認定 NPO 法人
日本システム監査人協会報
2018 年 12 月号
No 213
No.213（2018 年 12 月号）＜11 月 25 日発行＞

今月号の注目記事

連載中（全 3 回予定）

- **【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 2）**

巻頭言　『 DX レポートとシステム監査 』

会員番号 608 三谷 慶一郎（副会長）

今年の 9 月に経済産業省から「DX レポート」というものが発表され一部で話題になっています。

DX は、最近よく使われる用語で、デジタルトランスフォーメーションの略です。「デジタル技術を駆使して企業が新しいサービスや新しいビジネスモデルを創り出すこと」といった意味だと考えていいと思います。

このレポートが興味深いのは、企業が DX を推進し大きな成果を出すためには、AI や IoT をただ活用していくだけではなく、まずは足元の既存システムをしっかりさせなければいけない、と述べているところにあります。レポートでは「既存システムが老朽化・複雑化・ブラックボックス化する中では、新しいデジタル技術を導入したとしても、データの利活用・連携が限定的であるため、その効果も限定的になってしまう」と書かれています。さらには、「（老朽化したままでは）既存システムの維持、保守に資金や人材を割かれ、新たなデジタル技術を活用する IT 投資にリソースを振り向けることができない」といった問題も指摘もされています。これは確かにその通りだと思います。デジタル技術で新しいサービスを開発したとしても、既存の基幹系システムに接続できない、あるいは接続するための保守に時間がかかるようでは話になりませんから。

続きは、投稿記事「DX レポートとシステム監査」をご覧ください。

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>

2018.11

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、留意事項として、“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。

システム監査に当たって「情報セキュリティ監査基準」をあわせて参照する場合、これからのシステム監査人は、システム監査対象に応じ、管理策を具体化して管理項目を設定する必要がある。例えば、個人情報を取り扱う情報システムは、プライバシーバイデザインを考慮し、情報セキュリティ管理基準を参照すると、次のような管理策と管理項目が設定できる（14.2.3 以下は、記載省略）。（空心菜）

14.2.1 セキュリティに配慮した開発のための方針

管理策：ソフトウェア及びシステムの開発のための規則は、組織内において確立し開発に対して適用する。

＜管理項目例＞

a)セキュリティに配慮した開発のための方針には、開発環境のセキュリティを含める。

b)セキュリティに配慮した開発のための方針には、設計段階におけるセキュリティ要求事項を含める。

c)セキュリティに配慮した開発のための方針には、プロジェクトの開発の節目ごとにおけるセキュリティの確認項目を含める。

14.2.2 システムの変更管理手順

管理策：開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。

＜管理項目例＞

a)初期設計段階からその後の全ての保守業務に至るまで、システム、アプリケーション及び製品の完全性を確実にし、また、変更によって本来のシステム要件に齟齬を生じさせないため、正式な変更管理手順を文書化し、実施する。

b)新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、試験、品質管理及び管理された実装からなる正式な手続に従う。

c)変更管理手順には、変更の実施は最も適切な時期に行い、関係する業務処理を妨げないことを確実にすることを含める。

d)変更管理手順には、変更することによる新たなリスク(当初のプライバシーバイデザイン時のセキュリティの喪失やリスクの追加など)を認識して対応することを含める。

（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>

2018.11

投稿　【　DX レポートとシステム監査　】

会員番号 608 三谷 慶一郎（副会長）

今年の９月に経済産業省から「DX レポート」というものが発表され一部で話題になっています。

DX は、最近よく使われる用語で、デジタルトランスフォーメーションの略です。「デジタル技術を駆使して企業が新しいサービスや新しいビジネスモデルを創り出すこと」といった意味だと考えていいと思います。

このレポートが興味深いのは、企業が DX を推進し大きな成果を出すためには、AI や IoT をただ活用していくだけではなく、まずは足元の既存システムをしっかりさせなければいけない、と述べているところにあります。レポートでは「既存システムが老朽化・複雑化・ブラックボックス化する中では、新しいデジタル技術を導入したとしても、データの利活用・連携が限定的であるため、その効果も限定的になってしまう」と書かれています。さらには、「（老朽化したままでは）既存システムの維持、保守に資金や人材を割かれ、新たなデジタル技術を活用する IT 投資にリソースを振り向けることができない」といった問題も指摘もされています。これは確かにその通りだと思います。デジタル技術で新しいサービスを開発したとしても、既存の基幹系システムに接続できない、あるいは接続するための保守に時間がかかるようでは話になりませんから。

レポートではこの「老朽化・複雑化・ブラックボックス化」しているシステムのことを「レガシーシステム」と呼んでいます。レガシー化の原因としては、単に使っている技術が陳腐化しているということだけではなく、システムのノウハウがユーザー企業側でなくベンダー側に多く流出してしまっていること、さらには有識者の退職によるノウハウの喪失といったマネジメントの不十分さなどがあげられています。どの状況もシステム監査人の立場から見て「問題あり」と言えるのではないでしょうか。

経済産業省は、このままの状況が放置されたままでは、2025 年以降、毎年最大１２兆円の経済損失が生じる可能性があると試算し、これを「2025 年の崖」と名付けています。その上で、このような状況を打破するために、2025 年までに国内企業のレガシーシステムを一新し、DX を実現していこうと呼びかけ始めています。我々システム監査人も自らの役割を通じてこの流れを推進することができるといいですね。

<目次>

2018.11

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２）
－事例、中核市の CIO 補佐官の活動姿勢と成果、その成功要因－

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

私は、民間企業を退職後 U ターンし、一昨年３月に中核市のＣＩＯ補佐官（５年任期）を退任した。

昨年、第２次情報システム最適化基本計画が後任の CIO 補佐官、職員の努力で策定・公開された。この中で、第１次計画の事業成果の確認が行われ、また取組の姿勢も継承されている。私は、これは私達が進めてきた取組がひとり合点ではなく、間違ってはいなかった、との思いを強くし、「基礎自治体の CIO 補佐官というセカンドキャリのすすめ」を提案したいと考えた。

提案は（その３）で述べるとして、本稿では CIO 補佐官の活動について理解いただくために、私自身の CIO 補佐官の活動の経験について紹介する。

２．CIO 補佐官任用の経緯

（1）CIO 補佐官任用の目的

CIO 補佐官を公募した市（以降当市）の目的は、「第１次情報システム最適化基本計画という事業を推進するため、民間の IT マネジメント力を市の IT マネジメント力強化に生かしたい」との事であった。この IT マネジメント力強化の目標は、情報政策において行政経営の視点に立って、IT ガバナンス の強化を進めることでもあった。

私は自治体システムについて、事前に知識を持ってはいなかったが、IT マネジメントの専門家の使命感を持って応募し、当市も私も所期の目的を『無事達成』した。

（2）次期 CIO 補佐官の任用

当市は情報システム最適化事業の執行過程において、CIO 補佐官の有用性を認め、私の退任後も引き続き CIO 補佐官の採用を決定した。

当市に限らず、自治体業務が情報システムへの依存を益々高め、情報化投資が継続する中で、前稿で確認した IT 課題に対応するため IT ガバナンス・マネジメント力の強化を図ることは、重要な政策課題である。

そして、この IT ガバナンス・マネジメント力の強化は、外部の専門家の助言・活用によって、短期間に完了する短距離走ではなく、情報システムに携わる職員が駅伝のように世代をつないで発展強化してゆくべき、組織文化の定着である。

この観点から、CIO 補佐官の任用が継続されることで、これまで進めてき IT ガバナンス・マネジメント力強化の取り組みが、無に帰すことなく、更に維持向上されることを、私は嬉しく感じた次第である。

３．基礎自治体の CIO 補佐官の仕事

（1）CIO 補佐官の責務（説明責任）

当市が公募で CIO 補佐官に求めたことは、①IT ガバナンスの強化、②情報システムの最適化事業の推進支

援であった。このことは入口であり、CIO 補佐官に求められる IT マネジメントは、行政経営にかかわる IT 施策全般について、利害関係者に対し説明責任を果たすことができる業務遂行であろうと、私は理解した。

すなわち、説明責任を求める問いかけを、システム管理基準（ここでシステム管理基準は在職中の旧基準）に対比すれば、図表１のことであろうと考えた。

図表１　CIO 補佐官の責務（説明責任）

システム管理基準	ステークホルダーの主な関心事
１）情報戦略	IT政策はICT活用リスク全体への目配りができていますか？　具体的には、
（全体最適化・組織・人材・リスク管理）	・市民サービス、行財政改革にITは活用できていますか？
	・同規模の自治体と比較しIT予算は適切ですか？
	・IT部門、ITにかかわる職員の教育は、計画的に実施していますか？
２）企画業務	企画案件は市民など第三者の評価に耐えられるものですか？　具体的には、
（開発計画、分析、調達）	・最適化事業や各部局の事業において、事業の事前評価をしていますか？
	・最適化事業をはじめ、市のIT調達は適正ですか（競争原理の導入・見積査定）？
	・最適化事業や各部局の事業において、事業の事後評価をしていますか？
	・導入システムはその効用の最大化を図っていますか？
	・最適化事業によって、市民サービスの向上・職員の事務効率の改善・情報セキュリティの強化は図られましたか？
	・最適化事業によってIT経常費用は何割縮減しましたか？
	・当市のIT経常経費は、他市と比較してどのような状況ですか？
３）開発業務	他市ではシステム開発プロジェクトが破綻する事例も見られるが、当市の最適化事業は、行政経営の信頼にこたえられますか？
（開発手順、要件定義、受入テスト、移行）	・品質・コスト・工程の管理はどうなっていますか？
	・情報セキュリティ対策はどうなっていますか？
	・移行時にトラブルが発生した場合、どのように対処しますか？
４）運用保守業務	運用・保守は委託先に丸投げでなく、職員による統制が図られていますか？
（運用・保守管理）	・情報セキュリティに関する委託先の管理（契約・運用）は適切ですか？
	・システム変更など、実施時の事前・事後の管理は適切ですか？
５）共通業務	ICTを活用する一方で、情報セキュリティ・災害対応など高まるリスクへの対策は市民の信頼に応えられるものとなっていますか？
（情報セキュリティ・事業継続計画など）	・情報セキュリティ対策は他市に比較し遅れているということはありませんか？
	・個人情報保護管理の体制は整備できていますか？
	・サイバー攻撃への事前・事後の体制は整備されていますか？
	・IT部門の業務継続計画（BCP）は策定され、実効性は確認していますか？
	・情報セキュリティ対策は内部・外部監査により点検・改善していますか？
	・各種ガイドラインに従い、PDCAを回し情報セキュリティは維持強化されていますか？

図表１の問いかけへの具体的な実施内容を改めて解説することは、本稿の読者である専門家諸氏には釈迦に説法であり、限られた紙面の都合もあり、ここではしない。

ただ、こうした姿勢で取り組んだ最適化１次計画の成果は、私が退任後の 2017（平成 29）年３月に発表された第２次情報システム最適化基本計画において、事後評価されている。これを図表２に示す。

図表２　IT ガバナンスのこれまでの取組の成果

図表２は、情報部門自身が実施主体となる情報システム最適化基本計画に基づく、「情報システムの再構築」事業を除くものである。この事業においても、調達の適正化を図り、総事業費のコスト縮減を果たしている。

なお一般に、パッケージ利用・オープン化による情報システムの再構築においては、２０%~３０%の経常経費の削減を期待でき、当市においてもその成果が見込まれている。地方自治体の厳しい財政事情の中で、経常経費削減によって生みだされた新たな情報化投資の余力が、マイナンバー対応の情報セキュリティ対策や新庁舎での ICT 活用など、新たな ICT 投資需要への対応を可能にしている。

そして、費用対効果で言えば、CIO 補佐官の報酬と事業費の削減を対比すると、当市は CIO 補佐官任用に関して、財務的な面でも十分な投資効果を得たことが理解できる。

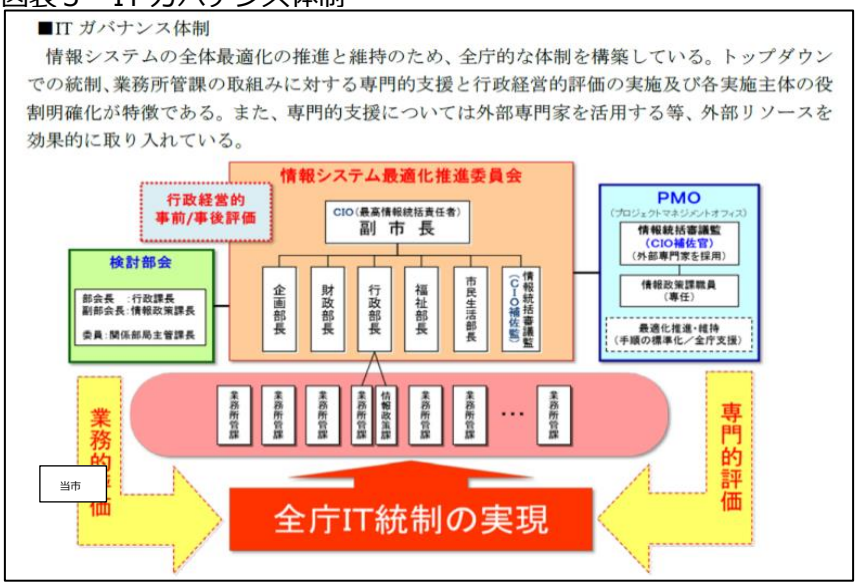
(2)　IT ガバナンス強化の取組

総務省は、「電子自治体の取り組みを加速するための 10 の指針」（2014 年 3 月）を提示している。この指針では、重点施策として行政情報システムのオープン化・クラウド化、オープンデータの推進、そして情報セキュリティ対策の強化を示すとともに、その推進体制として、CIO や PMO（Program Management Office）による、IT ガバナンス体制の整備の重要性を、図表 3 の通り例示している。

