認定 NPO 法人
日本システム監査人協会報
2018 年 11 月号
No 212
No.212（2018 年 11 月号）＜10 月 25 日発行＞

今月号の注目記事

写真提供：0557　仲厚吉　　岩手小岩井農場

巻頭言

システム監査基準・管理基準連絡会について

会員番号：0555　松枝憲司（IT アセスメント研究会主査）

皆様ご存知のように、今年の４月にシステム監査基準と管理基準が改訂されました。
この改訂作業に携わった４団体（システム監査学会・ISACA 東京支部・日本 IT ガバナンス協会・SAAJ）を中心に、システム監査基準並びにシステム管理基準の普及及び継続的改善に貢献することを目的として「システム監査基準・管理基準連絡会（以下連絡会）」を立ち上げました。（力・松枝副会長が参加）
連絡会では、目的を達成するために、次の事業を行うとしています。

(1)「システム監査基準」及び「システム管理基準」の周知・普及を図る活動

(2)「システム監査基準」及び「システム管理基準」に追加すべき項目の検討に関する活動等

これまでに隔月で３回の会合を持ち、各団体における両基準の周知に関するイベントや活動内容等についての情報を共有しています。また連絡会の趣旨に賛同した他の団体（日本内部監査協会等）の参加も呼び掛けており、今後のシステム監査・管理基準の普及に関する活動の幅を拡げていく予定です。

当面のアクションプランとして、次を行います。

(1) 現在の両基準における問題点の洗出し

現在の基準に関する問題点について各団体で洗い出し持ち寄る。

(2) 連絡会Ｗｅｂサイトの立上げ

外部に対して情報発信する場としてＷｅｂサイトを立上げ、講演会の資料等の成果物を公開する。

今後の活動につきましては、理事会議事録及び会報で継続的に報告いたします。

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>

2018.10

めだか　【　システム監査基準・管理基準改訂とこれからのシステム監査人　】

システム監査基準は、留意事項に、“組織体の内部監査人がシステム監査を実施する場合には、日本内部監査協会の「内部監査基準」又は内部監査人の国際組織 IIA の「専門職的実施の国際フレームワーク」を、また情報セキュリティ監査制度に基づく監査を実施する場合においては、「情報セキュリティ監査基準」をあわせて参照することが望ましい。”としている。日本内部監査協会は、「内部監査基準改訂の背景および主な改訂点 平成 26 年 6 月 1 日」を公表し、改訂の背景に、内部監査の法的環境の変化（会社法の平成 17 年 7 月制定、金融商品取引法の平成 19 年 5 月改正）、平成 16 年以降の組織体をめぐる多数の不祥事の露見、ビジネス・リスクの識別と対応、ガバナンス・プロセス等々の社会情勢の変化を挙げている。システム監査基準・管理基準改訂の背景も、内部監査基準の改訂と同様の社会情勢の変化によっている。

2018 年 9 月 7 日の SAAJ 月例研究会は、SAAJ 監修「発注者のプロジェクトマネジメントと監査―システム開発トラブル未然防止の神髄に迫る―」をテーマに開催された。同書は、SAAJ 創立 30 周年記念出版であり、講演は、同書の構成と同じ、導入部、発注者のプロジェクトマネジメント、成功に導くプロジェクト監査という章立てに沿ってシステム開発の発注者と受注者が Win/Win となる秘訣をわかりやすく解説していた。同書は、これからのシステム監査人に必携の書である。

東京国立博物館の縄文展を見学したが、人間は、縄文の太古より、人工知能（AI）には難しいといわれるフレーム、即ち、ものごとの枠組みを考える力がある。そして、ある枠組みの中で、ものづくりをしている。考えたことを試してみて、見直しを行い、よりよいものを作るのである。ところが、システム構築の規模が大きく複雑になると、全体の枠組みをとらえることが難しくなる。失敗の本質を一言でいうと、設計図が未完のまま、急いで大伽藍を建てるようなシステム構築をしてしまう。システム構築の規模が大きく複雑である場合、先ず設計し、試してみて、設計を見直し、ものづくりを始めるという試行の過程が必要である。また、システム変更の場合、変更作業を急ぐ結果、変更が影響する枠組みを十分把握できないことから、重篤なトラブルを招くことが多い。この場合も試行の過程が必要である。

「発注者のプロジェクトマネジメントと監査―システム開発トラブル未然防止の神髄に迫る―」は、抽象的な理論ではなく、具体的に現場で役立つ方法論を提案している。プロジェクトマネージャ（PM）は、経営課題を情報システムにより解決するため、プロジェクトチームを率いる権限を与えられ、プロジェクト完成の責任を負っている。プロジェクトのトップとして孤独な立場であるが、システム監査人をプロジェクトの初めから参画させ、システム監査人の協力を得て、設計図を完成し、要所で見直しを行えば、発注者と受注者が Win/Win となる情報システムを構築することができる。（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、ＳＡＡＪの見解ではありません。）

<目次>

2018.10

投稿　【　基礎自治体の CIO 補佐官というセカンドキャリアのすすめ　】（その１）
―課題、包括外部監査報告と新システム監査基準及びその＜着眼点＞を対比してー

CIO 補佐官経験者

※本投稿については、実名が原則であるが、自治体が特定されることで、問い合わせにより業務に支障を来たす可能性を考慮し、特に匿名とすることとした。ご了承願いたい。（会報主査）

１．はじめに

システム監査視点を持った情報システムの専門家である SAAJ メンバー等が、自治体の CIO 補佐官として活動し、SAAJ の倫理規定にあるように、社会性の高い自治体の ICT 活用の健全な発展に寄与することを、CIO 補佐官経験者として、改めて提言したい。

民間とは異なる環境の自治体CIO補佐官への応募をためらう向きもあろうかと思うが、少しでも自治体CIO補佐官の活動への理解と誤解を解くために、『基礎自治体の CIO 補佐官というセカンドキャリのすすめ』と題して、連続３稿を投稿する。

（その１）では、自治体が実施する包括外部監査の結果を新システム管理基準と対比し、自治体の抱える IT ガバナンス・マネジメントの課題を明らかにする。

（その２）では、この IT ガバナンス・マネジメント課題に対し、自治体はどのように取り組み、CIO 補佐官の活動はどうあるべきなのか、５年間の CIO 補佐官体験をもとに、事例を示したい。

最後に（その３）では、最大の眼目である、CIO 補佐官の任用の状況と任用形態について考察し、その上で、「基礎自治体の CIO 補佐官というセカンドキャリのすすめ」について、思いを述べたい。

自治体の IT ガバナンス・マネジメント課題については、先行自治体において既に認識され、改善の取組が進んでいるところであるが、本稿では中核市４８市の包括外部監査報告書から、その課題を確認する。

私は CIO 補佐官在職中に、業務遂行にあたって、システム管理基準等による監査視点を踏まえて進めてきた。また、近隣市等における包括外部監査報告書も「他山の石」として活用してきた。

2018 年４月に、システム監査人の共通言語ともいえるシステム管理基準が改定され、IT ガバナンスの監査が強く打ち出されたことから、改めて「新システム管理基準」と「包括外部監査報告書」を対比することで、最大公約数として、基礎自治体の IT ガバナンス・マネジメント課題を共通認識できるのではないかと考えた。

なお、中核市制度とは、政令指定都市以外で、人口 20 万人以上の要件を満たし、市に都道府県の事務権限の一部を移譲する都市制度で、政令に基づく指定により、政令指定都市に準じた事務の範囲が移譲されている。

２．包括外部監査とは

(1) 制度の背景

地方分権を推進していくに当たって、地方公共団体のチェック機能を強化するもので、一部の地方公共団体で見られた不適正な予算執行の問題に対処するため、地方公共団体の監査機能を制度的に強化するものである。

(2) 制度の内容

地方公共団体の長が、地方自治法第 2 条第 14 項（住民の福祉の増進、最小の経費で最大の効果）及び第 15 項（組織及び運営の合理化、規模の適正化）の趣旨を達成するため、外部監査人の監査を受けるとともに監査の結果に関する報告の提出を受けることを内容とする。契約により行うものであり、中核市においては実

施が義務付けられており、1999（平成 11）年度から実施されている。

⑶ 外部監査人となることができる者

弁護士、公認会計士、公務精通者及び税理士（弁護士、公認会計士及び税理士については、これらの者となる資格を有するものを含む。）

⑷ 包括外部監査の手順

ア　議会議決 ― 契約の相手方及び予算

イ　契約締結

ウ　監査の実施

エ　監査結果の報告（市長、議会、監査委員、その他関係行政委員会）の提出。監査委員は、これを公表

オ　市長、議会、監査委員、その他関係行政委員は監査の結果により措置を講じたときはその旨を監査委員に通知し、監査委員はこれを公表する

カ　監査結果・措置の公表

各市ホームページにて監査報告書と後年度における監査指摘（結果)・意見に対する措置状況を公開する

3．包括外部監査報告から抽出した指摘・意見の件数

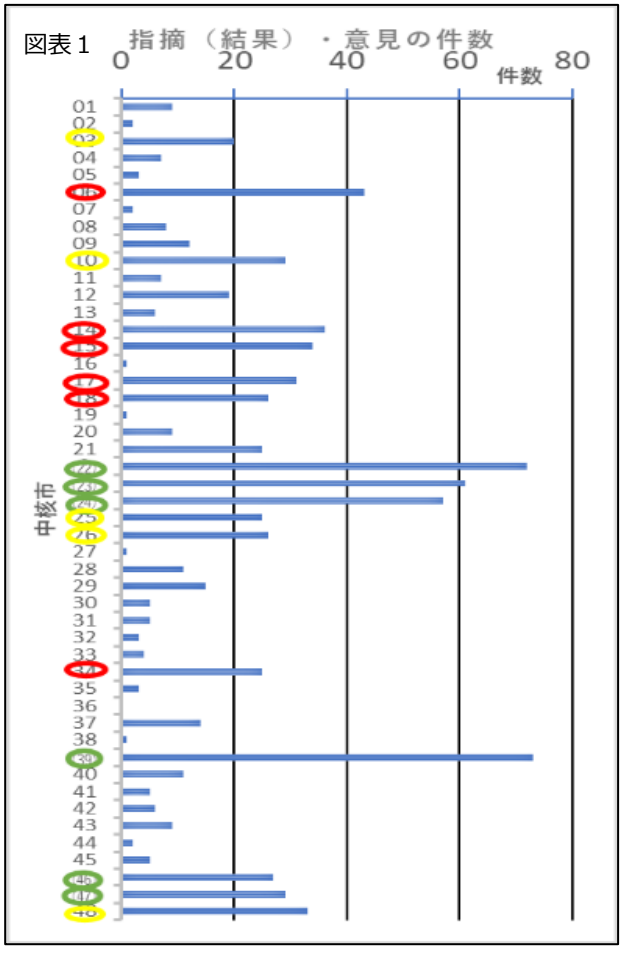
中核市４８市の 2012（平成２４）年度から 2017（平成２９）年度までの６年間を対象とし、８５８件の「指摘」・「意見」を抽出した。各市の件数分布を図表１に示す。

なお、包括外部監査報告書では「指摘」と「結果」が混在するが、本稿では「指摘」と表記する。ここに、

【指摘】とは　「法令や規則等に違反している事項、著しく不当な事項等」、あるいは「法令、条例、規則等の形式的な違反、裁量権の逸脱などの実質的な違反のある場合、もしくは、実質的な違反とは言えないが、社会通念上、適切でないものであり是正すべきもの、あるいはそれに準じるもの」

【意見】とは　「規則違反ではないが、自治体運営の有効性・効率性・経済性を踏まえた結果、改善することが望ましい事項」あるいは「是正を必ずしなくてはならないものではないが、事務の執行について参考にすべきものとして監査人が市に対して提言するもの」と説明されている。

図表１



本抽出は情報システムに係るものに限定しているため、監査人が問題とする監査テーマの選定や、業務全般に係る情報システムの活用状況が、指摘・意見の件数に影響する。具体的には、

① 監査テーマで、「情報部門の事務」を取り上げている自治体は、件数が多い（図中緑）

② 監査テーマで、「委託」「契約」に関する事務を取り上げている自治体も比較的件数が多い。（図中黄色）

③ 情報セキュリティに係る件数が総数の半数近くに及ぶ自治体は、他に比較し件数が相対的に多い。（図中赤）

本図表から、指摘・意見が少ない市は IT ガバナンス・マネジメント課題が少ないととらえるのは早計にすぎる。むしろ、監査テーマとして「情報部門の事務」を取り上げないことで、ICT 活用を進める上で重要な IT ガバナンス・マネジメントの課題・リスクの発見が遅れること、あるいは、指摘・意見が取り上げられるほどに、市の ICT 活用が業務に浸透していないのではないかなど、逆の面から吟味する必要がある。

なお、2012（平成２４）年度以降に中核市に指定された７市は、指定後の包括外部監査で、相対的に件数が少ない。

４．新システム管理基準により分類した指摘・意見

新システム管理基準に示された、監査項目、及び当該項目の＜着眼点＞と対比し、包括外部監査の指摘・意見を分類した。その結果を、図表２に示す。

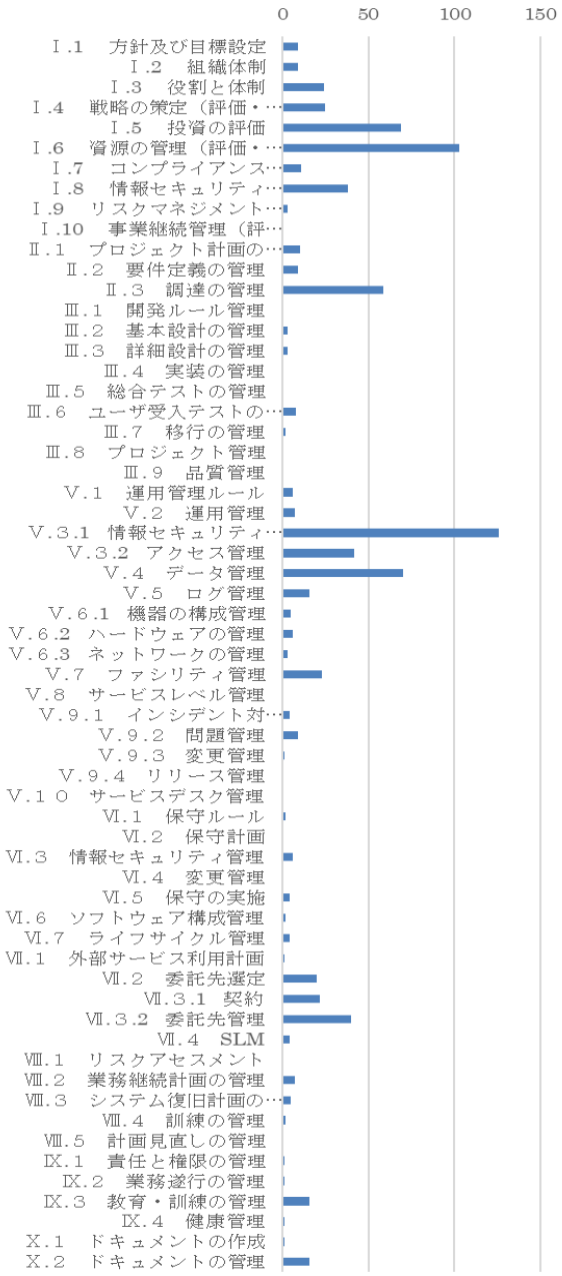
また、図表２の結果を５つの大分類（大きなくくり）の件数比率を、図表３に示す。

包括外部監査の趣旨から考えれば当然であるが、「投資の評価」「資源の管理」「調達の管理」「委託先の選定・契約・管理」といった、情報システムの『企画（予算化）』『調達（発注）』『評価（事後評価）』という財務的視点が 37%、「コンプライアンス」「情報セキュリティ・管理ルール」、「データ管理」、「アクセス・ログ管理」、「ファシリティ管理」「事業継続計画・システム復旧計画・訓練」といった、『情報セキュリティ等』の視点が 41%で、全体の 80%近くを占めている。

