認定NPO法人

日本システム監査人協会報

2016年11月号
No 188

— No.188（2016年11月号）<10月25日発行> ——————————

今月のテーマは

「システム監査の効果的活用」です。

システム監査を効果的に活用していくには、
どうすればよいのでしょうか？
ちょっと考えてみませんか・・・・

写真提供：仲会長

巻頭言

『「つながるシステム」とシステム監査』

会員番号 608 三谷 慶一郎（副会長）

IT が急速に発展し、コモディティ化していくことによって、新しいサービスを立ち上げ、グローバルに展開することのハードルが低くなってきています。最近よく話に出る、個人宅の空き部屋を貸し出す民泊のマッチングサイト「Airbnb」や、個人の自動車による配車サービスを行う「Uber」等がその典型例です。

このような状況を追いかけていると、複数のシステムがつながって新しいサービスが生まれていることをよく見かけます。例えば、航空会社やレストラン、ホテルのサービスが Uber のサービスを取り込むことによって、顧客が自社サービスを予約した瞬間に、自宅から空港まで、レストランまで、ホテルまでの移動について自動的に配車を行うようになっているわけです。近い将来、様々なサービスが有機的に結合することによって、より高度なサービスがより容易に作りだすことができるようになるでしょう。

とても素敵な未来ではありますが、システム監査人の視点から見るとここにも新しいリスクが出現しそうです。システムとシステムが連携することは、今でも珍しいことではありませんが、そのほとんどが自社内のみか、関係の深いプレイヤー間に閉じたものが多く、様々な独立した主体が保有するシステムを、動的につなげていくことはあまりありません。

複数主体のサービスが融合して構築されたサービスの信頼性はどのように確保すればよいのか、障害時の責任分担はどう考えるのか、主体毎にセキュリティポリシーが異なるときはどのように評価していくべきなのか等、様々な論点がありそうです。

リスクが多様化して広がっていく社会においては、第三者としてそれを評価するシステム監査人の存在意義は増していくに違いありません。是非議論を進めていきましょう。

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>

2016.10

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ITの利活用を評価する「ITアセスメント」を研究することは大きな課題である（表1）。また、独立行政法人情報処理推進機構（IPA）は、「“システム監査技術者試験（AU）”において期待する技術水準」のなかで、ITガバナンスの向上やコンプライアンスの確保に寄与する技術水準を求めている（表2）。

作家の橘玲氏は、“自由で効率的な情報社会の到来は、すべてのひとに自分の得意な分野で評判を獲得する可能性を開いた。・・・だとしたら必要なのは、その評判を収入につなげるちょっとした工夫だ。”と書いている。当協会の会員は、システム監査を核にした活動をしている。これからは、自由で効率的な情報社会の中で、「ITアセスメント」を行う「ITアセッサ」として大いに「評判」を獲得して、ビジネスにつなげるよう、日々、工夫していくことが大切だと思う。（空心菜）

（表1）

「ITガバナンス(JIS Q38500:2015)」の6原則	「情報セキュリティガバナンス（JIS Q27014:2015）」の6原則
①責任	①組織全体の情報セキュリティを確立する
②戦略	②リスクに基づく取組みを採用する
③調達	③投資決定の方向性を設定する
④パフォーマンス	④内部及び外部の要求事項との適合性を確実にする
⑤コンフォーマンス	⑤セキュリティに積極的な環境を醸成する
⑥人間行動	⑥事業の結果に関するパフォーマンスをレビューする

（表2）

IT ガバナンスの向上やコンプライアンスの確保に寄与するために、ビジネス要件や経営方針、情報セキュリティ・個人情報保護・内部統制などに関する関連法令・ガイドライン・契約・内部規定などに合致した監査計画を立案し、それに基づいて監査業務を適切に管理できる。

参考：「残酷な世界で生き延びるたったひとつの方法」橘玲 著　幻冬舎文庫

（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>

2016.10

めだか　【「リスク・フォーカス、フォワード・ルッキング」アプローチ（システム監査の効果的活用）】

システム監査を効果的に活用するには、どうしたらよいのか？　これは、システム監査が誕生して以来の永遠の課題かもしれない。

金融業界における監査の歴史を振り返ってみると、これまで「検査から監査へ」「プロダクト監査からプロセス監査へ」など、監査の効果的活用を図るために、監査の手法も高度化してきた。そうした中、最近金融業界で言われるようになってきたのが、「リスク・フォーカス、フォワード・ルッキングな監査」である。「リスク・フォーカス、フォワード・ルッキングな監査」として言われているのは、以下のような監査スタイルである。

（１）リスク・フォーカス（Risk-focused）な監査

監査資源には限りがあることから、「システム監査の効果的活用」のためには、深刻な問題が潜んでいる分野や、将来大きなリスクが顕在化するおそれのある分野に、監査資源を効果的に投入することが重要になる。

そのためには、「被監査部門におけるリスク管理状況等を把握した上、リスクの種類・程度に応じて、頻度・深度に配慮した効率的かつ実効性のある内部監査計画を立案し、状況に応じて適切に見直すとともに、内部監査計画に基づき効率的・実効性ある内部監査」（金融庁「主要行等向け総合的な監督指針」）を実施する必要があるとされる。

（２）フォワード・ルッキング（Forward-looking）な監査

従来の監査は、問題が発生してから、なぜその問題が発生したのかの原因を解明し、対応策を考えるという事後チェックが基本となっていた。しかし、既に発生している問題に対する事後チェックでは遅いということで、リスクが顕在化する前の事前予防に重点を置いた監査が求められるようになってきている。「事後チェック型監査から未然予防型監査」への動きである。

こうしたことから、金融機関では、内外の動きを踏まえてリスクが顕在化する前に監査スケジュールを組み換えるなど、機動的な監査態勢の整備に力が注がれてきている。また、実際の監査活動においても、実地監査だけでなく、日常のオフサイトモニタリング活動が重要性を増している。

こうした「リスク・フォーカス、フォワード・ルッキングな監査」は、まさに「言うは易く、行うは難し」であるが、システム監査として目指すべき方向ではあろう。

試行錯誤が続くとは思うが、「リスク・フォーカス、フォワード・ルッキングな監査」を目指して、引き続き活動していきたい。

（やじろべえ）

（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>

2016.10

投稿　【　システム監査の活性化　】

会員番号 0557　仲 厚吉（会長）

「システム監査」は、情報システムの信頼性、安全性、有効性について、独立した立場から監査し、当該システムの責任者に報告し、あわせて、報告書の公表により、システム責任者の社会的説明責任を果たすことを支援する活動ですが、「ITアセスメント」は、「ITガバナンス」の6原則（経営責任、戦略性、調達、有効性、準拠性、人間行動）の課題や、「情報セキュリティガバナンス」の6原則の課題を洗い出し、ITの利活用へ評価を行い、経営層に助言し、IT利用者のニーズに応えていく活動になります。

当協会の「ITアセスメント」は、「システム監査」を核として展開していくため、「システム監査の活性化」につながるものです。当協会は、「ITガバナンス」、「ITアセスメント」、評価を行う「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。会報187号「巻頭言」で、「ITアセスメント研究会」主査の松枝憲司副会長は、「ITアセメント研究会」を立ち上げるため会員の皆様に、次のように呼びかけています。「ITガバナンス」を広く普及させ、企業等に有効に活用を図る方策を検討していきますので、会員の皆様のご協力をお願い致します。

以上

SAAJの新たなビジョンに対する具体的な活動の一環として、ITアセメント研究会を立ち上げていく予定です。現在想定している主な研究テーマは、以下のとおりです。

1．ITガバナンス関連

(1) JISQ38500：2015の活用の検討

ITガバナンスを広く普及させ、企業等に有効に活用を図る方策を検討する。その結果としてITガバナンスに関するアセスメントへのニーズの高まりに繋げる。

(2) ISO38500関連基準及びISO38500：2015の日本語化の検討

上記(1)のJISQ38500の活用を図るうえでは、その関連基準であるISO38501,38502、38504,38505等の理解は不可欠である。また現在のJISQ38500はISO38500：2008をJIS化したものであるが、既にISO38500：2015が発行されており、この日本語化も必要である。