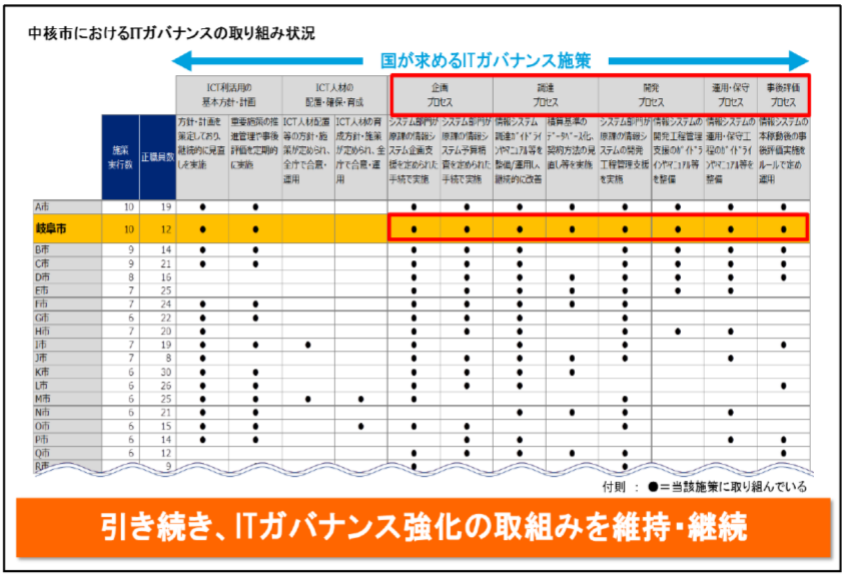
IT ガバナンス体制では、中央官庁同様に、ＩＴに関する専門能力と、民間の感覚をもって CIO を補佐し、かつ PMO チームをリードする CIO 補佐官が重要なポイントとなる。専門性と経験豊富な IT マネジメント人材を内部で調達することが難しい状況において、IT ガバナンスを強化し、ステークホルダー（市民、議会、事業者）への説明責任を果たしてゆくためには、外部人材の CIO 補佐官への任用が有効と考えられている。

また、この具体的な取組項目を、総務省はすでに 2007（平成 19）年 7 月「地方公共団体における IT ガバナンスの強化ガイド」として示している。このガイドライン等を参考に、当市の実施状況を他の中核市と比較し、改めて点検したものが、図表 4 である。

図表 3　IT ガバナンス体制



図表 4　中核市における IT ガバナンスの取組状況



（3）IT ガバナンス強化と PMO 活動の進め方

CIO 補佐官の活動に対して、行政経営幹部をはじめステークホルダーの関心は、つまるところ

・IT ガバナンスの強化はどのように進展しましたか？

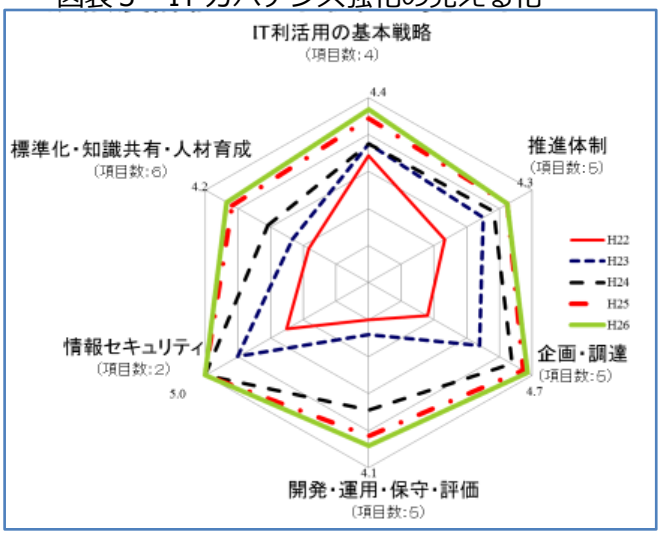
・IT ガバナンスの中核となる情報部門（PMO チーム）の活動はどのように進展しましたか？

ということである。

そこで、IT マネジメント力強化の活動成果を見える化するにあたって、総務省の「地方公共団体における IT ガバナンスの強化ガイド」にある、「IT ガバナンスレベルチェックシート」を活用した。一般の評価者の分かりやすさを考慮し、原典が４段階であるものを５段階評価に拡張した。また、IT ガバナンス強化のステップを意識し、「企画・調達・評価」から「評価」を分離し、「開発・運用・保守」に「評価」を加えて、６つの軸での成熟度評価とした。

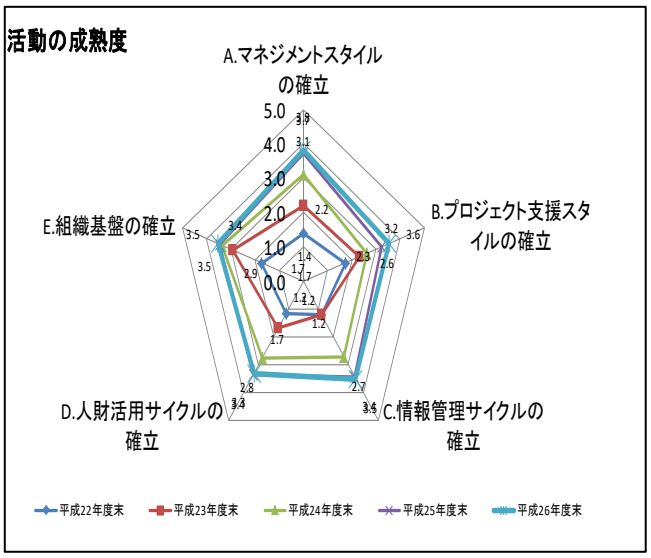
自己評価ではあるが、図表５に示すように、当初平均２点台だったものが、最終段階においては平均４点台となり、数年スパンで継続して IT ガバナンスを強化してきた様子を理解していただけると思う。

図表５　IT ガバナンス強化の見える化



一方、基礎自治体の IT マネジメント力の中核は PMO チームの活動で、この活動が、継承し定着されなければ、IT ガバナンスの強化は一過性に終わってしまう。そこで、この PMO チームの活動を、図表６に示すように、５軸５段階で評価し、活動の成熟度の見える化により、職員が成長を実感できるよう指導してきた。５軸の意味内容は次項で説明を加えるが、PMO チームの活動が一歩一歩成長してきたことを、理解していただけると思う。

図表６　PMO 活動の成熟度の見える化



とはいえ、IT ガバナンスも PMO 活動も、この最終レベルを維持することは、基礎自治体の人事ローテーション（通常３～５年の在籍期間）を考えれば、無理がある。それでも、CIO 補佐官のサポートのもと、職員の事務引継ぎにより、IT ガバナンスで４．０以上、PMO 活動で３．０以上が維持できれば、IT ガバナンス・マネジメント力の継承は、及第点ではないかと考えている。

（４）自治体における PMO 活動の留意点

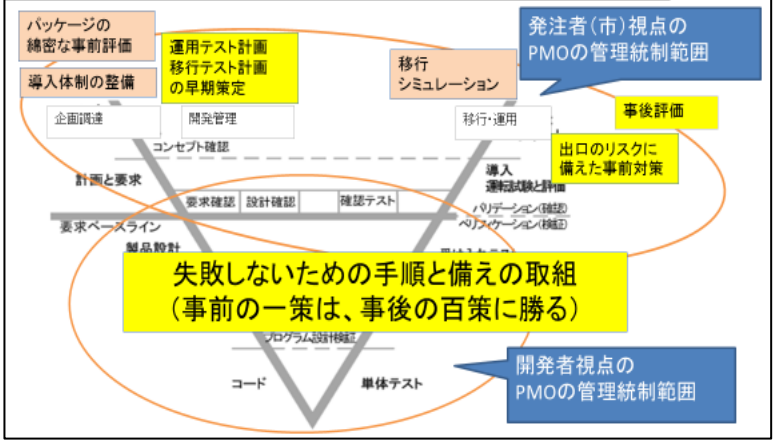
自治体においては、大規模なシステム開発において、開発プロジェクトの計画管理を工程支援事業者に委託する場合がある。当初の工程支援は、開発業者のプロジェクト工程の監理という開発者視点が中心で、開発の川上と川下で、プロジェクトに携わる職員が主体的に進めるべき作業の工程管理やリスク管理といった、発注者視点が不十分であった。

そこで、PMO チームは、プロジェクト管理責任者を支援し、調達仕様書において改めて発注者視点での重点的な管理統制範囲と工程管理項目を明確にし、その上で工程支援事業者を選定委託した。この自治体の開発業務における PMO 支援の重点範囲を、開発の V 字型モデル上にプロットしたものを図表７に示す。

発注者側の視点で、例えば職員側が主体的に進める「パッケージの事前評価」、「導入体制の整備」、既存システムからの「移行シミュレーション」といったことはもちろんであるが、更に「事前の一策は、事後の百策に勝る」の精神から、リスク対策を行った。

具体的には、「運用テスト計画」、「移行テスト計画」に早期に着手し、その過程で仕様の漏れを発見する、あるいは、システム切替時の万が一の障害に備えて「出口のリスクに備えた事前対策」（ある意味の事業継続計画）といった業務管理である。また、工程支援の締めくくりとして、導入後のシステムの問題管理・解決はもちろん、導入システムの効用の最大化を図るため、稼働後半年～１年後を目途とした「事後評価」の実施と改善計画の策定も支援する。

図表7　自治体の開発業務（PMO支援）の重点範囲
―V字型モデルにおけるプロジェクトマネジメントの対象―



PMO チームは、この発注者の管理統制範囲を踏まえ、図表８に示す PMO 活動の管理項目について、機能を向上するための取組項目を定め、前頁の図表６の通り成熟度の見える化を図ったものである。

図表８　IT ガバナンス強化を支える、発注者側の PMO の管理項目・視点

PMO活動の管理項目	開発者視点	発注者視点
A.マネジメントスタイルの確立（プロセス資産管理）	開発PJのPMの高度化に関わる理念方針・標準化・ツール導入、技法導入などの成熟	PJの川上（企画・調達）と川下（受入・移行）に特化した管理方針・標準化・ツール・技法の成熟
B.プロジェクト支援スタイルの確立（パフォーマンス管理）	開発PJの進捗・生産性・品質にかかわるモニタリング活動、リスク管理、プロジェクト支援活動の成熟	PJの納品に至るまでの契約・変更・出来高の管理や、納期・課題・リスクといったプロジェクトの質にかかわる管理の成熟
C.情報管理サイクルの確立（情報管理）	プロジェクト推進に関わる知識・経験の集約、個々のプロジェクト情報の管理についての成熟	経験したPJの知識・経験の蓄積、査定ガイドラインやチェックリスト、ひな形・様式など、情報管理の成熟
D.人財活用サイクルの管理（人財管理）	PMOに携わる人財の人事・評価と育成、及びPMに関わる社内コミュニティの組織化	PMOに関わる業務を継承し、発展させてゆくための人財管理やPMOに関わる人財を軸としたコミュニティ形成の成熟
E.組織基盤の確立（組織管理）	PMO組織の体制、役割、PMO成熟度管理	上記管理を確実ならしめるためのPMOの体制、役割とその成果評価

４．CIO 補佐官任用の成功要因

さて、CIO 補佐官を任用し PMO チームの活動が期待した成果を得るためには、この活動を受入れ、また支える庁内の態勢が重要である。以下、環境、支援、人材等について述べる。

（1）環境

①基礎自治体の改革風土

CIO 補佐官として採用されても、それは球団で言えば、人事権のないコーチであり、限られた期間で成果上げるためには、トップの啓蒙や体制作りから始めたのではとても間に合わない。当市は民間から転身した首長のリードにより、既に市債の大幅削減、組織・職員のスリム化など行財政改革で大きな進展を遂げており、職員の行財政改革に取り組む意識が全体に定着していた。また、2009（平成 21）年度の情報システムに係る包

括外部監査で、「調達の適切性」７件、「有効性・経済性・効率性」９件、「情報セキュリティ」15 件が指摘・意見として示された。この様な環境で、当市は IT ガバナンスの強化や最適化計画という改革の必要性を認識し、外部有識者の意見も参考に、情報システムの最適化基本計画を策定し、組織承認していた。