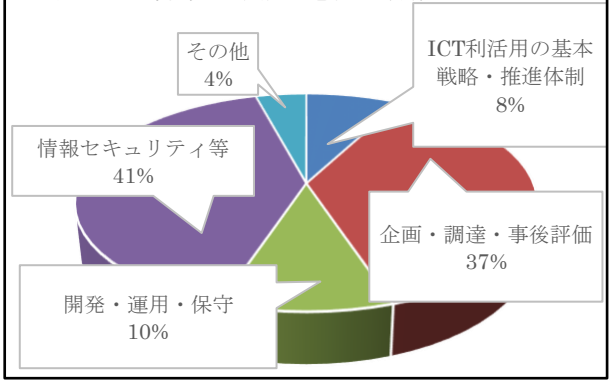
それでも、「方針及び目標設定」、「組織・役割と体制」、「戦略の策定」といった、『ICT 利用の基本戦略』、『推進体制』に係る件数が８%あることは、IT ガバナンス強化の必要性を理解する上で、心強いものがある。

また、『開発・運用・保守』の業務遂行に関する件数は、10%と少ない。自治体は多くの情報システム関係業務において外部委託している。その中で、発注側の「プロジェクト管理」や「要件定義」「受入テスト」の管理で指摘・意見件数が一定規模あることは、自治体でも不完全なシステム導入や失敗プロジェクトが懸念されていることを想起させる。

図表２　項目別　指摘/意見　出現回数



図表３　大分類の指摘・意見の件数比率



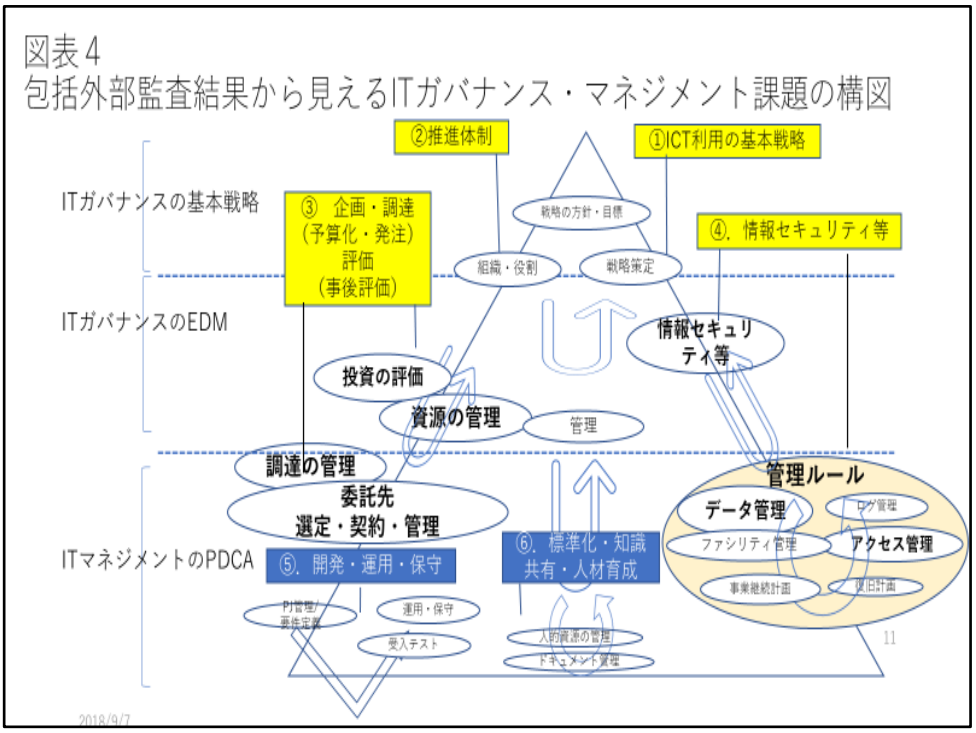
5．基礎自治体 IT ガバナンス・マネジメント課題の構図

包括外部監査報告を新システム管理基準と対比した図表２の集計結果を、自治体における IT ガバナンス・マネジメントの３層構造として、図表４に整理した。図表中、システム管理基準の節の文字サイズは、指摘・意見の総数を反映した文字サイズで重み付け表示している。また、いくつかの関係深い項目はひとくくりにした上で表示している。

また、（その２）で触れる総務省における「地方自治体における IT ガバナンスの強化ガイド」のレベルシートにある六つのくくり（図中黄色・青色枠）とも対比し、課題を整理し直した。

以下、①~⑥の区分ごとに指摘・意見の概要を示す。

図表４
包括外部監査結果から見えるITガバナンス・マネジメント課題の構図



① ICT 利用の基本戦略 及び ② 推進体制

市の総合政策の目標と整合をとった ICT 利活用の基本戦略を、行政経営の政策の一環として全庁横断的立場で打ち出し、その推進体制の中核として情報システム委員会等の全庁組織や情報システム部門を機能させることが求められている。IT ガバナンス強化の具体策として、調達ガイドライン等の整備と、その実効性を徹底するための管理プロセスの整備が求められている。

③ 企画・調達・評価

情報システムの導入にあたって、まず企画段階（予算化）における事前の事業評価（投資対効果、基本戦略との整合性など）、調達段階における事業者依存の排除（見積査定等）や明確な選定基準に基づく公正な競争原理の導入が求められる。そして、事後評価段階においては、システム導入後の成果と当初の目標との対比、更なるシステム・データベースの活用に向けた利用の徹底、共用化などの取り組みが求められる。

更に、業務委託における実績の把握と評価が必要で、評価結果の次期調達への反映が必要である。

そして、情報部門には、企画・調達・評価における全庁的支援の中核組織としての役割認識と、説明責任の発揮が求められる。

④ 開発・運用・保守

開発・運用・保守においては、外部委託先との契約・業務管理の適正化とともに、システム開発における最川上のプロジェクト管理・要件定義、そして最川下の受入テストでの重点的管理項目が指摘されている。

具体的には、川上での個人情報保護や誤謬防止・不正防止の要件の明確化、川下での受入テスト・データ移行の厳格な実施である。

⑤　情報セキュリティ等

IT ガバナンスレベルの情報セキュリティに係る方針や対策の整備はもちろんであるが、マイナンバーなど個人情報保護に係る、データ管理・アクセス管理・ログ管理や、サイバーテロや自然災害に対応した事業継続計画･復旧計画など､実効性のある対策の実施と徹底を IT マネジメントレベルの取組として求められている。

⑥　標準化・知識共有・人材育成

IT ガバナンス・マネジメントに係る知識・経験の継承のため、個人依存を脱却する、その一環として、ドキュメント作成・管理ルールの整備と周知徹底が求められる。更に、それら知識・経験を継承する人材の確保及び育成に向けた取り組みも求められている。

６．指摘・意見とシステム監査基準の主な着眼点の対比

前節の①~⑥の区分ごとに、指摘・意見と照合した＜主な着眼点＞を示す。（末尾は照合した件数）

なお、行政の職務執行を対象とするため、＜着眼点＞に、公務員倫理に基づく､「公正な職務」､「市民目線」､「透明性の確保」､「公共の利益」といった観点を加味して判定したことは、ご承知おき頂きたい。

①ICT 利用の基本戦略

主な指摘・意見
・情報システムの導入や情報セキュリティに関する、ガバナンスの方針を全庁的に示す必要性がある。
・市の総合政策の目標と整合をとったICT利活用の基本方針・基本計画の策定手続き、及び計画に盛込むべき内容について助言する。
・自治体の新たな政策課題に対する、ICT活用ニーズや現行システムの課題の調査分析の必要性。また、システム更新計画において、長期的視点に立ち、「ストーブパイプ」システムを排し、全庁横断的なシステム連携や情報共有を考慮すべき。
・既に基本計画に基づくシステム整備や情報セキュリティ対策を進めつつある自治体では、システム化の環境変化と計画の進展に基づき、基本計画を点検・更新し、全庁の共通理解を図りつつ進めること。
・ITガバナンス強化において、情報システムの調達プロセス（企画（予算化）・調達~運用・保守）の適正化のため、調達ガイドライン等の整備が必要性である。
・既に調達ガイドライン等を整備し運用を開始している自治体では、運用の周知徹底や、実施結果に基づく管理プロセスの改善が必要性である。

対比

主な着眼点	件数
【情報システム戦略の方針及び目標設定】	
・組織のビジョン、使命及び経営戦略を評価して、情報システム戦略の目標及び情報システム化基本計画を策定していること。	3
・情報システム戦略の目標達成状況を中長期の情報システム化基本計画に照らして適時にモニタリングし、適切な対応に結びつけていること。	5
【情報システム戦略の策定の評価・指示・モニタリング】	
・事業及び情報システムの内部及び外部環境の変化について、適切に評価を行なっていること。	8
・情報システムの企画、開発及び運用、保守のための標準化、並びに品質確保の方針を明文化していること	7
・標準化及び品質確保の方針について周知徹底すべき関係者及び関係者の理解をモニタリングする方法を定めていること	4

②　推進体制

主な指摘・意見
・情報部門が、専門部署として情報システムの調達や情報セキュリティ対策において、業務所管課を主体的に指導・支援すること
・情報システム委員会等の全庁組織が、情報システムの調達や情報システムの安全管理などについて、モニタリングし、指導すべきこと
・技術指針の検討、システム選定など必要に応じて、適切で客観かつ公正な外部専門家の助言を得て、これを反映させるべきこと
・長期にわたる委託業務契約により、特定の委託先に依存しないこと。例えば、予定価格の積算がブラックボックス化し、積算根拠が明確でない、委託契約の仕様が不十分なまま、長期間契約が繰り返されているなど、情報システム部門として、説明責任を果たせていない。

対比

主な着眼点	件数
【情報システム戦略遂行のための組織体制】	
・情報システム戦略委員会等がモニタリング対象とする情報システムの活動を明確にしていること、等	4
・必要に応じて、適切で客観かつ公正な外部専門家の助言を得て、これを技術採用指針に反映させていること	4
【情報システム部門の役割と体制】	
・情報システム部門長は、情報システム投資、及び情報システムに関わる諸資源を集約して管理していること、等	3
・特定の委託先、業務提携先等に依存していないこと	18

③　企画・調達・評価

システム導入前の投資対効果、調達時の公正で効果的な手続き、更に、導入後におけるシステム利用・データ活用等の効用の最大化への取組について、説明責任の発揮が求められる。

主な指摘・意見
③－1　企画（予算）
・情報システムの導入にあたって、企画段階（予算化）における事前の事業評価（投資対効果、基本戦略との整合性など）がされていない
・予算額の算定において、特定の業者の見積に依存し、他の選択肢の評価によるなど、妥当性について説明責任を果たしていない。
・調達方法、設計金額、契約内容など、情報システム部門の知見を活かした調達が全庁的になされていない
・調達ガイドラインを既に運用している市において、ガイドラインを逸脱する運用を防止できていない
・既存システムを更改する際に、既存システムの機能評価をしないまま調達をしている
・調達の要求事項をまとめるにあたって、実務に精通している利用部門の担当者が参画できていない
③－2　調達
・特定の事業者に依存している。例えば、明確な選定基準に基づく公正な競争原理の導入がなされていない、求める要件や仕様が具体化されていない、また、事業者の再委託を安易に認めている
・複数の調達先を比較することなく、安易な考え方で随意契約を選択している、
・外部委託業務の特性を考慮して、プロポーザル、総合評価方式など業者選定の方式や選定基準を決定すべきである。また、選定基準において、ライフサイクルコストの観点が考慮されていない。
・指名入札において、辞退が発生している。原因を調査し、余裕をもって適切な業者を指名するなど改善すべきである。
・関係部署による契約内容のチェックが無く、契約書の条項に個人情報の取扱、著作権の取扱、再委託の可否、再委託時の手続、など不備がある。また、契約後の委託業務の実態把握がなされていない
③－3　事後評価
・システム導入後の成果と当初の目標との対比できていない
・システム稼働後の活用や問題点の改善など、投資効果や情報資源の活用を最大化する取り組みがなされていない、これは多くの面から指摘されているが、例えば、システムの導入メリットを最大化するため、システムの全庁的な利用を徹底する。システム導入の目標を達成するため普及や運用を工夫する。システムが保有する情報を分析・評価し、業務方針・活動の検討に活用する、あるいは、活用のためシステム機能・データ整備の改善を図る。また、優良な成果・活用方法を組織的に横展開する。市民・事業者への告知・情報公開で市のホームページを有効に活用する
・情報資産（ファシリティ、ハード、ソフト、情報）の全庁的な共有化や連携が図られていない
・情報資産の管理体制が不備である。情報資産の管理台帳への登録が網羅的ではない、資産の棚卸が行われておらず、無駄が生じている
・市のシステム化状況や外部委託方針に照らし合わせ、システム化人財の確保について事後評価し、見なおされていない
・委託業務の実績把握と結果の分析・評価が必要である。そして、評価結果が、次期調達計画に反映されるべきである

対比

【情報システム投資の評価・指示・モニタ】	
・情報システム投資の有効性を評価する指標及び目標が定められ、経営戦略の指標及び目標と整合がとれていること	4
・影響、効果、期間、実現性等の観点において明確な差がある複数の選択肢が挙げられていること	6
・具体的な選択肢を選択した理由を利害関係者に説明できるようにしていること	19
・不適切な執行を防止するための内部統制が存在していること	7
・投資効果が不明確なまま情報システム投資が行われることを防止する内部統制があること	10
・情報システムの全体的な業績及び個別プロジェクトの実績を財務的な観点からモニタリングして、問題点に対しては対策を講ずることがルールとして定められていること	5
・投資した費用が適正に使用されたこと及び妥当性の評価が行われないまま放置されることを防止する内部統制があること	11
【情報システムの資源管理の評価・指示・モニタ】	
・情報資産の管理方針及び体制について、関係者に周知徹底していること	5
・情報資産の効率的かつ有効な活用方法を指示していること	40
・情報資産が効率的かつ有効に活用されているかどうかをモニタリングしていること	31
・情報資産の共有化を図っていること	17
・情報資産の共有化による生産性向上をモニタリングしていること	7
・経営陣は、内部人材の育成の方針、計画を明確にしていること、等	2
【プロジェクト計画の管理】	
・既存システムを更改する場合は、既存システムの評価を行うこと	6
・実務に精通している利用部門の担当者が参画すること	3
【要件定義の管理】	
・PMは、要求を出した利害関係者に要求の必要性及び重要性を確認し、機能要件、非機能要件毎に優先順位を付けること	7
【調達の管理】	
・PMは、情報システム部門の協力を仰ぎ、調達に必要な情報を収集すること	6
・PMは、調達先を客観的に評価できるよう評価基準を策定し、評価すること	28
・PMは、調達に際して、複数の調達先を比較することが望ましい	9
・PMは、競争入札を用いて、複数の調達先を比較すること	12
【委託先選定】	
・選定基準は、外部委託業務の特性を考慮していること（総合評価・最低価格・企画競争）	3
・可能な限り複数の委託候補先が提示した提案内容の比較検討を行ったうえで委託先を選定すること	11
・項目ごとに点数化した選定基準にする等、選定理由を明確にすること。	2
【契約】	
・関係部署による契約内容のチェックを受けるなどして、契約書を作成すること	9
・外部委託等契約書には、委託業務内容・範囲及び責任分担、委託方法、委託期間又は納期、特約条項・免責条項、損害賠償条項、守秘義務条項、暴力団排除条項、瑕疵担保責任（不具合時の責任）、知的財産権や使用権等の権利の帰属、再委託の可否（再委託を認める場合は、再委託先が外部委託先と同等の義務を負うこと等責任の所在、再委託時の手続（委託元への届出、委託元の承認等）を明確にすること）等を含むこと	12
【委託先管理】	
・委託業務の実施結果を分析及び評価結果を記録し、外部委託元部門長が承認していること。	7