(3) ISO38503（Assessment of the governance of IT）のISO化の支援

ITガバナンスのアセスメントに関する基準であり、過去数年に渡って行ってきたISO化の支援を継続する。

2．システム管理基準の改訂の検討

現行のシステム管理基準については、経済産業省に動きがなく、現状のままでは利用価値が低下するばかりである。このテーマに関しては、システム監査学会とのコラボレーションにより実現させていきたい。

以上について、進め方等を固め次第、会員の皆様に参加募集を予定しています。奮ってご参加ください。

<目次>

2016.10

投稿　【 基礎自治体のシステム・トラブルに見る、自治体のシステム運用・監査の課題<第 3 回> 】

会員番号 1566　田淵 隆明

本会の会報 173 号及び 177 号において、2014 年 8 月 4 日に発生した某基礎自治体の基幹システム(外部のデータ・センタのクラウドを使用)が丸一日停止した問題について報告させて頂いた。それらの内容は、本会の 2016 年 1 月の近畿支部の月例研究会でも発表させて頂いた。今回は、その後、重要な進展があったので、報告する次第である。

§1.発生したシステム・トラブルの概要

2014 年 8 月 4 日、東京都心からほど近い某基礎自治体の基幹システム(外部のデータ・センタのクラウドを使用しており、他の 3 つの基礎自治体との共同利用システム)が丸一日停止し、住民票の発行や転入・転出の受付、婚姻届・出生届の受理などの重要業務が停止した。原因調査の結果、以下のことが判明した。

①システム停止の原因は、Web システムの手前の負荷分散装置(Load Balancer)が過負荷になっていた為であり、その原因はファームウェアのバグであった。

②負荷分散装置自体は二重化していたが、本番系→待機系への切り替えも失敗し、即時復旧が出来なかった。

③通常、過負荷の場合、システムの再起動により解決することが多いが、負荷分散装置のみ他の 3 基礎自治体と同一の筐体上にあり、いわば”一連托生”状態になっていた。**その為、他の基礎自治体への影響を回避するため、他の基礎自治体の業務終了時刻まで再起動を待たねばならなかった。**

※1.再起動により、システムの当該不具合は解消された。

※2.負荷分散装置以外の、DB サーバ、アプリ・サーバ、Web サーバは”一連托生”になっていなかった。
なお、2015 年 6 月にシステムの改修が実施され、負荷分散装置の”一連托生”状態は解消された。

※3.データベースの暗号化(トラッシング対策)は対策済みであることが判明した。

システム監査人の立場から言えば、①については「ファームウェアの時差更新の徹底」が望まれるところである。また、③については SPF(Single Point of Failure)が生じている。これは設計上の欠陥であり、それを見逃したシステム監査人の責任は重大であると言わざるを得ない。

§2.その後の経過

本年 1 月に「マイナンバー制度」(社会保障・税番号制度)が施行されたが、肝心のマイナンバーの「カード管理システム」においてトラブルが断続的に発生し、マイナンバーの発行が大幅に遅延する事態が発生した。また、国民年金機構の大規模な情報漏洩事件もあり、国民の間では、基礎自治体の期間システムの安定運用について非常に関心と懸念が高まっている。

本件の事案については、当該基礎自治体住民の生活にとって非常に重要なことであるので、その後、5 回

(2014 年 10 月の決算委員会、2015 年 3 月の予算委員会、2015 年 10 月の決算委員会、2016 年 3 月の予算委員会、及び、2016 年 10 月の決算委員会)で取り上げられた(いずれも、企画総務委員会所管質疑)。2014 年 10 月の決算委員会、及び、2015 年 3 月の予算委員会で判明したことについては第 173 号を、2015 年 10 月の決算委員会で判明したことについては第 177 号をそれぞれご覧頂くこととして、ここでは、その後の進展について取り上げることとする。

まず、当該基礎自治体では、共同利用している他の 3 基礎自治体と協議の上、**2015 年 6 月にシステム改修を実施し、負荷分散装置の"一連托生"を解消**した。**今後同様の過負荷が発生した場合は、直ちに再起動が可能となり、MTTR は大幅に改善**されることとなった。

また、再発防止及び総務部情報政策課職員のスキル向上の観点から、当該基礎自治体の「ICT 人材育成計画」を改定し、情報処理試験の受験の奨励、情報処理試験の有資格者の積極的登用を開始した。また、CIO アドバイザーに「システム監査技術者」取得者だけでなく「公認システム監査人(CSA)」取得者も加えるなど、体制の強化を実施している。

§3.2016 年 3 月の予算委員会での進展

2016 年 3 月の予算委員会では、以下の進展が判明した。情報政策課の迅速なる対応に敬意を表したい。

①「情報セキュリティ基本法」の改正により、「情報処理安全確保支援士」の制度が創設されることを踏まえ、人材育成指針を改定した。

②総務部情報政策課の職員に、「情報セキュリティ・マネジメント試験」、「情報セキュリティ・スペシャリスト試験」などの受験をさせている。

③CIO アドバイザーには、引き続き、「システム監査技術者」、「公認システム監査人(CSA)」を確保している。

§4.2016 年 10 月の決算委員会での進展

2016 年 10 月の決算委員会では、以下の進展が判明した。

①総務部情報政策課の職員に、「情報セキュリティ・マネジメント試験」、「情報セキュリティ・スペシャリスト試験」などの受験をさせている。

②CIO アドバイザーには、引き続き、「システム監査技術者」、「公認システム監査人(CSA)」を確保している。

③総務部情報政策課の職員(複数)を、外部ベンダーが開講する情報セキュリティに関する専門研修や、**実戦的サイバー防御演習に参加**させ、実務上必要な知識・技術を習得させている。それを下に、**庁内で実践的訓練も定期的に実施中**している。

④外部の情報セキュリティの専門家(有資格者)を招聘して、定期的にシステムの情報セキュリティの評価を実施している。

特に、**情報政策課の担当職員を③の実戦的サイバー防御演習への参加させている**ことは特筆すべきことである。ともすれば外部ベンダーへの技術面での依存度が高いと指摘されることの多い基礎自治体においては珍し

いことと思われる。本会の会員にも、総務省や地方自治体関係の方も少なくないと思われるが、この基礎自治体の対応は大変参考になると思われる。

§5.今後の残された課題

当該基礎自治体の場合、DB のバックアップは毎日取得しており、アーカイブ・ログの保持により、障害発生時にはロール・フォワード処理により直前復旧が可能である。また、データベース自体のミラーリングを実施している。しかし、バックアップ媒体の多重化・遠隔地管理は未実施であり、2018 年度に新データ・センタを設置するのに合わせて、相互に遠隔地管理の体制を整えるとしている。

しかし、近年の台風の大型化・ゲリラ豪雨の頻発化等の災害の増加を考えると、2018 年度までの暫定策として、バックアップ媒体の二重化及び別室保管などの対策は講じられるべきである。

同様の問題を抱えている基礎自治体も少なくないようであるが、「過疎過密」などの自治体間格差の問題が指摘される中、他府県の友好都市との間でのデータの相互的「遠隔地バックアップ保管」なども、今後、鋭意検討するべき課題であろう。

§6. 全国の基礎自治体のシステム運用における課題

今回取り上げた基礎自治体のケースは、全国の基礎自治体の平均像からすればかなり優秀なほうである。特に再発防止策の策定の迅速さ、及び、人材育成の強化などは特筆に値する。確かに、**当該基礎自治体は、いわゆる"富裕層"も多く、比較的税収に恵まれた基礎自治体であるが、それと同時に、情報政策課長が元 IT 会社勤務であったことが幸いしている**とも言える。この 2 年間、全国の地方自治体のシステムの運用・管理の状況を調査したが、やはり地方自治体のシステム運用に関しては、次の 2 点が大きな課題ではないかと思われる。

①地方自治体(都道府県・市区町村)を所管する国の機関は総務省である。通信事業は総務省の管轄である。その為、地方自治体の IT 施策自体が「通信」及び「セキュリティ」に重点が置かれがちであり、ITAC(IT 業務処理統制)や DB の整合性管理には注力される割合が少ない。

