワークである陰陽道では、森羅万象は陰と陽の2つから成立するとされていた。男と女、昼と夜、太陽と月等である。このカテゴライズで言うと、セキュリティ技術者とサイバー犯罪者も該当するだろう。

さらに陰陽師が駆使する易（占い）では、この陰陽から四象を生じ、さらには八卦を生じるという。まるでITの根幹を成す、0と1による2進法の考え方である。また万物は木・火・土・金・水の5種類の元素からなるという五行思想とも結びつき「陰陽五行」と呼ばれ、こちらは10進法変換とでも言おうか。

陰陽道では、天体の動きは人間社会に影響を与えるとされており、天文観測も盛んに行われていた。今や社会の安全に関わる、サイバーインテリジェンスと呼ばれるネット上での諜報活動に、世界中の国家がしのぎを削っている。

**3. 鬼門**

平安京では、鬼は「鬼門」と呼ばれる丑寅（北東）の方角から、忍び込むと信じられていた。鬼を阻止するには障壁の設置が必要だ。天皇家の住まいである京都御所の鬼門には、安倍清明宅や赤山禅院、比叡山といった幾重ものバリアが張られていた。

マルウェアが一般にセキュリティホールから侵入してくるのは、諸氏もご存じの通り。こちらは、インターネット、すなわち外部からの入口でのUTM（統合脅威管理）やWAF（Web Application Firewall）によるフィルタリング、エンドポイントでのワクチンの導入やパッチの適用、出口でのDLP（Data Loss Prevention）といった、多層防御/多段防御が有効だ。

そもそも平安京は究極の地相とも言える、東に川、西に道、南に湖、北に山という「四神相応」の地に造営された。余談だが、この四神は時計回りだと玄武（爬虫類）→青竜（恐竜類）→朱雀（鳥類）→白虎（哺乳類）となり、恐竜の一部は恒温動物であり、羽毛も存在し爬虫類とは一線を画すとか、後に鳥に進化したといった学説と附合しているのは興味深い。

4. 式神

陰陽師は「式神（しきがみ）」という精霊を使役し、警戒の厳重な場所へ潜入しての情報収集や、場合によっては敵の殺害も行ったという。式神は基本的には主人の命令通りに動くが、任務遂行のための、ある程度の自律機能も備えていたようだ。

ITの世界では「エージェント」に該当するだろう。我々はMTA（Mail Transfer Agent）やHTTPのWebエージェント等、知らず知らずのうちに彼らの世話になっている。C&Cサーバを介して操られるボットはまさしく悪の式神と言えるだろう。IMD（Implantable Medical Devices）を代表するペースメーカーへのサイバー攻撃は、式神と同様、人命を奪うことも可能だという。対策として、心臓の形状や心拍による生体認証が考案されている。

また2017年には、詐欺メール対策としてAI（人工知能）技術を用いた、いかにも相手に騙されているふりをする「Re:scam」ボットなるものを開発したことが、ニュージーランドの非営利団体によって発表された。時間稼ぎで詐欺師を疲弊させることで、被害者の数を減らすことを目論んでいるそうだ。

5. 免状

正統な陰陽師には、土御門本庁から免状が発行されていた。江戸時代のものが、高知県香美市に現存している。また、なんとローマ法王庁（教皇庁）は、2005年からエクソシスト（悪魔払い師）の養成講座を開いているという。現在、IPAは情報処理安全確保支援士（旧セキュリティスペシャリスト）を認定している。セキュリティ資格は今後もますます重宝されるだろうが、陰陽道は迷信からの脱却による近代化の名のもとに、明治政府により禁止された。

免状もそうだが力量の維持向上も必須だ。口上の割に実力の欠ける陰陽師は、ライバルに自身の式神を隠されたり、木箱の中身を言い当てられずに恥をかかされたりしたという。サイバー攻撃は、WEF（世界経済フォーラム）でも重要なグローバルリスクと認識されている。「経営に役立つシステム監査」を標榜しながら、こうした大局が見通せず、世界的権威が重視しないような細事に拘泥しているシステム監査人も、社会からの信頼を失っていくだろう。