一方、利用部門においても、システムを刷新し、利便性の高いシステムを活用したいとの意欲は高かった。

②基礎自治体は自らが望む CIO 補佐官像を描けているか

CIO 補佐官を任用する目的も、期待する人材要件を明確化することも、CIO をトップとする情報システム最適化推進委員会にて共有される必要がある。そして、CIO 補佐官は単に IT の専門家としてだけではなく、情報部門のマネジメントに関し十分な能力と実績を持っていることを、情報部門任せにせず人事採用責任者が判定しなければならない。また、任用ありきで、処遇・経費の制約から、中途半端な任用をすべきではない。行政経営の立場に立って、しっかり基礎自治体の情報政策課題に対応できる人材を採用すべきである。

(2) 支援

① 首長のコミット

首長の情報部門への信頼・期待として、「情報システムの活用において、奇をてらうことなく、また、風潮に流されることもなく、着実に安定・信頼のシステム化の推進を望む」旨の言葉があった。組織トップの言葉に振り回されて、足元を誤るようなことはなく、着実に業務に取り組むことができた。

また、PMO の活動成果が、市長表彰となり、職員がモチベーションを高め、改革意欲を持つ機会に恵まれた。表彰は、情報部門のステータスを向上し、活動・取組を全庁に波及するための大きな支えとなった。

システム障害発生時の対応では、一般に情報部門と業者との持ちつ持たれつの関係から、原因究明・損害賠償など業者への責任追及が甘くなるきらいがあるが、行政においてはステークホルダーへの説明責任こそ第一で、原因追及と責任の所在を明確にし、二度と起こさないための対策こそ重要との姿勢が堅持された。

② CIO をはじめとした行政経営幹部の支援

情報システム最適化事業は、５年間で基幹となる住民情報系と内部事務系を次々と刷新し、一方で IT ガバナンスの体制も改革するという、基礎自治体にとっては、３０年に一度あるかないかの一大事業で、それまでの情報化投資とは桁が違う規模が予定されていた。職員にとって事業の推進は、技術知識の不足もあって、相当なプレッシャーであった。私が入庁直後に、調達業務の過労から、一部職員が休職に追い込まれる事態も発生していた。そのような場合でも CIO（副市長）が組織全体として支えるとのリーダシップを発揮し、最適化推進委員会のメンバー（部長級）の機動的な要員支援と精神的な支援で職員に安定をもたらした。

また、私の入庁前から既に走り出していた一部事業では、工程支援事業者を選定し、プロジェクト管理支援を委託していたにもかかわらず、システム受入テスト段階で多くの不具合が判明し、躓きかけたこともあった。この際、CIO 補佐官が前面に立って対処することはもちろんであったが、行政経営幹部の何としてもプロジェクトを軌道に乗せるという関与の姿勢は、職員への励ましはもちろん、IT ベンダーの真摯な対応を引き出し、そして職員は苦い経験を積みながらもプロジェクトを軌道に乗せることで、大きな自信を得た。

また、庁内幹部の懇親会等を通じ、CIO 補佐官が関係者と話しやすい人間関係も整えていただいた。

③　CIO 補佐官の任用を評価できる外部関係者の支援

市議会においても IT ベンダー経験者をはじめ、IT 施策の難易度を理解した上で、市議会での厳しい質問と同時に励ましの言葉を頂いたことは、庁内の支援体制を引き出す上で、心強い援軍であった。

また、行政の IT 化を推進する団体の機関誌等において、当市の活動を紹介する機会を頂いた。業務に忙しい職員も原稿作成を通じて、事業の理解を深め、足元を見直し、モチベーションを高めることができた。

（3）人材

①　情報部門の要員体制

・中長期の人事施策

情報部門の要員構成においては、全庁に睨みが効くベテラン課長の下、IT ベンダーから転身した職員と部門業務を熟知した職員とがコアになり、若手を引っ張るというバランスの取れた構成が徐々に実現できてきた。これは、IT ベンダー経験者の中途採用による人材補強を中長期で取り組んできた成果であった。

・プロジェクト遂行型チーム

自治体の組織運営は、課長を頭とする縦割りの業務管理のため、最適化事業という大きなプロジェクトにおいても、限られた職員が縦割りにプロジェクト業務を分担しており、私には大きなプロジェクトを一丸となって進める態勢とは思えなかった。部長級である CIO 補佐官が課の運営に口をはさむことは、着任早々で控えていた。しかし、一部職員の戦線離脱や工程遅延もあって、毎週 CIO 補佐官が課内ミーティングに参加するようにした。課内態勢の見直しにより、課内及び関係者とのコミュニケーションの改善を図るとともに、担当業務の正副体制を確立し、チームとして一体感を持てるような環境づくりができた。

・自治体の人事異動を考慮した職務分担

自治体の人事ローテーションは、数年もしくは長くても 5 年である。幅広い知識と経験を積んだ情報部門の専門家を育成する上では、このローテーション制度は敵のような存在である。限られた要員体制ではあったが、あえてプロジェクト業務分担で正副体制を組むことは、この自治体特有の人事ローテーションへの備えとして有効であった。職員が情報を共有し、主担当以外にも副担当の業務にも目配りしなければならず、自然と業務引き継ぎができる体制になった。また、災害やパンデミック時の人的リスクを考えれば、事業継続性の点においても正副体制は有効である。

②　IT 人材の育成

採用試験の面接で今でも覚えていることは、人材育成の要点はとの問いに、「成功も失敗も色々経験してきた立場の人間として、人材を育てるためには成功体験が重要である。」と答弁した事である。事業当初のつまずきを CIO 補佐官・職員が一体となって乗り越え、職員は多くを学び経験し、やりきるという成功体験を積んだ。苦いながらも職員が成功体験を獲得したことは、その後の事業推進において貴重な財産となった。

職員育成については、職員の学ぼうとする意欲が高く、現在あるいは近未来の担当業務と関連する外部の研修を、毎年計画的に活用できた。また、この職員育成にかける予算も、行政経営幹部の理解のもと確保できた。

そして、職員は、情報システム最適化事業というビッグプロジェクトに挑戦し、座学によって高まった問題意識と実践による問題解決を経験することで、IT ガバナンス・マネジメント人材として成長した。

この実践経験に基づく職員の成長は、当市にとって将来に渡り大きな人財を得ることになったと思う。

（4）心掛け

① IT ベンダーとともに成長し、プロジェクトを成功に導く職員の自覚

各種事業の推進は、自治体職員のみではできない。関係する事業者に教えられ、あるいは、時には導いてゆくという、双方向のコミュニケーションが重要である。昔上司に言われたが、システム開発で、『私食べる人、あなた作る人』で、まずかったら食べないというのでは、プロジェクトの成功はおぼつかない。プロジェクトの遂行は、共同責任であること、そして発注者側として進めるべき作業をしっかりやらなければ、ステークホルダーに対し、説明責任を果たせないという認識を、職員は自覚していった。

② 施策の実施に当たっては、経験値に頼らない

CIO 補佐官は、民間経験を買われてその任に当たるが、経験知のみで、一方的に方向付けしないことである。関係する基準や他市調査を行い、現状を客観視し、理論と事実に基づいた内容とすることである。

5．おわりに

CIO 補佐官の任用について、懐疑的な評価も聴く。しかし、本稿で示した CIO 補佐官を中心とした PMO チームの活動や成功要因を認識し、CIO 補佐官が活用され、活躍できる場を提供すべきではないかと考える。

当市は既に次の情報化ステージの取組を始めており、私の数年前の経験は旧くてもう参考にならないのではと、危惧もした。しかし、前稿で確認した基礎自治体の IT ガバナンス・マネジメント課題の現状や、（その 3）で述べる CIO 補佐官の任用状況を踏まえると、あながち旧いわけでもなく、CIO 補佐官を中心とした PMO チームの活動や庁内幹部など関係者の支援の在り方など、参考にしていただく余地があると考える。

CIO 補佐官から離れて 2 年経ち、苦労したことは忘れ、多少美化している様にも思うが、次稿では、CIO 補佐官を何故キャリアパスではなく、セカンドキャリアとしてすすめるか、その思いを述べたい。

参考資料：

1．「第 1 次当市情報システム最適化基本計画」（2010.3）
2．「第 2 次当市情報システム最適化基本計画」（2017.3）
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）
4．「電子自治体の取り組みを加速するための 10 の指針」総務省自治行政局　地域情報政策室（2014.3.24）
5．「IT ガバナンス強化・推進の取組み」当市行政部情報政策審議監兼情報政策課長　諸江 康晃
月刊 LASDEC　（2012.9）
6．「当市の情報システム最適化事業の取組」　当市行政部情報政策課主査　吉元　一弘
県市町村行政情報センター　Net＆Line　2012　Autumn
7．戦略的 PMO　－新しいプロジェクトマネジメント経営―　PMI 日本支部編（2009．5．20）

<目次>

2018.11

投稿　【　レジリエンス認証制度から始める IT 事業継続管理の試み　】

（SAAJ 近畿支部　BCP 研究プロジェクト）
会員番号　1709 荒町弘、2551 伊藤聖子、1497 尾浦俊行
2645 尾崎正彦、1531 金子力造、0283 松井秀雄

はじめに

近畿支部 BCP 研究プロジェクトでは、IT-BCP の推進に向けた研究・啓発活動を続けており、当然のこととして、「システム監査基準」「システム管理基準」（経済産業省）を規範、基準とした BCP 策定をベースとしつつ、内閣府による「事業継続ガイドライン」や ISO に源を持つ「JIS Q 22301（BCMS）」とのベストミックスを模索してきた。そのなかで、完璧な事前措置ばかりを追い求めることの限界と非合理性にぶつかっていたところ、内閣官房国土強靭化推進室による「レジリエンス認証」制度を知り、「回復力」に注目したその着眼に大きく共感する部分があった。

このような経緯から、2017 年末からレジリエンス認証制度の内容と IT-BCP への活用について検討を進めてきた。折しも、その最中、2018 年 4 月に「システム監査基準」「システム管理基準」が改定され、事業継続計画の章も改定された事から、レジリエンス認証制度との比較を交えて、検討成果について報告する。

第 1 章　レジリエンス認証について

（1）レジリエンス認証の概要

地震等の自然災害が多く発生する日本では、災害発生時における被害の縮小や迅速な復旧・復興が特に重要であることは誰もが承知している。さらに、新潟中越沖地震の際のリケンショックや、タイ洪水時の HDD 供給ストップに代表されるように、迅速な復旧が、当該企業の存続のみならず地域全体ひいては国全体の経済にとっても大きな問題となることが認知されるに至っている。

災害時などに事業活動が滞ると、自社の経営に影響するのみならず、地域の経済にも打撃を与え、さらには取引関係を通じて他の地域へ影響が飛び火することも想定されます。このような事態を防ぎ、事業を継続させるため、「事業継続計画（BCP）」の策定が必要となる。

しかし、我が国の大半を占める中小企業などにおいては、災害時の事業活動の継続確保のために事前準備が求められる BCP（事業継続計画）の策定率が 1 割程度と低いまま伸び悩んでいる現状である。

そこで、政府は、社会全体の強靭化を目指すため、災害等の被害に対して強い回復力を持ち、社会全体のレジリエンスの向上に寄与できる事業者を認証する「レジリエンス認証制度」を 2016 年に創設した。

レジリエンス認証では事業継続に係る体制に経営層の関与が必要条件である。経営者のリーダーシップの下、自社の重要業務と目標復旧時間を的確に現場層も把握していることが求められる。

経営層は危機事象において、判断基準（価値観）とミッション（いつまでに何を達成する）を現場に対して付与し、達成方法（HOW）は現場に任せる「権限付与（委譲）」がなされていることが必要条件であり、これにより統制を維持しつつ迅速かつ柔軟な対応が実現されると考えられている。

また、危機事象において重要な司令塔として、事業継続について必要な知見や経験を有する責任者又は担当者を任命していることが必須となっている。

（2）レジリエンス認証の『取り組みやすさ』について

必須とされている BCP 策定では、軽微な被害と甚大な被害、壊滅的な被害の段階に応じた対策を示し、身の丈に合ったものでよいとされている。そこには、「現場が動きやすく、できるだけ簡潔に分かりやすい文書からスモールスタートし、運用しながら「絵に描いた餅」にならぬよう改善を繰り返すことが重要だという考え方が窺がえる。

さらに、目標復旧時間を意識した訓練を事業規模に応じて行い、訓練後の「気づき」を経営層と従業員の共通認識とし、費用対効果や優先順位を検討したうえで順に改善していく予定を立てておけばよいとされる。以降、改善が認められるように訓練を繰り返すことにより、「許容限界時間」を上回る「目標復旧時間」が守られる組織へと「事後対応力」の強化につなげていこうという発想である。

従って、申請において「必須事項」のすべてについて、満たしていることを示す書面等が提出されていれば 1 次審査合格となる。提出した書面等が不足していても、事務局からの質問に適切に応えて追加や修正をすることで合格することもできる。一部の「必須事項」に関して、企業秘密であること等の理由から書面等の「提出」は 行わないが面接の際に説明する、といった取扱いも認められている。この場合には、申請者のその意思を事務局が確認したうえで、二次審査に進むことが可能となる。