②多くの地方自治体において、情報システムは「総務部」や「総務課」の所管となっており、採用区分が「技術職」ではなく「事務職」となっている。「ゆとり教育」の影響もあり、「数学の入試を経験していない大卒者」が少なからず情報システム担当となっており、情報システムの管理・運用がベンダー任せとならざるを得ないケースが少なくない。

※1.②については、2020 年度の大学入試より、私立も含めて「新センター試験」(5 教科必須)の受験が義務化されるため、「数学の入試を経験していない大卒者」は原則としていなくなることになる。また、数学と物理・化学の中間に位置する「理数探究」が 2022 年度より文系も含めて履修必修化されることとなり、「数学を知らない経済学部・法学部生」の問題も解消する見込みである。

※2.IFRS(国際会計基準)も数学の知識が必要になることが多いため、今後の我が国の産業競争力の強化のためには、この教育制度・大学入試改革は大変有効であると考えられる。

なお、上述したようにマイナンバーの「カード管理システム」では、本年 1 月以降、システム障害が断続的に発生した。本年 8 月に、地方公共団体情報システム機構（J-LIS）が、当該障害について、システム構築ベンダー側に最大 69 億円の損害賠償を求める方針を明らかにしたことが報道された。このことは甚だ遺憾なことであるが、再発防止のためにも、**システム監査の法令に依る義務化の早期実現の必要性**を再確認した次第である。少なくとも、公共性の高いシステムに関しては、最優先で取り組むべき課題である。

※医療機器に関しては、「医薬品・医療機器等法」(旧薬事法)の規定により、システム監査が義務付けられている。情報システムが公共・民間を問わず広範に普及していることを考えると、横断的な「システム監査基本法」のような立法措置よりも、省庁別・産業分野別のシステム監査を義務化する法改正のほうが現実的であると思われる。

終わりに、本件について、昨年来より引き続き、様々な示唆・助言を頂いた荒町弘氏、吉田博一氏、近畿支部のシステム監査法制化推進プロジェクトの神尾博氏、中田和男氏、横山雅義氏に深く御礼申し上げたい。

<<参考文献>>

1.「システム監査の法的義務化等の IT 政策提言」(田淵隆明、横山雅義、中田和夫、神尾博)
http://www.saajk.org/?cat=76

2.『新しい「IT 事業者評価制度」導入の政策提言』(中田和男，田淵隆明，神尾博，横山雅義)
http://www.saajk.org/wordpress/wp-content/uploads/saaj_20130706_thesis04.pdf

3.「『時事論評』IoT/M2M 時代のシステム監査」(神尾博)
http://skansanin.com/saaj/201503/201503SAAJKaihoNr168_toko1.pdf

4.「制御システムに対する不正アクセスの危惧」(日本セキュリティ・マネジメント学会 神尾博・安本哲之助)

5. SAP ジャパン　IFRS 支援室「エキスパート・コラム」(全 29 回)(田淵隆明)

6.「第 4 回山梨県の食品安全を考える会」(2016 年 2 月)講演録(中田和男)

7.「軽減税率」田淵隆明が語る、IFRS＆連結会計入門 ～"In Varietate Concordia", EU の知恵に学べ～
(ギャラクシー・ブックス 2015 年 7 月, Amazon オンデマンド)

8.「軽減税率」田淵隆明が語る、IFRS＆連結会計入門(Ver2) ～"In Varietate Concordia", EU の知恵に学べ～
(ギャラクシー・ブックス 2015 年 9 月, Amazon オンデマンド)

9.「軽減税率」田淵隆明が語る、IFRS＆連結会計入門(Ver3) ～"In Varietate Concordia", EU の知恵に学べ～
(ギャラクシー・ブックス 2016 年 3 月, Amazon オンデマンド)

10.「軽減税率」田淵隆明が語る、IFRS＆連結会計入門(Ver4) ～"In Varietate Concordia", EU の知恵に学べ～
(ギャラクシー・ブックス 2016 年 11 月, Amazon オンデマンド)

以上

（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>

2016.10

第 216 回月例研究会：講演録

【 顕在化しにくくなったサイバー脅威のリスクコントロール 】

会員番号 2581　斉藤 茂雄

【講師】株式会社サイバーディフェンス研究所　　専務理事　名和 利男 氏

【日時・場所】2016 年 9 月 7 日（水）18：30～20：30

【テーマ】「顕在化しにくくなったサイバー脅威のリスクコントロール」

【要旨】

サイバー攻撃は高度化・巧妙化し、かつ進展速度を上げてきている。そのためサイバー脅威は、我々の対応限界を遥かに超えたものとなっている。その結果、情報システムの現場では、サイバー空間利用における脅威及びリスクを実情に見合った形で見積もることが困難となり、日々発生するインシデント対応に追われている状況が見られる。

本講演では、なぜこのような状況に陥ってしまったのか、そして今後サイバー脅威のリスクコントロールをどのようにしていくべきかについて、サイバー空間における攻撃側と防御側の観点で考察する。

【講演録】

1．激変するサイバー攻撃メカニズム

（1）攻撃側と防御側の関係位置の変化

エベレストのような高い山への登山には高度な訓練が必要だが、サイバー攻撃の攻撃者がこのレベルだとすれば、防御側の大多数は、幼稚園児が砂場に作った標高 10cm の砂山で遊んでいるようなレベルであり、残念ながら私達のサイバー攻撃に対する本質的理解及び対処スキルのレベルは極めて低い。

（2）日本へのサイバー攻撃で利用される「日本特有の仕組み」

米欧の組織内ネットワークでは、その文化的な背景から、一人一人のアカウントに対して権限を厳格に定めている特徴がある。対して日本は、ある社員が休めば、他の社員がその仕事を代わることができるといったように、権限管理に甘いところがある。米欧でのマルウェア被害は 1 台の PC で納まることが多いが、日本では 1 台の PC が被害を受けるとまたたくまに内部ネットワーク全体に広がることがある。

（3）既成概念を覆す斬新な発想に基づく攻撃手法

最近の攻撃者は、マジシャンと同じような既成概念を覆す斬新な発想に基づく攻撃を行うことがある。昨年 12 月にウクライナの電力供給会社がサイバー攻撃を受け、8 万戸（実際は 12 万戸）の住居やビルが停電したと報道されているが、これなど人間を騙してマルウェア感染させた事例である。

2．注目すべき動向変化

（1）「標的型攻撃」「水のみ場攻撃」の増加

攻撃者が直接的に行う攻撃には、「なりすましメール」や「フィッシング詐欺サイト」などがあるが、2014 年のトレンドマイクロ社の調査では、マルウェア感染の 90%以上が標的型メールによるという情報があった。

またここ 1～2 年多くなっているものに、正規アカウントからのマルウェア感染がある。例えば会社の部下や上司、同僚からのメールを介するものだけではなく、配偶者や子供からのメールが乗っ取られているケースもある。

2015 年からは「水のみ場攻撃」が相対的に徐々に増えている。よく見ているサイトにアクセスするだけでマルウェアに感染するという攻撃である。一方この手法は国によっては不法分子を炙り出す目的で、あえて有用な情報を置いたサイトを立ち上げ、そこにアクセスした者を統計学的に分析しテロ活動を行う可能性のある者とみなし、諜報を目的としたマルウェアを感染させるという使い方もある。

（2）文書ファイルからのウイルス感染

今年 2 月にトレンドマイクロ社が報道発表しているが、マクロ型不正プログラムを含む文書ファイルを添付した標的型攻撃メールが急増している。この文書ファイルはソフトウェアとしてのマルウェアを一切使っておらず、コードとしてのマクロ（VBA 等）を使っているだけなので、Windows から見れば正規のプログラムが動作しているようにみえるため、一般のウイルス対策ソフトでは対策が難しい。