（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。）

支部報告 【 近畿支部 第170回定例研究会 】

会員番号 2531 岩崎 真明 (近畿支部)

1. テーマ 「サイバー空間を取り巻く現状と課題、サーバーセキュリティ政策について」
2. 講師 内閣サイバーセキュリティセンター 山下 浩司 氏
3. 開催日時 2017年12月16日(土) 15:00~17:00
4. 開催場所 SMGアクシア 四ツ橋・近商ビル館 10A
5. 講演概要

(1) テーマ

I o T、ビッグデータ、A Iをはじめとして、ビジネスにおいてはI Tの利活用により価値を生むことが期待されているが、一方では、サイバー攻撃事案は日々発生しており、企業においては、リスクマネジメントや人材育成を含めた対応が求められている。本講演では、現状認識として「サイバー空間の変化」を共有化し、その変化が起因となり発現したともいえるリスクの振り返りとして「サーバーセキュリティの個別事案と考え方」を取り上げ、その対策としての「サーバーセキュリティ政策の方向性」について解説いただきました。

(2) 「サイバー空間の変化」について

人類発展史の視点からは、狩猟・農耕社会から始まった社会であるが、現在は「情報社会(Society4.0)」の段階にあると考えられるが、今後は「超スマート社会(Society5.0)」という新たな経済社会へと発展していくと見込まれている。この変化の特徴は、I C T活用による「個別最適化」からサイバー空間と現実空間の融合による「社会全体の最適化(全体最適)」にある。これを「変化」と「テクノロジー」の視点から整理すると「変化：つながる」と「テクノロジー：I o t」、「知能化する」と「A I、ビッグデータ」、「広がる」と「ネットワーク技術の高度化(5G、S D N、ブロックチェーン等)」になると考える。特に「つながる」というところでは、いろいろな物・いろいろな産業が「つながる」ことで新たな価値が創造される期待感があるが、その反面では「弱いところに引きずられる」というリスクがあり、この脆弱性を攻撃されることで発現するリスクの影響度を想定した対策が必要となる。

(3) 「サーバーセキュリティの個別事案と考え方」について

最近発生したセキュリティ事故事案の振り返りと、どこに事故発生の原因があったのかについて解説いただきました。原因としては、「繋げる必要ない機器を不用意に外のネットワークと繋げてしまった」「パスワード設定のルールが緩かった」などであったことから、どれも「基本的な対策ができていなかった」ということが原因であったとのことでした。では、何をすればよいのかという事については、経済産業省より発信されている「サーバーセキュリティ経営ガイドライン」の中で「サーバーセキュリティ経営の3原則」「サーバーセキュリティ経営の重要10項目」があり、特に「検知・復旧」について意識した内容となっている。

(4) 「サイバーセキュリティ政策の方向性」について

取り組みの基本姿勢は、「自助：まずは企業自らが主体的に取り組む」「共助：一組織では限界があるので業界を越えて連携する」「公助：政府からの情報提供と支援」「国際連携：国境を越えた連携」である。この基本姿勢の中で、まずは企業の社会的責任として主体的に対策を講じる必要があると考えるが、完璧な防御は不可能であるので、事業継続の観点からも、攻撃の早期検知や被害拡大の阻止、対応復旧として「経営>事業>業務>システム>IT」の中で「何を、どこまで守るのか」という視点からの対策を講じておくことが重要である。例えば、図書館のHPがサイバー攻撃により、閲覧不可能となり、インターネット経由で「予約する。検索する。」というシステム機能が使えなくなり不便さを訴える声が上がったとしても、「図書の貸し出し業務」そのもののリアルな基本業務については人手による運営が一時的に継続出来る、すなわち、図書館まで足を運べば「本を選んで予約する。貸し出しを受ける。」という機能は継続されるような仕組にしておくことが必要である。こうした「自助」への取り組みを基本としつつ、「共助・公助」としては、サイバー攻撃に備えるため、情報収集・共有・活用を率先して行うことが重要であるとの認識から、共有・活用する情報の5W1H（目的、類型、共有の場、階層、タイミング、手法等）の整理・標準化について、企業・業界・官民・国境を越えて迅速な情報を共有する仕組み作りが動き出している。総じて言うならば、「超スマート社会（Society5.0）」実現に向けて、人材、情報、技術に重点的に資金を投入し、その資金が効率的に循環する仕掛けや制度を作ることが重要である。