④　開発・運用・保守

④－１　開発

市のシステム導入においては、発注者側の管理として、川上の「基本・詳細設計」と川下の「ユーザ受入テスト・移行」の範囲とした。

主な指摘・意見
川上では、
・新システムの導入と同時に、新システムの機能を考慮した、新しい業務モデルの作成ができていない
・昨今の自治体の誤請求・誤給付・不正受給を考慮すると、基本設計・詳細において、誤謬防止、不正防止の仕組みを考慮すること。
・市全体として、システム導入時に網羅すべきセキュリティ要件（パスワード要件、脆弱性対策、利用可能なサービスの定義等）がばらつかないよう、対策基準に基づき明文化する必要がある
川下では、
・受入テストでは、業者テストに依存することなく、発注者としてシステム稼働前の検査を実施する体制やプロジェクト終了判定チェックリスト等が準備されていない
・導入後の不具合発生時の原因追及等に備え、プロジェクト終了判定チェックリストなど、ユーザ受入テスト結果を記録保管できていない
・新旧システムにおいて、システム移行とセットで移行すべきデータが漏れなく移行されたか検証結果が記録されていない

対比

主な着眼点	件数
【基本設計・詳細設計の管理】	
・誤謬防止、不正防止、機密保護等を考慮すること、等	3
・新しい業務プロセスの手順、業務処理上のルールが明確になっていること	2
【ユーザ受入テストの管理】	
・ユーザ受入テスト結果は記録され、保管されていること	4
・ユーザ受入テストの終了基準を充足していること	2
【移行の管理】	
・移行期間中のデータが必要十分であることが検証されていること	2

④－２　「運用・保守」

主な指摘・意見
運用管理では、
・運用委託先（再委託先を含む）の業務実態を把握できていない。
・運用業務のスケジュール変更、作業指示が、承認・指示の記録のないまま口頭等で行われている。
・自動スケジュールのバックアップの実行結果など、確認を運用記録として残していない
・利用環境の変化に合わせ、運用管理ルールが見直されていない
データ管理では、
・共有フォルダー等の保存データの管理基準、データの更新手順など、データ管理ルールが定められていない
・バックアップにおいて、記憶媒体の保管場所等、災害時のリスクや復旧方法が考慮されていない。
・データ資産持ち出し時の紛失、盗難対策の実施がなされていない、また、データの授受について記録し、管理者が承認していない
・業務システムの利用において、データ作成手順、取扱等で、誤謬防止、不正防止、機密保護等の対策がなされていない、あるいは、入出力情報に係る誤謬防止の手続き・チェック体制が整備されていない
・資産管理、物品管理システムにおいて、データの更新忘れ、入力誤りなどデータベースの内容に誤りがあるままで、定期的に検証もされていない
・ホームページによる公開情報が、不足・誤り・古いまま、訂正されず放置されている
インシデント、問題・変更管理では
・障害対応など、対象機能、対応者、ステータス、障害原因、再発防止策等といった、インシデント対応を記録し管理できていない
・問題発生の根本原因を究明し、対策が講じられていない
・ソフトウェアの変更計画において、システム管理責任者の承認がなされないまま実行されているものがあった
・プログラム変更に伴う、トラブルや混乱等を防止するような受入れ手順が実施されていない。例えば、利用部門が受入テストに参加していない、テストの実施結果を記録していないなど

対比

主な着眼点	件数
【運用管理ルール・運用管理】	
・実行ジョブ名、使用設備、資源などを具体的に明示した指示書（オペレータに対する作業指示書のこと）を作成すること、等	3
・運用記録があり、運用のモニタリングを行い、結果の分析と評価を行っていること	5
【機器の構成管理・ハードウェアの管理】	
・ソフトウェア、ハードウェア及びネットワークの導入及び変更を運用管理者が承認していること	3
・リスク分析の結果に基づき、リスクに対応できる環境条件を明確にしていること	3
【委託先管理】	
・業務報告書には、委託業務の進捗状況又は稼動状況、品質管理状況、発生した問題点と対策状況、セキュリティ対策の実施状況及び今後の予定等の必要な事項が記載されていること	8
・立入監査等では、契約で取り決めた事項に対する遵守状況、情報セキュリティ管理態勢、事故等(サイバーセキュリティ事案を含む)への対応態勢や再委託先（再々委託先以降も含む）の管理状況等を確認すること。	11
・委託先において再委託が行われている場合は、契約に基づき、再委託（再々委託以降も含む）先の業務の実施状況を把握すること	3
・サービスや成果物の検収は、検収方法に基づいて実施していること	4
【データ管理】	
・使用するデータを網羅した体系的なデータ管理ルールを作成すること	4
・データが正常であることを検証していること	12
・バックアップの範囲、タイミング、記録媒体、保管方法等を、業務内容、処理形態及びリカバリの方法に応じて定めていること	5
・データの授受を記録し、運用管理者が承認していること	7
・利用部門の管理者は、入力データ作成手順、取扱等で、誤謬防止、不正防止、機密保護等の対策を講ずること	8
・利用部門の管理者は、データの入力の誤謬防止、不正防止、機密保護等の対策を、有効に機能させること	11
・利用部門の管理者は、出力情報が漏れなく、重複なく、正確であることを確認していること	4
【インシデント管理】	
・インシデントが解決した段階で、問題解決に向けて講じたステップを記録し、利用部門と合意した対応が取られていることを確認すること	4
・問題の原因を究明し、解決すること	5
【保守ルール・保守の実施】	
・「保守手順書」には、次の事項を記載すること。 保守の基本方針、保守対象、保守実施体制、保守依頼の受領からソフトウェアの修正を実施するかの判断、修正実施、修正したソフトウェアの本番システム環境へのリリースに至る基本手順、変更管理手順（仕様変更に伴う修正の実施手順）、保守において想定されるリスクと対応策	2
・受入テストの実施結果を記録すること、等	4
【ライフサイクル管理】	
・計画には、バージョンアップ、他のソフトウェアへの移行などの選択肢を考慮すること	4

⑤　情報セキュリティ等

『高度情報化社会においては、自然災害や大事故等の他に、機密性の高い情報の漏洩がそれらに匹敵する危機を招く可能性がある。しかし、多くの地方自治体において、情報管理の重要性に対する認識は民間企業のそれと比較し低いと言わざるを得ない』とまで指摘するものもあり、具体的には下表のとおり。

主な指摘・意見
「情報セキュリティ管理」では、
・情報セキュリティ対策など、リスク対策について、教育責任者あるいは教育体制を定め、教育の周知徹底が図られていない
・情報セキュリティの管理体制の役割、責任があいまい、あるいは、情報部門の主体性を発揮できていない
・セキュリティ対策を全庁的に実施しているが、当該対策が、理念的・概括的方針及び対策が定められているにとどまり、個別具体的で詳細な実施手順等は示されていない
・情報セキュリティ委員会等は、情報セキュリティに対する対策・ルールの有効性に関する自主点検・監査ができていない、あるいは点検・監査結果が対策の改善に生かされていない
・情報セキュリティ対策の方針を委託業務に関係する財団、指定管理者等に周知徹底できていない
「ファシリティ管理」では
・自然災害による影響を考慮した場所に情報システムやバックアップ媒体が設置されていない
・情報システム関連設備の設置スペースに対し侵入防止の設備がない
・サーバ室等の入退室の記録がなされていない、あるいは、記録に不備があるものが発見されている
・サーバ室等の機器媒体の持込・持出しの監視ができていない
・情報システム関連設備の保守点検がなされていない
「アクセス管理」では、
・職員の異動・退職に伴うアクセス権の設定・変更・削除が速やかに実施されていない
・個人IDの付与、共用IDの利用、共有フォルダーの利用などで、アクセス権付与及びアクセス権設定の運用ルールを見直すべきである
・特権IDの利用者・アクセス権限の管理強化がされていない
「ログ管理」では
・アクセス・ログ、障害ログを記録できていない
・アクセス・ログを定期的に分析できていない、このため分析結果にもとづく必要な対策を講ずることもできていない
・ソフトウェアのインストールなど、管理者権限による特別な操作の記録・検証ができていない
「事業継続計画」では、
・情報システムの被災・障害に対する事業継続計画が策定されていない
・業務継続計画の実現可能性を検証するため訓練やリカバリ手順の検証がなされていない、

対比

〈主な着眼点〉	件数
【情報セキュリティの評価・指示・モニタ】	
・経営陣は、情報資産のセキュリティ対策の方針を関係者に周知徹底することを指示していること	6
・情報セキュリティ対策の有効性、及び内外部の要求事項への適合性をモニタリングしていること	25
【情報セキュリティ管理】	
・物理的、実務管理的、及び技術的な情報セキュリティ管理ルールを作成し、文書化すること	21
・情報セキュリティ管理ルールの有効性をレビューし、改善を図ること	85
・情報セキュリティ管理基準の該当箇所を参照すること	15
【ファシリティ管理】	
・自然災害の影響が最小になる場所に設置していること	5
・侵入を防止する設備を設置していること	6
・建物及び室への入館及び入室の状況を記録していること	5
【アクセス管理】	
・運用システムのアクセス管理ルールの適用範囲を明確にすること	4
・運用要員の採用・異動・退職や職務変更の際には、速やかにアクセス権の設定・変更・削除を行い、運用管理者が承認すること	8
・アクセス権付与及びアクセス権設定について、定期的に見直しを実施すること	13
・一般より高い権限レベルを持つ特権的アクセス権については、設定・変更・削除について厳格に運用管理すること	14
【ログ管理】	
・通常の運用範囲を超えたアクセスや違反行為を含めて、運用の作業ログ、利用部門の活動ログを記録し、保管すること	3
・保管したログを定期的に分析し、分析結果に応じて必要な対策を講じること	8
【事業継続計画の管理・システム復旧計画の管理】	
・情報システム部門長は、関係者と協議し、事業継続計画と整合した業務継続計画を作成すること	3
・情報システム部門長は、実現可能性を検証する（訓練等）計画を策定していること、等	5

⑥　標準化・知識共有・人材育成

主な指摘・意見
教育・訓練の管理では
・業務を遂行するにあたり、業務マニュアルが存在しないことから、職員の異動に伴う適切な引継ぎ作業が行われないおそれがある。
・情報セキュリティについて、職員全員が対象となるような研修及び訓練を定期的に実施していない
・外部委託事業者の従業員に対する教育の実施を記した報告書を受領していない
・適切な業務遂行のため、システム管理者と電算担当者に必要なスキルを明確にし、計画的・継続的な教育訓練計画を策定することが望ましい。
・管理者は、カリキュラムの有効性を評価できていない、対象者の役割・情報セキュリティに関する理解度などに応じたカリキュラムとなっていない
ドキュメントの管理では、
・文書保管期限に関わらず、少なくともシステム稼働期間中はシステム導入時の検討資料以後のドキュメントを保存すべきである
・ドキュメント管理ルールをドキュメントの作成者、利用者及び管理の関係者に周知徹底できていない
・ドキュメントの保管、複写及び廃棄は、ドキュメントの形態及び重要度（機密度）に応じた不正防止及び機密保護の対策を講じていない、また、定期的に保管の状況を把握していない

対比

〈主な着眼点〉	件数
【教育・訓練の管理】	
・情報システム部門長の全関係者をも対象にした情報セキュリティにかかわる教育を実施していること	5
・情報システム部門長は、教育及び訓練を計画的に実施していること	3
・管理者は、カリキュラムの有効性を定期的に評価していること	8
【ドキュメントの管理】	
・ドキュメント管理ルールをドキュメントの作成者、利用者及び管理の関係者に周知徹底していること	8

７．IT ガバナンスの強化における包括外部監査の限界と CIO 補佐官の役割

（１）IT ガバナンスの強化をパッチワークとしない助言が必要

IT ガバナンス強化は、一過性の活動ではなく、組織文化として定着させてゆくべきものである。前節で述べた IT ガバナンス・マネジメントの①~⑥の諸課題を、相互に関連つけながら、活動レベル・適用範囲を拡大しなければならない。知識・実務経験に裏打ちされた CIO 補佐官が、IT ガバナンスの EDM と IT マネジメントの PDCA を取り持ち、着実に IT ガバナンスを強化してゆく必要がある。

IT ガバナンス強化において、こうした継続的・着実な取組が必要にもかかわらず、包括外部監査の指摘・意見への個々の対応を優先すると、限られた要員体制の中では対策のつまみ食い、即ち、対策がパッチワークに陥る危険性がある。ここは、包括外部監査等においても、IT ガバナンス強化の全体的な視野をもって、活動がパッチワークとならないよう助言してゆく必要があると思うが、IT ガバナンス強化の活動が緒についていない組織では、助言の仕方も難しい。

逆に、IT ガバナンス強化に取り組む姿勢・活動が現れてくると、包括外部監査は、IT ガバナンス強化の成熟度を客観的に評価することで、活動の有効性を高める助言として役立つ。現に、IT ガバナンス強化に取り組み始めた或る市の包括外部監査においては、「③企画・調達・評価」に係る調達ガイドラインの遵守状況を評価し、調達ガイドラインの運用の有効性を高めてゆくための助言を行っている。ただ、そうした監査報告事例も見られるが、この場合でも包括外部監査の性質上、課題の①~⑥全てにわたる成熟度評価とはならない。

（２）チェックではなく、IT ガバナンス強化の実践的な指導支援による職員育成が必要

市は IT ガバナンス・マネジメントの強化という課題にどう取り組めばよいのであろうか？

監査助言に促され情報システムの最適化基本計画（５W）を策定しても、「さて具体的にどのように活動を進めてゆけばいいのか？」と職員は悩む。職員が必要とするのは、具体的にどのように進めるか（How）である。この意味で、現場で実践的に指導支援する CIO 補佐官の必要性が明確になってくる。

IT ガバナンスの強化は日常の業務活動の一環であり、特別な短期プロジェクトではない。IT ガバナンス強化という日常において、CIO 補佐官が、その中核としての役割を認識させ、情報部門・職員が主体性を発揮できるよう成長を促してゆく必要がある。

８．おわりに

自治体の IT ガバナンス強化の課題と、その解決にあたり、助言だけではすまず、市職員と日常を共にする CIO 補佐官の必要性について述べた。次稿では、具体的事例により、CIO 補佐官の役割について紹介する。