どんなに先進的な高い技術をしても見つけることができないという、それだけ攻撃者は技術レベルを上げているだけでなく、私達の先入観の裏をかいた攻撃を仕掛けている。

（3）USB 端子からの被害

最近は少なくなったが、一昔前は USB メモリを PC に差し込んだだけでウイルス感染する被害が多かった。USB 端子を使うものは他にも、マウスやキーボード、単なる充電に使うものなどがあるが、この形状に人間が騙される。差し込むと Windows が入力デバイス（キーボード）と認識し、勝手にコマンドを打ち込み、マルウェアをダウンロードするというものもある。こういったものが廉価で販売されているし、展示会やカンファレンスで配布される USB メモリにまれに仕込まれている場合があるので、注意を要する。

（4）攻撃者の手口

マルウェアに感染すると、攻撃者は PC の中の設定情報（IP アドレス、どこのホストと繋がっているか、パッチの適用状況等々）を「systeminfo」といったコマンドなどを用いて見つけ出す。この十数 KB 程度の情報にはその PC の多くの基礎情報が含まれるが、これを入手した攻撃者は、例えば OS のパッチの情報を見て、この PC で確実に動くマルウェアを作り出す。

1 台の PC が他の PC と通信していることが分かれば、攻撃者は取得したパスワードハッシュを用いて Pass-the-Hash 攻撃でネットワークログオンを成功させる。

SE はトラブルがあるとすぐに何台もの PC にログオンしなければならないので、管理者権限のパス

ワードを同じにする傾向がある。Windows10 未満の OS では、パスワードをハッシュ化し、1 回でも管理者権限で入るとそのハッシュが記録されており、攻撃者はこのハッシュを使って他の PC に入り込む。このことはマイクロソフト社やセキュリティベンダから口うるさく警告されているが、多忙な SE は社外で勉強する機会が少なく、ランゲージギャップもあり（情報の多くは日本語ではなく英語）、対策ノウハウや知見を身につけていない。

3．緊急対処支援の活動から見出されたこと

（1）情報の分散化と流通活性化

他組織との連携業務（サプライチェーンを含む）の効率化と意思決定の迅速化のために急激にネットワーク化が進んでいる。それに伴う情報資産の分散化と機械的機能の増加（人が入り込む部分の減少）が進み、そこに脆弱性が生じている。

現在多くの組織は PC サーバに出来合いの OS の下アプリケーションソフトウェアを稼働させ利用している。汎用ソフトウェアのお陰で、あまり技術力が高くないエンジニアでもメンテナンスが出来るようになっている。また、壊れにくくなっており、保守員の常駐も必要ない。一方では IT 予算が減らされ、少ない予算で高機能が求められる。そのため低賃金の技術者を採用したり、外部委託により人件費の削減を図っている。また、システム開発についても多層化して、２次請負、３次請負は常態化していると見られる。業務情報は各階層に必要であるが、末端に行くほど管理が甘い傾向があり、例えば末端の階層では自宅で業務を行うなど、攻撃者はいとも簡単に情報入手できる環境になっている。これは役務契約におけるサプライチェーンの問題と考えている。

（2）攻撃側の状況変化

昔のハッカーまたはギーク（おたく）と呼ばれた人達は裕福で、技術力の誇示や目先の利益の獲得のため、場当たり的にハッキングを行った。現代では若年層の経済的不安定と一部の困窮化による不平不満の増大により職業的ハッカーになっている人達がいる。

昔から貧富の格差が、戦争や革命、あるいは日本の場合一揆といった事態を発生させたが、現在はサイバーテロという形で現れているともいえる。また、これらに便乗した形の攻撃者もいる。

（3）侵入可能な入口の増加

IT 関係業務における役務のサプライチェーンなどから、ネット上の相互接続性・相互運用性の拡大による侵入可能な入口は増加している。自組織の IT 環境は堅牢でも、周辺からはあっさり情報が漏れる。特に SNS の多用で、誰と誰が繋がっているか、誰が今どこに居るのかといった解析が出来るような仕組みもあり、攻撃者はいつも情報を見ていると思ってよい。今はどうやって会社を守るのか、どうやって委託関係を守るのかといったことが課題になっている。

（4）CMS の脆弱性

コスト削減、コンテンツのリアルタイム更新の要請から Web サイト開発ツールとして CMS（コンテンツマネジメントシステム）が利用される。CMS には多くのプラグインが提供されているが、このプラ

グインに脆弱性を持つものが多い。そのため、攻撃者はこういった CMS ほどハッキングし易いことになる。わが国の Web サイトは世界的に見て、極めて脆弱性の多い Web サイトが多く、海外のハッカーがハッキングの教材にするほどであり、対策が必要である。

4．サイバー攻撃の実態解明で見出されたこと

サイバー空間においては軍事活動と同様、Kill Chain が実施可能な状態になっている。米空軍における Kill Chain とは米空軍オペレーションセンターで軍事作戦に採用されている「攻撃目標処理プロセス」のことであるが、サイバー攻撃者の観点で、APT（Advanced Persistent Threat）攻撃のシーケンスを、軍事作戦（攻撃者の活動）に当てはめたものとして、図のようなサイバー空間における Kill Chain が整理できる。

「サイバー空間における Kill Chain」　名和 利男 氏講演資料より抜粋

「予備調査」から「実行」までの流れはプロセスである。発見されるサイバー攻撃の挙動は各プロセスのいずれかの事象に当てはまる。システムの動きを見て、この挙動がどこのプロセスに位置づけられるのかを分析することにより、攻撃の活動が手に負えるのか、もう手に負えない段階なのかの見当がつく。大事なことは残念なことであるが、私達は攻撃者と同じ目線でシステムを見なければいけないということである。

5．学ぶべき教訓

（1）攻撃側と防御側の技術レベルの格差の急拡大

緊急対処支援の活動などから感じるのは、防御側の技術者は攻撃側の手口を理解しておらず、リスクコントロールが出来ていないことである。

攻撃側は私達以上に私達のシステムを知っている。例えば官公庁のシステムの調達では仕様書を公開するが、攻撃者は良く見ていると思われる。攻撃者は自分の多くの時間を攻撃のための技術の習得に費やすのに対して、防御側の私達には攻撃側には無い仕事として、上司への報告、予算の獲得といった仕事があり、ハンデキャップが多すぎる。技術の習得は業務時間以外の時間になり、どんなに頑張っても追いつかない現実がある。

（2）“情報セキュリティ”に偏重したコンサルサービスが存在

国内のセキュリティコンサルは、「情報の遷移」に着目したしたものが大多数である。情報資産を区分けして、管理策・防御策を講ずる学問的側面に意味が無いとはいわないが、「システム防護」をベースにしたセキュリティ対策には「サイバー脅威対処の豊富な経験」を活用したコンサルが必要で、それが国内には少ない。

もう一つの側面は、セキュリティ対策が個人情報や営業秘密情報の漏えいなど「情報漏えい」に重きをおいた対策に偏重していることである。しかしサイバー攻撃には「侵入させないこと」に重きをおいた対策も重要である。攻撃者には失敗も多く、その足跡はシステムの中に残る。また、攻撃者がコアの情報に辿り着くまでに相当長い期間を要しているといわれ、この間に攻撃への対処をすることが重要となる。通常、これらのインシデント対応は委託業者の仕事となるが、委託業者は頑張って仕事をするが、あくまで契約範囲内にとどまり、また予算的な面から高度な技術者の対応は難しく、十分な対応が出来ていないのが現実ではないだろうか。

（3）サイバー空間における脅威を適切に把握する必要性

サイバー空間における脅威を把握する場合、一般メディア等が発信する情報を鵜呑みにしてはいけない。特に日本語だけの情報では不十分で、真の情報は英語、ロシア語、中国語など外国語で発信されている。例えばリオオリンピックでのサイバー攻撃情報の多くはポルトガル語で発信されており、日本語だけの情報ではリオにサイバー攻撃は無かったかのような印象だがそれは大間違いである。

真の情報を得るには、オジリナル・レポーター（Original Reporter）が発信する情報を追求することである。オジリナル・レポーターの位置づけの一つに CSIRT（Computer Security Incident Response Team）がある。CSIRT は自らの問題に対処出来ない時、他の CSIRT の協力を仰ぎ対処することがある。サイバー空間では物理的距離はゼロなので、ここに協力した CSIRT は同様の事態に対処する経験を積むことになる。