二次審査における面接で、どのような項目を確認されるのかも公表されている。

費用は、従業員数に応じて審査料、登録料を含め 3 万円（税別）から最大でも 10 万円（税別）と低価格に設定されている。参考までに、BCMS の取得費用はコンサルティング費用を含めると規模にもよるが数百万円以上と高額で中小企業にとってはハードルが高い。

レジリエンス認証の取得は大きなハードルを越えるものではなく、今できるところから一段ずつ低い階段を上るイメージで取り組み、それがレジリエンス強化につながっていることが評価され、組織の状況に応じたステップアップで「良し」とされる点が取り組みやすいと感じられる。

（3）レジリエンス認証を取得するメリット

認証を取得するメリットの一つとして「企業価値の向上」が期待される。

認証取得のために必要な事業継続計画書（BCP)の策定や見直しの効果により、不測の事態から会社を守り、事前の備えにより信用力の向上なども期待できる。また、レジリエンス認証を受けた団体は、レジリエンス認証マークを用いることができ、内閣官房国土強靭化推進室のホームページに認証取得団体として掲載されることや名刺、広告、社内報およびホームページへの認証マークの使用が可能となる。

これにより、その企業が事業継続のために積極的な取り組みを行っている企業であることをアピールすることができ、企業価値の向上、事業の機会の拡大につながる。

第 2 章　新システム管理基準

新「システム管理基準」における「Ⅷ．事業継続管理」は、旧版に比べて「４．訓練の管理」、「５．計画の見直しの管理」が追加され、担当者の技量をたかめる訓練と事業継続計画の成熟度を高めるための論点が充実した。しかし、システム監査人が当管理基準を用いて監査を行う場合、監査人の経験度合いによっては判断に迷いそうな箇所があり、それらの点について以下に述べる。

（1）経営層の「理解」と「関与」をどこまで求めるべきか判断に迷う。

「情報システム部門長は、リスクアセスメントの結果に基づき、経営陣が定めた事業継続計画と整合を取った情報システムの業務継続計画を策定すること。・・<中略>・・経営陣が業務継続計画を承認していること。」とあるが、経営陣が自らの口で説明できるほど業務継続計画の内容を理解しているかとか、どの程度の主体性をもって関与しているかの確認を求めておらず、「承認していること」を求めているので、経営層の理解度や関与度合いまで確認すべきかどうか迷う可能性がある。

（2）いざという時に司令塔となる人物像やその存在の確認が曖昧である。

何年くらいBCPの経験を積んだ人材の存在を求めるべきかといった具体的な年数を含めた人材の存在確認までは言及されていない。文面では情報システム部門長が中心的存在として期待されているともとれるが、現実の組織における情報システム部門長は必ずしもIT-BCP発動時の司令塔として相応しいとは限らない例が散見される。

（3）被監査組織の規模や成熟度にあった基準の適用判断が曖昧である。

システム管理基準は論点の網羅性を担保しあらゆる規模の組織にも適用できる事を意図してあるべき姿が記述されているので止むを得ない面もあるが、結果として「どの組織にも必須の事項」と「成熟度に応じて望ましい事項」の色分けがなく、被監査組織の成熟度に応じて指摘事項と改善提言をどこまで言うかは監査人の力量に依存することになる。

（4）過剰に分厚いIT-BCP文書を求める懸念がある。

システム管理基準の業務継続管理では、網羅性を求めるあまり分厚いIT-BCP文書の作成を求める事になると、いざという時に参照するには大量になりすぎて実用性が危惧されるが、適量の判断は監査人の経験に依存する。

（5）復旧許容時間の理想像だけを追い求めると現状との乖離が大きくなりすぎる懸念がある。

1.リスクアセスメント (3) で「情報システム部門長は、業務の復旧許容時間及び復旧優先順位を定めること。」とある。またその<着眼点>では、「① 復旧許容時間及び復旧優先順位の設定は、業務の重要性、緊急性、影響範囲及び他の業務との整合性及び実現可能性を考慮していること。」とある。現状との乖離に対する考察については「実現可能性を考慮していること」の記述だけであり、現状の情報機器類や人的資源ではあるべき復旧許容時間に比べて大きな乖離がある場合、次の一歩としてどこから改善を提言すべきか監査人が判断に迷う可能性がある。

（6）監査費用が高額になりがちな課題

システム監査にかかる費用は数百万円に及ぶことは珍しくないが、中小規模の被監査組織にとっては容易に調達できる金額ではない。　事前準備のコンサル費用は別として、数万円程度の費用で何らかの認証やお墨付きを与えてくれる手段を望む声があるが、最初からシステム管理基準を用いた監査を提案すると小規模

組織では費用負担に耐えられない可能性がある。

第３章　レジリエンス認証と新システム管理基準の比較に基づいたチェックポイント（案）

レジリエンス認証は、企業における経営理念や経営方針に基づいた事業継続計画があることを前提としている。また、認証を認めるための前提として、事業活動全般を範囲として認識している。システム管理基準における事業継続管理は、経営陣が定めた事業継続計画と整合を取った情報システムの業務継続計画であることから、業務システムを対象としている点で範囲が限定的であると考える。また、レジリエンス認証はあらゆる検討事項や設定目標に対して実現可能性を検討あるいは検証していることを示すドキュメントの提示を求めている点で実務レベルでの細かな点検を行うガイドラインとなっているといえる。

企業活動全般に対する事業継続計画を網羅的に審査するためには、レジリエンス認証における事業継続計画の考え方を上位概念として位置付けたうえで、システム管理基準における事業継続管理に沿った体制や取組みが行われていることを点検チェックすることで、より実効性のある事業継続計画の策定と運用を行うことが可能であると考えた。

以下に、レジリエンス認証審査項目の「必須事項」および「推奨事項」と、システム管理基準における「着眼点」を中心に行った相互の比較結果を踏まえて、BCP 監査のチェックポイントについてまとめたものを提示する。

表１．レジリエンス認証と新システム管理基準の比較に基づいたチェックポイント（案）

レジリエンス認証	情報システムに係るチェックポイント（案）
1．事業継続に係る方針が策定されていること 1－1 事業継続方針が BCP に含まれているか。	1. 情報システムに係る事業継続の基本方針が策定されていること。 （新規追加） ・情報システムに係る事業継続の基本方針が IT-BCP に含まれていること。 （新規追加）
2．事業継続のための分析・検討がされていること 2-1 事業影響度分析を実施しているか。 2-2 リスク分析・評価を実施しているか。 2-3 重要業務の選定がされているか。 2-4 資源の脆弱性（ボトルネックとなる資源（リソース）など）を把握しているか。 2-5 目標復旧時間を重要業務ごとに設定しているか。	2．情報システムに係る事業継続のリスクが、IT 部門において分析・検討されていること。 （システム管理規準Ⅷ.1.より抜粋） （1）自然災害等のリスク及び情報システムに与える影響範囲を明確にすること。 （システム管理規準Ⅷ.1.(1)より抜粋） （2）情報システムの停止等により組織体が被る損失を分析すること。 （システム管理規準Ⅷ.1.(2)より抜粋） （3）重要業務に繋がる、重要情報システムが選定されているか。 （新規追加）

	(4) 自然災害等による情報システムの脆弱性を把握しているか。 （新規追加） (5) 情報システムの復旧許容時間及び復旧優先順位を定めること。 （システム管理規準Ⅷ.1.(3)より抜粋）
3. 事業継続戦略・対策の検討と決定がされていること 3-1 事業継続戦略・対策に関する検討をし、決定している。	3. 情報システムに係わる事業継続戦略と対策が、IT部門において検討されていること。 （新規追加） （1）情報システム、データ及び関連設備のバックアップ方法及び手順を業務の復旧目標に対応して定めること。 （システム管理規準Ⅷ.3.(1)より抜粋） (2) 情報システムに係わるバックアップ方法及び手順を検証すること。 （システム管理規準Ⅷ.3.(2)より抜粋） (3) 情報システムの復旧までの手作業を含めた代替処理手続及び体制を定め、検証すること。 （システム管理規準Ⅷ.3.(3)より抜粋） (4) 情報システムの復旧手続及び体制を定め、検証すること。 （システム管理規準Ⅷ.3.(4)より抜粋）
4. 一定レベルの事業継続計画（BCP）が策定されていること 4-1 不測の事態が発生しても重要な事業を中断させない、または中断しても可能な限り短い時間で復旧させるための体制、対応手順が策定されている。	4. 情報システムの事業継続計画が策定されていること。 （システム管理規準Ⅷ.2.より抜粋） （1）リスクアセスメントの結果に基づき、経営陣が定めた事業継続計画と整合を取った情報システムの事業継続計画を策定すること。 （システム管理規準Ⅷ.2.(1)より抜粋） (2) 情報システムに係わる災害及び重大事故発生時に対応した事業継続計画を作成し、経営陣の承認を得ること。 （システム管理規準Ⅷ.2.(2)より抜粋） (3) 情報システムに係る事業継続計画の実現可能性を確保すること。 （システム管理規準Ⅷ.2.(3)より抜粋）

	(4) 情報システムに係る業務継続計画を関係各部に周知徹底すること。 （システム管理規準Ⅷ.2.(5)より抜粋）
5. 事業継続に関して見直し・改善できる仕組を有し、適切に運営されていること 5-1 事業継続に関して見直し・改善を行う仕組を有しているか。 5-2 見直し・改善が実施されているか。	5. 情報システムに係る事業継続について、見直し改善できる仕組みを有し適切に運営されていること (1) 情報システムに係る事業継続計画を必要に応じて見直すこと。 （システム管理規準Ⅷ.2.(6)より抜粋） (2) 情報システムに係わる業務の中断・阻害を引き起こす事故が発生し、事業継続計画の発動に至った場合、事故発生後に事業継続計画の評価及び見直しを行うこと。 （システム管理規準Ⅷ.5.(1)より抜粋） (3) 情報システムに係わる事業継続計画が、引き続き、適切かつ有効であることを確実にするために、あらかじめ定められた間隔で、業務継続計画の評価及び見直しを行うこと。 （システム管理規準Ⅷ.5.(2)より抜粋）
6. 事前対策（施設の強化・装備品の確保等）が実施されていること 6-1 事前対策が実際に行われているか。	6. 情報システムに係る事業継続のための事前対策が実施されていること。 （新規追加） (1) 情報システム、データ及び関連設備のバックアップ対策が実施されていること。 （新規追加）
7. 教育・訓練を定期的に実施し、必要な措置が取られていること 7-1 事業継続に係る教育・訓練を計画に基づき定期的に実施しているか。	7. 情報システムの事業継続に係わる教育・訓練を定期的に実施し、必要な措置が取られていること。 (1) 情報システムにかかわる適切な事業継続手順・計画が、事業継続目的に合致していることを確かにするために、手順に基づき訓練を実施すること。 （システム管理規準Ⅷ.4.(1)より抜粋） (2) 訓練は、策定後の維持管理のために、定期的に訓練の目的に応じて適切な訓練を実施、継続していること。 （システム管理規準Ⅷ.4.(1)より抜粋） (3) 訓練の実施手順に則り実施し、マネジメントレビューを行い、マネジメントサイクル（PDCA）を回

	すること。 （システム管理規準Ⅷ.4.(2)より抜粋）
8. 事業継続に関する一定の経験と知識を有する者が担当していること 8-1 上記の要件を満たす事業継続の担当者を 1 名以上任命しているか。	8. 情報システムの事業継続に関する一定の経験と知識を有するものが担当していること。 （新規追加） （1）情報システムに関する一定の経験（２年以上）と知識に加え事業継続に関する一定の経験と知識を有するものが担当していること。 （新規追加）
9. 法令及び法令に基づく命令その他法令に違反する重大な事実がないこと	9. 情報システムに係わる法令及び法令に基づく命令その他法令に違反する重大な事実がないこと。 （新規追加） （1）情報システムの事業継続管理にあたっては、情報セキュリティにも配慮すること。 （新規追加）

レジリエンス認証は、導入しやすい構成であるが、情報システムに関する視点が不足している。

今日災害時の事業継続のためには、情報システムに係わる事業継続管理策も重要である。この情報システムの事業継続管理策をレジリエンス認証のサブセットとして活用して貰うことで、よりリスクを減らすことが可能となる。また、事業継続管理のシステム監査を実施する際、システム管理基準で不足する視点を補う目的で使用することもできる。

むすび

システム監査基準はその前文でも明記されているとおりシステム監査人の行為規範であり、併記されている解釈指針は例示に留まっている。また、システム管理基準は網羅性が高く、前文において、適時、項目の取捨選択や内容の修正、他の基準等から補完を行うよう求めている。よって、どちらの場合も、十分な取捨選択に必要な知識とスキル無しに被監査組織に適用するとむやみに重厚長大な対策を求めることになりがちである。引いては、当該組織基準の見直しに向けた PDCA が回らない状況を生み出し、パッチワーク的対策の積み重ねになるといった悪循環にも繋がりかねない。