6. 所感

本講演と合わせて、日本経済団体連合会からの「Society 5.0 実現に向けたサイバーセキュリティの強を求めろ」という提言に目を通しました。そこには「完璧な防御は不可能であり、サイバー攻撃を自然災害と同様に避けられないリスクと捉えるべきである」と記されていました。サイバー空間による新たな価値を享受するなら、企業としても、個人としても、それ相応なリスクが伴うことを覚悟する必要があると考えるので、サイバーセキュリティに対する意識を国全体で向上させることは本当に重要なことであると考えます。その意味では、「我々個人」としても「自助とは何か。日常生活の中で意識できることは何か。」を真剣に考えて行動すべき時代に入っていくとするなら、「大人として何を学び行動するのか、子供達としては学校教育の中で何を学んでいくのか」について、まさに政府としての「公助」が効率的に循環する仕掛けや制度が必要になると考えますが、その反面では、制度であるが故に、そこに潜むリスクにも目を向けておくことも大切と考えますので、世の中は益々、便利で難しい時代に進化していくのだということを改めて認識できた講演でした。

以上

<目次>

注目情報 (2018.1~2018.1)**■「情報セキュリティ対策支援サイトの公開 (IPA)」**

2018.1/15に情報セキュリティ対策支援サイトが公開されました。

情報セキュリティ対策の「知りたい」、「学びたい」、「始めたい」、「続けたい」と、それを後押しする方々の活動のサポートいたします。

<https://security-shien.ipa.go.jp/>

■「平成30年度春期情報処理技術者試験・情報処理安全確保支援士試験受験申込み開始 (IPA)」

～今年で試験制度創設 50 年、累計応募者数は 1,900 万人超～

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）情報処理技術者試験センターは、2018 年 4 月 15 日（日）に実施する「平成 30 年度春期情報処理技術者試験・情報処理安全確保支援士（登録セキスペ）試験」の受験申込みの受付を、2018 年 1 月 11 日（木）から開始しました。

<https://www.ipa.go.jp/about/press/20180111.html>

■「第四次産業革命スキル習得講座認定制度 (経済産業省)」

経済産業省は、IT・データ分野を中心とした専門的・実践的な教育訓練講座を経済産業大臣が認定する「第四次産業革命スキル習得講座認定制度」について、厳正な審査の結果、16 事業者 23 講座を認定しました。

<http://www.meti.go.jp/press/2017/01/20180110001/20180110001.html>

■「IoT国際競争力指標(2016年実績)の公表 (総務省)」

総務省は、我が国の ICT 産業の国際競争力の強化に向けた測定指標である「IoT 国際競争力指標 (2016 年実績)」をとりまとめましたので、これを公表します。