CSIRT はサイバー攻撃の「火消し」の役割で、消防士のように弛まない訓練と対応能力が問われる。実際の火消しができなければ、名ばかりの CSIRT になるが、残念ながら管理者だけで構成される情報の集約窓口になっているケースが多い。

（４）サイバー空間における動向情報を積極的に収集する必要性

社内ネットワークの中でセキュリティ対策部門にいる技術者は、サイバー空間から見ればごく狭い小さな領域の中に存在している。セキュリティ対策には多くの情報が必要となる。しかし他社のネットワークの情報を知りたくても、それぞれ自社の情報は出せないという立場があり、情報流通は非常に難しい。そこで、外部の専門家コミュニティやセキュリティカンファレンスを活用するのが望ましい。専門家コミュニティを構成するファーストレスポンダーや捜査機関などに質問を投げかければきちんと答えてもらえるなど、動向情報を積極的に収集すると良い。

（５）攻撃経路を見出した上で、適切なセキュリティ対策をすべき

セキュリティ対策部門は攻撃の仕組みを理解することが重要で、しかもサイバー攻撃を「静的な絵」として理解するのではなく、組織全般に関わり、また時間経過の中で「動的ストーリー」として理解することが必要である。

日々のイベント（セキュリティ事象）やインシデントが適切に収集される仕組みが必要で、これには例えばインシデントの原因となった者を処罰するということではなく、インシデントを報告した者ほど評価を得るような業務慣習や企業風土も考慮することが必要となる。この場合組織内 CSIRT は信頼を構築するということが、平時の仕事ともいえる。

（６）すべてのサイバー攻撃対処に明確な目的を設定すべき

日本国内の対策は、「防御策（Protect）に偏重」しているため、いたずらにコストがかかってしまう状況がある。最近のサイバー防衛策におけるベストプラクティス（最善策）は、対処策（Respond）である。最低限のリスクを受容し、実質的な被害を発生させないことで、結果的に有効な防衛策となる。具体的には攻撃を完全に跳ね除けるのではなく、多層防御の概念で一部の侵入を許容するがそれ以上深く入り込ませない対応をとる。つまりサイバー脅威に対して、メリハリのついた対策を検討し、実装及び確実な運用をすることが重要になる。

【記録者所感】

今回のご講演では、名和氏の広範な活動内容とサイバー攻撃に立ち向かうという深刻な実践体験に基づく知見や事例の紹介をいただいた。また実演もまじえていただき、サイバー攻撃とその対応について非常に示唆に満ちた内容であった。

私自身は ISMS の監査などを担当してきているが、情報セキュリティへの対応が、情報資産を区分けして、“形式的に”管理策を講ずるだけの机上の対応となってしまっていることや、セキュリティ対策が個人情報や営業秘密情報の漏えいなど「情報漏えい」に偏重しているとのご指摘に対して反省の念を強く持った。

私のこの講演録では、今回のご講演の内容をとてもお伝えしきれていない。名和氏はマスメディアにも多く登場するし、ご講演の機会も多いので、是非機会があれば皆さまも直接ご聴講されることをお勧めする。

以上

<目次>

2016.10

【「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７回 】

会員番号 0557　仲 厚吉（個人情報保護監査研究会）

今月号では「第５章　個人情報保護委員会」を解説します。この章の内容はもともと番号利用法に規定されていたものですが、2015年９月９日の改正により、新個人情報保護法に移行され「特定」の文字が消えました。この章に限り、番号利用法制定時は黒字のままとし、新個人情報保護法に移行時に改定された内容を赤字で記載します。

第５章は、既に施行されています。ただし、例えば第59条は2016年9月現在第五十条として公表されており、この連載では、全面施行後の第59条としてご紹介しています。

また、2016年5月27日に「行政機関等の保有する個人情報の適正かつ効果的な活用による新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するための関係法律の整備に関する法律」によって改正されました。2016年5月27日の改正については、緑字で記載します。

ただし、この緑字の部分は未施行です。

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５章　個人情報保護委員会

第59条（設置）　　（旧番号利用法：第三十六条、現在第五十条）

内閣府設置法第四十九条第三項の規定に基づいて、個人情報保護委員会（以下「委員会」という。）を置く。

２　委員会は、内閣総理大臣の所轄に属する。

※　個人情報保護委員会は、日本版プライバシー・コミッショナーと言われています。「EU一般データ保護規則」　（GDPR：General Data Protection Regulation）では、EU全域で一つの欧州データ保護委員会（EDPB: European Data Protection Board）を置き、その傘下に各加盟国のデータ保護局（DPA: Data Protection Authority　プライバシー・コミッショナー）を置き、各国を相互に連携させることにより、個人情報保護のワンストップショップを実現しています。事業者やデータ主体（data subject（本人））は、個人データに係る係争について、EU各国の複数の機関に個々に申し出する必要がないとされています。

※　プライバシーマーク制度では、プライバシーマーク付与機関（JIPDEC)が、制度に係る基準等を策定し、適正に運用する役割を担っており、事業者からの事故報告書の徴収や、本人などからの苦情等への対応措置を実施しています。ただし、対象がプライバシーマーク事業者に限定されています。

第60条（任務）　　（旧番号利用法：第三十七条、現在第五十一条）

委員会は、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ること（個人番号利用事務等実施者（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号。以下「番号利用法」という。）第12条に規定する個人番号利用事務等実施者をいう。）に対する指導及び助言その他の措置を講ずることを含む。）を任務とする。

※　旧番号利用法においては、“国民生活にとっての個人番号その他の特定個人情報の有用性に配慮しつつ”と、個人番号利用事務実施者に対する指導及び助言等に限定していましたが、新個人情報保護法に移行したことに伴い、対象を広げています。

（赤字は追加された条文ですが、厳密な変更点については省略して表示しています。）

第61条（所掌事務）　（旧番号利用法：第三十八条、現在第五十二条）

委員会は、前条の任務を達成するため、次に掲げる事務をつかさどる。

一　基本方針の策定及び推進に関すること。

二　個人情報及び匿名加工情報の取扱いに関する監督、行政機関の保有する個人情報の保護に関する法律第二条第一項に規定する行政機関における同条第九項に規定する行政機関非識別加工情報（同条第十項に規定する行政機関非識別加工情報ファイルを構成するものに限る。）の取扱いに関する監視、独立行政法人等における独立行政法人等の保有する個人情報の保護に関する法律第二条第九項に規定する独立行政法人等非識別加工情報（同条第十項に規定する独立行政法人等非識別加工情報ファイルを構成するものに限る。）の取扱いに関する監督並びに個人情報及び匿名加工情報の取扱いに関する苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関すること（第四号に掲げるものを除く。）。

三　認定個人情報保護団体に関すること。

四　特定個人情報（番号利用法第二条第八項に規定する特定個人情報をいう。第６３条第四項において同じ。）の取扱いに関する監視又は監督並びに苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関すること。

五　特定個人情報保護評価（番号利用法第二十六条第一項　に規定する特定個人情報保護評価をいう。）に関すること。

六　個人情報の保護及び適正かつ効果的な活用についての広報及び啓発に関すること。

七　前各号に掲げる事務を行うために必要な調査及び研究に関すること　。

八　所掌事務に係る国際協力に関すること。

九　前各号に掲げるもののほか、法律（法律に基づく命令を含む。）に基づき委員会に属させられた事務

※　赤字は、新個人情報保護法に移行したときに追加されました。

※　緑字は、2016年5月27日に追加されました。

これにより、行政機関が保有する非識別加工情報は個人情報保護委員会の監視、独立行政法人等が保有する非識別加工情報は個人情報保護委員会の監督の対象となることが明確にされています。

※　緑字の部分は2016年9月現在未施行です

※　行政機関非識別加工情報や独立行政法人等非識別加工情報は、匿名加工情報とは異なり、照合禁止義務から除外されます。行政機関等では本人を特定することが業務であり、非識別加工情報と作成の元となったデータを照合する必要があるためです。

