

システム監査を知る ための小冊子

～情報社会に不可欠な
システム監査～

認定NPO法人 日本システム監査人協会
Systems Auditors Association of Japan

目次



はじめに	
✓ 監査とは	1
✓ システム監査とは	3
✓ システム監査へのQA ～監査にご協力いただくために～	5
✓ システム監査に適用される基準とは ～システム監査における判断の拠りどころ～	7
✓ システム監査基準 ～システム監査人の行為規範～	9
✓ システム監査とITガバナンス ～システム管理基準の有効活用～	11
✓ FISCの各種基準の概要	13
✓ COBIT2019について	14
✓ システム監査への期待の変化 ～経営を支えるシステム監査～	15
✓ リスクマネジメントは経営課題 ～リスクアプローチの勧め～	17
✓ 情報セキュリティ監査	19
✓ システム監査人に求められる能力	21
✓ システム監査人を目指すということ ～システム監査経験を通じ、将来の能力発揮場面を拓く～	23
✓ システム監査人の新たな活躍の場 ～AIの世界とシステム監査～	24
✓ システム監査の役割と効果 ～（図解）システム監査～	25
✓ システム監査の勘所	27
✓ システム監査と“学び” ～新技術のシステム監査にどう取り組むか～	29
✓ システム監査人の体験から ～外部委託管理の監査では、委託元・委託先双方に対する調査が必要～	31
✓ 成功に導くプロジェクト監査 ～システム開発成功の鍵～	33
✓ 効果的かつ安心してクラウドサービスを利用するためのシステム監査 ～第三者評価も活用したシステム監査の実践～	35
✓ ISMAP制度 ～政府情報システムのためのセキュリティ評価制度～	37
✓ IT統制監査 ～財務報告に係る内部統制の 評価及び監査の基準とIT統制監査～	39
✓ 官民一体化！2021個人情報保護法 ～GDPR十分性認定の法的根拠～	41

- ✓ [産業用オートメーションのセキュリティ対策](#) 43
～社会・産業基盤を支える制御システムが狙われる～
- ✓ [国のDX提言と推進施策](#) 45
～DX監査の可能性～
- ✓ [テレワークを監査する](#) 47
～どのような視点で監査するか～
- ✓ [リモート監査](#) 48
～監査品質の確保のために～
- ✓ [SAAJのこれからの取り組み](#) 49
～IT経営の推進に取り組むすべての方へのメッセージ～

【認定NPO法人日本システム監査人協会（SAAJ）入会のご案内】

<https://www.saa-j.or.jp/>

協会HPの「入会・退会について」から手続き出来ます。
「出版案内」では現在刊行している書籍のご案内をしています。

〇会員の特典

- (1)研究会活動への参加（巻末の「主な部会・研究会」参照）
- (2)会報（PDF）のご案内や投稿
- (3)会員メールによる情報提供 例：官公庁や自治体からのシステム監査人募集案内情報
- (4)協会主催セミナー、関連団体セミナーのご案内
- (5)月例研究会、システム監査実務セミナー、システム監査実践セミナー等参加費割引
- (6)出版物購入割引
- (7)公認システム監査人(CSA)・システム監査人補(ASA) 認定申請手数料の優遇
- (8)CSA/ASA更新手数料の優遇

公認システム監査人資格

～公認システム監査人(Certified Systems Auditor : CSA)を目指そう～

公認システム監査人とは

「公認システム監査人」は、SAAJによる公認システム監査人認定制度（2002年2月25日制定）に基づく、システム監査人です。

- ・システム監査技術者試験合格者もしくは同等の能力を有し^{注1)}且つ2年以上の実務経験者^{注2)}が申請可能。書類審査、面接試験を経て資格認定。その後2年毎に資格更新。

注1) 下図の資格保有者で特別認定研修受講済者

注2) 実務みなし制度あり

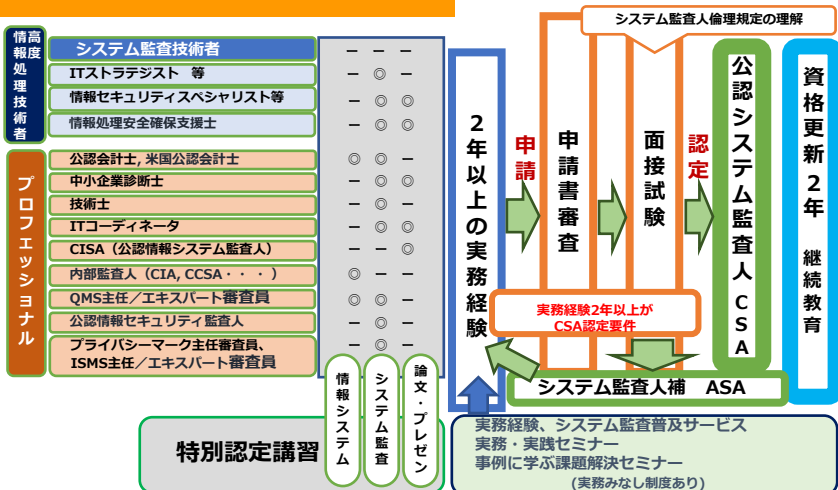
- ・資格継続には、継続的な実務及び教育受講が必須です。
- ・認定制度は1999年通商産業省（現経済産業省）の産業構造審議会・情報化人材対策小委員会の提言を受け誕生しました。

「公認システム監査人(Certified Systems Auditor : CSA)」および「システム監査人補(Associate Systems Auditor : ASA)」で構成されます。

