



認定 NPO 法人

日本システム監査人協会報

2017 年 1 月号

No 190

No.190 (2017 年 1 月号) <12 月 25 日発行>

**2017年の幕開けにあたり
スマート社会到来に向けて
SAAJは新たな取組みを始動
します。**



写真提供：藤井 仁至

巻頭言

『年頭に当たって』

会員番号 0557 仲 厚吉 (会長)

2017 年度は、スマート社会計画「ソサエティー5.0」など IT の利活用が社会全般に広がるなか、システム監査の普及・促進のため協会の信頼性を高めるべく次のように協会運営を行う方針です。

1. 協会事業の方向性は次の3点とする。

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

協会組織を整備し体制を充実させ世代交代に取り組む。

2. システム監査の活性化の一環として次の活動を行う。

1) 「IT アセスメント」の ISO 化を推進する。

2) システム監査に関連する他団体との交流を進める。

3) 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。

会員の皆様にご協力をお願い申し上げ、年頭のご挨拶と致します。

以 上

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

○ 巻頭言	1
【年頭に当たって】	
1. めだか	3
【システム監査の効果的活用】	
2. 投稿	4
【システム監査の活性化】	
3. 本部報告	5
【第 218 回月例研究会講演録（情報処理安全確保支援士制度について（通称；登録セキスペ））】	
4. 支部報告	10
【北信越支部 2016 年度 石川県例会・研究報告】	
【北信越支部 2016 年度研究報告】	
5. 注目情報	21
【「長期休暇における情報セキュリティ対策」を更新】 I P A	
【「第 4 次産業革命と情報連携-これからの情報活用とプライバシーを考える-」の講演内容を公表】	
JIPDEC	
6. セミナー開催案内	22
【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	23
【第 16 期通常総会のご案内】	
【CSA/ASA 資格をお持ちの方へ：資格更新手続について】	
【新たに会員になられた方々へ】	
【協会行事一覧】	
8. 会報編集部からのお知らせ	27

めだか 【 システム監査の効果的活用 】

システム監査の効果的活用のため、IT利活用の評価、即ち「ITアセスメント」におけるシステム監査の役割を考えると、システム監査は、ITマネジメントでの「PDCA」サイクルの「Check」、ITガバナンスや情報セキュリティガバナンスでの「EDM」サイクルの「Monitor」、データ収集と分析における「PPDAC」サイクルの「Analysis」への評価などを担っている。これらのシステム監査の実施に当たっては、システム環境に合わせた管理策（コントロール）の策定が必要になる。

「システム監査基準」と「システム管理基準」は、2004年（平成16年）の発行であり、12年間が経過している。この間、情報社会はシステムに対し、「情報セキュリティ」、「個人情報保護」、「内部統制」、「ITガバナンス」などを求めてきた。このため、システム監査人は、「システム管理基準」をベースに、他の基準などを参考に管理策（コントロール）を見直してきた。

現在は、「ビッグデータと人工知能」の時代であり、ビッグデータには、大データ量（Volume）、データ種類の多様性（Variety）、高速度（Velocity）という3つの特徴がある。また、機械学習などの人工知能は、ビッグデータの利活用と不可分な関係になっている。

「ビッグデータと人工知能」の時代に、システム監査人は、「システム管理基準」をベースに、「AIネットワークシステム開発原則」などを参考に管理策（コントロール）を見直すことが求められている。（空心菜）



〔AIネットワークシステム開発原則〕

透明性の原則：AIネットワークシステムの動作の検証可能性及び説明可能性を確保すること。
利用者支援の原則：AIネットワークシステムが利用者を支援し、利用者に選択の機会を適切に提供するように配慮すること。
制御可能性の原則：人間によるAIネットワークシステムの制御可能性を確保すること。
セキュリティ確保の原則：AIネットワークシステムの頑健性及び信頼性を確保すること。
安全保護の原則：AIネットワークシステムが利用者及び第三者の生命・身体の安全に危害を及ぼさないように配慮すること。
プライバシー保護の原則：AIネットワークシステムが利用者及び第三者のプライバシーを侵害しないように配慮すること。
倫理の原則：AIネットワークシステムの研究開発において、人間の尊厳と個人の自律を尊重すること。
アカウントビリティの原則：AIネットワークシステムの研究開発者が利用者など関係するステークホルダーに対しアカウントビリティを果たすこと。

参考：「ビッグデータと人工知能 可能性と罠を見極める」西垣通 著 中公新書2384
「耕論 AIと生きる」新井紀子、栄藤稔、新保史生 朝日新聞2016年11月9日
「AIネットワーク化検討会議報告書2016の公表」総務省情報通信政策研究所
（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 の見解ではありません。）

2016.12

投稿 【 システム監査の活性化 】

会員番号 0557 仲厚吉（会長）

当協会は、システム監査の活性化のためSAAJのビジョン（3年後に目指す姿）に沿って、システム監査を核にした「ITアセスメント」や「ITアセッサ」の普及活動、及び「公認システム監査人」と並ぶ「公認ITアセッサ」の認定に取り組んでいきます。「ITアセスメント」は、「ITガバナンス」や「情報セキュリティガバナンス」の6原則のもと、「EDM」サイクル、即ち、「Evaluate」（評価）、「Direct」（指示）、「Monitor」（モニタ）のサイクルにより、統制が維持・向上されているか評価を行い、経営層に助言し、IT利用者のニーズに応じていく活動です。

日本ITガバナンス協会は、「ITGI Japan カンファレンス 2016（11月14日、東京コンファレンスセンター品川）」を開催し、当協会は後援団体として協力しています。当カンファレンスは、「10周年記念講演会～ITガバナンスこれまでの10年、そしてこれから～」と題して次のような内容でした。

- 講演 1：「金融機関におけるAI技術の活用状況」
- 講演 2：「日立の鉄道ビジネス海外展開について」
- 講演 3：「日本企業が直面するグローバルなガバナンス・コンプライアンス」
- 講演 4：「攻撃側の観点から眺めたサーバーセキュリティの状況とあるべき姿」
- 講演 5：「SOE・SORの両立とアプリケーションオーナー制度」

当協会は第218回月例研究会（2016年11月15日、機械振興会館）を開催し、「情報処理安全確保支援士制度について」と題して、経済産業省商務情報政策局地域情報化人材育成推進室長 藤岡伸嘉氏を講師にお招きし、ご講演、その後の活発な質疑応答や、懇親会での歓談を行いました。

講演要旨：近年、ソフトウェアの脆弱性（サイバー攻撃を受ける危険性がある弱点）に起因する被害や情報漏洩が深刻化しています。一方で我が国のサイバーセキュリティの専門人材については不足しています。政府機関や企業等のサイバーセキュリティ対策を強化するため、最新のセキュリティに関する知識・技能を備えた高度かつ実践的な人材を確保するため、このたび新たな国家資格である「情報処理安全確保支援士制度」が創設されました。今回は、この情報処理安全確保支援士制度について解説します。