http://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000119.html

■「プライバシーマーク新審査基準を公表 (JIPDEC)」

JIS 改正に伴うプライバシーマーク審査基準を改正し公表しました。

https://privacymark.jp/system/operation/jis_kaisei/index.html

協会からのお知らせ（予告）【第 17 期通常総会の開催】

会員番号 1760 斎藤由紀子（事務局）

日本システム監査人協会（SAAJ）会員各位**■第 17 期通常総会のご案内**

日本システム監査人協会の第 17 期通常総会を、下記の通り開催致します。

万障お繰り合わせの上ご出席をお願い申し上げます。

総会、懇親会の参加申込は 2018 年 1 月末より、協会ホームページにて受け付けます。

1. 日時：2018 年 2 月 23 日（金） 13 時 30 分～（受付開始：13：00）

2. 場所：機械振興会館 地下 3 階 研修 1 室

東京都港区芝公園3丁目5番8号

アクセス：<http://www.jspmi.or.jp/kaigishitsu/access.html>

3. 第 17 期通常総会 議事（予定） 13 時 30 分 ～ 15 時

13:30 開会

13:35 通常総会

1) 定款一部変更

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

5) 理事選任の件

15:00 閉 会

4. 特別講演 15 時 30 分～17 時

15:30 開演

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 国立情報学研究所教授 山田誠二 氏

17:00 閉演

5. 懇親会 17 時 30 分 ～ 19 時

17:30 開場 （機械振興会館地下 3 階会議室）

19:00 閉場

<目次>

【 SAAJ協会行事一覧 】		赤字：前回から変更された予定	2018.1
2017	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	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 27：法務局：資産登記、活動報告提出 理事変更登記 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
3月	1：NPO事業報告書、東京都へ提出 5：年会費未納者宛督促メール発信 8：理事会	1-31：春期CSA・ASA書類審査 14：第230回月例研究会	
4月	12：理事会 30：法人住民税減免申請	初旬：春期CSA・ASA書類審査 中旬：春期ASA認定証発行	15：春期情報技術者試験
5月	10：理事会	中旬：春期CSA面接	
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）
前年度に実施した行事一覧			
7月	5：支部助成金支給 13：理事会	3：第224回月例研究会「IoTにおけるサイバ 攻撃の実態とその対策」 下旬：秋期CSA・ASA募集案内	14：支部会計報告〆切
8月	（理事会休会） 26：中間期会計監査	1：秋期CSA・ASA募集開始～9/30	
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 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：総会開催予告掲示 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

会報掲載「論文」募集要項の改定について

会員番号 1795 藤澤 博 (会報部会 主査)

会報掲載「論文」募集要項を改定しましたので、お知らせします。

(2018年1月11日 SAAJ 理事会承認)

1. 本要項の目的

本要項は、会員が会報に掲載する論文について、投稿手順ならびに審査要項について定める。

2. 会報掲載「論文審査基準」 会報掲載「論文」は、以下の「論文審査基準」に従って評価する。

基本事項	評価基準	点数	合格基準
1 内容	公序良俗に反する/政治的偏向/宗教的宣伝等の内容を含む	不可	1
	システム監査・セキュリティ監査関連啓発、普及、理論深化、情報提供、実践、手法開発等に役立つ	1	
	上記との関連は無いが会報掲載にふさわしいと認められる	1	
2 字数	6000字より相当少ない、又は17千字より相当多い	不可	1
	6000字以上17千字程度(図表を含める)である	1	
評価基準	論文審査基準	点数	判定
3 論理の 首尾一貫性	論理の首尾一貫性があるとはいえない	0	1
	論理の首尾一貫性がある	1	
4 実務の 裏づけ	実務の裏づけが確認できない	0	1
	実務の裏づけがある(1.匿名による事例紹介)	1	
	実務の裏づけがある(2.執筆者の所属で判断できる)	2	
	実務の裏づけがある(3.顧客了解による実名)	3	
5 有用性	すでに一般常識とされている内容である	0	1
	内容が優れている	1	
	適切なタイミングで発表され価値が高い	3	
	内容に優れ、参照や応用の可能性が高い	5	
6 文章表現力	文体に統一が取れておらず読みにくい	0	1
	普通である	1	
	優れている	2	
7 独創性	独創性がない、または独善的である	0	1
	独創性がある	1	
	優れて独創性がある	2	
合計点数	不可を含まず、7点以上を合格とする。(満点15点)		