＝＝＝＝＝

※　第62条（職権行使の独立性）は、旧番号利用法第三十九条から改定されていないため省略します。

第63条（組織等）　　（旧番号利用法：第四十条から移行、現在第五十四条）

委員会は、委員長及び委員八人をもって組織する。

2　委員のうち四人は、非常勤とする。

3　委員長及び委員は、人格が高潔で識見の高い者のうちから、両議院の同意を得て、内閣総理大臣が任命する。

4　委員長及び委員には、個人情報の保護及び適正かつ効果的な活用に関する学識経験のある者、消費者の保護に関して十分な知識と経験を有する者、情報処理技術に関する学識経験のある者、特定個人情報が利用される行政分野に関する学識経験のある者、民間企業の実務に関して十分な知識と経験を有する者並びに連合組織（地方自治法（昭和二十二年法律第六十七号）第二百六十三条の三第一項の連合組織で同項の規定による届出をしたものをいう。）の推薦する者が含まれるものとする。

※　旧番号利用法では、委員六人、うち三人は非常勤とされていました。

※　“特定個人情報が利用される行政分野に関する学識経験のある者”の部分は、旧番号利用法では、“社会保障制度又は税制に関する学識経験のある者”と記述されていましたが、より具体的に整理されました。

＝＝＝＝＝

※　第64条（任期等）以降の第65条（身分保障）、第66条（罷免）、第67条（委員長）については、旧番号利用法（第四十一条～第四十四条）と変更はありませんので省略します。

第68条（会議）　　（旧番号利用法：第四十五条から移行、現在第五十九条）

委員会の会議は、委員長が招集する。

2　委員会は、委員長及び四人以上の委員の出席がなければ、会議を開き 、議決をすることができない。

（以下省略）

※　委員の定数が八人になったことに伴い、四人以上の出席が必要となりました。

第69条（専門委員）　　　（新設、現在第六十条）
委員会に、専門の事項を調査させるため、専門委員を置くことができる。
2　専門委員は、委員会の申出に基づいて内閣総理大臣が任命する。
3　専門委員は、当該専門の事項に関する調査が終了したときは、解任されるものとする。
4　専門委員は、非常勤とする。

※　専門委員とは、事故や紛争など専門的な知識を必要とする訴訟において、審理の充実・迅速化を図るために、争点整理など手続きの早い段階から専門家の協力を得ることができるようにした制度です。2003年7月に、民事訴訟法第五章第二節に規定され、その任免に関し必要な事項は、最高裁判所規則に定められています。

＝＝＝＝

※　第70条（事務局）、第71条（政治運動等の禁止）、第72条（秘密保持義務）、第73条（給与）　は、それぞれ、旧番号利用法の第四十六条～、第四十九条から移行されました。内容に改定はありませんので、省略します。

第74条（規則の制定）　　　（新設、現在第六十五条）
委員会は、その所掌事務について、法律若しくは政令を実施するため、又は法律若しくは政令の特別の委任に基づいて、個人情報保護委員会規則を制定することができる。

※　2016年7月15日に「個人情報の保護に関する法律施行令（改正案）」および、「個人情報の保護に関する法律施行規則案（以下施行規則（案）と呼ぶ）」が公表されました。今後、正式制定により、新個人情報保護法の施行が加速化していくと思われます。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

次回は、「第六章　雑則　（旧第５章）　」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。　！！

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>

2016.10

中部/北信越支部報告　【 2016 年度 SAAJ 中部/北信越支部　JISTA 中部合同研究会 】

『新技術の導入におけるプロジェクトリスクの管理・監査』

会員番号 1732　田中 勝弘（中部支部　中部支部/北信越支部合同研究会）

次の通り 2016 年度 SAAJ 中部/北信越支部　JISTA 中部合同研究会を開催しました。

・日時：2016 年 9 月 24 日(土) 13:30 から 25 日(日) 12:00

・会場：ORE 名古屋伏見ビル　11 階

・主催：SAAJ 中部/北信越支部　日本 IT ストラテジスト協会(JISTA)中部支部

・後援：特定非営利活動法人　ITC 中部

・研究テーマ：新技術の導入におけるプロジェクトリスクの管理・監査

・研究会内容：

1）講演：「新ネットワーク技術「SDN」の導入と留意点について」

SAAJ 中部支部　進　京一氏

2）グループディスカッション：各グループにてテーマを決めてディスカッションを行う

SAAJ 中部/北信越支部　JISTA 中部合同研究会は、今年で 5 年目を迎えました。情報システムは社会へ広く浸透し、ビジネスにおいて ICT の活用は優勝劣敗の差別要因ともなって参りました。そのような状況の中で、情報セキュリティに関する事件・事故とともに、情報システムの導入・開発・運用にかかわる失敗・障害が取り上げられ、社会と企業活動への影響を懸念されているところです。

本年度 SAAJ 中部支部では、『プロジェクトリスクの管理・監査』を年間テーマとして、発注者側・受注者側及びその支援に当たるコンサルタントの立場で、プロジェクト全般に関するリスク管理の在り方について情報交換をしてきました。

そこで、本合同研究会においては、プロジェクトの属性を「新技術の導入」に特化し、その際のリスク管理・システム監査の在り方や今後について議論し、情報交流を図ることを目的として 18 名の参加により名古屋市内で開催しました。

1．講演

グループディスカッション実施に先立ち、「新ネットワーク技術「SDN」の導入と留意点について」と題して、SAAJ 中部支部会員の進　京一氏より、新技術の事例として SDN(Software Defined Networking)について、その概要と誕生の経緯、導入事例の紹介があり、新技術導入における留意点について提言する講演が行われました。

2．グループディスカション

グループディスカッションテーマ候補を紹介後、３つのグループに分かれて、各テーマに沿って、各参加者の事前の課題認識、講演での気づきを元に議論を進めました。

◇Ａグループ（進、宮本、山崎敏、堤、若原(敬称略)）　　報告者：No.808　若原達朗

このチームには経験豊富なメンバーがそろいました。合宿事務局も同様の認識のようで、他のグループが（仮）のディスカッション・テーマを指定されている中、このグループはテーマ設定も任されていました。

最初の自己紹介の後、いきなり議論が始まります。しかしその大半は雑談で、その中にテーマに関する話が少し含まれているといった感じです。ただ、この雑談の話題が非常に多彩で「ミトコンドリア」、「忍者」、「花火」、「原発」など、本当に皆さん、博識です。毎年この合宿に参加している人にとっては常識のようなものですが、ほとんど無駄話のようなこの雑談が後で成果につながります。

撮影担当のため、議論を途中で抜けて他グループの写真を撮りに行った堤さんから、「他のグループは着々と進めている」という情報がもたらされると、突然、その場はとりまとめモードにチェンジします。これまでの雑談で出てきた「キーワード」をどんどんポストイットに書き、ホワイトボードに貼っていきます。その際、ＫＪ法的に、キーワードの意図が似ているものを近くに貼ってグルーピングし、そのグループ間の関係を矢印などで示していきます。その過程でも「そのワードはもっとこちらに」等、活発に議論がなされ、あっというまに発表の骨子ができあがります。「それ自身が目的化しがちな新技術導入はあくまで手段であり、新技術を導入する真の目的を忘れてはならない」という発表主旨はあたりまえなことですが、メンバーの経験と雑談の中で出てきた多くの事例が特徴的であり、最後は山崎敏さんが発表して、うまくまとめてしまいました。

「常識」といったものの、いつもこの合宿では皆さんの「瞬発力」に感服させられます。普段の仕事もきっとこんなふうに、雑談をしながらもスパッと片付けているのでしょう。そんな姿を自分の目で見たいという皆さま、ぜひ来年の合宿に参加してみてください。ご参加をお待ちしています。

◇B グループ「新技術の導入を伴う開発プロジェクトの監査について」

(長谷部、村松、久保田、小山、安井、田中(敬称略))　　報告者：No.1732　田中勝弘

当グループは SAAJ、JISTA、ITC 中部所属会員で、金融機関など社会インフラ企業所属や一般企業向けコンサルタント、監査法人所属などバックボーンが異なる混成チームでした。そこで、ディスカッションを始めるにあたり、検討する開発プロジェクトの定義並びに新技術の定義について確認した。その結果、開発プロジェクトについては、システム開発管理態勢(管理体制とは異なり形だけではなく心が入るという意味)の在り方について、北信越支部での意見交換での内容を参考にして認識の統一を行った。具体的には、