スマート社会計画「ソサエティ5.0」などのITの利活用を上手く行っていくため、ITガバナンスと情報処理安全確保が求められます。当協会では、それらに資するよう他団体と協力し、また、「システム監査」の活性化、及び「ITアセスメント」の普及に積極的に取り組んでいきます。会員及び公認システム監査人等の皆様のご協力をお願い致します。

以上

<目次>

第 218 回月例研究会：講演録【 情報処理安全確保支援士制度について（通称；登録セキスベ） 】

会員番号 2023 戸室 佳代子

【講師】 経済産業省商務情報政策局 地域情報化人材育成推進室長 藤岡 伸嘉 氏

【日時・場所】 2016 年 11 月 15 日（火） 18：30～20：30 機械振興会館 B2F ホール

【テーマ】 「情報処理安全確保支援士制度について（通称；登録セキスベ）」

【要旨】

近年、ソフトウェアの脆弱性（サイバー攻撃を受ける危険性がある弱点）に起因する被害や情報漏えいが深刻化している。その一方で我が国のサイバーセキュリティの専門人材は不足している。そこで、政府機関や企業等のサイバーセキュリティ対策を強化、最新のセキュリティに関する知識・技能を備えた高度かつ実践的な人材を確保するため、このたび新たな国家資格である「情報処理安全確保支援士制度」が創設された。今回は、この情報処理安全確保支援士制度について解説する。

【講演録】

1. サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の概要

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策の抜本的強化を図るため、以下の改正を行う必要があった。

① 国が行う不正な通信の監視、監査、原因究明調査等の対象拡大

対象となる特殊法人・認可法人はサイバーセキュリティ戦略本部が以下のとおり指定。

日本年金機構、国家公務員共済組合連合会（KKR）、地方公務員共済組合連合会、地方職員共済組合、都職員共済組合、全国市町村職員共済組合連合会、日本私立学校振興・共済事業団、公立学校共済組合、地方公共団体情報システム機構（J-LIS）の9法人。

② サイバーセキュリティ戦略本部の一部事務を独立行政法人情報処理推進機構（IPA）に委託

秘密保持義務等を規定し、IPA その他政令で定める法人に一部事務を委託する。

また、サイバーセキュリティ対策の強化に係る観点から、情報処理の促進に関する法律（以下「情促法」と言う。）に以下の規定の整備を行った。

- ・サイバーセキュリティ戦略本部から委託を受ける事務に係る IPA の業務追加
- ・情報処理安全確保支援士制度の創設（名称独占、更新制、秘密保持義務等）
- ・ソフトウェアの脆弱性情報等の公表の方法・手続を整備

なお、サイバーセキュリティへの対応が重要であることから、経済産業省内にもサイバーセキュリティ課を新設した。（本法改正事項とは別の措置）

2. 情報処理安全確保支援士制度の創設

（1）必要性・特徴

情報セキュリティ対策の強化に向けて専門人材の確保・育成が肝要であるが、その数は国全体では不足

している。経済産業省が今年 6 月に出した調査結果では、IT 企業及びユーザ企業（情報システム部門）における情報セキュリティ人材については、2016 年時点で 13 万 2 千人不足、2020 年には 19 万 3 千人不足という推計結果が出ている。

現在、IPA や民間団体によりセキュリティ能力を測る試験が複数実施されているものの、人材の所在が「見える化」されていない。また、日進月歩のセキュリティ知識を適時・適切に評価できるものとなっていない。例えば、昭和の頃に取得した情報処理の資格は現在の技術に照らし合わせて妥当とは言えない。そのため、最新のセキュリティに関する知識・技能を備えた、高度かつ実践的な人材に関する国家資格が必要。

（２）業務等

「情報処理安全確保支援士は、サイバーセキュリティの確保の取り組みに関し、

- ① 相談に応じる。
- ② 必要な情報の提供及び助言を行う。
- ③ 実施状況について調査、分析及び評価を行う。
- ④ ③の結果に基づき指導・助言を行う。
- ⑤ 事業者、コンピュータを利用する者のサイバーセキュリティの確保を支援する。

ことを業とする。」（注；「」内は情促法第 6 条の規定内容を講師が分解し、表現した文章である）

サイバーセキュリティ対策を「業」とする資格で、サイバーセキュリティ担当部門における緊急対応、監査、管理業務やサイバーセキュリティスキルを必要とするセキュアなものづくり、セキュアな運用・保守、管理業務などが仕事として想定される。スキルレベルとしては情報処理技術者試験のときの情報セキュリティスペシャリスト試験のレベル 4 と同等だが、後述するが、講習受講が義務付けられていて、常にサイバーセキュリティに関する最新の知識及び技能を有していなければならない点が大きく異なる。

（３）関係法令

改正された法令（施行日：平成 28 年 10 月 21 日）

情報処理の促進に関する法律（昭和 45 年法律第 90 号）

情報処理の促進に関する法律施行令（昭和 45 年政令第 207 号）

情報処理の促進に関する法律施行規則（平成 28 年経済産業省令第 102 号）

3. 情報処理安全確保支援士の通称、ロゴマーク

国家資格としての法律上の正式名称は、「情報処理安全確保支援士」だが、

通称は、登録セキスペ（登録情報セキュリティスペシャリスト）

英語表記は、RISS（Registered Information Security Specialist；アールアイエスエス）

ロゴマークはサイバーセキュリティ対策を業とする仕事人をイメージしたもので、登録した者は IPA に申請いただくことで無償で名刺等に使用できる（実物は本議事録末尾の URL から参照してください）。フレームは、盾（シールド）を意味し様々な脅威から情報組織や社会を守るエージェントを、深みのある青

は誠実と冷静さを意味する。地球は、国際社会とデジタル社会を現す。羽は、IT による人々の生活と拡がりと飛翔を意味する。4 つの星は、技術水準レベル 4 の 4 を現し、重要性の高い存在となることをイメージしている。

4. 情報処理安全確保支援士制度（登録セキスペ）の全体像

（1）登録セキスペとなる資格を有する者になる段階

①「情報処理安全確保支援士試験」の合格者

本試験は、平成 29 年春期（4 月）から実施する。

試験時間や出題形式、出題範囲、シラバスなどは情報処理技術者試験の「情報セキュリティスペシャリスト試験」をベースとする（従前の情報処理技術者試験と同様に午前 I 免除も継続）。

受験手数料は 5,700 円、実施回数は年 2 回（4 月・10 月）とし、情報処理技術者試験と同日・同じ会場で行う。

②経過措置対象者

情報処理技術者試験の以下の試験区分の合格者は情報処理安全確保支援士試験合格者とみなす。ただし、制度開始から 2 年間（平成 30 年 10 月 20 日まで）に登録を受ける場合に限る。