参考資料：

１．中核市　包括外部監査報告書（2012（平成 24）年度~2017（平成２９）年度）
２．システム管理基準　経済産業省（2018.4.20）
３．「地方自治体における IT ガバナンスの強化ガイド」　総務省（2007.7）

<目次>

2018.10

エッセイ【アリの巣の居候】

会員番号　2089 阪口博一

アリの巣にはアリ以外の生物が大挙して「居候」しているらしい。なるほど、巣内は温度も安定しておりエサも豊富で、何より外敵に襲われることもない。このようなアリの巣に依存する昆虫は「好蟻性昆虫（こうぎせいこんちゅう）」と呼ばれ、非常に多くの種がさまざまな分類群で進化しているとのことだ。しかし、入り口は兵アリによって厳重に守られ、別のコロニー（同じ巣内の集団）に属する同種のアリでさえ、巣内に侵入すれば殺されてしまう。そんな場所にどうして居候できるのだろうか。

話は変わるが、以前勤めていた企業で、私が初めてシステム運用部門に責任者として就任した時の話である。マシンルームは当然ながらセキュリティエリアとして、社員でも限られた者しか入室できなったが、記録を確認したところ、あまりに多くの者が入室していることに驚いた。運用部門や協力会社の社員、機器やソフトウェアの保守担当者などは当然として、その他にも、ビル全体の電気系統管理者や警備員、配送業者、さらには耐火金庫のメンテナンス担当者などというのもあり、多岐にわたっていた。それぞれの者がシステム運営に直接的・間接的に携わっており、入室許可者であった。

アリにとっての巣内への「入室許可証」は匂いであるらしい。アリの匂いはコロニーごとに異なり、臭覚で認識している。巣の中は真っ暗で、臭覚に頼るのが妥当なところだろう。好蟻性昆虫は、様々な方法でこの匂いの問題をクリアし、アリの巣の居候となっている。例えば甘い蜜を分泌し彼らの「家畜」として巣に運び込まれるチョウの幼虫や、その巣のアリを殺して背負うことでクリアしているカメムシの仲間など物騒なものまでいる。どんな手段を使っても、巣内に入りこんで、本来の住人であるアリに襲われなければ、居候生活は安泰なのだ。

我々の世界で、入室許可者を観察していると、その多くは運用担当社員と顔見知りで、入室時と退室時以外はマシンルーム内での作業を任せきりにすることも多く見られた。協力会社社員とは言え、入館証を得て入室してしまえば……というころが気になった。情報セキュリティ管理基準（平成 28 年版）の 11.1.2.11 項には、セキュリティ領域への外部要員によるアクセスは認可を必要とするだけでなく「監視する」とも明記されている。そこで、作業中には必ず立ち合うよう指示した。疑ってかかるという態度ではなく、若い社員に勉強のために立ち合わせれば会話も生まれ、何かしら得ることもあるだろうと。しかし、さすがに金庫メンテまでというのはやりすぎだという声もあり、金庫は防犯カメラの正面だったので、その対象は「できる限り」というところに落ち着いた。

ずさんな入退室チェックや入室者の放任は、不正を誘う「甘い香り」のようなものであり、虫の出すフェロモン（誘引物質）を髣髴させる。身内を疑いたくないという心理から甘さが露呈し、不正の機会を与えてしまっては元も子もない。機会を奪うことで内部不正を防ぐ。それが情報資産を守るだけでなく、結果的に人をも守ることになるであろう。

（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。）

<目次>

2018.10

本部報告　　第２３３回　月例研究会

会員番号　495 山内美佐子

【講師】日本アイ・ビー・エム株式会社　東京基礎研究所インダストリーソリューションサービス
品質エンジニアリング　部長　細川 宣啓　氏

【日時・場所】2018 年 6 月 13 日（水）18：30～20：30　機会振興会館　B2F　ホール

【テーマ】「IT システム開発のトラブルはどこからくるのか？」

【要旨】

企業にとっての IT システムの在り方やこれからの活用方法は様々ですが、実は近年発生したシステムトラブルは業態・業界を問わず同様の傾向を示しています。特に予想外・想定外のトラブル発生には、技術者のスキル・経験・勘所が深く関わっているようです。本講演では、システムトラブルの主原因の一つであるソフトウェア品質に焦点を充て、従来技術では補えない品質課題とトラブル解決・回避のコツを共有します。

【講演録】

１．品質に対する一般認識

①品質の一般定義は絶対的なものでなく相対的なものです。

ISO8402 によれば「ある“もの”の明示されたまたは暗黙の必要性を満たす能力に関する特性の全体」。

ISO9000 によれば「本来備わっている特性の集まりが、要求事項を満たす程度」。

②顧客の IT に対する期待も顧客の中の立場によって異なり、品質の一律的な定義はできません。

③プロジェクトの失敗について

プロジェクトの成功率については過去からいろんな調査がなされています。ここで紹介された事例（2003 年日経コンピュータ）によれば、プロジェクトは 3 割しか成功していません。また、失敗の半数以上が品質問題となっています。品質の問題となっていますが、開発手法や開発者の品質の問題なのかもしれません。

失敗プロジェクトの分類の方法として、プロジェクトそのものに問題がある場合と、業界や組織に構造的な問題がある場合に区別する方法もあります。

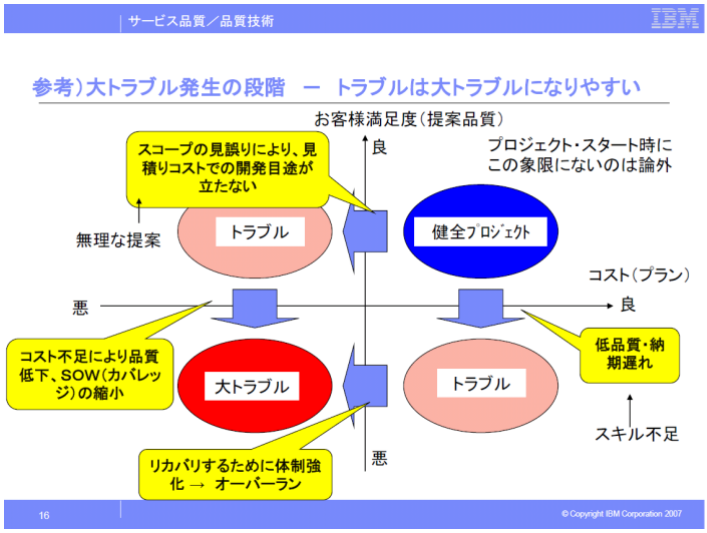
④情報システム部門のミッションも変わっています

情報システム部門のミッションも変わってきています。一時的にはアウトソーシングをしたり、オフショアを活用することが流行となった時期もありますが、最近では内部統制やセキュリティの問題から内包化に進む情報システム部門も増えてきています。

２．大トラブルの発生について

大トラブルの発生と負の連鎖には大きな関連があります。負の連鎖を断ち切らないと大トラブルは発生し続けます。では、どのように大トラブルが発生するのでしょうか。

1)大トラブル発生の段階　－　トラブルは大トラブルになりやすい

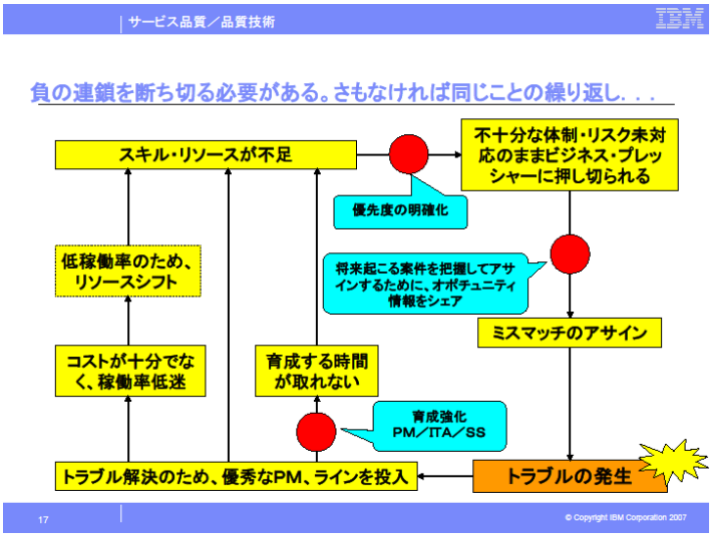


この図はトラブルが大トラブルに移る変遷を示したものです。

最初は健全なプロジェクト（右上）も、スキル不足により低品質・納期遅れが発生するとお客様満足度が低下するトラブルプロジェクトになります（右下）。トラブルの手当が出来なかったり、対応不十分だったりすると「体制強化によるコストオーバー」が発生し、大トラブルとなります(左下)。

スコープの見誤りにより、提案した見積コストでは開発目途が立たずコスト面の問題が発生しすることもあります（左上）。そして、コスト不足により品質低下やスコープの縮小を引き起こし、お客様満足度（提案品質）が下がり、大トラブルになるケースもあります（左下）。

2) 負の連鎖を断ち切る必要がある。さもなければ同じことの繰り返し



この図は負の連鎖を示したものです。負の連鎖とは、①トラブルの発生(右下)、②トラブル発生のために優秀な PM・ラインを投入、③リソースが不足する、④新たなプロジェクトを推進するもリソースがミスマッチ(スキルアンマッチ)、⑤次のトラブルの発生という、一つのトラブルが次のトラブルを引き起こす連鎖のことです。これを断ち切るには「要員の育成」「プロジェクトの優先度の明確化（QCD の何を優先にするか明確にすること）」「オポチュニティ（リソースとスキル）情報の共有」などの対策が必要です。特に育成（PM や IT アーキテクチャー等）の育成が重要です。育成により武器（スキル）を持たせることが出来ます。逆に育成をせずに実践をさせることは、武器を持たせずに戦わせるのと同義で無謀なことです。

どちらのケースも「スキルにマッチした人材の投入」が対策としては有効かつ必須となります。マッチした人材をアサインできないことは「経営の問題」なのです。このことを、「経営」が意識して対策しないと、トラブルはなくなりません。しかも、数年間トラブルに対応していると、世の中の技術の進歩から遅れてしまい、ますます技術力（武器）がなくなってしまいます。ここにも負の連鎖が入り込みます。

適正な教育ができていないことは大きな問題です。1980 年以降生まれの人とそれより前に生まれた人の間にジェネレーションギャップがあります。というのも、80 年代や 90 年代は開発、システム構築をしていた技術者がいろんなことを学べるいい時代でした。知らなければならない技法も限られており、他人と同じように

悩みながら手法を確立できていました。しかし、同じように今の若い人が学ぶためのチャンスを与えていますか？(*2)、そのフォローをしていますか？ 若い人にフィードバックしていますか？

逆に有効に教育している事例として、ブラックボックス化したシステムを維持するために若手だけで作り変えることを行っている企業もあることが紹介されました。

プロセスを整えるという対策もあります。しかし、プロセスを整えれば整えるほど使用者はプロセスの意味を考えなくなり、そのプロセスの意味を説明できず、何も疑問を持たずに使ってしまうという問題があります。しかも、プロセスそのものが意味ないものになっていることも有り得ます。

3. トラブルを解消するためのポイント

トラブルを解消するためのポイントとして、まずは、トラブルを早めにキャッチする方法を紹介されました。

1）プロジェクトの健康度を図るために７つの観点（７Keys）をモニタリングして月次でプロジェクト状況を把握するという方法を実施しています。品質、コスト、進捗、リスクに加え、ステークホルダーがコミットしていること、スコープは現実的で的確に管理されていること、チームは高いパフォーマンスを実現していることの７Keys です。 7Keys の分析値の時系列変化をモニタリングすることによって得られたプロジェクトがトラブルに至るパターンを共有して、当該プロジェクトがトラブルになりそうかを判断します。

2）品質欠陥の兆候の把握

マススケジュールやコミュニケーション状況により把握できます。例えば

3）失敗プロジェクトの共通項として、「プロセスや標準からの逸脱」がありますので、逸脱していないかをモニタリングすることも有効です。

4.品質向上のポイント

まず、品質を「顧客の要求を満たすこと」と定義しています。

品質を高めるためには、サービスを提供するデリバリーチームのプロジェクトマネジメント能力、CRM プロセス、QA レビューがポイントです。

1）「お客様の要求を満たす」ためにはデリバリーチームの品質が高い必要があり、高いプロジェクトマネジメント能力が求められます。プロジェクトマネジメントの使命は、①決められた品質以上の成果を②決められた期間以内で③決められた予算以内で実行することです。

ソフトウェア開発の生産性の個人差が３～２５倍以上あるということは従来と変わっていません。そのため、品質を高めるためには、デリバリーチームメンバーのスキルの維持向上が必須となります。そのための教育が重要なのです。ここで言うスキルは、3 つの領域（経営、ビジネス、IT）により定義しています。また、プロジェクトマネジメント体系に沿ってプロジェクトを遂行することが求められています。

プロジェクト内のインスペクションやチームレビューなど日常の品質管理活動も重要です。この欠陥除去活動は規模の大きなプロジェクトほど効果が期待できます。

2）CRM プロセス

オポチュニティ・マネジメントによる、企画計画段階でのトラブル除去を図っています。

3）QA レビュー

QA とは、お客様のご要望を満たし、高品質かつ一定の利益の確保が出来るソリューション提供を確実にするための独立したレビュー活動のことです。QA の目的は、①トラブル予防、②発生トラブル対応、③スキル向上です。レビュー内容によってプロジェクトを止める権限を持っています。

QA では製品品質(正しいものを作っているか)およびプロセス品質（正しく作っているか）の両面で品質を検証しています。

QA 部門は市場を理解しておくことも大切です。スキル維持のために定期的に QA 部門と現場との入れ替えをしています。QA がないがしろにしているところはトラブルになる確率が高い傾向があります。

これらの活動により、トラブルプロジェクトの数は減少しています。

【所感】

当日の朝、米朝会談のシンガポールからのフライトで海外出張を終えて会場に来られた細川様は、旅の疲れを見せることなく、十分なアイスブレークを行ったうえで本題に入られました。

まず、品質管理手法やプロセスが硬直しているのではないかとの問いかけがありました。ISO9001 が導入されたのは1990年代前半で、製品の品質管理プロセスをシステムのプロセスに当てはめて使っていました。2015 年版の ISO9001 でずいぶんプロセスは変わりましたが、システム開発におけるプロセスには大きな変更はありません。製造品質について 70 年近く前の品質管理手法がいまだに使われていることを考えると、手法としては正しいかもしれませんが、現実のプロジェクトの現場には合わなくなってきています。そうやって考えると、古い（硬直した、有効でない）プロセスを順守しても品質面には改善が図られないという主張はもっともなことです。プロセスの有効性に対して疑問を持つことの重要性を改めて認識しました。

さらに、教育の重要性についても語られていました。「この研究会に来ている参加者は恵まれている時代にシステムを構築するという経験を持っているが、今の若い人に経験してもらえるだろうか。また、過去に受けた教育（や経験）を若い人にはたしてフィードバックしているだろうか」ということがずっと頭に残り、果たして筆者も若い人にどこまでフィードバックしているだろうかと反省する気持ちにもなりました。戦う（システムを品質良く効率的に作る）ためにはまず武器（手法）を与えること、このことが、将来の IT の発展につながるだろうということ。また、若い人たちに教育やスキルアップの機会を与えることが重要だというメッセージは今更ながら強烈なメッセージとして響きました。