(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

(3)新技術評価手続き(システム全体最適化、技術標準整備)
(4)対象システムのプロファイル(システム全体最適化、技術標準整備、前提となる条件(性能、情報セキュリティなどの要件))
(5)開発部門・ユーザ部門・運用管理部門の連携
に視点を整理して、個々の具体例などをディスカッションした。

また、新技術の定義についても、必ずしも世界最先端技術を他者に先駆けて導入すると捉えるのではなく、当該適用組織では初めて適用する技術や新しい開発環境の導入などを適用する場合など広く捉えて、議論を行った。

ディスカッションの中で、新技術適用の有無に関わらずシステム開発管理態勢の基本的なポイントはそのまま適用できるのではないかとの考えから、新技術を適用する場合の留意点について議論を進めた。

議論のポイントとしては、経営計画(業務計画、投資計画、システムプロジェクト計画)での整合性が前提であるとともに、

・経営計画を実現するために新技術適用の是非(経営計画実現のために新技術適用の必要性)
・品質/技術の調査分析(導入事例等の情報収集、必要な資源調達の可能性、技術者(経験者)の確保)
・適用技術の将来性、新技術の持続性（特にサプライヤが提供している製品やサービスを適用する場合、サプライヤの都合でサービスの打ち切りや変更などのリスクをどの程度盛り込んでいるか）
・導入コスト(新技術導入に伴う調査、分析コストや新技術導入に伴う生産性低下などのコストをどの程度見込んでいるか)
・納期・リリースとして例えばリスクや効果を確認するためにパイロット導入やプロトタイプによる評価などの適用計画
・体制(技術サポート、ユーザ部門、運用管理部門の関与)

などを考慮する必要があるとともに、万一新技術適用に問題がある場合の、代替手段や運用手段の事前の検討が重要であるとの意見が出された。

計画後のプロジェクト運営においても、マイルストーン管理や、利用部門への教育・訓練の実施なども合わせて適切に行われているかを確認することも必要である。また、リリース後においても事業目的に沿った(新技術導入)効果の確認が必要である。

さらに、適用後も新技術導入を一過性のものとしないためにも技術伝承(具体的には事業者の持っている技術標準の改訂など属人化を防ぐ対策)が重要であるとの意見が出された。

これらを踏まえて、監査実施のタイミングとしては、

(1)要件定義のレビュー前
(2)開発(各工程での完了確認)
(3)総合テスト前
(4)システム移行(リリース)の判定前

などが効果的ではないかとの意見に達した。

◇Cグループ「システム開発におけるヒューマンリスクに対するコントロールについて」

（鈴木、小島、大喜、梶川、萬代(敬称略)）　　報告者：No.615　萬代みどり

私たちは、発注者の立場のヒューマンリスクについて事実・課題を検討し、提言をまとめました。検討を通じ、常時開発を行っているのではないが故の課題もあると気づくことができました。

【提言】

(1)　モチベーションが高く、勘の鋭い人を大切にする（つぶさない）。

①　モチベーションを維持する仕組みを持つ。

・コミュニケーションを十分に取り一体感を育む。

②　プロジェクトの危険予測は行う。

・ＳＡＡＪのガイドラインなども活用する。

③　プロジェクトの当初の目的に立ち返ることのできる仕組みを持つ。

・計画のチェックと見直しは適宜行う。

(2)　プロジェクトの見える化を行う（予算の獲得に活かす）。

①　プロジェクトの虚偽の報告を見抜く。

・当初は「天気予報」のような形で直観的に把握できる表示をする。

・進捗に従い、プロジェクトダッシュボードのような形で、客観的な数字で状況を把握できるようにする。

②　プロジェクトの結果をあいまいにせず、人事考課に適正に反映する。

(3)　言わなければならないことをプロジェクトに言う憎まれ役を用意する。

①　社内での調達が難しければ、社外の第三者で調達する。

グループディスカッション並びに２日目の発表と、他グループからの質疑応答を通して、課題を深め、新技術の導入のみならず、プロジェクト運営におけるリスク管理・システム監査の在り方などについて、活発な意見交換が行われました。今回の研究を通して、各参加者の今後の活動に生かされれば幸いかと思います。

３．懇親会(情報交流会)

初日の研究会終了後、研究会参加者に懇親会のみの参加者を加え、計 19 名の参加で情報交流会を兼ねて懇親会を開催しました。

４．オプションツアー

最終日の研究会終了後、９名の参加者による、ひつまぶし(名古屋めし)昼食後、復元中の名古屋城本丸御殿の見学を行いました。

以上

<目次>

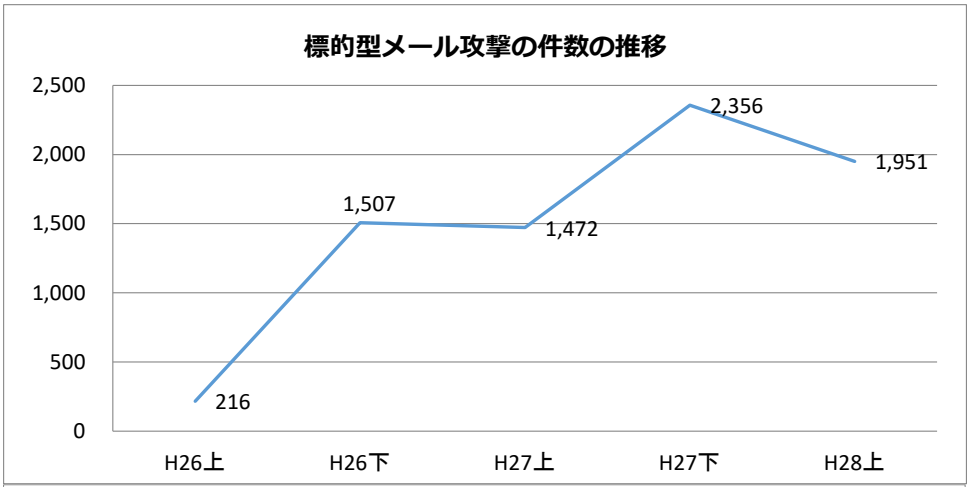
2016.10

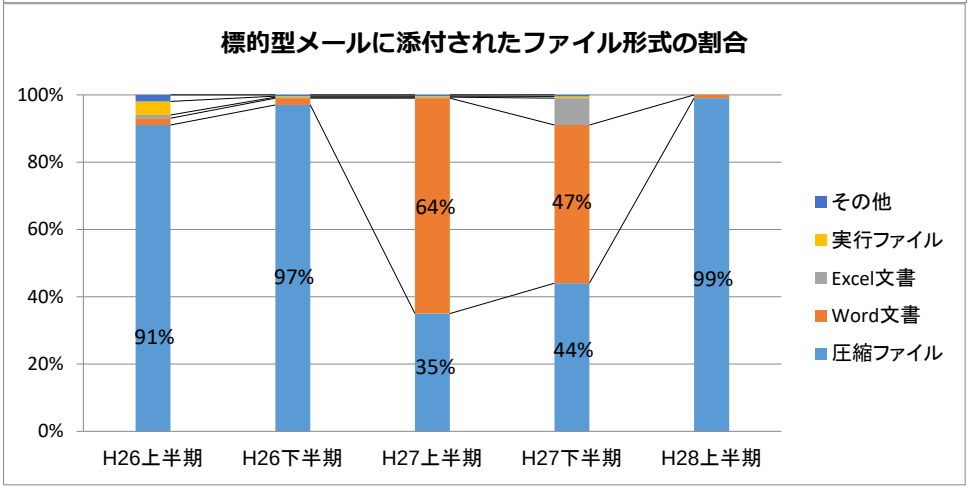
注目情報（2016.9～2016.10）

■「平成28年上半期におけるサイバー空間をめぐる脅威の情勢等について」を公表【警察庁】

警察庁は9月15日、「平成28年上半期におけるサイバー空間をめぐる脅威の情勢について」をまとめ、発表した。

サイバー攻撃の情勢については、警察が報告を受けた標的型メール攻撃は1,951件と、前期から405件の減少となったが、添付ファイルは圧縮ファイルが99%を占め、これまでほとんど報告のなかった「.js」形式ファイルが急増している。