- ・情報セキュリティスペシャリスト試験（平成 21～28 年度）

- ・テクニカルエンジニア（情報セキュリティ）試験（平成 18～20 年度）

※情報セキュリティアドミニストレータ試験合格者は、当初対象とする予定であったが、平成 13～18 年に実施された試験であり直近のサイバー攻撃への対処等を考慮すると新しい知識・技能が要求されること、試験出題範囲が情報セキュリティスペシャリスト試験やテクニカルエンジニア（情報セキュリティ）試験と異なり人材像も異なること、試験レベルがレベル 4 ではないことから対象外となった。

（2）登録を受けて登録セキスペとなる段階

申請者（登録セキスペとなる資格を有する者）は、申請書類を準備し、登録免許税（9,000 円の収入印紙）・登録手数料（10,700 円を IPA 指定銀行口座に振込み）を納付後、申請書類を IPA に提出（簡易書留で郵送）する。IPA は、これを受理・審査後、登録簿への登録、登録証交付、登録事項などの公開を行う。ただし、欠格事由に該当する場合は登録不可となる。登録セキスペの欠格事由は、成年被後見人又は被保佐人、禁錮以上の刑に処せられ執行後 2 年を経過しない者、登録セキスペの登録を取り消され 2 年を経過しない者のいずれかに該当する場合である。（情促法第 8 条）

申請書類は、下記のものが必要となる。

- ① 登録申請書
- ② 戸籍謄本（抄本）又は住民票の写し
- ③ 試験合格証書（コピー）
- ④ 登記されていないことの証明書
- ⑤ 身分（身元）証明書

⑥ 欠格事由に該当しない旨の誓約書

⑦ 登録事項等公開届出書

登録申請は、2016 年 10 月 24 日から開始し、随時受け付けている。現時点で 400 人程が手続きを開始されている。登録簿への登録、登録証の交付は 4 月 1 日（申請締切日：1 月 31 日）、10 月 1 日（申請締切日：7 月 31 日）の年 2 回とする。ただし、経過措置対象者の最終登録分は、経過措置対象期間が 10 月 20 日までのため、申請受付を 2018 年 8 月 19 日までとする。

（3）登録セキスぺとして活動、資格を維持する段階

企業等がその人材を安心して活用できるようにするため登録セキスぺの登録情報などを IPA のウェブサイトで公開する。公開情報は、登録番号、登録年月日、支援士試験の合格年月、講習の修了年月日で、継続講習（後述）の受講状況も公開される。継続講習は、最新のサイバー攻撃の状況や情報セキュリティ技術について学ぶ場でもあり、最新のサイバーセキュリティに関する知識・技能を有していることの裏づけとなる。

また、登録セキスぺの業の特徴から、氏名、生年月、試験合格証書番号、自宅住所（都道府県のみ）、勤務先名称、勤務先住所（都道府県のみ）は、任意公開情報とし、本人からの届出書に基づき公開される。これを踏まえ、自己 PR ページも今後準備予定である。

資格を維持するには、経済産業省の許可を受けて IPA が実施するサイバーセキュリティに関する講習を継続的に受講しなければならない。講習未受講の場合は、資格名称の使用停止または登録抹消となることがある。講習は、オンライン講習と集合講習を組み合わせる実施する。

① 講習の科目及び範囲

知識：攻撃手法及びその技術的対策、関連制度等の動向

技能：脆弱性・脅威の分析、情報セキュリティ機能に関連する企画・要件定義・開発・運用・保守、
情報セキュリティ管理支援、インシデント対応

倫理：登録セキスぺとして遵守すべき倫理

② 実施形式及び時間

オンライン講習：毎年 1 回（1 回当たり 6 時間）

集合講習：3 年に 1 回（1 回当たり 6 時間）、ケーススタディによるグループ演習が中心

③ 講習受講料

オンライン講習：20,000 円程度、集合講習：80,000～90,000 円程度を想定している（2016 年 11 月に正式決定し IPA から公表予定）。3 年間で 150,000 円程度となる見込みだが、本制度においては、更新のための手続きや手数料は発生しない。

④ 講習受講の基本パターン

試験合格日から登録日までの期間が 3 年以内の者（基本パターン）

オンライン講習：年 1 回受講

集合講習：登録日を起点として、3 年目に 1 回受講

4 年目以降もこのサイクルを繰り返す。

⑤ 試験合格日から登録日までの期間が 3 年を超えている者

登録日を起点として、1 年以内にオンライン講習と集合講習をそれぞれ 1 回受講

2 年目以降（2、3、4 年目）は基本パターンで受講

基本パターンで登録する者より、初年度においては、80,000～90,000 円程度余計に費用がかかってしまう。情報処理安全確保支援士試験合格後は、速やかに申請を出し、登録セキスペとして活躍していただくことを期待したい。

詳細は次のページを参照してください。 <http://www.ipa.go.jp/siensi/>

【記録者所感】

セキュリティ対策は管理・運用とセキュアなものづくりの両面から構成され、どちらが欠けてもそこに穴があいてしまう。また、欠けていなくても古くなれば弱くなってしまう。技術や知識は知っているだけでは意味がなく、使えて初めて自分の強みになる。継続維持が大変な資格ではあるが、知っていることで満足せず、常に最新を知り、それを使うことできる人材であることを証明する資格であると思った。

以上

<目次>

支部報告【北信越支部 2016 年度 石川県例会・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 石川県例会を開催しました。

- ・日時：2016年12月10日（土） 13:00-17:00 参加者：7名
- ・会場：ITビジネスプラザ武蔵（石川県 金沢市）
- ・議題：1. 西日本支部合同研究会 in Matsue 報告

2. 研究報告

「新技術等の導入に対するシステム部門及び監査部門のあるべき姿」

長谷部 久夫 様

「情報セキュリティ対策（運用と技術的対策）を考える」

梶川 明美 様

3. 2017年度活動計画の検討

◇研究報告

「新技術等の導入に対するシステム部門及び監査部門のあるべき姿」

報告者（会員番号 1766 長谷部 久夫）

当支部から3名が出席したSAAJ中部・北信越支部、JISTA中部支部合同研究会の出席報告、及び報告者からの関連報告に基づき、標記テーマについて意見交換した。

1. SAAJ中部・北信越支部、JISTA中部支部合同研究会の出席報告（詳細は会報No.188 支部報告 参照）

当支部の出席者が、「新技術導入」に係るグループディスカッションの概要を以下のとおり報告した。

- （1）新技術はあくまでも「手段」であり、新技術導入の真の「目的」を達成する視点から監査対象を明確化する必要がある。システム監査人には、幅広い知識をベースとして「どの分野で高い知識が必要か」を見極める目利き（必要な知識を知り、助けを求める）が必要。スローガンは「大胆にして細心」。
- （2）新技術導入を伴う開発プロジェクト管理では、前提となるシステム開発管理態勢の整備が重要となる。上流工程の開発目的の設定、新技術リスク評価をはじめ、各開発工程における経営陣やユーザー部門の関与、各種の教育・訓練、プロジェクト振返りと技術標準の改訂等については組織としての取組が必要。
- （3）最先端技術でなくとも、発注者側の組織にとっての「新技術導入」はヒューマンリスクがある。新技術リスク見落とし、システム部分最適化、QCD計画未達成等を防ぐためには、本来の目的を明確化し、それに立ち返る仕組、プロジェクト見える化、危険予測やコミュニケーションのスキルアップが必要。