3. 会報掲載「論文」の投稿方法 「論文」を会報に掲載できるのは、会員のみとする。投稿は随時受け付けるものとし、投稿者は、以下のページから投稿用フォーマットをダウンロードし、saajeditor@saaj.jp 宛に、メール添付ファイルで送信する。

http://www.saaj.or.jp/members/kaihou_dl.html

4. 論文審査の手順

- (1) 会報部会主査は、投稿された論文について、1週間以内に会報編集委員もしくは役員のうち3名を指名し、以下の論文審査基準に従って評価実施を求める。

- ・ 3名のうち1名は、会報主査自らも可とする。
- ・ 論文提出者は、評価に加わることはできない。
- ・ 評価者は公表しない。

- (2) 論文評価を依頼された者は、原則として2週間以内に判定結果を会報部会主査に提出する。
- (3) 会報部会主査は、3名の評価がすべて7点以上であるとき、会報掲載を承認する。
- (4) 会報部会主査は、応募者に会報掲載の可否を連絡する。ただし点数については通知しない。
- (5) 会報部会主査は、評価結果が会報掲載とする7点に満たない場合、その理由を付して応募者に通知する。
- (6) 応募者の希望により、その理由に基づく訂正について1回のみ再提出を認める。
- (7) 再提出された論文については、会報主査が上記論文審査基準によって再評価する。
- (8) 再提出された論文について、合格点数に達しない場合は、会報掲載は行わない。
- (9) 論文評価結果は、保管しない。

5. 会報掲載

- (1) 会報主査は、会報掲載を承認した後、会報編集担当者に原稿をメール送信する。
- (2) 毎月15日を締切として、原則として当月25日発行の会報に掲載する。
- (3) 会報編集担当者は、発行前の会報(案)を、15日迄に執筆者にメール送信し、最終確認を20日までに行うよう求める。
- (4) 20日までに執筆者から最終確認が得られない場合は順延とし、1ヶ月後の会報掲載とする。

6. 原稿料について

- (1) 原稿料は、2万円とする。
- (2) 会報主査は、会報掲載が決定後、執筆者の金融機関口座を取得する。
- (3) 会報掲載後、原稿料の「支払依頼書」を会計宛に提出する。
- (4) 原稿料は、会報掲載翌月末日までに執筆者に支払う。

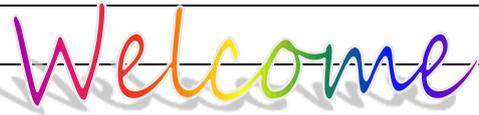
7. 継続教育算入時間 会報に掲載した「論文」については、公認システム監査人(補)継続教育で、10時間/1稿として認める。

8. 著作権について 著作権は、執筆者に帰属する。ただし、執筆者は、会報に掲載した論文の再掲載、引用についての権利を当協会に付与するものとする。

■ ===== 附則 =====

2003年7月：「会報掲載論文審査要綱」	制定
2003年10月：「判定基準(点数)」	改定
2006年6月：「会報掲載論文 審査ガイド」	制定
2009年5月1日：「会報掲載論文募集要項」	制定
2018年1月11日：「会報掲載「論文」募集要項」改定(全文書を統合)	

【 新たに会員になられた方々へ 】



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



ご確認ください

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



特典

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



ぜひ
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。

【 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（2019年2月号まで）の年間テーマは、「システム監査人の新たな活躍」です。皆様のご投稿をお待ちしています。

システム監査人にとって、報告や発表の機会が多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマも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 (2018. 1.11 改訂)

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 New! 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。 ※今月の会報掲載「論文」募集要項の改定についてをご確認ください。

■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 会報主査：藤澤

企画も今後ご案内させていただきますので、ご協力をお願い致します。

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

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.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。

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。

■□■ S A A J 会報担当

編集委員： 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子

編集支援： 仲厚吉（会長）、各支部長

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

Copyright(C)1997-2017、認定 NPO 法人 日本システム監査人協会

<目次>