トラブルの技術的解決を図る専門家として、品質が単にプロセスだけで向上するわけではないという現場思考の考え方をしつつ、技術力の絶え間ない向上が不可欠で、かつ標準化を図ることが効率的であるという話が印象的でした。プロジェクトの成功とは？品質とは？プロセスの有効性とは？教育できていますか？等様々な問いかけをされていましたが、そのことにより、いろいろ考えさせられる講演でした。

<目次>

2018.10

法人部会報告　【　日産証券株式会社様　情報セキュリティ研修　実施　】

会員番号 7075 佐々野未知 （理事、法人部会）

法人部会では、2018 年 9 月 8 日（土）、日産証券株式会社様からの依頼を受け、「情報セキュリティ対策基本コース」研修を実施しました。日産証券様は、「顧客本位」と「地域密着」を経営方針とし、また、めまぐるしく変化する経済環境、金融情勢及びお客様の投資ニーズに迅速かつ適切に対応すべく、M&A による業容の拡大、地域補完を行い、今年で設立 70 周年を迎えた証券会社です。

同社では､年に 1 回定期的に全役職員を対象に研修会を実施し、毎年テーマを定め社員教育に取り組んでおられます。特に、情報セキュリティ対策は最重要経営課題の一つと位置づけておられ、2 か月に 1 回情報セキュリティ委員会より、情報セキュリティ研修リーフレットを配布し、役職員の情報セキュリティ意識向上を図る取組みなどを行っておられますが、今回は、役職員に対し、情報セキュリティを取り巻く環境や技術の変化など、最新動向などを認識させるとともに、基本的な対策を改めて徹底するために、集合研修の開催を企画されたとのことです。

会場は 「SMBC ホール」（東京丸の内）で、社長以下役職員 315 名の皆様が受講されました。講師は当協会理事で法人部会の佐々野未知（コントロールソリューションズ株式会社代表取締役、公認会計士）が務めました。セミナーの時間は 90 分で、事前に事務局であるコンプライアンス本部様のご要望をお伺いした上で、以下のような内容としました。

1．情報セキュリティとは ～基本知識と概念の整理
　1-1 情報セキュリティとは？　1-2 情報セキュリティの脅威とリスク、インシデント
2．身近に潜む情報セキュリティの脅威とリスク
　2-1 2018 情報セキュリティの 10 大トレンド（JASA）
　2-2 2018 情報セキュリティの 10 大脅威（IPA）
　2-3 具体的な脅威について　ー　マルウェア/ウイルス、ランサムウェア、標的型メール攻撃、
　　水飲み場型攻撃、ビジネスメール詐欺、フィッシング、パスワードクラック、
　　DoS 攻撃/DDoS 攻撃、ゼロディ攻撃、ネット上の誹謗・中傷
3．情報セキュリティ対策はじめの一歩　―　従業員が注意すべき 8 つのセキュリティ対策
(1)電子メールのルール、(2) インターネット /ウェブサイトの利用・閲覧、(3) 無線 LAN のルール
(4) 情報もしくは端末の使用・持出、(5) 事務所の安全管理、(6)安全・確実な情報の廃棄
(7)ソーシャルエンジニアリング対策、(8)SNS 利用

今回の研修では、日産証券様は情報セキュリティに対する取り組みが行き届いているので、基本的な初歩のお話をすることに若干のためらいがありました。しかし、皆さま最後まで熱心にご聴講いただき、基本的な事項を分かり易く説明いただいたとのご感想もいただきました。

今回の研修が日産証券様のお役に立てたことを、講師として、また協会として大変に意義深いと考えております。終わりに、今後の日産証券様のご発展を祈念致します。

<目次>

2018.10

本部報告　PMS 要求事項【JIS Q 15001:2017】と「個人情報取扱規程」の事例　　管理策 8

会員番号　1760 斎藤由紀子　（個人情報保護監査研究会）

保有個人データとは、新個人情報保護法第 2 条 7 で定義されており、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。とあります。
旧 JIS:2006 では、"開示対象個人情報"と称していましたが、新 JIS において”保有個人データ”となり、法と用語が統一されました。

今回も、附属書 A（規定）および附属書 B（参考）の要求事項を確認しつつ、できるかぎりシンプルな規程として「3300 個人情報取扱規程」のサンプルをご紹介します。

※ この連載を基にした HTML 版を公開しています。
規格本文＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/000JISQ15001_2017.html
管理策 1＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/001JISQ15001_2017.html
管理策 2＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/002JISQ15001_2017.html
管理策 3＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/003JISQ15001_2017.html
管理策 4＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/004JISQ15001_2017.html
管理策 5＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/005JISQ15001_2017.html
管理策 6＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/006JISQ15001_2017.html
管理策 7＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/007JISQ15001_2017.html
管理策 8＞https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/008JISQ15001_2017.html

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

赤字：【2006 年版 JIS】から追加、変更となった規格

青字：PMS 監査研究会のコメント

A.3.4.4　個人情報に関する本人の権利　　（2006：3.4.4）		
A.3.4.4.1	個人情報に関する権利 2006:3.4.4.1 法第 2 条 7 法第 28 条 2 令第 4 条 令第 5 条 令第 9 条	組織は、保有個人データに関して、本人から開示等の請求等を受け付けた場合は、A.3.4.4.4 ～ A.3.4.4.7 の規定によって、遅滞なくこれに応じなければならない。ただし、次に掲げるいずれかに該当する場合は、保有個人データには当たらない。 a)当該個人データの存否が明らかになることによって、本人又は第三者の生命、身体又は財産に危害が及ぶおそれのあるもの b)当該個人データの存否が明らかになることによって、違法又は不当な行為を助長する、又は誘発するおそれのあるもの c)当該個人データの存否が明らかになることによって、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれのあるもの d)当該個人データの存否が明らかになることによって、犯罪の予防、鎮圧又は捜査その他の公共の安全及び秩序維持に支障が及ぶおそれのあるもの 組織は、保有個人データには該当しないが、本人から求められる利用目的の通知、開示、内容の訂正、追加または削除、利用の停止、消去及び第三者への提供の停止の請求などの全てに応じることができる権限を有する個人情報についても、保有個人データと同様に取り扱わなければならない。
	附属書 B.3.4.4.1	A.3.4.4.1a)の場合とは、例えば、家庭内暴力又は児童虐待の被害者の支援団体が、加害者（配偶者又は親権者）及び被害者（配偶者又は子）を本人とする個人データをもっている場合などをいう。 A.3.4.4.1b)の場合とは、例えば、いわゆる総会屋などによる不当要求被害を防止するため、組織が総会屋などを本人とする個人データをもっている場合、不審者、悪質

		なクレーマーなどからの不当要求被害を防止するため当該行為を繰り返す者を本人とする個人データを保有している場合などをいう。 A.3.4.4.1c)の場合とは、例えば、製造業者、情報サービス事業者などが、防衛に関する兵器・設備・機器・ソフトウェアなどの設計、開発担当者名が記録された個人データを保有している場合、要人の訪問先やその警備会社が、当該要人を本人とする行動予定、記録などを保有している場合などをいう。 A.3.4.4.1d)の場合とは、例えば、警察からの捜査関係事項照会や捜査差押令状の対象となった組織がその対応の過程で捜査対象者又は被疑者を本人とする個人データを保有している場合などをいう。 “保有個人データには該当しないが、本人から求められる利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の請求などの全てに応じることができる権限を有する個人情報”とは、組織が取得してから政令で定める期間以内に消去する個人データなどをいう。消費者など、本人の権利利益保護の観点から、組織は、保有個人データ、個人データに限らず、取得した全ての個人情報について、保有個人データと同等に取り扱うことが望ましい。
	【P マーク審査対応のポイント】 ・更新事業者の規程類において「開示対象個人情報」と称していても差し支えない。 ・個人データだけでなく、保有個人情報についても保有個人データと同様に取扱う。 ・コールセンターの音声記録、監視カメラの画像、未整理の応募ハガキ、従業者個人が管理する名刺なども対象となる。 ・受託している個人データおよび個人情報は、保有個人データおよび保有個人情報ではない。 ・旧 JIS の、3.4.4.1 では、「開示対象個人情報」（電子計算機を用いて検索することができるように体系的に構成した情報の集合物又は一定の規則に従って整理、分類し、目次、索引、符合などを付すことによって特定の個人情報を容易に検索できるように体系的に構成した情報の集合物を構成する個人情報）と規定されていたが、その規定が外されたため、未整理の応募ハガキ等も対象となる。 ・法第二条第七項では、保有個人データから除外されるものとして、以下を定めている。 1.その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの。 ※政令 4 条の定めでは、公益その他の利益が害されるものについては、A.3.4.4.1 のただし書き a)～d）と同じ。 2.一年以内の政令で定める期間以内に消去することとなるもの ※政令 5 条の定めでは、消去までの期間を 6 ヶ月としている。ただし JIS 規格では消去までの期間を問わない。 ・旧 JIS では、"容易に検索できる状態に無い"個人情報については、A.3.4.4.4（利用目的の通知）以外の、A.3.4.4.6（訂正、追加又は削除）、A.3.4.4.7（利用又は提供の拒否権）の請求について、本人に対し、対応が困難である旨理由を説明することで、対応しないことが容認されていた。今後対応が困難だと回答した場合は、個人情報の保管に関する安全管理面の不備を、個人情報保護委員会もしくは認定個人情報保護団体へ苦情申し立てされる可能性があることに注意が必要である。	

【3300 個人情報取扱規程】サンプル

3.4.4　個人情報に関する本人の権利

3.4.4.1　個人情報に関する権利

本人から、保有個人データおよび保有個人情報（以後、保有個人データ等と呼ぶ）について利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止、消去および第三者への提供の停止（以下「開示等」という）を請求された場合に遅滞なくこれに応じるための責任者および権限を「3341-01 個人情報保護体制別紙：3341-02PMS に関する責任と権限一覧表」に定める。

2　開示等の請求があったときは、「3440-01 個人情報開示等請求書兼回答書」によって個人情報保護管理者の承認を得た後に、遅滞なく（10 日以内をめどとする）結果を本人に通知しなければならない。詳細は 3.4.4.8、3.4.4.9 に規定する。

3　ただし、当該個人データ等の存否が明らかになることによって、次のいずれかに該当するおそれのあるものは保有個人データ等ではないため、開示請求等に応じる必要はない。

	当該個人情報の存否が明らかになることによって・・・
a)	本人又は第三者の生命、身体又は財産に危害が及ぶおそれのあるもの
b)	違法又は不当な行為を助長し、又は誘発するおそれのあるもの
c)	国の安全が害されるおそれ、他国もしくは国際機関との信頼関係が損なわれるおそれ又は他国もしくは国際機関との交渉上不利益を被るおそれのあるもの
d)	犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序維持に支障が及ぶおそれのあるもの

4　ただし書きを適用して開示請求等に応じられない場合は、3.4.4.9 の手順に従い、本人に対し、回答に応じられない旨を通知しなければならない。

■

<table>
<tr><td rowspan="3">A.3.4.4.2</td><td>開示等の請求等に応じる手続

2006：3.4.4.2

法第 32 条
法第 33 条 2
令第 10 条
令第 11 条</td><td>組織は、開示等の請求等に応じる手続として次の事項を定めなければならない。
a)開示等の請求等の申出先
b)開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式
c)開示等の請求等をする者が、本人又は代理人であることの確認の方法
d)A.3.4.4.4 又は A.3.4.4.5 による場合の手数料（定めた場合に限る。）の徴収方法
組織は、本人からの開示等の請求等に応じる手続を定めるに当たっては、本人に過重な負担を課するものとならないよう配慮しなければならない。

事業者は、A.3.4.4.4 又は A.3.4.4.5 によって本人からの請求等に応じる場合に、手数料を徴収するときは、実費を勘案して合理的であると認められる範囲内において、その額を定めなければならない。</td></tr>
<tr><td>附属書 B
3.4.4.2</td><td>A.3.4.4.2b)は、本人が容易かつ的確に開示等の請求等をすることができるよう、組織が当該保有個人データの特定に資する情報の提供その他本人の利便性を考慮した適切な措置を講じることを求めている。

A.3.4.4.2c)については、開示等の請求等をすることができる代理人は、次の代理人である。
－未成年者又は成年被後見人の法定代理人
－開示等の請求等をすることにつき本人が委託した代理人

組織が、開示等の請求等を受け付ける方法を合理的な範囲で定めてある場合に、請求等を行った者がそれに従わなかったときは、開示等を拒否することができる。 ただし、本人確認に当たっては、例えば、通常業務において ID 及びパスワードで本人確認をしているにもかかわらず、開示等の請求等に応じる手続については、一律、運転免許証又はパスポートの呈示を求めるなど、本人に必要以上の個人情報の提供を求めないことが望ましい。</td></tr>
<tr><td colspan="2">【P マーク審査対応のポイント】
・本人は、事業者が定めた方法に従って開示等の請求等を行わなければならない。（法 32 条 1）
・a) 開示等の請求等の申出先は、消費者窓口など実際に保有個人データを取扱っている部門が望ましい。取扱いが従業者の保有個人データしか無い事業者の場合は、人事部門でも差し支えない。
・b) 本人が開示等の請求等を行う場合には、対象となる保有個人データを特定するに足りる事項の提示を行う必要がある。そのため、事業者は本人が必要事項を記入できるための「開示等請求書式」を定めることが望ましい。また、できればダウンロード可能とすることが望ましい。
・c) 開示等の請求等ができる代理人は、施行令第 11 条に定めがあり、附属書 B に記載の通りである。
・未成年については、民法第 2 章第 2 節第 4 条に年齢 20 歳未満の者とされているが、2022 年 4 月 1 日より 18 歳未満に引き下げられる予定である。
・成年被後見人については、民法第 2 章第 2 節第 9 条に、本人が行った行為で不利益が起きた場合は取り消すことができるとしており、本人保護のための法律である。事業者が本人が成年被後見人であるかどうかをわざわざ確認する必要はない。
・本人が委託した代理人とは、民法第 5 章第 3 節（第 99 条～第 118 条）に定めがある。委任状の書式に定めはないが、本人の氏名と代理人の氏名は必要である。
・d) 手数料は、A.3.4.4.4 利用目的の通知、A.3.4.4.5 開示の請求のみ徴収することができる。その徴収方法は、合理的でなければならず、徴収方法として例えば切手同封や定額小為替（手数料 100 円）、金融機関への振込時の手数料の負担など明確にしなければならない。もちろん無料でも差し支えない。</td></tr>
</table>

【3300 個人情報取扱規程】サンプル

3.4.4.2　開示等の請求等に応じる手続

本人からの開示等の請求等に応じる手続は、本人に過重な負担を課さないよう配慮し、下記について公表文書「3220 個人情報の取扱いについて」に定める。

a)	開示等の請求等の申し出先
b)	開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式
c)	開示等の請求等をする者が、本人又は代理人であることの確認の方法
d)	利用目的の通知、又は開示の場合の手数料およびその徴収方法