2. 報告者からの関連報告

報告者が、本年度の支部例会や各研究会への参加、及びリスク管理・システム検査の担務を通じ考えた「新技術等の導入に対するシステム部門の変革と、それに対する監査部門のあるべき姿」を報告した。

(1) 新技術等の導入に係る動向

近年、クラウド環境やスマートデバイスを利用した取引やサービスが業態を問わず広く普及する等、IT新技術の導入が相次いでいる。あらゆる分野において IoT (Internet of Things) が普及しつつあり、制御システムの一部はスマートコミュニティ実現に向けての位置付けがされている。

また、金融分野では、Fintech (Financial と Technology を組み合わせた造語、IT を駆使し新たなサービスを生み出したり、顧客の目線でサービスを見直したりする動きのこと) が注目を集めている。その業務範囲は、①モバイル／インターネットバンキング、②金融資産の一元管理、③送金・決済業務、④貸出業務、⑤仮想通貨、⑥人工知能 (AI) のサービス利用、⑦ビッグデータ対応等、多岐にわたる。

新技術等による業務の革新は、顧客の利便性向上や、社会・経済の発展に寄与することが期待され、奨励されるものである。しかしながら、その安全性には懸念があり、企業健全性の確保、消費者保護、プライバシー保護、不公正な取引防止などに配慮した「責任ある革新」が行われることが期待される。

(2) 新技術等の導入に対するシステム部門の変革

ア. 経営陣を支える中核部門

経営におけるITの重要性が高まっていることを受けて、新技術等の導入による「責任ある革新」にシステム部門が担う役割は重くなっている。システム部門には、組織内の他部門との連携により、経営資源配分の意思決定、ITガバナンスを支える中核部門として以下の役割が求められる。

- (ア) 経営企画部門との連携により、経営計画策定上、業務計画、投資計画、システム開発計画の整合性を確保し、最大の投資効率をもたらす新技術等の導入を含むIT化方針を立案
- (イ) リスク管理統括部門との連携により、外部委託先を含む組織全体のシステムリスク管理手続を整備
- (ウ) 業務所管部門（ユーザー部門）との連携により、各業務における顧客の満足度向上、リスク改善、及び消費者保護等の観点から、有用な新技術等の導入を検討して実現

システム部門が役割を果たすには、経営陣が、経営計画方針、リスク管理方針、情報管理方針等のITに係るポリシーを定め、システム開発規程、外部委託管理規程等でIT導入、及びリスク管理に係る各部門の役割を明確にするなど、組織横断的に経営陣を支える体制を整備することが前提となる。

イ. 組織全体の人材育成部門

システム部門は、組織内の他部門との連携による「自助」に加え、外部機関との連携による「共助」、官民一丸となり取組む「公助」を活用すべきである。要員には、広い視野、コミュニケーション力、及び情報リテラシーが必要となる。その能力は、システム部門のみにとどまらず、他部門の管理者、ひいては、経営層となって発揮することが期待される。システム部門は、IT新技術による業務革新を契機として、組織全体の戦略を担う人材を輩出する「人材育成部門」になることを目指すべきである。

(3) システムリスクに対する監査部門のあるべき姿

ア. リスクベース監査

限られた監査資源の制約の下で、効果的なシステム監査を実施するには、リスクベースアプローチによる監査計画の策定が必要。それには、システム部門が中心となり、①システム現況と変更計画、

②システム全体最適化を志向する技術アーキテクチャ, ③新技術リスク評価手続等を整備し, それらに基づいたリスク管理 PDCA に取り組むことが前提. 監査部門は組織全体の PDCA サイクルを検証・推進する役割を担う.

イ. CSA (コントロール・セルフ・アセスメント) への助言, 防止型監査

システム監査では, システム部門及び関連部門のリスク管理プロセスを検証し, 特に CSA で改善すべき点を助言すべきである. CSA が定められた手続をなぞるだけにならないように確認が必要.

更に, システムリスクが顕在化した際に内部影響にとどまらず, 顧客や外部機関に重大影響を及ぼすリスクを想定しているかの視点に立つ, リスク発生未然防止, 及び危機管理に関する監査が重要.

(4) 今後の展望と課題

今後, 新技術等の発明は枚挙にいとまがなく, 前述の通り, その適用業務は質・量とも急速に広がる事が展望される. 新技術の普及等のシステムリスク管理を巡る環境変化と, それに伴い高まるリスクに適切に対応する管理態勢を整備したうえで, 実際に成果を出しているか検証することが重要になる.

3. 支部会員間の意見交換

前述の報告内容を踏まえ, 支部会員間で以下のとおり意見交換を行った.

(1) 新技術等の導入に対するシステム・監査業務の留意点

- ア. システム部門には, 新技術等のメリットやリスクを適正に評価・報告する等, 経営層がリスクベースアプローチに基づいた IT ガバナンスを発揮できるように情報発信する責任がある. 一方, システム部門が役割を果たす環境をつくるのは経営陣の責任.
- イ. 新技術等のサービス利用にあたっては, 顧客目線での快適な操作性, 顧客とのリレーション全体への貢献等についての考慮が不可欠. 全社的な業務デザインが重要であるとともに, きめ細かく調査して顧客の声に耳を傾けることも必要.
- ウ. システム監査では, IT のみに注目するのではなく, 新技術を利用する「業務」におけるリスク管理のモニタリングが必要.

(2) 新技術等の導入に対するシステム・監査部門の人材育成

- ア. ユーザー企業の IT 人材の不足は深刻. システム部門は, 開発・運用等の専門性を有する人材育成に加え, 他部門や外部機関との有効な連携のため, 要員の視野を広げ, 危険予測やコミュニケーションのスキルアップに取り組むことが必要.
- イ. システム部門は, 次のシステム監査人を育てる役割も担う. システム部門における新技術等の導入を含むリスク管理策の企画や, システム検査等の経験はシステム監査スキルを持つ人材の育成に有効. 更に他部門や営業拠点等の IT 利用現場へのローテーションや, 要件どおりシステムを開発する以外の経験を積ませることが必要.