一方、レジリエンス認証が求める書類はその組織全体が整合性を持って危機管理対策を進めていることを確認できることを求めており、パッチワーク的対策の積み重ねに走らせる懸念は少ない。このことは、インシデント発生時の縮退運転の発動や手作業へのスムーズな移行を促し、過度な IT 依存による事業継続リスクを防止する効果がある。比較的小規模な組織の危機管理対策として適切なアプローチとなりそうである。

IT-BCP の普及にあたり、システム監査基準／システム管理基準からのアプローチと合わせ、適切に使い分けることが有用といえる。

以上　<目次>

2018.11

【エッセイ】空鉢護法

会員番号　0707 神尾博

産業用ドローン市場が活況である。インプレス総研によると、我が国の 2018 年の市場規模は、機体以外のサービス等も含め 860 億円、2020 年には 3711 億円に達すると予測されている。用途も地形測量や設備点検、最近テレビ番組でよく見かける俯瞰撮影等と日々拡大している。2018 年度には国交省が中心となり、離島や山間部での荷物の配送の解禁に向けて、検証実験が開始された。また自動車学校での操縦教室や受講証明の発行も始まっているという。ドローンを取り巻く企業は、まさに前途洋々だ。UAV（Unmanned Aerial Vehicle）と呼ばれる軍事用無人航空機の技術が民生へ転用され、典型的な「スピンオフ」の成功例となりつつある。

さて「空鉢護法（くはつごほう）」と銘打つ、いにしえのドローンを紹介しよう。飛鳥時代に播磨国（現在の兵庫県の一部）の法道（ほうどう）が、法力で鉢を飛ばし船中の年貢米を運んだという伝承が残されている。また平安時代の大和国（現在の奈良県）には命連（みょうれん）が、鉢によって米蔵ごと空中を移動させたという言い伝えがある。いずれも架空の話だろうが、それはさておき驚異的な積載量ではある。

実は現代のドローンには、サイバーセキュリティ上の様々な脆弱性が存在する。たとえば自身の飛行位置の特定に使用する民生用 GPS では、衛星とのやり取りの信号は暗号化されていない。したがって偽の信号と入れ替えて攪乱することが可能である。ただし、ジャイロセンサを用い飛行姿勢も制御する慣性航法装置等で補完されており、今後は航空レーダー測定装置の実装も検討されている。もっとも仮に人為的な攻撃を回避したとしても、宇宙空間から降り注ぐ放射線による電子回路の一時的故障である、ソフトエラーという厄介なハザードは残る。

一方でドローンを悪用したテロや犯罪、ホビー機の稚拙な運転技術による事故にも、危惧の念を抱かざるを得ない。米国では、操縦者を特定できるリモート ID（無線等による識別信号送信機能/デバイス）搭載の義務化について議論されている。

前述の法道は、運搬途上で一俵だけ地面に落としてしまったという。また容器ではなく自身が空を飛び、女の色香に惑わされて落下したという久米の仙人の話は、諸氏もご存じだろう。色欲や金銭欲には落とし穴が付き物だ。久米の仙人のように無事だった場合は笑い話で済むだろうが、ドローンの利用範囲拡大の解禁に際しては、たとえ墜落しても被害は当事者の物損に限定され、周囲には迷惑をかけないよう、安全対策には万全を期して欲しいものである。

（このエッセイは、記事提供者の個人的な意見表明であり、SAAJ の公式見解ではありません。画像は Wiki により著作権保護期間満了後のものを引用しています。）

<目次>

2018.11

第 235 回月例研究会：講演録

テーマ：【事例から学ぶ「発注者視点のプロジェクトマネジメントと監査」

～「発注者のプロジェクトマネジメントと監査」出版記念～】

会員番号　2574　竹原 豊和　（月例研究会）

【講師】SAAJ 理事　SAAJ プロジェクト監査研究会　主査

原田　憲幸　氏

【日時・場所】2018 年 9 月 7 日（金）18：30 – 20:30、機械振興会館　地下 2 階ホール（神谷町）

【テーマ】テーマ ： 「事例から学ぶ「発注者視点のプロジェクトマネジメントと監査」」

【要旨】

SAAJ で 3 月に出版した本「発注者のプロジェクトマネジメントと監査」のご紹介を兼ねて、「発注者視点のプロジェクトマネジメント」と「プロジェクト監査」のポイントについて、具体的な事例をひも解きながら、ご説明する。

【講演録】

1. この本が目指したことと本の構成

この本は、9 人のメンバーが 3 年間かけて作成しており、特に 3 年目については毎週土曜日、もしくは日曜日に朝 9 時から夕方 5 時まで話し合い、完成させている。この本が目指したことは、「絶対に外してはいけない肝・Point を明らかにする」「直ぐに役立つ指南書とする」「発注者の教本とする」「成功に導くプロジェクト監査を具体的にまとめる」の 4 点となっている。

本書については大きく分けて、「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」の 3 部構成となっており、詳しくは本書を読んでいただきたいと考える。

また、本日については本書の内容について事例を元に詳しく説明する。

2. 事例 1 ：業務抜本改革の新システム開発事例

とある企業において、業務の抜本改革を行うべく新システム開発に際して、大手コンサル会社の A 社に対してコンサルタントを依頼した。この際に要件定義を行い、業務フローの作成をしてもらうこととなった。但し、成果物については概要レベルとなっていた。

SIer に関してコンサルタントと同様に A 社に担当してもらうよう経営陣が希望したが、この企業の情報システム部門のトップは「A 社のインテグレーションが上手ではない」ことから反対をした。しかし結果的にコンサルと同様に SIer に関しても A 社が担当することとなった。

いざ、開発フェーズになったタイミングで企画を担当したコンサルタントが抜けてしまい、A 社の SIer から納期を延期して欲しいと要望があったが、発注側の企業はその要求を突っぱね、結果的に 1 年の遅延となった。

コンサルタントがいた際には業務の現場は要求を出さなかったが、コンサルタントがいなくなったタイミングで要求を出したこともトラブルの要因となっている。

プロジェクト監査人の意見としては「開発期間を 1 年延期して全体計画を見直す必要がある」というものだっ

たが、発注側の経営陣はこの意見を受け入れずに開発を続行した。

今回の大トラブルになった根本原因は「外部仕様の膨張・確定の遅れ（発注者の問題）」「業務改革リーダーシップが弱体（発注者の問題）」「業務を知らない設計者（受注者の問題）」「プロジェクトを一丸に出来ない PM（発注側 PM の問題）」「監査人の意見を採用せずに続行（発注側経営陣の問題）」の 5 点となっている。発注者側が受注者である A 社を責めた結果、A 社は非難をされないように分厚い資料を提出して取り繕い、状況の把握が難しい状態となっていた。システム監査人としても経営陣を納得させることができなかった。

3. 事例２：機能追加開発の順調な繰返しが・・・・

とある企業において、3 年目となる第 6 次開発の段階で「自動制御対象装置」の開発が行われたが、結合テストの段階でバグが多発する問題が発生した。なお、それまでの開発に関しては品質に問題等無く何年も大トラブルをおこしていないプロジェクトだった。

この際、単体テストまで順調となっており、結合テストで設計バグが多発した形となった。他のプロジェクトの要員を急遽このプロジェクトへ投入する形で設計そのものをやり直したが、それでも抜けが出てしまい、同様に結合テストでバグが多発することとなった。最終的に、全てのプロジェクトから要員を投入して対応を行うこととなり、トラブル対応に 1 年を費やした。

今回の大トラブルになった根本原因は「品質不安なのにサービス開始を強行（発注者の問題）」「過去の成功体験が判断を誤らせた（発注者の問題）」「無理な計画（発注者の問題）」「設計対象を知らない設計者（受発注者の問題）」の 4 点となっている。今回の開発については、老朽化した自動制御システムの作り直しという非常に難しい案件となっていたが、単なる機能追加開発という認識にて短期開発という形で開発計画を立てていた。これについては、今まで半年という短期開発で品質良く成功させてきた、という成功体験を元にした計画となっていた。また、設計のやり直しと決めた際においての開発期間も半年という短期な開発計画となっており、無理な計画となっていた。

4. 事例３：パッケージで開発するはずが・・・・

とある企業において、ワークフローエンジンの搭載パッケージを活用して柔軟にシステム構築を行う予定であったが、結果的にシステム構築はできず結果的にシステム構築は中止となった。

システム構築は C 社に対して発注され、C 者がパッケージを活用したシステム構築を提案していたのだが、パッケージを活用できないことが判明し、スクラッチ開発を C 社から提案された。スクラッチ開発にかかる費用増分は C 社側が負担するという条件で C 社にて開発が続行したが、総合テストで設計バグが多発し、開発が中止となった。

外部設計の計画がパッケージとスクラッチ開発で同じスケジュールにしていたため、結果的に 2 か月延期の計 4 か月で対応となったが、これに対するシステム監査人の見解は不可能というものだった。

今回の大トラブルになった根本原因は「無理な計画（受注者及び承認した発注者の問題）」「設計対象を知らない設計者（受注者の問題）」「開発中止と早く判断すべきだった（発注者の問題）」の 3 点となっている。

業務部門にヒアリングしたものを設計者が設計している時点で設計対象のシステムを理解していなかった。また、発注者側の社長に対して、正しい判断を促すことができないことが、開発中止の判断を遅らせた要因と

なっている。

5. トラブルプロジェクトにおける特徴と原因

「プロジェクトを一丸にする」ことが PM の最重要ミッションとなっているが、結果的にはそれぞれの立場において利害関係が相反しており、一丸にすることは難しい。特に業務の現場においての反発が大きく、それが結果的に要件確定を遅らせることや追加変更が多い状況につながっていき、企画・計画段階が要因のトラブルへと発展していく。

あるシステムインテグレータの 1 年間のプロジェクトを分析したデータを参考にした場合、企画・計画段階におけるトラブルの根本原因の比率は 42%となっており、このトラブルを解消することで約半分のプロジェクトはうまくいくことになる。スケジュールには「仕様凍結日」の完了予定はあってもその具体的な日程の約束をしていないことが多いが、必ず仕様凍結日は最初に約束することが重要となる。

6. トラブルを未然に防止するプロジェクト監査

「プロジェクト監査を受ける」ことは重要となっており、プロジェクトのすべてが終了した後ではなく、途中段階にて実施することが望ましい。発注者の役割として重要なことは「仕様を決めること」であり、何をどうやってほしいか、ということを決めるのは発注者側の役割となっている。開発の成功及び失敗は企画が決めるため、計画段階においてシステム監査を実施することは重要となる。

リスクの視点で考えてみた場合、リスク評価がおざなりとなっており、形骸化しているプロジェクトが多い。本当のリスクをつきとめる必要があり、「懸念するリスクを 3 つ挙げ、必ず対策する」ことを実行することが重要となる。品質面の視点においては、品質カルテが発注者側のマネジメントに役立つ。試験でバグを取る方法があるが、机上のトレースでバグを取る方法もある。総合テストの理想はバグが無いことを確認するためのテストであり、バグがないからこそコストを低減できる。

プロジェクト当事者は自分のことはわからないが、監査人は成功例も失敗例もたくさん見てきたので、すぐに問題がわかる。結果の監査だけではなく、企画・計画段階といった早めの監査は成功の鍵となる。

「システム開発企画審議の事前監査」「外部委託先選定の事前監査」「プロジェクト計画の事前監査」といった 3 つの段階における事前監査は特に重要となる。また、監査の観点として「システム構築の目的、必然性」は重要となる。コストや効果は審議されることが多いが、そのシステムが本当に必要なのか、という議論はあまりないため、この辺りについての議論は事前監査を実施する際に重要となる。

7. 新たな「プロジェクト監査研究会（略称 PJA 研」のご紹介

「プロジェクトを成功に導く」プロジェクト監査の具体化と、現場ですぐに役立つ実践的な成果物の作成を目的として、新たに研究会を発足した。こちらの活動は、現在 16 名の方が参加されており、全体会議を月に 1 回、第 3or4 金曜日の 19 時から開催している。SAAJ の地方支部の方については Web 会議での対応となっており、いくつかのチームに分けることを検討している。また、チームごとの議論を行い、その結果を全体会議の場で発表する形を検討している。新しい研究会ではシステム監査に焦点を絞り、掘り下げる形を目指しており、システム監査に役立つガイドラインやチェックリストについても作成したいと考えている。

成果物に関しては 2019 年 4 月に 0 版、同年 12 月に 1 版の完成を目指している。但し、0 版の完成スケジュールについては、同年 9 月になる可能性がある。

【所感】

本講演において切に感じたことは、早い段階でトラブルの要因を検知し、対策を行うことは重要である、という当たり前のことであった。これは、システム開発に限らず、多くのことに共通していえることであるが、実際に私自身が早い段階においての対応が行えているのか、といえば答えは NO となっている。頭ではわかってはいるが、様々な言い訳をして早い段階で対応ができていないのである。例えば病気においても、早い段階において病気を検知し治療を行えば重篤な病気に発展しない、ということは誰でもわかることである。多くの方は、1 年に一度健康診断や人間ドックを（半ば強制的に）受けることで、病気へのリスクを低減しており、短いスパンで定期的に検診を受けている人ほど重篤な病気にかかりにくいことも一般的な常識と考える。

これはシステム開発や様々プロジェクトにおいても同様であり、今回の原田先生のご講演をお聞きする中で、システムやプロジェクトに対する人間ドック的な役割である「システム監査」を早い段階で、更に定期的なタイミングで実施することの重要性を改めて感じた講演であった。

以上.