2 手数料は、利用目的の通知、又は開示についてのみ徴収することとし「3220 個人情報の取扱いについて」に定めて公表する。

■

A.3.4.4.3	保有個人データに関する事項の周知など 2006：3.4.4.3 法第 27 条 1 法第 47 条 令第 8 条	組織は、当該保有個人データに関し、次の事項を本人の知り得る状態（本人の請求等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。 a)組織の氏名又は名称 b)個人情報保護管理者（若しくはその代理人）の氏名又は職名、所属及び連絡先 c)全ての保有個人データの利用目的[A.3.4.2.4 の a)～c) までに該当する場合を除く。] d)保有個人データの取扱いに関する苦情の申し出先 e)当該組織が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先 f)A.3.4.4.2 によって定めた手続
	附属書 B 3.4.4.3	“本人が知り得る状態（本人の請求などに応じて遅滞なく回答する場合を含む。）”とは、ウェブ画面への掲載、パンフレットの配布、本人の請求などに応じて遅滞無く回答を行うことなど、本人が知ろうと思えば知ることができる状態に置くことをいい、組織が、常にその時点で正確な内容を本人が知り得る状態に置くことをいう。必ずしもウェブ画面への掲載、又は事務所などの窓口などへ掲示することなどが継続的に行われることまでを指すものではないが、事業の性質及び個人情報の取扱状況に応じ、内容が本人に理解される合理的かつ適切な方法によることが望ましい。 なお、組織は、家族から開示等を求められることもあり得るため、そのような場合も含め、開示等の請求等に対する対応方法の詳細を定めた上で、知り得る状態に置いておくことが望ましい。
	表 B.1 表示事項整理表	（略） f)A.3.4.4.2 によって定めた手続 f)a) 開示等の請求等の申出先 f)b) 開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式 f)c) 開示等の請求等をする者が、本人又は代理人であることの確認の方法 f)d) 本人から、利用目的の通知又は保有個人データの開示の請求などをされた場合の手数料（定めた場合に限る。）の徴収方法
	【P マーク審査対応のポイント】 ・個人データだけでなく、保有個人情報についても保有個人データと同様に取扱う。 ・周知の方法として、一般的にはホームページに「開示等の請求等について」等を公開する。ホームページを持たない場合は、会社案内もしくは、リーフレットを用意すること。 ・b）個人情報保護管理者については、氏名又は職名、所属を掲載し、また、連絡先（住所、電話番号、メールアドレス等）を公表すること。 ・c）全ての保有個人データの利用目的の公表とは ・A.3.4.2.4 において、事業で取扱う全ての個人情報の利用目的を公表するよう求めている。そこでは、受託する個人情報なども含まれており、必ずしも保有個人データではない。 ・従って、A.3.4.2.4 の公表事項の備考欄に「※受託する個人情報については、当社に開示等の権限はありません」と掲示するか、もしくは別途「保有個人データの利用目的」を公表する必要がある。 ・d）苦情と開示請求とは趣旨が異なる。苦情の申出先は個人情報保護管理者でもよい。 ・e）新規申請事業者は、認定個人情報保護団体には加入していないため、省略してよい。 ・f）　前項で定めた手続きの内容	

【3300 個人情報取扱規程】サンプル

3.4.4.3　保有個人データに関する事項の周知など

公表文書「3220 個人情報の取扱いについて」には次の事項を含め、個人情報保護管理者の承認を得て、事務局がホームページに公開する。ホームページを閲覧できない本人からの問い合わせがあった場合は、ホームページを印刷して郵送、FAX 送信など、本人の希望する手段で送付する。

a)	会社名
b)	個人情報保護管理者の氏名、所属および連絡先
c)	すべての保有個人データの利用目的（3.4.2.4 の a)～c)に該当する場合を除く）
d)	保有個人データの取扱いに関する苦情の申し出先
e)	認定個人情報保護団体の名称および苦情の解決の申し出先
f)	3.4.4.2 によって定めた、下記の手続
	a)開示等の請求等の申し出先
	b) 開示等の請求等に際して提出すべき書面の様式その他の開示等の請求等の方式
	c) 開示等の請求等をする者が、本人又は代理人であることの確認の方法
	d) 利用目的の通知、又は開示の場合の手数料およびその徴収方法

■

A.3.4.4.4	保有個人データの利用目的の通知 2006：3.4.4.4 法第 27 条 2、3 法第 31 条 法第 32 条	組織は、本人から、当該本人が識別される保有個人データについて、利用目的の通知を求められた場合には、遅滞なくこれに応じなければならない。ただし、A.3.4.2.4 のただし書き a)～c) のいずれかに該当する場合、又は A.3.4.4.3 の c) によって当該本人が識別される保有個人データの利用目的が明らかな場合は利用目的の通知を必要としないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。
	附属書 B	なし
	表 B.1 表示事項整理表 (要旨)	本人に遅滞なく通知する。 利用目的の通知をしないときは、理由を説明する。
	【P マーク審査対応のポイント】 ・個人データだけでなく、保有個人情報についても保有個人データと同様に取扱う。 ・法第 18 条では、取得時にその利用目的を本人に通知、又は公表しなければならないと規定しており、既に本人に伝えて同意を得て取得した場合であっても、再度利用目的の通知を求められた場合には、応じなければならない。ただし、A.3.4.4.3 の c）によって、既にホームページに公表されている場合は、本人にその URL を示せばよい。 ・ただし書きによって利用目的を通知しないのは、3.4.2.4（個人情報を取得した場合の措置）の通知もしくは公表を省略する場合と同じ。 ・3.4.2.4 b）当社の権利又は正当な利益を害するおそれがある場合、とは、通知される利用目的の内容によって新製品などの開発内容など企業秘密にかかわるようなものが明らかになる場合などをいう。	

【3300 個人情報取扱規程】サンプル

3.4.4.4　保有個人データの利用目的の通知

本人から、保有個人データの利用目的の通知を請求された場合には、3.4.4.9 の手順に従い遅滞なくこれに応じる。

2　利用目的を通知しない場合は、下記の場合に限定する。ただし、その場合は、「3440-01 個人情報開示等請求書兼回答書」に利用目的を通知しない理由を記入し、個人情報保護管理者の承認を得て、本人に通知する。

利用目的通知・公表により		4.例外の項目
a)	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	3.4.2.4　a)
b)	当社の権利又は正当な利益を害するおそれがある場合	3.4.2.4　b)
c)	国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することによって当該事務の遂行に支障を及ぼすおそれがあるとき	3.4.2.4　c)
d)	取得の状況からみて利用目的が明らかであると認められる場合	3.4.2.4　d)
e)	ホームページに既に保有個人データの利用目的を掲載している。	3.4.4.3　c)

■

A.3.4.4.5	保有個人データの開示 2006：3.4.4.5 法第 28 条 法第 31 条 法第 32 条 令第 9 条	組織は、本人から、当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。）の請求を受けたときは、法令の規定によって特別の手続が定められている場合を除き、本人に対し、遅滞なく、当該保有個人データを書面（開示の請求を行った者が同意した方法があるときは、当該方法）によって開示しなければならない。ただし、開示することによって次のa)～c) のいずれかに該当する場合は、その全部又は一部を開示する必要はないが、そのときは，本人に遅滞なくその旨を通知するとともに，理由を説明しなければならない。 a)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 b)当該組織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 c)法令に違反する場合
	附属書 B 3.4.4.5	A.3.4.4.5b)の、“当該組織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”とは、試験実施機関において、採点情報の全てを開示することによって、試験制度の維持に著しい支障を及ぼすおそれがある場合、同一の本人から複雑な対応を要する同一内容について繰り返し開示の請求があり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなるなど、業務上著しい支障を及ぼすおそれがある場合などをいう。 なお、消費者など、本人の権利利益保護の観点から、事業活動の特性、規模及び実態を考慮して、個人情報の取得元又は取得方法（取得源の種類など）を可能な限り具体的に明記し、問い合わせなどがあった場合には、本人からの請求などに一層対応していくことが望ましい。
	表 B.1 表示事項整理表 (要旨)	法令の規定によって特別の手続が定められている場合を除き、本人に対し、遅滞なく、書面（開示の請求を行った者が同意した方法があるときは、当該方法）によって開示する。開示をしないときは、理由を説明する。
	【P マーク審査対応のポイント】 ・個人データだけでなく、保有個人情報についても保有個人データと同様に取扱う。 ・法令の規定によって特別の手続きが決められている場合とは、例えば行政機関情報公開法第 15 条で、有価証券届出書等や宅地取引業者名簿の開示の方法が定められている場合などを指す。	

【3300 個人情報取扱規程】サンプル

3.4.4.5　保有個人データの開示

本人から、保有個人データの開示もしくは、開示個人情報が存在しないことの確認を請求されたときは、3.4.4.9 の手順に従い遅滞なくこれに応じる。

2　法令の規定によって特別の手続が定められている場合は、その法令に従う。

3　開示請求に応じない場合は、下記の場合に限定する

a)	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
b)	当社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
c)	他の法令に違反する場合

■

A.3.4.4.6	保有個人データの訂正、追加又は削除 2006：3.4.4.6 法第 29 条 法第 31 条 法第 32 条	組織は、本人から、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いう理由によって当該保有個人データの訂正、追加又は削除（以下、この項において“訂正等”という。）の請求を受けた場合は、法令の規定により特別の手続が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該保有個人データの訂正等を行わなければならない。また、事業者は、訂正等を行ったときは、その旨及びその内容を、本人に対し、遅滞なく通知し、訂正等を行わない旨の決定をしたときは、その旨及びその理由を、本人に対し、遅滞なく通知しなければならない。
	附属書 B	なし
	表 B.1 表示事項整理表 (要旨)	訂正等を行わない旨の決定をしたときは、その理由説明する。

	【P マーク審査対応のポイント】 ・個人データだけでなく、保有個人情報についても保有個人データと同様に取扱う。 ・訂正、追加又は削除は、無償で行う。

【3300 個人情報取扱規程】サンプル

3.4.4.6　保有個人データの訂正、追加又は削除

本人から、内容が事実でないという理由によって、訂正、追加又は削除（以下「訂正等」）を請求された場合は、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づいて、当該保有個人データの訂正等を行い、3.4.4.9（本人への回答方法）の手順に従い無料でこれに応じる。

2　法令の規定によって特別の手続が定められている場合は、その法令に従う。

3　訂正等を行わない場合は、下記に限定する。

・	利用目的からみて訂正等が必要ではない場合（評価に関する情報など）

4　日常的に実施する顧客情報の訂正等についても「3440-01 個人情報開示等請求書兼回答書」の手順に従う。

■

A.3.4.4.7	保有個人データの利用又は提供の拒否権 2006：3.4.4.7 法第 30 条 法第 31 条 法第 32 条 令第 10 条 令第 11 条	組織は、本人から、当該本人が識別される保有個人データの利用の停止、消去又は第三者への提供の停止（以下、この項において“利用停止等”という。）の請求を受けた場合は、これに応じなければならない。また，措置を講じた後は，遅滞なくその旨を本人に通知しなければならない。ただし、A.3.4.4.5 のただし書き a)～c) のいずれかに該当する場合は、利用停止等を行う必要はないが、そのときは、本人に遅滞なくその旨を通知するとともに、理由を説明しなければならない。
	附属書 B 3.4.4.7 法第 30 条 2、4	本人の同意を得た範囲内で組織が取り扱う場合でも、本人が求めた場合は、組織はそれに応じることが望ましい。 なお、当該保有個人データの第三者への提供の停止に著しく多額の費用を要する場合、その他の第三者への提供を停止する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講じるときは、法令等によってこの限りでないとされている。 また、消費者など、本人の権利利益保護の観点から、事業活動の特性、規模及び実態を考慮して、保有個人データについて本人から請求などがあった場合には、ダイレクトメールの発送停止など、自主的に利用停止に応じるなど、本人からの請求などに一層対応していくことが望ましい。
	表 B.1 表示事項整理表(要旨)	利用停止等を行わないときは、その理由を説明する。
	【P マーク審査対応のポイント】 ・個人データだけでなく、保有個人情報についても保有個人データと同様に取扱う。 ・対応するための費用は、無償で行う。 ・当該保有個人データの利用停止に著しく多額の費用を要する場合、A.3.4.4.5 b）適正な実施に著しい支障を及ぼすおそれがある場合、のただし書き適用が可能としているが、"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講じるときは"と、のただし書きが付いているため、"これに代わる措置"を準備し、本人に説明しなければならない。 ・ EU 一般データ保護規則（GDPR）では「データポータビリティの権利」として、本人が自分の保有個人データについて、現在の管理者から一般の機械可読性のある形式（例：CSV 形式）で受け取り、他の管理者に移行する権利があると規定している。現在の新個人情報保護法や JIS Q 15001：2017 ではその規定はないが、今後法改正の動向に注意する必要がある。	

【3300 個人情報取扱規程】サンプル

3.4.4.7　保有個人データの利用又は提供の拒否権

本人から、保有個人データの利用の停止、消去又は第三者への提供の停止（以下「利用停止等」という）を請求された場合は、遅滞なく措置を講じ、3.4.4.9（本人への回答方法）の手順に従い無料でこれに応じる。

2　法令の規定によって特別の手続が定められている場合は、その法令に従う。

3　利用又は提供の拒否に応じない場合は、下記の場合に限定する。

a)	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
b)	当社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で、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講じるとき
c)	法令に違反することとなる場合

3.4.4.8　本人および保有個人データの確認

本人から開示等の要求があった場合、本人であることの確認、および保有個人データであるかどうかを、以下の方法で確認してから対応する。

2　本人かどうかの確認は、「3440-01 個人情報開示等請求書兼回答書」に記載された氏名、住所、電話番号によって、当社が保有している個人情報と照合して行う。当社が保有している個人情報と異なる場合、および訂正、削除を請求された場合は、運転免許証、住民票など、本人確認できる書類の提示を求める。

3　開示等受付担当者は、「3312 個人情報管理台帳」により保有個人データかどうかを確認する。もし保有個人データではない場合、又は開示等の要求が 3.4.4.1 のただし書き a)～d)に該当する場合は、開示等の請求等に応じられないため、「3440-01 個人情報開示等請求書兼回答書」の、回答できない理由欄にその旨記入し、個人情報保護管理者の承認を求める。

4　代理人からの開示請求については、以下の a)代理人であることを証明する書類、および代理人の身許を証明する b)のいずれかの書類の提示を求める。

a)	代理人であることを証明する書類（委任状等）
b)	・運転免許証、パスポート等の写真の写し（代理人の名前・住所が記載されたもの）
	・住民票の写し（開示等の請求等をする日前 30 日以内に作成されたもの）
	・代理人が弁護士の場合は、登録番号のわかる書類

3.4.4.9　本人への回答方法

本人への回答は、開示等受付担当者が「3440-01 個人情報開示等請求書兼回答書」に記載し、個人情報保護管理者の承認を得て、書面もしくは本人が同意した方法によって回答する。

2　開示等の請求等に応じられないときは、開示等受付担当者が「3440-01 個人情報開示等請求書兼回答書」の回答できない理由欄にその旨記載し、個人情報保護管理者の承認を得て、書面もしくは本人が同意した方法によって回答する。

■

次回は、3.4.5　認識、および　3.5 文書化した情報　から考察します。

以上　■■

<目次>

2018.10

支部報告　【　北海道支部　2018 年 9 月の月例研究会　】

会員番号　1448 宮崎雅年　（北海道支部）

北海道支部では、以下のとおり 2018 年 9 月の月例研究会を開催しました。

- **日時：2018 年 9 月 27 日（木）18:30～20:30　　参加者：5 名**
- **会場：札幌市男女共同参画センター OA 研修室（札幌市）**
- **内容：ＤＶＤ視聴（約 2 時間）と意見交換**
- **演題：「残念なＢＣＰとこれからのＢＣＰ」（本部の第 230 回月例研究会の映像）**
- **講師：指田朝久氏**
  東京海上日動リスクコンサルティング株式会社
  ソリューション創造本部　主幹研究員　兼
  立教大学 21 世紀社会デザイン研究科特任教授