ウ. システム監査人は、新技術等による業務革新などの環境変化を適切に把握するため、IT と業務全般に関する専門的知識・スキルの向上に継続して取り組むことが必要。IT・業務双方のスキルを維持していくのは容易ではない。

(3) システム部門及び監査部門の今後のあるべき姿

ア. システム部門は、業務を革新するうえで、今後とも中核的な役割を担っていく。新技術等を利用した業務革新に係る他社動向、及び自社の対応状況を分析し、経営陣へ適時に報告するとともに、他部門と情報共有することが重要。

イ. システム開発・運用管理等を外部委託する組織が多くなっているが、システム部門はシステム企画、開発・運用管理に係る外部委託管理、及び緊急時対応など、自組織内に確保すべきスキルを発揮し、継承していく。スキル習得や継承のための具体的な方策は、各組織における工夫のしどころ。

ウ. 監査部門は、新技術等による業務革新の先行きを展望し、大規模化・複雑化していくシステムに伏在する重大なリスクを明らかにする一方で、収益機会を逃さない視点も必要になる。システム監査は、経営陣にとって「責任ある革新」の最後の拠り所となるべき。経営に役立つ監査の実践が求められる。

本年度は、西日本支部合同研究会、及び SAAJ 中部・北信越支部、JISTA 中部支部合同研究会をはじめ、当支部例会においても、「新技術等の導入に対するシステム部門や監査部門の在り方」について考える機会を多くいただいた。本年度最終の支部例会において、そのまとめとなる有意義な意見交換ができた。

今後も3ヶ月ごとの支部例会・研究会と合わせて、インターネットを活用した組織コミュニケーションの向上を図り、支部会員間で幅広く意見交換を行う活動を展開していきたい。

◇研究報告

「情報セキュリティ対策（運用と技術的対策）を考える」

報告者（会員番号 947 梶川 明美）

報告者が、情報セキュリティ対策の考え方を発表したうえで、支部会員間で技術的対策に関する考慮点や具体策について意見交換した。

1. 情報セキュリティ対策の考え方

情報セキュリティ対策は、情報セキュリティポリシーを作って実施、組織の構成メンバーに教育及び技術的対策を施すことが方策として考えられる。

技術的対策には目に見えるコストが必要なこともあり、組織の現状を分析し、どこからどのように対策していくか、複数年計画を立てて考えていく必要がある。

「企業（組織）における最低限の情報セキュリティ対策のしおり」（独立行政法人情報処理推進機構セキュリティセンター）から情報セキュリティ対策の全体像を表形式で作成（次ページ参照）し、この検討に役立てられるよう整理したい。

2. 技術的対策に関する考慮点

- (1) 情報セキュリティの脅威（内部不正・ソフトウェア脆弱性・サービス不能攻撃・標的型攻撃等）及び情報システムの構成要素（サーバー・端末・通信回線等）の両面から網羅性を確保すべき。
- (2) 特に重要な情報に係る情報システムの構成要素は、複合機や特定用途機器等の見落としがないように情報データフローで把握すべき。金融分野では、ATM に存在する暗証番号等の「顧客の機密情報」を見落としした結果、預金の不正引き出し事案が発生。
- (3) 情報システムのライフサイクルである、①企画・要件定義、②調達・構築、③運用・保守、④更改・廃棄等において、技術的対策で考慮すべきことを明確にすべき。
- (4) 技術的対策の中軸である主体認証機能、アクセス制御機能、及びログ取得・管理機能等は、導入するのみでなく、適正な運用が特に重要。それらに係る「IT」「プロセス」の全体最適化は必須。
- (5) サイバー攻撃対策は、未然防止策（入口対策及び内部対策）を実施したうえ、実害防止策（出口対策）も講じる多層的なセキュリティ対策を実施し、最悪の事態を迎えるリスクを低減すべき。

情報セキュリティ対策の全体像		「企業（組織）における最低限の情報セキュリティ対策のしおり」（独立行政法人情報処理推進機構セキュリティセンター）から		
分類	No.	内容	具体的な運用方法	技術的対策（うっかりミス・故意への対応）
保管	1	重要情報がみだりに扱われないようにする	・封書やFAX・電子メールの誤送信に注意 ・重要情報を机の上に放置しない ・鍵付き書庫に保管し施錠 ・ちょっと席を外す場合や退社時	—
持ち出し	2	重要情報を社外に持ち出すときは、盗難・紛失対策をする	【情報の持出管理】 ・情報を持ち出しは許可制 ・持ち出す情報の記録をきちんととる 【紙媒体（書類等）】 ・社外では必要もなく鞆から出さない ・ファイルバインダーやクリアファイル／ホルダー等にきちんと綴じておく ・鞆は体から離さない ・鞆を持っている時は居眠りしない 【電子記憶媒体（USB可搬記憶媒体等）】 ・データの暗号化（パスワードによるロック） ・媒体をなくさないための工夫（大きなタグを付ける、ストラップを付け体から離さない、落としてもすぐ分かるように鈴を付ける） ・媒体を入れた鞆は飲み会には持って行かない 【パソコン（ノートPC、タブレット、スマホ等）】 ・パソコン等を推測されないパスワードで保護（ログインパスワードの設定やBIOSパスワードロック） ・格納されたHDDを丸ごと暗号化	【携帯電話】 ・キャリア等のリモートロックサービス 【電子記憶媒体】 ・各ポートやドライブをふさぐ ・強制的に暗号化するソフト 【パソコン等のハードディスク】 ・暗号化ソフト
事務所	6	退社時に盗難防止対策	・机の上の備品やノートパソコンを引き出しに片付けて施錠	・ワイヤーロックを使用（工具で容易に切断できるが） ・ロッカー、キャビに収納・施錠 ・シンクラ、HD暗号化 ・場所のセキュリティを上げる（内外の監視カメラ、入退室）
	7	最終退出者は事務所の施錠を管理	・事務所を施錠 ・退出の記録（日時、退出者）を残す ・机の上の大事な書類チェック ・パソコンの電源チェック ・コピー機やシュレッダーの電源チェック ・消灯・施錠チェック	・入口の施錠と退出記録はセキュリティ会社との契約
パソコン	8	常にソフトウェアを安全な状態にする	・Windows Update ・IPAの脆弱性対策情報ポータルサイト参照	—
	9	ファイルが流出する危険性が高いソフトウェアの使用を禁止	・ファイル交換ソフト（Winny他多数存在）を入れない ・フリーソフト、私物ソフトは危険 ・自宅で使用するパソコンで会社の情報を処理しない	・管理者権限でのログインをさせない
	10	業務で個人パソコンを使用することは是非を明確にする	・社内外での個人パソコンの業務使用を許可制にする ・会社が用意した電子メール環境、リモートアクセス環境、会社の記憶媒体以外は使用しない ・ログインパスワードを設定	・業務使用の個人パソコンに暗号化などの情報セキュリティ対策を施す
	11	退社時にパソコンを他人に使われないようにする	・パソコンの電源を落とす ・離席時にはパソコンにロックをかける	—

以上
[＜目次＞](#)

支部報告【北信越支部 2016 年度研究報告】**「環境変化に対応するシステム開発管理態勢の整備とその監査について」**

会員番号 1739 小嶋 潔

近年新たなIT技術の普及は目覚ましい状況にあります。北信越支部では、西日本支部合同研究会に向け、情報システムを取り巻く環境変化や、新技術導入に伴うリスクへの対応事例について情報収集したうえで、システム開発に係る管理態勢の整備とその監査のあり方について意見交換や検討を行いました。その結果について報告いたします。