https://www.npa.go.jp/kanbou/cybersecurity/H28_kami_jousei.pdf

■偽警告で電話問い合わせへ誘導する手口の相談が急増～被害防止に向けたセルフチェック診断チャートを公開～【ＩＰＡ】

9月29日、ＩＰＡ（独立行政法人情報処理推進機構、理事長：富田達夫）セキュリティセンターは、安心相談窓口で相談件数が急増している「“ウイルスに感染した”という偽警告でサポートに電話するように仕向ける手口」の被害防止に向けたセルフチェック診断チャートを公開しました。

https://www.ipa.go.jp/security/anshin/mgdayori20160929.html

<目次>

2016.10

【 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218回	日時：2016年 11月 15日（火曜日）18:30～20:30 場所：機械振興会館 地下2階ホール	
	テーマ	「情報処理安全確保支援士制度について」
	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
	講演骨子	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戦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。
	お申込み	ＨＰでご案内中です。 http://www.saaj.or.jp/kenkyu/kenkyu/218.html

■ＳＡＡＪシステム監査実践セミナー（東京）

第29回	日時：2016年 11月 17日（木曜日）～11月18日（金曜日）日帰り 9:30～17:00（進行状況により若干の変更が生じる場合があります。） 場所：晴海グランドホテル（申込み状況により変更する場合があります）	
	概要	当協会のシステム監査事例研究会「システム監査普及サービス」で実施したシステム監査事例を教材として、ロールプレイングを中心とした演習によりシステム監査を修得することを狙いとしたきわめて実践的なコースです。
	お申込み	ＨＰでご案内中です。 http://www.saaj.or.jp/kenkyu/jissenseminar/jissenseminar29.html

■ＳＡＡＪ西日本合同研究会（松江）

2016年度	日時：2016年 11月　5日（土曜日）13:00～17:00 場所：くにびきメッセ－島根県立産業交流会館－601 大会議室	
	統一テーマ	「情報システム開発とシステム監査 ～ 近年の情報技術やシステム開発手法（アジャイル、DevOps、クラウド、スクラム開発等）にシステム監査はどう対応するか～」
	概要	近年の情報技術やシステム開発手法にシステム監査はどう対応するかをテーマに西日本支部の会員各位より発表して頂き、現代のシステム監査の手法等についての議論をします。
	お申込み	ＨＰでご案内中です。 http://www.saaj.or.jp/shibu/chugoku/nishi_godo_kenkyu2016.html

<目次>

2016.10

【 外部主催イベント・セミナーのご案内 】

■システム監査学会　公開シンポジウム（東京）

第29回	日時：2016年 10月 28日（金曜日）10:00～17:00 場所：機械振興会館 ホール他	
	統一論題	つながる社会とシステム監査
	基調講演	「ITを利用した監査の展望～未来の監査へのアプローチ～」 講師：中村公認会計士事務所 公認会計士 中村 元彦 氏
	お申込み	ＨＰでご案内中です。 http://www.sysaudit.gr.jp/taikai/2016taikai.html

■ITGI Japan カンファレンス（東京）

2016	日時：2016年 11月 14日（月曜日）10:00～17:40 場所：東京コンファレンスセンター品川	
	テーマ	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～
	講演１	「金融機関におけるAI技術の活用状況」 講師：公益財団法人金融情報システムセンター 調査部 主任研究員 本山 一秀 氏
	講演２	「日立の鉄道ビジネス海外展開について」 講師：株式会社日立製作所 理事 鉄道ビジネスユニット マネージングダイレクタ [日本・アジアパシフィック] 兼 CSO 光冨 眞哉 氏
	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」 講師：オリンパス株式会社 執行役員 CSR本部 本部長 北村 正仁 氏
	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」 講師：（株）サイバーディフェンス研究所 専務理事／上級分析官 名和 利男 氏
	講演５	「SOE・SORの両立とアプリケーションオーナー制度」 講師：東京海上日動火災保険株式会社 常務執行役員 稲葉 茂 氏
	お申込み	ＨＰでご案内中です。 http://itgi.jp/conf201611/

<目次>

2016.10

協会からのお知らせ　【 年会費納付時期について 】

会員番号 1760　斎藤 由紀子（事務局長）

会員各位

いつも、協会活動へのご協力を賜りありがとうございます。

早速ですが、会員規程に従い、2017 年度年会費の請求書を、2016 年 12 月 1 日付で発送いたしますので、ご準備のほどよろしくお願い致します。

【会員規程】　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf

第３条（会費）：会員は、当該年度（１月～１２月）の年会費を、請求書に記載された期日までに支払わなければならない。いったん支払われた会費は返却しない。

【2017 年度会費請求の内容】

＜金額＞ 正会員個人：　￥10,000－　（消費税非課税）

正会員団体：　￥10,000.-　～　￥100,000.-　（消費税非課税）

＜払込期限＞2017 年 2 月末日

なお、正会員団体に限り、事業年度予算等の事情による、「納付期限延長願い」をご提出いただくことで、納入期限の延長が可能です。（原則 2017 年 4 月末期限。ただし時期についてはご相談ください。）

お申し出先： http://www.saaj.or.jp/toiawase/index.html　（事務局）

＜振込先＞ **郵便振替口座**：00110-5-352357　（請求書発送時に振込依頼書を同封します）

加入者名：日本システム監査人協会事務局

銀行振込口座：みずほ銀行八重洲口支店（普通）2258882

口座人名：特定非営利活動法人日本システム監査人協会

トクヒ）ニホンシステムカンサニンキヨウカイ

※銀行振込の際は、«会員№»４桁の数字を氏名の前に付けて下さいますようお願い致します。

（会員番号が付けられない場合は、メールで振込内容をお知らせください。）

【重要事項：2016 年度会費未納の場合】

一部の会員の方について、2016 年度会費のお支払が確認できません。2016 年 12 月 31 日までに納付が確認できない場合は、除名処分となりますので、至急お手続きいただきますようお願い致します。

なお、http://www.saaj.or.jp/kenkyu/index.html　の「会員ログイン画面へ」から、会員ページにアクセスしていただきますと、会費のお支払状況をご確認いただくことができます。

【ご寄附のお願い】

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

＜寄附金額＞　￥3,000/一口　ご寄附は、何口でも承ります。

＜振込先＞　ご寄附は、協会会費に合算して、会費振込先にお振込みください。

＜東京都への個人情報の提供＞法令に基づき、寄附者名簿（氏名、ご住所）を、認定 NPO 法人所轄庁の東京都へ報告致します。何卒ご了承賜りますようお願い致します。

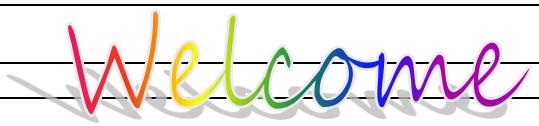
【会費、ご寄附等に関するお問い合わせ先】： http://www.saaj.or.jp/toiawase/index.html　（事務局）

以上

＜目次＞

2016.10

【 新たに会員になられた方々へ 】



新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
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

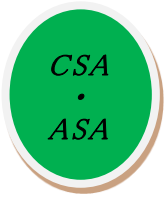
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・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　　2016.10			
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
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 活動説明会（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）
12 月	1： 2017 年度年会費請求書発送 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	15： CSA/ASA 更新手続案内メール〔申請期間 1/1～1/31〕 16：秋期 CSA 認定証発送	
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	
2015	過去に実施した行事一覧		
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 回システム監査実践セミナー（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
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

<目次>

2016.10

【 会報編集部からのお知らせ 】

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

□■ 1． 会報テーマについて

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。11 月号から来年 1 月号までの四半期テーマは「システム監査の効果的活用」です。

経営者には、システム監査を経営に活かすということが必要ですし、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。システム監査の効果的活用のためにはどうすればよいのか、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>