<目次>

2018.11

イベント報告【(2018 年度)関東地区主催　会員向け SAAJ 活動説明会】

会員番号　2581 斉藤茂雄（副会長）

システム監査活性化委員会では、昨年に続き会員活動（会員同士のコミュニケーションを含む）活性化を目的に、SAAJ の各研究会・部会活動にご参加頂けるよう、「(2018 年度)関東地区主催会員向け SAAJ 活動説明会」を開催致しました。

関東以外の支部からの 1 名を含む、21 名の方にご参加いただきました。

1．開催日時：2018年10月27日(土)　13:30～19:00 (17:40～交流会)

2．開催場所：NATULUCK茅場町 新館　2階大会議室

3．参加者　：21名(交流会9名)　理事13名

4．プログラム

	内容	時間	担当
13:30	開会の辞 (会長挨拶)	5分	小野会長
13:35	SAAJの研究会及び部会からの活動内容説明	55分	各主査または代理
14:30	休憩	10分	–
14:40	セミナー(1) 「システム監査基準／管理基準改訂のポイント」	50分	松枝副会長
15:30	休憩	10分	–
15:40	セミナー(2)　「JIS Q 15001改定内容について」	50分	仲理事
16:30	休憩	5分	
16:35	セミナー(3) 「情報セキュリティ関連基準の動向」	50分	舘岡副会長、豊田理事、山口理事、福田理事
17:25	閉会の辞　（挨拶）	5分	力副会長
17:30	休憩(受講証明書配付　・アンケート回収等)	10分	–
17:40	交流会	80分	–
19:00	終了	–	

５．開催内容（司会：力副会長）

最初に、小野会長より本説明会への参加の謝辞と主旨についてご挨拶いただきました。

5.1　SAAJ の研究会及び部会からの活動内容説明

研究会及び部会の主査より、目的・活動概要・メンバ・活動実績の紹介と共に、メンバの募集内容や参加メリットについて説明を行いました。

1. 会報部会～副主査：安部副会長
2. 法人部会～主査:山口理事
3. 月例研運営委員会～主査:力副会長
4. システム監査事例研究会～主査:野田理事
5. 情報セキュリティ監査研究会～主査:舘岡副会長
6. ITアセスメント研究会～主査:松枝副会長
7. 個人情報保護監査研究会～部会員:斉藤（茂）副会長
8. プロジェクト監査研究会～主査:原田理事
9. 認定委員会～委員長：舘岡副会長
10. CSA利用推進グループ～主査: 斉藤（茂）副会長

5.2 セミナー(1)「システム監査基準／管理基準改訂のポイント」

システム監査基準及び管理基準の改訂版が2018年4月20日に公開されましたが、本セッションでは一昨年来システム監査基準及び管理基準の改訂に携わったITアセスメント研究会を代表して、主査の松枝副会長より、システム監査基準及び管理基準の改訂の背景、狙い、ポイントなどを解説いただきました。

5.3 セミナー(2)「JIS Q 15001改定内容について」

個人情報保護監査研究会では、2017年5月30日の新個人情報保護法の全面施行、2017年12月20日の改正JIS Q 15001:2017の公布に対応し、会報に「新個人情報保護法がＰＭＳに及ぼす影響」に続き、「JIS Q 15001:2017と個人情報取扱規程」を連載しております。今回は研究会を代表して、仲厚吉理事よりこれまでの研究会活動の成果として、改正個人情報保護法のポイント、「６ヶ月で構築するPMSハンドブックJIS Q 15001:2017対応版」の核となる「個人情報取扱規程」概略について解説いただきました。

5.4 セミナー(3)「情報セキュリティ関連基準の動向」

「情報セキュリティ関連基準の動向」ということで、日頃情報セキュリティ監査研究会で注目しているテーマについて、研究会の4名の代表により以下発表いただきました。

（１）情報セキュリティ監査研究会の活動全体紹介、「情報セキュリティサービス基準」紹介

主査の舘岡副会長から活動の全体説明と個別テーマとして、経済産業省が2018年2月28日に公表した『情報セキュリティサービス基準』『情報セキュリティサービスに関する審査登録機関基準』について解説いただきました。

（2）情報セキュリティ監査基準／管理基準

豊田理事より、2003年に経済産業省が策定した情報セキュリティ監査基準／管理基準のその後の改正経緯を整理いただくと共に、システム監査基準及び管理基準の改訂版は、情報セキュリティ対応部分について情報セキュリティ管理基準を参照していることから、その対比を解説いただきました。

（3）FISC安全対策基準の改訂／クラウド監査基準

FISC安全対策基準は金融業界の環境変化に対応し、数年ごとに改訂されてきました。2018年3月に第9版が発行され、今回山口理事に概要を解説いただきました。また、併せてクラウド監査に関する基準の動向、JIS Q 27001:2014 (ISO/IEC 27001:2013) をベースとしたISMSクラウドセキュリティ認証制度についても解説いただきました。

（4）産業サイバーセキュリティ

産業サイバーセキュリティをターゲットとしたCSMS（Cyber Security Management System）とは、IEC 62443-2-1に基づく国際標準であり、CSMS認証とは、この要求事項に対する第三者認証制度です。本セッションでは、CSMS認証取得支援サービスに従事されている福田理事にCSMS認証について解説していただきました。

6. 受講された皆様の声(アンケート結果：21 名)　－アンケート抜粋－

(1)SAAJ 研究会・部会：　未所属 15 名、所属済 5 名、昔所属していた 1 名

(2)活動内容説明で興味を持った研究会・部会　（複数回答）：

情報セキュリティ監査研究会 9 名、プロジェクト監査研究会 6 名、
システム監査事例研究会 4 名、個人情報保護監査研究会 4 名、IT アセスメント研究会 2 名、
個人情報保護監査研究会 2 名、月例研運営委員会 1 名、システム監査事例研究会 1 名、
ＣＳＡ利用推進グループ 1 名

(3)今後のウェルカム・イベント：　毎年開催希望　17 名、 隔年開催希望　1 名、

(4)全体の感想・ご意見：

・多くの情報を整理されていて、役立ちます。
・こういうイベントを、テーマ別でもよいので、もう少し増やしていただきたいと思います。
休眠会員の掘り起こしになると思います。
・平日はほぼ無理ですので　土日イベントが有れば助かります。

7. 所感

今回は 21 名の方にご参加いただきました。申し込みは当初 30 名で、説明会への期待が大きいことを感じました。セミナーについては各セミナー共に好評で、アンケート結果にもありますが、「多くの情報を整理されていて、役立ちます。」という声があり、主催者の励みになりました。説明会終了後、軽食と飲み物を用意し、希望者による交流会を行いました。

以上　<目次>

2018.11

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 9

会員番号　1760 斎藤由紀子　（個人情報保護監査研究会）

他のマネジメントシステム規格との近接性のため、” 教育”は、”認識” となりました。”研修”、”教育”、”訓練” など、さまざまな手段によって身につけることを意味する ”認識” を確実にするために、旧 JIS:2006 と同様に、少なくとも年一回、適宜に行う必要があります。

マネジメントシステムを確実に運用するために、文書化は必要不可欠な要素です。旧 JIS:2006 の” 個人情報保護マネジメントシステム文書” から、”文書化した情報”と言い回しを変えています。

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
管理策 9＞ https://www.saaj.jp/03Kaiho/saajpmsJISQ15001_2017/009JISQ15001_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.3.4.5	認識 2006:3.4.5	組織は、従業者が 7.3 に規定する認識をもつために、関連する各部門及び階層における次の事項を認識させる手順を確立し、かつ、維持しなければならない。 a)個人情報保護方針（内部向け個人情報保護方針及び外部向け個人情報保護方針） b)個人情報保護マネジメントシステムに適合することの重要性及び利点 c)個人情報保護マネジメントシステムに適合するための役割及び責任 d)個人情報保護マネジメントシステムに違反した際に予想される結果 組織は、認識させる手順に、全ての従業者に対する教育を少なくとも年一回、適宜に行うことを含めなければならない。
	附属書 B.3.4.5	“認識”とは、従業者に、A.3.4.5 の a)～d)に定める事項を理解させ、自覚させ、個人情報保護体制における各々の役割・権限を確実に果たすことができるようすることをいう。 具体的には、従業者に対する教育を少なくとも年一回計画書（A.3.3.6）に基づき実施するにあたり、従業者の理解度確認を行うこと、アンケート又は小テストを実施するなどによって従業者の理解度を把握し、必要に応じて教育内容の見直しを図ること、及び教育を受けたことを自覚させる仕組みを取り入れることが A.3.4.5 に適合する。 また、従業者に対する教育を実施した場合の欠席者を把握し、欠席者を対象としたフォローアップ教育及び／又は理解度確認を行うなどの措置を講じることも A.3.4.5 に適合する。

	【P マーク審査対応のポイント】 ・”7.3 に規定する”とは、JIS 規格本体の”7.3 認識”を指す。 ・文書の名称は、「教育計画書」や「教育計画書兼報告書」など、事業者が定めた名称で差し支えない。 ・教材には、規格の a)～d)を含めなければならない。 ・a)「個人情報保護方針」を教育することが追加された。方針は、組織の個人情報保護の理念を表すものだからである。 ・b) ”PMS に適合することの重要性及び利点”では、PDCA の手法を用いることについて認識させる。 ・c)”役割及び責任” では、すべての事業およびすべての組織を PMS の範囲とし、代表者をトップマネジメントとして、全従業者が PMS を適切に運用することを認識させる。 ・d)”PMS に違反した際に予想される結果”では、”本人の権利を侵害する” ことへの認識が重要である。また、就業規則の罰則規定が適用されることを認識させる。 ・個人情報の漏洩事故の結果、組織が本人に支払う損害賠償金について、違反者がその責を負う罰則規程を定める組織が増えている。2004 年に発覚した、ジャパネットたかた「顧客情報流出事件」では、51 万件の個人情報流出に関与した社員に対し、組織が 1 億 1000 万円の損害賠償を求め、2008 年 5 月 15 日、長崎地裁佐世保支部において全額認められた事例がある。 ・「認識」の手段として、受講者の理解度確認を行うことは必須である。その結果、認識が不足している項目があれば、正解を説明し、可能な限り全項目について認識したことを目指す必要がある。特に重要な個人情報を取扱う従業者に対しては、認識が不足したままで当該業務に従事させてはならない。 ・定期教育では、全従業者が受講し、十分に理解度したことを示す「受講者記録」が必要である。 ・「教育報告書」には、教育の有効性の結果を報告しなければならない。 ・新たに入社した者に対しては、業務に従事する前に PMS 教育を実施しなければならない。 ・1 年間に実施した教育の結果は、次年度の教育計画の見直しに反映させることが重要である。

【3300 個人情報取扱規程】サンプル

3.4.5　認識

当社は、「3451PMS 教育計画書（兼報告書）」に従い、少なくとも年 1 回、適宜に全従業者に業務内容に応じた教育を実施する。

2　全従業者に以下の a)～d)を理解させるため「3456 教育テキスト」を作成する。「3456 教育テキスト」は直近の事故事例を含めるなど、毎年見直さなければならない。

a)	「3210 個人情報保護方針」
b)	PMS に適合することの重要性および利点
c)	PMS に適合するための役割および責任
d)	PMS に違反した際に予想される結果

3　教育にあたっては、下記の内容を含める。特に個人情報の取扱いに応じて「3313 リスク分析表」で検討した必要な対策については、重点的に教育しなければならない。

a)	「3200 個人情報保護方針」
b)	「3300 個人情報取扱規程」（本規程）
c)	「3305 個人番号関係事務規程」
d)	「3430 安全管理規程」
e)	「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」
f)	「3312 個人情報管理台帳」
g)	「3313 リスク分析表」

4　全従業者に教育を実施したことを、「3451PMS 教育計画書（兼報告書）」の受講者リストで管理する。

5　以下の状況が発生した場合には、随時「3451PMS 教育計画書（兼報告書）」により、トップマネジメントの承認を得て教育を実施する。

a)	採用者に対する初回教育（業務に就く前に教育を実施する）
b)	事故等の緊急事態発生に関連する是正処置において、新たなルールを規定した場合
c)	施設の移転、設備の更新など、セキュリティルールの変更があった場合
d)	法令、国が定める指針その他の規範の改廃により、自社のＰＭＳが見直された場合
e)	同業他社で発生した事故等から、自社の予防処置としてルールを見直した場合

6　受講者の理解度を確認するため「3457PMS 確認チェックシート 20XX 年版」を策定し実施する。満点に満たない者には、解説を加えてフォローアップし、満点になるまで継続しなければならない。