I. 情報システムを取り巻く環境の変化**1. 情報システムを取り巻く内外環境の変化****(1) インターネットや携帯電話を介した取引等による新チャネル・新技術**

ア. 顧客は、リアル店舗と同レベルのサービスを新たなチャネルに求めています。

ITの使い勝手の悪さは顧客満足度の低下を招き、顧客とのリレーション全体の悪化に繋がり、企業経営においてITの重要性は益々高まっています。

イ. システム構成が複雑化し、システム障害が発生した際の影響は甚大ですし、障害復旧が遅延した場合には、業務上重大な支障が生じることになります。

ウ. クラウドやタブレット端末等、新技術の普及は目覚ましい一方で、新技術の導入にあたり、導入目的をあいまいにした場合や、運用管理等の考慮が不足した場合には、期待する効果が得られないなどの支障が生じます。

(2) システム開発・運用における外部委託業務の拡大

外部委託先の障害により業務やサービスに影響。外部委託先の不正行為や人為的ミスによる重要情報の漏洩時には、委託元企業も責任を問われます。

(3) システムリスク管理態勢の整備に向けた社会的要請の高まり

- － 顧客情報保護（個人情報保護法、マイナンバー）
- － 業務継続態勢（新型インフルエンザ、東日本大震災、サイバー攻撃）

サイバー攻撃や被災に起因するシステム障害による業務停止、重要情報漏洩への対応不足は、訴訟や経営危機にも繋がるコアリスクとなっています。

2. 新技術の普及とリスクの発生**(1) 新技術導入を伴う失敗プロジェクト事例**

情報システムを取り巻く内外の環境変化は、すべからくシステム開発管理に影響しますが、なかでも新技術の普及は影響が大きく、例えば、近年導入例の多い①プライベートクラウド（サーバー統合基盤）、②シンククライアント（仮想デスクトップ）、③タブレット端末については、本番稼働後に様々な支障が生

じている事例も少なくありません。

①プライベートクラウド（サーバー統合基盤）

- ・当初期待していたほどコストが下がらない。想定外の費用が嵩んだ。

②シンクライアント（仮想デスクトップ）

- ・却ってパフォーマンスが落ちた。正常に稼働しないアプリがある。
- ・サーバー追加によるコスト増。サーバー障害時の障害影響範囲拡大。

② タブレット端末

- ・ビジネスモデル理解不足のまま導入したり、過度なセキュリティ面の対応により使い勝手が悪く、利用されないまま死蔵。

（2）まとめ

ア. 上記の3つは、現状では社会に変革を起こすような画期的な新技術とはいえないかもしれません。しかし、そのような技術でも個々の企業のシステムへのインパクトはそれなりに大きく、経営や業務における導入の目的・ねらいを曖昧にした場合には、期待される成果を出すことはできません。

イ. 新しい技術に基づくシステムにおいては、当然考慮すべきリスクやコストが従来のシステムに比べて増えることを覚悟する必要がありますが、目新しさや流行に目を奪われ、初めに導入ありきでプロジェクトがスタートしてしまうと、検討洩れが発生したりして、開発過程での大きな手戻り、稼働後の不具合発生リスクが高まることになります。

ウ. システム開発において「適切な実装」をしても、運用管理等の考慮が不足し「適切な運用やアクセス管理」が行われない場合は、情報の内容に直接関わる品質(信頼性)や非機能要件は達成できません。

II. 新技術導入に伴うリスクへの対応事例

1. 新技術導入に伴うリスクへの対応事例

新技術導入を伴う開発プロジェクトにおいて、リスクを回避、または軽減することに成功した事例について情報交換したところ、会員の所属する企業での成功事例には、以下の2つの共通点があると考えられました。

- ① 新技術のブームに流されず、経営陣の参画の下、導入のねらいを明確にした。
- ② 開発部門とユーザー部門及び運用部門とが連携し、運用管理やセキュリティに係るリスクを評価したうえで、適切な対応策を講じている。

（1）全体最適化の取組

以上のとおり、リスク評価を適切かつ綿密に行い、想定されるリスクへの対策を事前に構築しておくことが必要だと思います。さらに加えてシステム開発管理を効果的に行うには、個々の開発プロジェクトで新技術のリスク評価による対応策を実施するだけでなく、企業としてシステム構造の標準や技術アーキテクチャを定め、情報システムの全体最適化を維持する態勢を整備していくことが、継続的にシステムを維持発展させていくためには必要であると考え、下記のような取り組みを行っています。

「システム構造の全体最適化プロジェクト」

- ・情報システムに関するルールを社内標準化、現行システムのアーキテクチャを汎用化して明文化する
- ・技術アーキテクチャの対象領域をプラットフォームやアプリケーション、運用等について適宜見直す
- ・全体最適化プロジェクトを人材育成の場ともすることで、情報セキュリティ管理要員の育成取組み

Ⅲ. システム開発管理態勢の整備

前出の「環境変化とリスク」、「新技術導入に伴うリスクへの対応事例」に基づき、当支部で検討した「環境変化に対応するシステム開発管理態勢の在り方」を以下に示します。

- (1) 経営陣や上級管理者の参画
- (2) システムリスク管理の前提となる組織体制の整備
 - ア. 情報保護やシステムリスク管理に関する基本方針の策定、イ. 組織体制の整備、ウ. 社内規程の策定、エ. 内部管理態勢の整備、オ. 情報セキュリティ人材の育成
- (3) 新技術の評価手続と、システム全体最適化（システムアーキテクチャ）
- (4) 対象システムのプロファイル（システム重要度、情報重要度）の定義と、それらに適合させて充足すべきセキュリティ要件の明確化
- (5) システム開発部門と、ユーザー部門及び運用管理部門との連携強化

Ⅳ. システム開発に係る監査の在り方

1. システム開発プロジェクト監査の目的

当支部の意見交換での議論では、プロジェクト監査の目的としては、大きく2つあって

- (1) QMS(品質マネジメントシステム)の改善 [QMSの適合性・有効性評価]
 - ・対象プロジェクトのシステム開発プロセスに関連する基準に対する適合性評価
 - ・開発プロセスに関する有効性評価
- (2) プロジェクトのリスク低減 [開発プロジェクトのリスク評価]
 - ・対象プロジェクトのリスク評価

⇒ 個別プロジェクトのQCD(品質、コスト、納期)面での成功に対するリスクマネジメント強化

※監査の効果的運営を行うためには、これらの監査目的に応じて監査を運営する必要があります。

2. システム開発プロジェクト監査の効果的運営

- (1) QMSの改善を目的としたシステム開発プロジェクト監査
 - ①対象プロジェクトの選定：各部署からプロジェクトを選定（各部署を網羅しサンプリング）
 - ②実施タイミング等：QMS内部監査として年2回定期的に実施
 - ③主要チェックポイント
 - ・ISO9001規格を軸にQMSフレームワークに従って監査
 - a. 外部及び内部の課題、利害関係者のニーズ及び課題をどう捉え、リスク及び機会を決定しているか。その取り組みをどう評価し、結果がどうであったか。
 - b. 設定されている目標は適切、妥当なものか。進捗状況はどうか。目標達成に向け進捗管理をどう行っているか。結果がどうであったか。

c. パフォーマンス評価の結果を改善にどのように活かしているか。

(2) プロジェクトのリスク低減を目的としたシステム開発プロジェクト監査

①対象プロジェクトの選定

- ・ 重点プロジェクト（規模-ビジネス売上/損益、新規性[技術/業務/利害関係者等]、大規模改修）

②実施タイミング等

- ・ 重点プロジェクトの工程毎に実施。リスク大プロジェクトに対する工程段階に応じたプロジェクト監査や第三者検証（プロジェクトマネジメント計画書をベースにプロジェクト監査計画を策定）