＜ＤＶＤ視聴の前に＞

2018 年 9 月 6 日午前 3 時 8 分頃に最大震度 7 を記録した北海道胆振東部地震発生し、それに続いて北海道全域で停電が発生してブラックアウトを経験しました。

地震により、お亡くなりになられた方々に心よりお悔やみを申し上げますとともに、被害を受けた皆さまに心よりお見舞いを申し上げます。

また、スマートフォンが日常生活に深く関わっているなか、停電では大変な不便を経験し、いまだ無理のない範囲での節電が継続しており、改めて電気の大切さを認識いたしました。

今回の月例研究会の演題は北海道胆振東部地震発生前に決定したものですが、あまりにもタイムリーな内容であることから、本部月例研究会の DVD 視聴・意見交換ではありますが、支部報告としてまとめて会報に投稿するものです。

なお、月例研究会での意見交換の内容は、参加者の個人的意見であり、参加者の所属する組織の意見を代弁するものではありません。

＜ＤＶＤ視聴＞

ＤＶＤ視聴による講演の内容については、既に開催された本部月例研究会の内容であることから詳細は割愛いたしますが、これまでのＢＣＰは防災や安否確認を目的として策定されているものが多く、2016 年 4 月に発生した熊本地震では残念な結果になった一方、顧客目線にたって供給責任を果たすことを目的として策定されたＢＣＰは有効に機能したという内容が印象に残りました。

また、話には聞いていましたが実際に経験することがあるとは思ってもいなかったブラックアウトを経験し、顧客目線にたった供給責任を果たすというＢＣＰの目的に対して反省する次第です。

＜ＤＶＤ視聴後の意見交換＞

地震と停電が発生した９月６日は、公共交通機関も運行を停止したことから自宅待機となった企業・団体があった一方、北海道庁、市町村役場、警察、消防などの官公庁のほか、電力会社、通信事業者、公共交通機関、金融機関、放送事業者などの重要インフラに関わっている方々は、地震発生直後から非常事態態勢に移行して不休不眠で事態の対応にあたっていたことは、容易に想像できます。

札幌市内でも震度５強を観測したところがあり、地震による被害のほか、今回の停電とブラックアウトの原因と復旧の経過については、新聞などで報道されているため改めて記載しませんが、リスクの認識と対策という点で、どこまでリスクを許容するのか、回避しなくてはならないリスクは何か、リスクを移転することが可能なのか、リスクの低減（対策）が有効なのかという観点から、顧客への供給責任を果たすという目的に対して残念なＢＣＰとなっていないか見直す必要があるでしょう。

特に、電気がなければ水が出ない、電話が通じないなど、長時間の停電は、企業・団体・個人を問わず現在社会は電気があることを前提していることを改めて認識させてくれました。

北海道内のデータセンター事業者がどのような対応を取ったのかは、日経コンピュータ誌などに詳しく記載されています。記事によると、非常用発電機が稼働して安定した運用を継続したとのことですが、これまで地震が少ない地域ということで北海道にバックアップセンターを誘致してきた経緯もあり、影響は少なからずあるものと想定いたします。

また、酪農などの一次産業への影響、物流などの二次産業への影響、スーパーなどの三次産業への影響が強力なサプライチェーンの中で一気に拡大し、収束には長い時間を必要としているようです。

電子決済なども停電下ではまったく機能せず、現金決済だけという事態に、キャッシュレス社会の脆弱性を指摘せずにはいられません。

電気がなければ IT は利用できませんが、顧客の視点から供給義務を果たすＢＣＰの観点からシステム監査を実施する必要性を認識しました。

今回の地震と停電が９月上旬という比較的暖かい時期だったことは、暖房が不要で、水の凍結を心配せずに済んだという点で、不幸中の幸いだったと思います。

これが１月２月の厳冬期であったならば、暖房の利用が制限されたり、水が凍結したりと、さらに厳しい状況になったであろうと想像するだけでも恐ろしいものがあります。

企業・団体のほか、個人でも顧客の視点から供給義務を果たすＢＣＰを考えておくことが必要とのことで、９月の北海道支部月例研究会を終了いたしました。

＜支部長から全国の皆さまへ＞

地震が発生した９月６日から北海道支部に対してお見舞いやご支援申し出のメールを多数頂戴し、感謝いたします。本来であればメールをいただいた方々それぞれに対してお礼を申し上げるところではありますが、会報の場をお借りして御礼申し上げます。

北海道は元気です。今後とも北海道支部をよろしくお願いいたします。

<目次>

支部報告【北信越支部 2018 年度 長野県例会・研究報告】

会員番号　1281 宮本　茂明（北信越支部）

以下のとおり2018年度 北信越支部長野県例会を開催しました.

・日時：2018年9月8日（土） 13:00-17:00　　参加者：9名

・会場：長野市生涯学習センター 第1学習室

・議題：１．研究報告

「オープンAPIについて」 長谷部　久夫 氏

「内部統制後の考察」　　森　広志　氏

2. 近畿支部30周年記念シンポジウム「システム監査@ﾆｭｰﾌﾛﾝﾃｨｱ」参加報告　宮本　茂明

3. 西日本支部合同研究会準備検討

- 北信越支部報告検討・意見交換「キャッシュレス社会におけるデータ利活用とシステム監査」

- 運営検討（プログラム案，情報交換会，翌日ツアー等）

◇研究報告１

「オープン API について」

報告者 (会員番号　1766 長谷部　久夫)

１．報告概要

本報告は，銀行におけるオープン API（Application Programming Interface）の動向，及び方向性等を紹介するものである．API とは，アプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様・仕組みをいうが，銀行では Fintech 企業等に API を公開して，顧客の同意に基づき，銀行システムへのアクセスを許諾するオープン API の活用が始まっている.

２．オープン API を巡る動向

（１）制度的枠組みの整備

ア．金融審議会 金融制度ワーキング・グループ報告(2016 年 12 月 27 日公表)

上記の WG は，①金融機関と顧客の間に立ち，顧客の委託を受けて IT を活用した決済指図の伝達，口座情報の取得・提供を業とする者（以下「電子決済等代行業者」という）には制度的枠組みが存在しないこと，②銀行 API の非公開により，顧客から預かったパスワード等を使い金融機関と契約締結等の法的関係を構築せず，銀行システムにアクセスする「スクレイピング」によるサービスの提供に係る課題を認識した．本報告は，その認識の下で，金融機関と FinTech 企業等との連携・協働による革新（オープン・イノベーション）を進めていく上で，以下の制度的枠組みの整備を提言している.

（ア）電子決済等代行業者に対する規制の整備

（イ）金融機関におけるオープン API に対応できる体制の整備

イ．改正銀行法　（公布）2017 年 6 月 2 日，（施行）2018 年 6 月 1 日

上記ア．の報告を踏まえて，電子決済等代行業者（Fintech 企業等）に係る規制の整備を行うもの．利用者保護を確保しつつ，金融機関と Fintech 企業等とのオープン・イノベーション進めていくため

の制度的枠組みを整備した.

改正銀行法の主たる改正点は，①電子決済等代行業に対する登録制の導入，②電子決済等代行業者に対する規制（金融機関との契約締結等），③金融機関におけるオープン・イノベーション推進措置（電子決済等代行業者との連携･協働に係る方針公表,接続基準公表,オープン API 導入の努力義務）.

ウ．改正銀行法を踏まえた業界団体等の動向

全国銀行協会は，2017 年 7 月に「オープン API のあり方に関する検討会報告書」を公表している．本報告書は，銀行，IT 事業者，Fintech 企業，学識経験者，弁護士，消費者団体，関係当局等による検討会で「銀行分野におけるオープン API のあり方」を検討した成果をまとめたもので，①API 仕様の標準化，②セキュリティ対策および利用者保護，③今後の取組みが報告されている．また同協会は，2018 年 7 月に「銀行法に基づく API 利用契約の条文例（全 24 条の暫定版）」を公表している．

一方，金融情報システムセンター（FISC）は，2017 年 7 月に「API 接続チェックリスト（試行版）」を公表して「機密性」に関する共通的な確認項目を示している．現在，「可用性」「完全性」に関する確認項目の追加，及び確認項目の精緻化・類似項目の統合等の方向性で，チェックリスト（確定版）を検討中である.

（2）システム標準化の普及

上記（1）．ウの全国銀行協会の報告書は，「API 仕様の標準化」に関して，①開発原則（API 利用者目線の分かりやすくシンプルな設計等），②開発標準（アーキテクチャ・通信プロトコル・データ表現形式・認可プロトコル・バージョン管理等），③電文仕様標準（API のメッセージ上の標準項目等）の 3 つを示している．銀行オープン API のシステム標準化は，本報告書に則り進められている.

3．金融機関の対応状況

（1）電子決済等代行業者との連携及び協働に係る方針の公表

金融機関は，改正銀行法に則り，2018 年 3 月 1 日までに，電子決済代行業者との連携及び協働に係る方針（API 接続方針）を公表している．各金融機関の方針は区々だが，個人顧客・法人顧客の両方向けに，参照系 API・更新系 API ともに公開する方針を公表した金融機関が多数（日本銀行の集計では 2018 年 3 月 2 日時点で 138 先のうち 82 先が該当）.

（2）オープン API 導入に係る体制整備

API 公開に向けた方針を公表した金融機関に対しては，改正銀行法施行日より 2 年以内のオープ API 導入に係る以下のような体制整備の努力義務が課せられている．個別の銀行で体制を整備中である.

<体制整備>

○ オープン API の設計・開発，運用，保守等の対応

全国銀行協会報告等に記載の API 標準仕様，セキュリティ原則に則りシステム構築

○ オープン API 管理規程，電子決済等代行業者との接続に係る基準の策定・公表

○ 顧客に損失が生じた場合の電子決済等代行業者・銀行間の責任分担ルールの策定・公表

○ オープン・イノベーションへの取組みにおける API を活用したビジネス拡張の組織横断的な検討 等

4．オープン API のポイント整理

（1）オープン API の意義

オープン API は，単なるデータ連携上の意義を超えて，オープン・イノベーションを実現していくための手段（キー・テクノロジー）であるが、それ自体は目的ではない．経営戦略と整合させながら，ビジネス視点から組織横断的に取り組むことが重要である．

（2）オープン API のメリット

ア．ユーザー

- 送金処理や通帳の情報利用などがスムーズにできるようになる．
- ID・パスワードといった機密情報を預ける必要がなく，安心安全．

イ．電子決済等代行業者

- API 公開による提供サービスの拡張，金融機関との関係円滑化．システム改修負荷の削減．

ウ．金融機関

- 更新系 API 活用による決済を伴うビジネスや，サービスのアイデア獲得．
- 内部 API 活用による基幹システム等の軽量化，システムの疎結合化．
- インターネットバンキングへのスクレイピングの削減，負荷の軽減．

（3）オープン API の収支モデル

ア．収入

- API によるデータや機能提供の対価．
- API アクセスにより新たに入手できるデータの利活用．

イ．支出

- 外部が提供する機能活用の対価．
- API 基盤構築や利用に係るベンダーへの支払い．

（4）システムセキュリティ関連

ア．情報漏えい発生時における銀行と Fintech 事業者等の責任分担

イ．不正アクセス発生時における銀行と Fintech 事業者等の対応手順

ウ．API の標準化・・・全国銀行協会「オープン API のあり方に関する検討会報告書」推奨方式

エ．API 接続基盤・・・「アダプタ」,「ゲートウェイ」の位置づけである API 接続基盤の構築方法

5．今後の展望

全国銀行協会「オープン API のあり方に関する検討会報告書」の今後の取組みでは，オープン・イノベーションの活性化に向けて，銀行 API のみならず，他業態の事業者等においてオープン API の取組みが進展し，様々な事業者間で価値のある情報が相互にやりとりされていく生態系(API エコシステム)の形成が重要としている．オープン API については，それ自体が「目的」ではなく，あくまでも「手段」であることを正しく認識し，ＩＴ部門のみでなく，銀行経営における重要課題と捉えるべきである．

今後も，オープン API の関連技術，オープン API を利用したビジネスモデル等の動向を注視して，支部会員間で情報交換していきたい．

◇研究報告 2

「内部統制後の考察」

報告者 (会員番号　848 森　広志)

今回、過去に内部統制に携わり、実際の業務体験を通して分かったことを踏まえ、内部統制後の企業活動を推察し、監査業務のベクトルとシステム監査普及のための考察を行いました。

1. 内部統制に於けるデータ利用

内部統制評価は、社内データが揃っていないと実施できません。業務処理統制であれば、各職場の各業務データ項目に関連した財務データと共に、エビデンス(領収書・請求書、アウトプット、契約書他関係書類等)等。ＩＴ全般統制であれば、プログラム登録のシステム運用ログデータ、運用システム操作者のアクセス権限ログデータと共に、エビデンス(プログラム開発決裁書他関係書類、プログラム登録票、アクセス権限登録決裁書等)　等。

先ずは、企業内部での 1 年間の内部統制業務(内部統制評価は 1 年毎に御破算)を、データ利用の観点から概要を述べます。

① 年始に、財務データ等から重要な勘定科目を洗出し、内部統制の対象範囲を特定する。(事業所・業務の新増設・変更・廃止の場合も対象範囲を見直し。)

② 整備状況評価のためのデータ抽出。(業務サンプル 1 件を通して今年度行うリスクコントロールの仕組みが正しく機能するか、リスクコントロールマトリックス表、業務フロー図、リスクコントロールが示されている諸規定やマニュアル類、決裁権限者等を基に確認する。)

③ 運用状況評価のための母集団データ作成。(例　購買業務:期間内に於ける、購買依頼日から購買依頼業務、見積・発注業務、契約業務、検収業務に至るまでの一連のデータ(各工程の伝票番号、勘定科目別金額、購買依頼職場、購買契約職場、検収職場、各工程の担当・決裁権限者等)を、業務システムより、各種データ項目をダウンロードし作成する。等)

④ 母集団データよりサンプル決定と抽出。(②の整備状況評価が有効であるを持って、運用状況評価のリスクコントロール品質は、サンプル評価のみで可能であると考える。どのサンプルを抽出するかの決定は、内部統制の主幹部門が行う。通常は、母集団の数が十分に大きいため 25 件となる。25 件の理由は、評価者が許容範囲とする 10%以上の誤謬が、統計上発生しないためである。しかし、バックアップ訓練など年 1 回程の実施であれば、そのサンプルを抽出する。)

⑤ ロールフォワードやエラーの場合のサンプル抽出。(運用状況評価作業が完了するのは、大体 12 月下旬であると考えられる。運用状況評価以降から年度末までリスクコントロールが有効であるのとを証明するため、ロールフォワード(至近のサンプルを 1 件を評価する等)を実施する。又、運用状況評価やロールフォワードでエラー(リスクコントロールの文面に逸脱した行為)のある場合は、追加サンプル(統計に基づく件数)の評価を行い、リスクコントロールが有効であることを証明する。)

2. 内部統制の原点

内部統制の業務側概要を述べましたが、そもそも内部統制は随分と以前からあり、２０年前以前からシス

テム監査の学習項目でもありました。原点は入金管理や支払管理といわれます。私は毎日、多くの誤りに接する業務に携わり、リスクコントロールの仕組み(複数役職者印含む)が幾重にもあるにも係わらず、なぜ人は誤るのか？