7　定期教育および、随時の教育の実施結果は、「3451PMS 教育計画書（兼報告書）」によってトップマネジメントに報告する。

8　1 年間の教育の実施の結果についても、「3451PMS 教育計画書（兼報告書）」を用いて有効性の評価を行い、次年度の教育への反映の提言を加えて、トップマネジメントに報告する。

9 教育の計画及び実施、結果の報告及びそのレビュー、計画の見直し並びにこれらに伴う記録（紙媒体、電子データ）は、PMS 事務局で 3 年間保管する。

■

A3.5　文書化した情報　　（2006：3.5） 目的　文書化した情報を作成・維持するため		
A.3.5.1	文書化した情報の範囲 2006：3.5.1	組織は、次の個人情報保護マネジメントシステムの基本となる要素を書面で記述しなければならない。 a)内部向け個人情報保護方針 b)外部向け個人情報保護方針 c)内部規程 d)内部規程に定める手順上で使用する様式 e)計画書 f)この規格が要求する記録及び組織が個人情報保護マネジメントシステムを実施する上で必要と判断した記録
	附属書 B	なし
	【P マーク審査対応のポイント】 ・他のマネジメントシステムでは、組織の一部のみの適用が可能なため、内部向けと外部向けの個人情報保護方針を策定するが、P マークは、組織全体で構築し、維持するものであるため、個人情報保護方針は、一つ（外部向け個人情報保護方針）のみであっても差し支えない。 ・規程とは、取扱規程、安全管理規程などに加えて、バックアップ手順書などの業務手順書、役割権限表、セキュリティ区画表、文書管理台帳、記録台帳など、ルールが規定されている文書を含める。 ・様式とは、個人情報管理台帳、リスク分析表、個人情報取得変更申請書、通知と同意書、入退館安全確認記録簿、委託先管理台帳、監査チェックリスト、是正処置報告書、マネジメントレビュー議事録など規定したとおりに記録させるための文書をいう。 ・計画書とは、PMS 年間計画書、PMS 教育計画書、PMS 監査計画書などをいう。 ・記録とは、様式を用いて記入もしくは入力した書類もしくはデータをいう。記録には、日付、記録者、承認者等の記載が必要である。	

【3300 個人情報取扱規程】サンプル

3.5　個人情報保護マネジメント（PMS）文書

3.5.1 PMS 文書の範囲

当社は PMS の基本となる次の要素を書面で記述し、「3510PMS 文書体系」によって維持管理する。

a)b)	「3200 個人情報保護方針」(内部・外部向け用途に統一した文書)	
c)	内部規程	「3300 個人情報保護取扱規程」（本規程）
		「3305 個人番号関係事務規程」
		「3430 安全管理規程」
		上記の他、「3320 法令・指針・規範集」「3371 緊急時連絡網」「3341-01 個人情報保護体制」「341-02PMS に関する責任と権限一覧表」「3371 緊急時連絡網」「3432-012 フロアマップ（セキュリティ区画）」「3510PMS 文書体系」「3530PMS 記録台帳」についても、内部規程に準じて取り扱う
d)	様式	内部規程に定める手順上で使用する様式

e)	計画書	「3303PMS 年間計画書（兼点検表）」
		「3451PMS 教育計画書（兼報告書）」
		「3721PMS 監査計画書（兼報告書）」
f)	記録	JIS Q 15001:2017 規格が要求する記録
		当社が PMS を実施するうえで必要と判断した記録

2　個人情報保護方針、内部規程は、個人情報保護管理者が策定し、トップマネジメントの承認を得る。

3　個人情報保護方針、内部規程には、制定年月日、改定年月日、トップマネジメント名を記載する。

4　様式は、PMS の運用において規程に従い適切に記録されるために、事務局もしくは担当部門が策定し個人情報保護管理者が承認する。

5　記録には、作成者、作成日、承認者、承認日付を明確にしなければならない。詳細手順は、「3430 安全管理規程」５～７に定める。

■

A.3.5.2	文書化した情報（記録を除く）の管理 2006：3.5.2	組織は、この規格が要求する全ての文書化した情報（記録を除く。）を管理する手順を確立し、実施し、かつ、維持しなければならない。 文書化した情報（記録を除く。）の管理の手順には、次の事項が含まれなければならない。 a)文書化した情報（記録を除く。）の発行及び改訂に関すること b)文書化した情報（記録を除く。）の改訂の内容と版数との関連付けを明確にすること c)必要な文書化した情報（記録を除く。）が必要なときに容易に参照できること
	附属書 B 3.5.2	文書化した情報（記録を除く）の管理とは、書面に記述した A.3.5.1 の a)～f)を保存し、制定・改正の記録を残したうえで、常に最新の状態で維持しておくことである。文書化した情報のうち記録は、A.3.5.3 に規定する管理策に従って管理する。また、A.3.5.1 の d)では、内部規程に定める手順上で使用する様式も合わせて管理することが求められている。 文書化した情報（記録を除く）は、個人情報保護マネジメントシステムを構成する要素が互いにどのように関係しているか、及び特定部分の運用についての詳細な情報がどこに記述されているかを、十分に示せる程度にあればよい。文書化した情報（記録を除く）は、組織によって実施される他のシステムの文書化した情報（記録を除く）と統合してもよい。 当初は、個人情報保護マネジメントシステム以外の目的で作成した文書化した情報（記録を除く）を、個人情報保護マネジメントシステムの一部として使用してもよい。そのような使い方をする場合は、それらの文書化した情報（記録を除く）を個人情報保護マネジメントシステムの中で参照しておくことが望ましい。 なお、文書化した情報（記録を除く）の管理は、個人情報保護マネジメントシステムを確実に実施するための手段であって、目的ではない。手段と目的を混同しないよう留意することが望ましい。
	【P マーク審査対応のポイント】 ・記録を除く文書とは、規程、様式、計画書で、PMS においては、PDCA の P にあたり、ルールとなる文書類である。 ・文書の発行、改定は、従業者へ確実に周知され、常に最新版のみが参照されるようにしなければならない。 ・他のマネジメントシステムで作成した文書を、PMS 文書として位置付けてもよい。例えば ISMS のリスクアセスメントに基づき作成した「セキュリティ規程」を PMS で使用することは可能である。ただし、ISMS を部門単位で取得した場合は、そのまま全社で適用することができない場合がある。PMS 側で ISMS の範囲外の部門におけるリスクアセスメントを実施し、ISMS 側とも協議のうえ「セキュリティ規程」に追加するとよい。 ・他のマネジメントシステム文書を PMS でも使用する場合は、「PMS 文書一覧」に含めること。 ・文書化した情報（記録を除く）は、必要最小限とする必要がある。文書の数が増えれば重複記述が増え、管理も複雑になる。	

【3300 個人情報取扱規程】サンプル

3.5.2　PMS 文書管理（記録を除く）

PMS 文書（記録を除く）については、次の管理手順に従う。

2　PMS 文書の発行および改定を行ったときは、従業者にメールで通知しなければならない。

3　PMS 文書の改定を行ったときは、改定内容と版数との関連付けを明確にして従業者に通知しなければならない。

4　PMS 文書の原本は、全従業者が参照可能な　¥共有ファイルサーバー¥PMS フォルダ¥　に保管する。

5　旧版文書は、個人情報保護管理者および PMS 事務局のみがアクセスできるフォルダに保管する。

■

A.3.5.3	文書化した情報のうち記録の管理 2006：3.5.3	組織は、個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実証するために必要な記録として次の事項を含む記録を作成し、かつ、維持しなければならない。 a)個人情報の特定に関する記録 b)法令、国が定める指針及びその他の規範の特定に関する記録 c)個人情報保護リスクの認識、分析及び対策に関する記録 d)計画書 e)利用目的の特定に関する記録 f)保有個人データに関する開示等（利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止又は消去、第三者提供の停止）の請求等への対応記録 g)教育などの実施記録 h)苦情及び相談への対応記録 i)運用の確認の記録 j)内部監査報告書 k)是正処置の記録 l)マネジメントレビューの記録 組織は、記録の管理についての手順を確立し、実施し、かつ、維持しなければならない。
	附属書 B 3.5.3	この規格で必要とする文書化した情報のうち記録には、A.3.5.3 の a)～l)のほか、内部規程に定める手順上で使用する様式[A.3.5.1d)]を用いた記録がある。 A.3.5.3g)は、A.3.4.5 に基づき従業者全員に教育を実施したことの記録である。A.3.4.5 の a)～d)の事項を従業者に理解させるに当たり、実施した事項の記録となる。よって、結果を報告する際には、単に教育実施の結果を報告するだけではなく、教育の有効性の確認を報告することが、A.3.5.3g)に適合する。 また、"教育の実施記録"には、緊急時対応についての教育訓練の記録なども含まれる。 A.3.5.3j)には、内部監査実施の状況のほか、問題点として把握した指摘事項と、その中で改善すべき事項とについて区別して示すことが含まれる。 文書化した情報のうち記録は紙媒体である必要はなく、組織内において運用しやすい合理的な方法で作成することが望ましい。A.3.5.3 では組織は、必要な記録を特定し、保管、保護、保管期間及び廃棄についての手順を確立し、実施し、維持することが望ましい。記録自体も個人情報である可能性があるから、とりあえず何でも記録として残すという姿勢ではなく、その必要性を判断することが望ましい。また、文書化した情報のうち記録は、必要なときにすぐに検証できるように維持しておくことが望ましい。
	【P マーク審査対応のポイント】 ・規格の、a)～l)の記録は、P マーク現地審査で確認対象となる。f)開示等の対応記録、h)苦情・相談対応記録は、事象が発生していなければ、無いと報告することになるが、手順を整備し説明できるようしておく必要がある。 ・P マーク現地審査では、少なくとも直近の 1 年間の記録を確認する。審査の時期によっては、前年度の記録が確認対象となるため、記録は年度単位もしくは a)～l)の単位でファイリングし、提示を求められたときに直ちに示せるようにしておくこと。 ・記録は、必ずしも紙でなくてもよい。プロジェクターに投影して提示してもよい。ただし、直ちに示せるようインデックス化や目次化をしておくこと。 ・a)～ｌ）について「PMS 記録台帳」等に保管期間を定めること。「個人情報管理台帳」にも保管期間を記載するが、a)～ｌ）のうち「個人情報管理台帳」に記載されるのは、f)開示等への対応記録、g)教育受講者記録、h)苦情及び相談への対応記録のみである。	

【3300 個人情報取扱規程】サンプル

3.5.3　PMS 記録の管理

PMS 記録については、規格への適合を実証するために必要な記録として、次の事項を含む「3530PMS 記録台帳」を作成し、かつ維持する。

a)	個人情報の特定に関する記録
b)	法令、国が定める指針及びその他の規範の特定に関する記録
c)	個人情報保護リスクの認識，分析及び対策に関する記録
d)	計画書
e)	利用目的の特定に関する記録
f)	保有個人データに関する開示等の請求等への対応記録
g)	教育などの実施記録
h)	苦情及び相談への対応記録
i)	運用の確認の記録
j)	内部監査報告書
k)	是正処置の記録
l)	マネジメントレビューの記録

2　「3530PMS 記録台帳」には、記録が、必要な時に、必要な所で、入手可能かつ利用に適した状態で管理されるよう、保管期間、保管部門、保管方法を定める。

3　個人情報が記載された文書は、機密性の喪失、不適切な使用及び完全性の喪失からの保護のため、「3312 個人情報管理台帳」に詳細な取扱いを定める。

4　具体的な保管方法および廃棄の詳細手順は、「3430 安全管理規程」５～７に定める。

■

A.3.6　苦情及び相談への対応　　（2006：3.6） 目的　苦情及び相談に対応するため		
A.3.6	苦情及び相談への対応 2006：3.6 法第 35 条 法第 52 条	組織は、個人情報の取扱い及び個人情報保護マネジメントシステムに関して、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順を確立し、かつ、維持しなければならない。 組織は、上記の目的を達成するために必要な体制の整備を行わなければならない。
	附属書 B 3.6	“必要な体制の整備”とは、例えば、常設の対応窓口の設置又は担当者を任命することなどをいう。ただし、個人情報保護管理者とは兼任をしても差し支えない。 必要な体制の整備にあたっては、日本工業規格 JISQ10002（品質マネジメント－顧客満足－組織における苦情対応のための指針）を参考にしてもよい。
	【P マーク審査対応のポイント】 ・苦情・相談対応を、開示等の請求対応と同じ手順で対応している組織があるが、目的が異なるため、個別の手順とすることが望ましい。ただし、苦情・相談対応と開示対応を、同じ部門、同じ担当者とすることは差し支えない。 ・苦情は、改善のための提言と受け止める姿勢が必要である。 ・苦情は、「是正処置報告書」作成の対象であり、また、トップマネジメントへの報告が必要である。 ・苦情・相談の場合は、本人確認は必須ではないことに留意する必要がある。 ・電話やメール等で、問い合わせがあった時に、開示等の請求等であるのか、苦情・相談であるのか、判断に迷った場合のエスカレーションルールを定めておくことが望ましい。 ・電話でのヒアリングは、慎重さと技術を要する。常に「苦情・相談対応記録」の様式を手許に準備して、可能な限り正確にメモを取り、判断に迷った時は「責任ある者から折り返し電話する」ことを告げていったん電話を切ることが必要な場合もある。 ・ホームページに公表する苦情・相談窓口として、電話番号、メールアドレス、住所を掲載すること。 ・P マークを更新する組織で、認定個人情報保護団体に加入している場合は、当該団体の苦情解決の申し出先を公表すること。	