③主要チェックポイント

[立ち上り段階]

- ・ 商談発生時-QCD面での対応力、リスク評価・リスク対策評価
- ・ 見積時-より詳細化しQCD面での対応力

[計画段階]

- ・ 受注時-契約書・契約条件書の第三者評価、プロジェクトマネジメント計画書の第三者評価

[実行段階]

- ・ 定期的なプロジェクトのQCD面での状況報告、リスク評価・リスク対策評価
- ・ 工程完了判定時- QCD面での状況評価、・ 出荷判定時- QCD面での状況評価、

[終結段階]

- ・ QCD面での実績、計画との差異評価、今後の改善点検討、成功事例/失敗事例の横展開

V. 今後の展望 –金融分野におけるFinTech利用等–

1. 金融分野におけるFintech利用について

(1) Fintech とは

FinTechとは、FinancialとTechnologyとを組み合わせた造語で、ITを駆使して、新しい金融サービスを生み出したり、顧客目線でサービスを見直ししたりする動きのことです。取扱うサービスは、FinTech企業が提供する多様な新技術の導入を前提としています。

(2) Fintechのサービス分野

- ・ 【代理店業務】：モバイルやインターネットバンキングなど、顧客との接点をFinTech企業が担当し、実際の銀行業務は既存銀行に委託
- ・ 【モバイルバンキング】：生体認証ログイン、モバイルでの口座開設など
- ・ 【個人資産管理】：データアグリゲーションを行い、複数の金融機関から利用者の情報を集めて分析
- ・ 【送金・決済業務】： 個人間送金やモバイルペイメントなど
- ・ 【貸出業務】：インターネット上でスピード審査を行う。マーケットプレイス貸出と呼ばれる業者では、借り手と貸し手をオンラインで結びつける
- ・ 【仮想通貨】：ビットコインの電子帳簿であるブロックチェーンを利用する
- ・ 【人工知能（AI）】：運用等のロボアドバイザー、コールセンター業務支援

- ・【その他のキーワード】：ビッグデータ、チャネル、カード、IoT、ソーシャルメディア

2. Fintechの本格展開に向けて

(1) Fintechへの取組方針の在り方

米国 通貨監督庁が、本年3月に発行したFintechに関する白書の基本的な考え方は、「責任ある革新」。Fintech技術を利用したイノベーションはおおいに奨励するが、同時に、金融機関の健全性確保、消費者保護、プライバシー保護、マネーロンダリング対策、不公正な取引防止に責任を負いつつやるべき、という意味

(2) 今後必要とされる管理態勢の整備

ア. 一時的なブームに乗らない、銀行の戦略に合致したFintech戦略の採択

イ. 顧客目線での使い勝手/快適な画面遷移、有効なビジネスデザインの追求

ウ. オープンAPI ※ やブロックチェーン等、新技術に係るリスク評価と対策

※API : Application Programming Interfaceとは、コンピュータプログラムの機能やデータ等を外部の別プログラムから呼び出して利用するための手順やデータ形式等を定めた規約のこと

エ. Fintech企業に対する外部委託管理やサイバーセキュリティ対策の強化

(3) システム開発に係る監査におけるFintech対応

ア. 銀行経営に影響するような重大なリスクの発見と、是正に向けた助言

イ. 監督当局やセキュリティ関連団体等との連携による公助・共助の取組

VI. おわりに

1. システム開発管理態勢の整備について

個別のプロジェクトにおける進捗・品質管理は無論重要ですが、前提として環境変化を踏まえた開発管理態勢の整備に注力すべきです。経営陣の関与、新技術導入に伴う運用管理面の考慮、全体最適化の維持、開発部門と運用部門/ユーザー部門との連携等に不足がないよう、継続的な取組が必要です。

2. システム開発に係る監査について

システム開発に係る監査では、まず開発管理態勢が十分か確認し、必要に応じて態勢整備に向けて助言することが求められます。また、QMSにおけるプロジェクト監査では、パフォーマンス向上の枠組として内部監査を活用し、有効性監査の成熟度を上げていく必要があります。本日の発表の中で取り上げたようなプロジェクト監査の実施により、QCDやQMS面での向上は十分に図られ、成果が上がっていくものと考えられます。

3. Fintechへの対応について

金融分野では、Fintechの動向が注目されています。①企業戦略との合致、②新技術導入に伴うリスク評価、③ Fintech企業の外部委託管理を着実に実践していく必要があります。ただし、「責任ある革新」を実現するためには、そうした自助の取組のみでなく、監督当局との連携による公助、セキュリティ関連団体等との連携による共助を活用していく必要があります。

実際日々技術が進歩していくなかで、外部委託やパッケージ利用もさらに進展していくでしょうし、技

術面やリスクの評価といった面で、特に中小企業個々による対応には限界があるのも事実ですが、解決法の1つとして共同システム参加企業による共同研究の動きも始まっています。個人的にも新しい技術への対応面でこれからの監査をどのようにすすめていけばよいか戸惑うこともあります。日本システム監査人協会の活動への参加等により知見を深めて、少しでも新技術に対応していければと考えています。

以上

<目次>

注目情報（2016.11～2016.12）**■「長期休暇における情報セキュリティ対策」を更新【IPA】**

IPAでは、従来から公表していた「長期休暇における情報セキュリティ対策」を、2016/12/15付けで更新しました。組織のシステム管理者向け、組織の利用者向け、及び家庭の利用者向けに、長期休暇前、休暇明けの対策について纏めています。年末年始の休暇前に必見です。

URL : <https://www.ipa.go.jp/security/measures/vacation.html>

■「第4次産業革命と情報連携-これからの情報活用とプライバシーを考える-」の講演内容を公表【JIPDEC】

JIPDECが、2016年12月6日に開催されたJIPDECシンポジウム「第4次産業革命と情報連携－これからの情報活用とプライバシーを考える－」での3つの講演についての講演内容を公表しました。