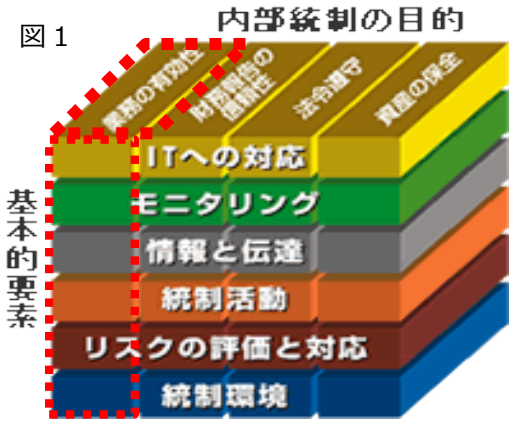
上記の誤りについて、性悪説では、当該業務のリスクが、当該役職者が責任リスク分散コントロール可能であり、責任リスク分界点を下回っていると考えれば押印に至る。又は、伝票の内容をチェックせずに押印している。

しかし内部統制は、性善説により、決裁権限者の押印をもってリスクコントロールを実施していると判断します。内部統制評価を効率的に行う目的もあると思いますが、私は、最近、ありのままを「正見」するのが正しいと考えるようになりました。「正見」は仏教の八正道にあり、トレーニングが必要です。

近年、企業でも、社員が効率的に仕事に取り組めるように、マインドフルネス(仏教に於ける八正道の１つ「正念」の意)が導入されています。

3.　内部統制の枠組みと統制の構成

図 1

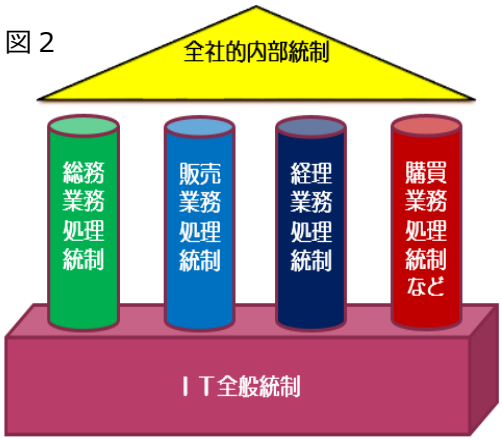


内部統制のフレームワーク(図 1)については、企業全体に適用されるものであり、目的について最初に、業務の有効性・効率性、次に財務報告の信頼性とあり、内部統制が制度化されると聞いた当初は、従業員の業務負担も効率化により軽減されると期待しておりましたが、実際に内部統制業務が分掌化され組織化されているのは財務報告の信頼性に止まっており、残念に思いました。

経営資源の制約上、目的の項目中、最もリスクの高い財務報告の信頼性について、法制度化したものと考えます。

各統制の全体構成(図 2)について、全社的内部統制は、内部統制のフレームワークの基本的要素が、整備・運用されているかの統制であり、企業全体に適用されるもの考えますが、多くの企業が金融庁の４２項目の評価事例に基づいて実施していると思います。又、業務処理統制・ＩＴ全般統制は、財務報告にかかわる対象範囲に限られた統制がおこなわれています。

図 2



全社的内部統制は、多くの企業では関係する各役員とその関係者が、関係する統制箇所の諸規定・文書類等を吟味して、整備状況・運用状況評価を行っていると推察します。

業務処理統制・ＩＴ全般統制については、従業員が作成した伝票や領収書・請求書等の証憑書類などを基に統制を評価しますが、残念ながら企業内部には押印体裁文化という根強い伝統があります。

しかしながら内部統制を実施したことで、リスクを中心に考える、事実がどうであったのか、ということが、紆余曲折を経て定着しつつあります。

4.　内部統制の非統制範囲

内部統制の対象範囲は、先ず重要な勘定科目を確定し、次にその勘定科目を生じている業務は何か、その業務を支えるアプリケーションシステムは何か、それを支えるハード・ソフト・ネットワークという具合に追ってゆきます。

会社全体の業務システム構成図を書くと分かり易いのですが、内部統制の非対象範囲は、主に財務データを発生しない業務システムが主なものです。そこで、内部統制の非対象範囲業務について調査すると、コア業務(企業活動を行う上で重要な直接業務)である場合が多いと考えます。

5.　内部統制後のシステム監査

企業の持つ生存系の機能構造は、大きく分けて戦略化経営機能と経営活動維持機能の２つに分けられますが、経営活動維持機能の 1 つが内部統制(他に、災害・テロ対策、事業継続計画、情報セキュリティ、個人情報保護、コンプライアンス等、多数有り)と考えます。

内部統制が対象としなかったコア業務、内部統制の目的として、最重要とされておりながら実際には実現されていない、業務の有効性・効率性には、大きなフロンティアが眠っていると考えます。

顧客であるトップマネジメントからすると企業の付加価値を高めることは当然のこと、システム監査人は、トップマネジメントの視点から付加価値向上に重要性を置くべきだと考えます。

現在まで、経営活動維持機能ついては、政府の施策もあり整備が進んできましたが、これからが本来、システム監査そのものの力を発揮する時代が近づいていると考えています。

以上

<目次>

2018.10

2018.10 注目情報（2018.9～2018.10）

■「制御システムのセキュリティリスク分析ガイド 第 2 版
～セキュリティ対策におけるリスクアセスメントの実施と活用～」(IPA)

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、2017 年 10 月に公開した上記ガイド第 1 版を元に、工数を削減できるようリスク分析の実施方法を見直した第２版を2018年10月２日に公開しました。

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

■「変革期における金融サービスの向上にむけて
～金融行政のこれまでの実践と今後の方針(平成30事務年度)～について」【金融庁】

金融庁は、本事務年度において、PDCA サイクルに基づく業務運営を強化する観点から、従来の「金融レポート」と「金融行政方針」を統合し、「変革期における金融サービスの向上にむけて～金融行政のこれまでの実践と今後の方針（平成 30 事務年度）～」として公表することとしました。

https://www.fsa.go.jp/news/30/20180926.html

金融行政の重点施策として、「デジタライゼーションの加速度的な進展への対応　～金融デジタライゼーション戦略」として 11 の施策が挙げられています。

主な施策

・オープンアーキテクチャーによるイノベーションの推進
・デジタライゼーションの基盤となるブロックチェーン、AI、ビッグデータ技術等の推進
・サイバーセキュリティその他金融システム等の課題への対応　他

<目次>

2018.10

【 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237回	日時	2018 年 11 月 21 日(水) 18:30～20:30
	場所	港区芝公園　3-5-8　機械振興会館 地下 2 階ホール http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
	テーマ	信頼できるインターネット社会の実現に向けて ―クラウドサービスの信頼性の評価のあり方―
	講師	山内 徹 氏 一般財団法人日本情報経済社会推進協会(JIPDEC) 常務理事 インターネットトラストセンター センター長 内閣官房 IT 担当室、経済産業省等において IT 政策の企画立案に携わった後、 一般社団法人 JPCERT コーディネーションセンター主席研究員を経て現職。 早稲田大学非常勤講師として「シンガポール／アジアの IT と社会」の講座を担当。 1985 年京都大学大学院原子核工学科修士課程修了。
	講演骨子	IoT、ビッグデータ、AI の進展により、インターネットの利活用があらゆる経済活動、人々の日常生活に浸透している。他方、高度化・複雑化するサイバー攻撃等を背景にインターネット上のデータの信頼性（トラスト）の確保が喫緊の課題となっている。近年、急速に普及しているクラウドサービスに関する安全性評価は、世界各国で注目されているところである。 本講演においては、欧米諸国における規制や政府調達等の動向を紹介しつつ、我が国としてのクラウドサービスに関する安全性評価のあり方を議論するものである。
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	協会ホームページ https://www.saaj.or.jp/ でご案内準備中

■SAAJ 月例研究会（東京）		
第238回	日時	2018 年 12 月 5 日(水)18:30～20:30
	場所	港区芝公園　3-5-8　機械振興会館 地下 2 階ホール http://www.jcmanet.or.jp/gaiyo/map_kaikan.htm
	テーマ	不正検査とシステム監査の関連。ＩＴ関連の不正事例紹介等。
	講師	不正検査士　甘粕 潔 氏（日本不正検査士協会　初代事務局長）
	講演骨子	（詳細準備中）
	参加費	SAAJ 会員 1,000 円　非会員 3,000 円
	お申込み	協会ホームページ https://www.saaj.or.jp/ でご案内準備中

■ＳＡＡＪシステム監査実践セミナー（東京：日帰り２日間コース）		
第33回	日時	2018 年 12 月 13 日(木)～14 日(金)　9:30～17:00
	場所	ホテルフクラシア晴海
	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、システム監査の実際を体験していただくことを目的とした日帰り２日間のコースです。
	参加費	SAAJ 会員　54,000 円　非会員　64,800 円 （費用には、教材費・食事代・消費税が含まれます。）
	副教材	情報システム監査実践マニュアル(第 2 版)　森北出版社　5,616 円 お近くの書店等にてご購入ください。
	定員	定員 15 名（最小催行人員 6 名）　　応募締切日：11 月 10 日（土）
	お申込み	https://www.saaj.or.jp/kenkyu/jissenseminar/jissenseminar33.html

【 外部主催イベント・セミナーのご案内 】

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

<目次>

協会からのお知らせ　【 年会費納付時期について 】

会員番号 2581 斉藤茂雄 （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、2019 年度年会費の請求書を、2018 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】 https://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。

【2019 年度会費請求の内容】

＜金額＞ 正会員個人 ： ￥10,000.- （非課税）

正会員団体 ： ￥10,000.- ～ ￥100,000.- （非課税）

＜払込期限＞2019 年２月末日

なお、正会員団体に限り、「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 2019 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： https://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。）

※振込手数料はご負担願います。

【重要事項：2018 年度会費未納の場合】

一部の会員の方について、2018 年度会費のお支払が確認できません。2018 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、https://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。

2018 年９月末現在、認定 NPO 法人の継続基準である、年間 100 人以上のご寄附の人数に達しておりません。12 月中のご寄附へのご協力をよろしくお願いいたします。

＜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】：https://www.saaj.or.jp/toiawase/index.html （事務局）

以上

＜目次＞

2018.10

【 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。

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

・「発注者のプロジェクトマネジメントと監査」「情報システム監査実践マニュアル」「６か月で構築する個人情報保護マネジメントシステム」などの協会出版物が会員割引価格で購入できます。
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。

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定			2018.10
	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	11：理事会	22：第 236 回月例研究会 27：会員向け活動説明会	21：秋期情報処理技術者試験
11 月	8：理事会 8：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/7〆切） 16：2019 年度年会費請求書発送準備 26：会費未納者除名予告通知発送 30：本部・支部予算提出期限	10,17,24：秋期 CSA 面接 21：第 237 回月例研究会 下旬：CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 30：　CSA 面接結果通知	17：「2018 年度西日本支部合同研究会　in Fukui」
12 月	1：　2018 年度年会費請求書発送 1：　個人番号関係事務教育 13：理事会：2019 年度予算案 会費未納者除名承認 第 18 期総会審議事項確認 14：総会資料提出依頼（1/7〆切） 14：総会開催予告掲示 19：2018 年度経費提出期限	13：第 33 回システム監査実践セミナー(日帰り２日間コース) 15：　CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕 26：秋期 CSA 認定証発送	12:協会創立記念日
1 月	7：　総会資料提出期限 16:00 10：理事会：総会資料原案審議 26：2018 年度会計監査 30：総会申込受付開始（資料公表） 31：償却資産税・消費税申告	1-31：CSA・ASA 更新申請受付 18：　春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕	7：支部会計報告期限
2 月	7：理事会：通常総会議案承認 28：2019 年度年会費納入期限	2/1-3/31：CSA・ASA 春期募集 下旬：CSA・ASA 更新認定証発送	22：第 18 期通常総会
3 月	8：年会費未納者宛督促メール発信 14：理事会 27：法務局：資産登記、理事変更登記 活動報告書提出 東京都：NPO 事業報告書提出	1-31:　春期 CSA・ASA 書類審査	
	前年度に実施した行事一覧		
4 月	12：理事会	初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行 17：第 231 回月例研究会	15：春期情報技術者試験
5 月	10：理事会	13,26：春期 CSA 面接 19：第 232 回特別開催月例研究会 「新システム監査／管理基準」 28：CSA フォーラム（茅場町 NATULUCK）	
6 月	1：年会費未納者宛督促メール発信 14：理事会 19：年会費未納者督促状発送 21～：会費督促電話作業（役員） 29：支部会計報告依頼（〆切 7/13） 30：助成金配賦額決定（支部別会員数）	13：第 233 回月例研究会 中旬：春期 CSA 面接結果通知 下旬:　春期 CSA　認定証発送	認定 NPO 法人東京都認定日 （2015/6/3） 30：近畿支部 30 周年記念 シンポジウム
7 月	5：支部助成金支給 12：理事会	12：第 32 回システム監査実践セミナー (日帰り 2 日間コース) 26：第 234 回月例研究会 28：事例に学ぶ課題解決セミナー 下旬：秋期 CSA・ASA 募集案内	13：支部会計報告〆切
8 月	（理事会休会） 25：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30 30、31:第 32 回システム監査実務セミナー (日帰り 4 日間コース)前半	
9 月	13：理事会	～　秋期 CSA・ASA 募集中　～9/30 迄 7：第 235 回月例研究会 13,14:　第 32 回システム監査実務セミナー (日帰り 4 日間コース)後半	

<目次>

2018.10

【 会報編集部からのお知らせ 】

1．会報テーマについて

2．会報バックナンバーについて

3．会員の皆様からの投稿を募集しております

□■ 1． 会報テーマについて

2018 年度の年間テーマは、「システム監査人の新たな活躍」とし、さらに四半期ごとに具体的なテーマを設定して、皆様からのご意見ご提案を募集いたします。
7 月号から 9 月号までの四半期に引き続き、10 月号から 12 月号までの四半期テーマも、「システム監査基準・管理基準改訂とこれからのシステム監査人」です。このテーマは、システムシステム監査人の皆様にとって、関心の高い重要なテーマであろうと思いますので、システム監査基準・管理基準の改訂に対して、システム監査人としてどう対応していくのか、皆様のご意見をお待ちしています。
システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。
会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

＊2018 年度会報テーマ

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

□■ 2． 会報のバックナンバーについて

協会設立からの会報第 1 号からのバックナンバーをダウンロードできます。

https://www.saaj.jp/03Kaiho/0305kaihoIndex.html

□■ 3．会員の皆様からの投稿を募集しております。

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

1.	めだか	匿名（ペンネーム）による投稿 原則１ページ ※Word の投稿用フォーム（毎月メール配信）を利用してください。
2.	記名投稿	原則４ページ以内 ※Word の投稿用フォーム（毎月メール配信）を利用してください。
3.	会報掲載論文 （投稿は会員限定）	会報掲載「論文」募集要項（2018. 1.11 改訂） 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。

■投稿について

・投稿締切：15 日（発行日：25 日）

・投稿用フォーマット　※毎月メール配信を利用してください。

・投稿先：　saajeditor@saaj.jp　宛メール添付ファイル

・投稿メールには、以下を記載してください。

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

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

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

■注意事項

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

・編集担当の判断で、字体やレイアウトなどの変更をさせて戴くことがあります。

お問い合わせ先：　saajeditor@saaj.jp

2018.10

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

■□■ＳＡＡＪ会報担当

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

編集支援：　小野修一（会長）、各副会長、各支部長

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

<目次>