【3300 個人情報取扱規程】サンプル

3.6　苦情及び相談への対応

当社は、個人情報の取扱い及び PMS に関して、本人からの苦情及び相談を受け付けて、適切かつ迅速な対応を行う手順を確立し、維持する。苦情・相談が寄せられた場合は、緊急事態発生に準じて取扱うこととし、必要な体制として苦情・相談窓口責任者を任命する。

2 「3220 個人情報の取扱いについて」に、苦情の申出先として、苦情・相談責任者の電話番号、メールアドレス、住所を掲載する。

3 プライバシーマーク適格性審査認定後は、「3220 個人情報の取扱いについて」に、「認定個人情報保護団体」の名称および苦情の解決の申出先を明示する。

4　電話で苦情・相談を受け付けた者は、概要と電話番号をヒアリングして「3601 苦情・相談報告書」に記入し、対応が長引く案件の場合は、"責任ある者から折り返しする"ことについて了解を得ていったん電話を切り、苦情・相談責任者に報告する。

5　苦情・相談責任者は、本人に電話連絡のうえ、苦情・相談の内容を「3601 苦情・相談報告書」に追記して個人情報保護管理者に報告する。

6　個人情報保護管理者は、苦情・相談の内容を確認し、関係者に調査を依頼し、その結果および回答案を「3601 苦情・相談報告書」を用いてトップマネジメントに報告し、承認を得たうえで、本人に回答する。ただし、個人情報保護管理者が、比較的軽微な苦情又は相談と判断した場合は、個人情報保護管理者の承認のみで対応することができる。

7　対応が終了後、すべての「3601 苦情・相談報告書」はトップマネジメントに報告しなければならない。

8　個人情報保護管理者は、苦情および相談の内容をもとに、原則として「3801 是正処置報告書」を策定し、真の発生原因を追究して改善策を講じなければならない。

9　苦情・相談の内容が緊急事態発生と判断した場合は、3.3.7 の手順に従う。

■

次回は、A.3.7　パフォーマンス評価　　から考察します。

以上　■■

<目次>

2018.11

支部報告　【　近畿支部　第 174 回定例研究会　】

会員番号　0655　荒牧 裕一（近畿支部）

1．テーマ　「ＡＩ・データの利用に関する契約の実務
～ＡＩ・データの利用に関する契約ガイドラインを踏まえて～」

2．講師　特定非営利活動法人 日本システム監査人協会 近畿支部 副支部長
弁護士、システム監査技術者、公認システム監査人
福本　洋一氏

3．開催日時　2018 年 9 月 21 日（金）　18:30~20:30

4．開催場所　大阪大学中之島センター　2 階　講義室 201

5．講演概要

近年 IoT・AI のビジネス活用の記事が報じられない日はないほどに、今後のビジネスにおけるデータ活用の重要性が取り上げられおり、経済産業省を中心に、民間事業者等がデータの利用等に関する契約や AI 技術を利用するソフトウェアの開発・利用に関する契約を締結する際の参考としての「ＡＩ・データの利用に関する契約ガイドライン」が策定されました。しかしながら、実務において契約ガイドラインの通りに契約が締結されているのかというと、必ずしもそうはなっていません。

本講演では、実務における AI やデータに関する契約の特性について、契約ガイドラインや講師自身の経験を踏まえた解説をしていただきました。

（1）ガイドラインの位置づけ（データビジネスとは）

従来ビジネスでは、顧客等へのサービス向上策としてデータを収集・取得していたが、データビジネスでは顧客等からのデータ取得等が目的となっており、目的や出発点が大きく異なる。

データ自体は無体物であり所有権や占有権の対象とはならず、誰もが無料で自由に利用可能なのが原則である。そこでデータを管理するために、媒体に記録して囲い込んだり、外部提供の際に秘密保持義務と目的外利用の制限が課されている。しかし、これでは当事者双方が利用できず死んだデータとなってしまう。

そこで、ガイドラインでは創出されたデータに対して契約による利用規制を排除し、双方の利用範囲を契約で合意することを求めている。ただし実務上はガイドラインの条項例をそのまま用いることは難しく、ビジネス上の力関係を踏まえた工夫が必要となる。

（2）「データ創出型」契約の実務

IoT サービスの課程で生じるデータに関する契約のように、複数当事者が関与することによりデータが新たに創出される場面において、当事者間で当該データの利用権限を取り決める契約である。

これについては、独立した契約ではなく本来のサービス契約（保守サービス規約）の一部として構成するなど、相手方に認識させずにデータを取得・利用できる工夫が必要である。

（3）「データ提供型」契約の実務

データ提供者から他方当事者に対してデータを提供する際にその利用権限等を取り決める契約である。

データが取引の対象である場合は、瑕疵担保責任の代わりにデータの品質不良に関して生成過程についての表明保証を行ったり、拡大損害の相当因果関係を認識させるためにデータをどのように利用することを想定しているのかを契約で明示することが必要である。また、契約における原データに関する取り決めは原則として派生データに及ばないので、派生データに対する効果についても明記すべきである。

（４）「データ共用型」契約の実務

複数の提供元からのデータを、プラットフォーム事業者が集約・分析・加工し、再提供する契約である。

事業者選定に当たって、中立性の確保、安定運営のための収入確保、セキュリティや透明性確保等の義務に留意すべきである。また、価格情報の共有等の独禁法で問題となり得る要素等についても留意する。

（５）「AI」総論（AI とは）

AI という語は定義が曖昧であるが、いわゆる「機械学習」（機械が数値やテキスト、画像、音声などの様々かつ大量のデータからルールや知識を自ら学習する）や「ディープラーニング」（ニューラルネットワークを用いた機械学習の手法の一つ）のような一般的に最近「ＡＩ」と表されているものだけではなく、機械学習ではなく人間が判断に必要なパターンを定義して事前に対応策を決めておく「似非 AI」も広告効果から「ＡＩ」と呼ばれており、ＡＩという用語が用いられてる際に、どのような意味で用いられているかには注意を要する。

AI の実用化における機能領域には、識別、予測、実行が挙げられ、ＡＩの導入を検討する際には、ＡＩにどのような機能を求めるかを明確にして検討する必要がある。AI を利用する目的は、効率化と高価値化に大別されるが、前者ではコストダウンのみが起き、後者ではイノベーションが起きる可能性がある。

（６）「AI 開発型」契約の実務

ユーザがベンダに依頼して学習済みモデルの開発を行う契約である。

これについては、データに関する利用権限、ベンダーによる学習済みモデルの流用リスク、担保責任の範囲、といった点に留意する必要がある。

（７）「AI 利用型」契約の実務

AI 技術を利用したサービスを提供する契約で、原則としてクラウドサービスのソフトウェア使用許諾契約と同じである。

しかしベンダ側の権利として、入力データの追加学習への利用、再利用モデルの利用権限、AI 生成物の帰属、が規定されている利用規約が多いので、安易にビジネスのコアな部分の判断にＡＩを導入するのは避けるべきである。

６．所感

講師は、IT や情報管理に関する法務に精通した弁護士としてビジネス実務の最前線で活躍している。その経験を踏まえて、経済産業省のガイドラインをどういった視点から修正して実務で活用していくかについて、具体的に解説していただき、非常に参考になった。

以上

<目次>

2018.11

注目情報（2018.10～2018.11）

■「中小規模向け IoT 品質確認チェックリスト」を公開」(IPA)

IPA は、2018 年 3 月 22 日に、IoT 機器・システムの品質確保を目的に、検証・評価の立場における考慮事項を示した「つながる世界の品質確保に向けた手引き」と、この手引きの内容が開発・運用の現場で考慮されているかを確認するための「つながる世界の品質確保チェックリスト」を公開しました。

このたび、上記のチェックリストから中小規模の IoT 製品・システムにおける品質確認のポイントを分かりやすくまとめた、「中小規模向け IoT 品質確認チェックリスト」を公開しました。

https://www.ipa.go.jp/ikc/reports/20181113.html

■「情報セキュリティサービス基準適合サービスの公開」(JASA)

特定非営利活動法人日本セキュリティ監査協会（本部：東京都中央区、会長：慶應義塾大学名誉教授 土居範久）は、情報セキュリティサービス基準（本年 2 月経済産業省公表）に適合する 80 サービスを台帳に取りまとめ、ホームページに公開しました。

http://www.jasa.jp/news/news_20181012.pdf

■「金融分野におけるサイバーセキュリティ強化に向けた取組方針」のアップデートについて」（金融庁）

デジタライゼーションの加速的な進展や国際的な議論の進展、「2020 年東京オリンピック・パラリンピック競技大会」等の開催など、金融分野のサイバーセキュリティを巡る状況は大きく変化しています。加えて、2018 年 7 月に政府全体の基本戦略である「サイバーセキュリティ戦略」が改訂されました。

これらの状況を踏まえ、金融庁として、実効性のあるサイバーセキュリティ管理態勢の構築に向けて、今般、新たな課題への対応方針や現在の取組方針の進捗・評価を踏まえた今後の取組み方針を明確化し、金融機関、金融サービス利用者及び関係機関と問題意識を共有するために、「取組方針」をアップデートしましたので、公表します。

https://www.fsa.go.jp/news/30/20181019-cyber.html

■「ISACA Refreshes COBIT Framework to Address Latest Business Technology Trends and Standards」(ISACA)

ISACA, the global association for information and technology (I&T) audit, risk, governance and security professionals, has released its first update to the COBIT framework in nearly seven years. The new version, COBIT 2019, provides comprehensive and more practical guidance to help enterprises better govern and manage their information and technology. The COBIT framework is used by enterprises in all industries around the globe, and COBIT publications have been downloaded more than one million times.

（ISACA 国際本部で、COBIT2019 が発刊されました）

https://www.isaca.org/　（記事のリンクはこちら）

<目次>

2018.11

【 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	公認不正検査士　甘粕 潔 氏 一般社団法人日本公認不正検査士協会(ACFEJAPAN) 専務理事 株式会社インタクト・コンサルティング執行役員
	講演骨子	1950 年代初頭に米国の犯罪学者ドナルド・クレッシーによって提唱された「不正のトライアングル」の仮説は、今や不正リスクを検討する際のディファクトスタンダードとも言われるほど浸透している。一方、当初発表から半世紀以上が経過する中で、複数の専門家がクレッシーの仮説の発展形ともいえるモデルを提唱している。本講演では、公認不正検査士協会（ACFE）の会員誌に寄稿された最近の研究成果等を概観し、不正リスクへの理解を深めるきっかけを提供する。
	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239回	日時	2019 年 1 月 22 日(火)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	今、振り返る安対基準第 9 版
	講師	公益財団法人 金融情報システムセンター 監査安全部 主任研究員　坂上 昇 氏 研究員　　宮島 吉昭 氏
	講演骨子	安全対策基準・解説書の第 9 版が発刊されて 1 年弱の期間が経過し、実際に当該解説書を利用した監査を経験したシステム監査人も出てきている中、改めて第 9 版発刊の意図や狙いを解説頂き、その内容を振り返ることで、実務経験も踏まえた理解を深める。
	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 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

<目次>

2018.11

協会からのお知らせ【年会費請求書を発送】

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 （〇一九店　019-0352357）
（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　トクヒ）ニホンシステムカンサニンキヨウカイ
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 10 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>

2018.11

協会からのお知らせ（予告）【第 18 期通常総会の開催】

会員番号　2581 斉藤茂雄（事務局長）

日本システム監査人協会（SAAJ）会員各位

■第 18 期通常総会のご案内

日本システム監査人協会の第 18 期通常総会を、下記の通り開催致します。

万障お繰り合わせの上ご出席をお願い申し上げます。

総会、懇親会の参加申込は 2019 年 1 月末より、協会ホームページにて受け付けます。

1．日時：2019 年 2 月 22 日（金）　13 時 30 分～（受付開始：13：00）

2．場所：東京都港区芝公園 3 丁目 5 番 8 号 機械振興会館 地下 3 階 研修 1 室

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

3．第 18 期通常総会 議事（予定）　13 時 30 分～15 時

13:30 開会

(1) 2018 年度 事業報告の件

(2) 2019 年度 事業計画の件

(3) 2019 年度 予算の件

(4) その他

15:00 閉 会

（休 憩）

4．特別講演　15 時 30 分～17 時

15:30 開演

演題：調整中

講師：調整中

17:00 閉演

5．懇親会　17 時 30 分～19 時

17:30 開場 （機械振興会館地下 3 階会議室）

20:00 閉場

以上

<目次>

2018.11

【 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			2018.11
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
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	13,14：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	
4 月	11：理事会	初旬：春期 CSA・ASA 書類審査 中旬：春期 ASA 認定証発行	21：春期情報技術者試験
	前年度に実施した行事一覧		
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	
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

<目次>

2018.11

【 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

2018.11

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：　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>