①「データ利用と情報管理」

講演者：JIPDEC 常任理事 坂下 哲也氏

URL : https://www.jipdec.or.jp/library/report/20161206_04.html

②「データは未来に何を伝えるのか？」

講演者：日本放送協会 報道局遊軍プロジェクト ディレクター 阿部 博史氏
東京大学大学院情報学環総合防災情報研究センター 客員准教授

URL : https://www.jipdec.or.jp/library/report/20161206_03.html

③「改正個人情報保護法の施行に向けた最新動向」

講演者：個人情報保護委員会事務局 参事官 小川 久仁子氏

URL : https://www.jipdec.or.jp/library/report/20161206_0.html

<目次>

【 協会主催イベント・セミナーのご案内 】

■ SAAJ 月例研究会（東京）

第 2 2 0 回	日時	2017年 1月 17日（火曜日）18:30～20:30（開場18:00）
	場所	機械振興会館 地下2階ホール
	テーマ	「A I とは何か? A I システムに対する監査の考え方」
	講師	産業技術総合研究所 人工知能センター 首席研究員 本村 陽一 様
	講演骨子	案内作成中。近日 H P で公表いたします。
	お申込み	近日 H P でご案内いたします。

■ 事例研究会【第 30 回システム監査実践セミナー】 予定

第 3 0 回	日時	2017年 1月 26日（木曜日）・27日（金曜日）
	場所	晴海グランドホテル
	テーマ	建設業におけるシステム運用に関する監査
	講師	吉田・畠中・（小佐野）
	詳細	https://www.saa-j.or.jp/kenkyu/jissenseminar/jissenseminar30.html

【 外部主催イベント・セミナーのご案内 】

■ 一般財団法人日本情報経済社会推進協会（JIPDEC） セミナー

日時	2017年1月17日（火曜日）13:30～16:15
場所	秋葉原コンベンションホール
中小企業向け改正個人情報保護法実務対応セミナー	
対象	中小規模企業の総務担当者 等
内容	改正個人情報保護法への実務対応 その1 情報管理の重要性について
お申込み	H P でご案内中です。 https://www.jipdec.or.jp/topics/event/2016kaiseiho-seminar.html?topbnr

協会からのお知らせ 【第16期通常総会のご案内】(速報)

会員番号 1760 斎藤由紀子 (事務局長)

日本システム監査人協会 (SAAJ) 会員各位**第16期通常総会のご案内**

日本システム監査人協会の第16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2017年1月末より、協会ホームページにて受け付けます。

記

1. 日時：2017年2月24日(金) 13時30分～ (受付開始：12:45)
2. 場所：東京都港区芝公園3丁目5番8号 機械振興会館 地下3階 研修1室
アクセス：<http://www.jspmi.or.jp/kaigishitsu/access.html>
3. 第16期通常総会議事 13時30分～15時
13:30開会
(1) 定款改定の件
(2) 2016年度 事業報告の件
(3) 2017年度 事業計画の件
(4) 2017年度 予算の件
(5) その他
15:00閉会
.....(休憩).....
4. 特別講演 15時30分～17時
15:30 開演
演題：「現代の情報化実践に伴うシステム監査の再考」(仮題)
講師：システム監査学会 会長 遠山 暁 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：予定)
懇親会費3,000円は、当日総会受付にてお支払ください。
19:00 閉場

以上

<目次>

協会からのお知らせ

【 CSA/ASA資格をお持ちの方へ：資格更新手続きについて 】

2017年度公認システム監査人及びシステム監査人補の更新手続きのお知らせです。

- ・資格認定期限が2016年12月31日で満了となる方について、認定の更新手続きを行います。
- ・資格更新申請の受付期間は2017年1月1日（日）から1月31日（火）までの1か月間です。
- ・今回の更新対象者は、資格認定番号が下表の方です（2014年度よりすべて2年度ごとの更新です）。

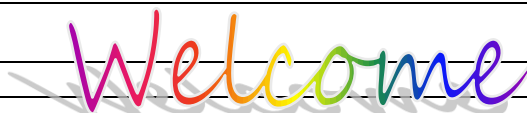
	取得年度	CSA 認定番号	ASA 認定番号	2017 年 1 月更新	ご参考 2018 年更新
1	2002 年度	K00001～K00253	H00001～H00193		○
2	2003 年度	K00254～K00320	H00194～H00263		○
3	2004 年度	K00321～K00357	H00264～H00316	○	
4	2005 年度	K00358～K00401	H00317～H00384		○
5	2006 年度	K00402～K00447	H00385～H00433		○
6	2007 年度	K00448～K00478	H00434～H00473	○	
7	2008 年度	K00479～K00518	H00474～H00514		○
8	2009 年度	K00519～K00540	H00515～H00538	○	
9	2010 年度	K00541～K00553	H00539～H00557	○	
10	2011 年度	K00554～K00568	H00558～H00572		○
11	2012 年度	K00569～K00580	H00573～H00586	○	
12	2013 年度	K00581～K00596	H00587～H00595		○
13	2014 年度	K00597～K00606	H00596～H00602	○	
14	2015 年度	K00607～K00615	H00603～H00618		○

- ・資格更新申請には、更新申請書や継続教育実績申告書などの提出が必要です。準備をお願いします。
- ・更新手続きの詳細は、HP の「CSA の資格をお持ちの方へ」(<http://www.saaj.or.jp/csa/forCSA.html>)をご覧ください。

以上

<目次>

【 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、見学也大歓迎です。

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

- ・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

- ・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>

【 S A A J 協会行事一覧 】 赤字：前回から変更された予定				2016.12
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	
12月	1：2017年度年会費請求書発送 1：個人番号関係事務教育 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：総会開催予告揭示 19：2016年度経費提出期限	7：第219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	2：北海道支部総会 10：東北支部総会 & 講演会	
1月	9：総会資料提出期限 16：00 12：理事会：総会資料原案審議 28：2016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	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〕	6：支部会計報告期限 25：SAAJ 創立記念日	
2月	2：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：年会費納入期限	1～3/31：CSA・ASA 春期募集	24：第16期通常総会	
3月	1：NPO事業報告書、東京都へ提出 6：年会費未納者宛督促メール発信 9：理事会	上旬：CSA・ASA更新認定書発送		
4月	13：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 A S A 認定証発行	未定：春期情報技術者試験	
5月	11：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		
過去に実施した行事一覧				
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	
7月	5：支部助成金支給 14：理事会	20：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 15-16：第28回システム監査 実務セミナー（東京：晴海）	24-25：SAAJ 中部・北信越支部 JISTA 中部合同研究会 in Nagoya	
10月	13：理事会	7：第217回月例研究会 22：関東地区主催新会員向け SAAJ 活動説 会（東京：茅場町）	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	12,19,26：秋期 CSA 面接 15：第218回月例研究会 17～18：第29回システム監査 実務セミナー（東京：晴海） 20：CSA・ASA更新手続案内 〔申請期間 1/1～1/31〕 29：IT アセスメント研究会 30：CSA 面接結果通知	5-6：西日本支部合同研究会 in Matsue （開催場所：松江）	

<目次>

【 会報編集部からのお知らせ 】

1. 会報テーマについて
2. 投稿記事募集

□ ■ 1. 会報テーマについて

2017 年度の年間テーマは、調整中です。2017 年 2 月号の記事募集の際にご案内させていただきます。

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。

□ ■ 2. 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/>

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>