公認システム監査人のバックボーン

監査実務並びにSAAJを通じて継続教育、研究会、情報交換などで研鑽しています。

公認システム監査人へのステップ



はじめに

～ITガバナンスを対象にしたシステム監査～

現在の企業経営にはITが不可欠であることは、どなたも異論がないことと思います。IT経営という経営スタイルがあります。ITと情報を有効に活用して経営活動および業務活動を効率化し、付加価値を向上させる経営スタイルをIT経営と呼んでいます。大企業だけでなく中小企業でもIT経営の重要性がいられています。勿論、官公庁や自治体でも同じことがいえます。

IT経営を成功させ、目的を達成するためには、企画・構築しようとしているITを利用した仕組みが経営目的に合致したものになっているか、経営活動および業務活動で利活用しているITを利用した仕組みが経営目的に合致し業務活動に効果をもたらしているかが重要であり、それはITガバナンスの範疇と捉えることができます。

システム監査は、ITを利用した仕組みの信頼性、安全性、効率性の観点でリスクを軽減させるためのアプローチとして、その役割を果たしてきました。そのことは何ら変わることはありません。リスクが存在するITを利用した仕組みによってITガバナンスが実現できることはあり得ません。リスクコントロールを含めてIT経営のベースとなるITガバナンスが確実に機能しているかという観点が、システム監査に求められる時代になってきたと言えます。そのことは、2018年に改訂されたシステム管理基準において、システム管理・システム監査の対象としてITガバナンスが明確に位置づけられたことにも表れています。

当協会では、そうした経営活動を含む領域までを対象にした評価・診断の取組みを、システム監査を核として、ITアセスメントと呼び、その実践方法の確立に取り組んでいます。

本小冊子は、新たな役割を担うシステム監査・ITアセスメントに関連する情報を提供するものです。ぜひ、ご一読いただき、システム監査・ITアセスメントについてご理解を深めていただければ幸いです。

監査とは

監査の目的は、企業や自治体などあらゆる組織体において、経営や業務活動が適切に行われていることを点検・評価し、その結果が適切でなければ、正しい方向へ誘導することです。会計監査の場合は、適切であることを外部へ保証することです。

監査とは

対象

企業や自治体などあらゆる組織体において、

内容

経営や業務活動が適切に行われていることを、法令や規定などに照らして点検・評価し、

目的

その活動が適切でなければ指摘し、正しい方向へ誘導すること。会計監査に代表される一部の監査では適切であることを外部へ保証すること。

監査の種類には、誰が行うかという監査主体による分け方としての内部監査と外部監査、監査対象による分け方としての業務監査と会計監査など、さらに目的による分け方として保証型監査と助言型監査などがあります。

例を挙げれば、株主の利益を損なわれないことを目的とした会計監査の場合は、決算書などの財務諸表が適正に作成されていることを株主に保証する必要があることから、保証型監査であり、外部監査が望ましいといえます。

一方、企業内部で不適切な業務処理が行われ、大きな損失が発生することがないために行われる業務監査は、不適切なところを指摘して改善を促す助言型監査になり、一般的には内部監査として行われます。

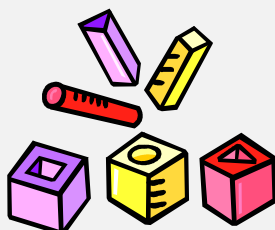
監査を切り口の違いにより整理したのが、下の表です。

監査 の 種類	主体による分類	内部監査、外部監査
	対象による分類	業務監査、会計監査 など
	目的による分類	助言型監査、保証型監査

監査を行うことによってどんな良いことがあるのでしょうか。

それは、監査対象業務の態勢が検証されて、経営者や利用者に経済的な面や利便性に大きなメリットが生まれることです。また、現状を放置しておくとは大事件や大損害になることを未然に防止できることです。事業規模にもよりますが、何億円も使いこみをされると企業にとっては存続に関わることになるかも知れません。倒産すると取引先や従業員に多大な迷惑をかけることとなります。

このような大事件にならないよう小さな事象のうちに間違いを発見することや、さらには、そもそも間違いを起こさないような仕組みの整備などを促すことが、監査を行うことのメリットといえます。



システム監査とは

「システム監査基準」（経済産業省、2018年4月版）では、『システム監査とは、専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型である』としています。

たとえば、「経営陣が、経営戦略とIT戦略との整合性、IT利用の有効性などについて評価が知りたい」というニーズをもっている場合、情報システムのガバナンスを対象とするシステム監査を実施することで、客観的な評価や助言を得ることができます。あるいは、システム監査にはたとえば、「情報システムの大きな事故・災害につながるリスクの発生を未然に防止すること」が期待されます。具体的には、システム停止により業務遂行ができなくなることや、機密情報・個人情報の漏えいなどによってセキュリティが守れないこと、その他経済損失に関わる事件などの発生を未然に防ぐことなどです。

システム監査の目的

また、システム監査の目的は、『システム監査は、情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする。』としています。

つまり、システム監査は、組織体自身がそれを通して組織体の目標達成に寄与すること、または、利害関係者に対する説明責任を果たすことが目的であり、システム監査人はそれを支援する立場であるといえます。

こうしたシステム監査の目的を達成するためには、組織体におけるシステム監査を円滑に実行することが必要になります。被監査部門にとっては、システム監査というと監査人によって何か自分たちが調べられて責任を問われるのではないかと、といったネガティブな印象を受けがちです。そうした印象を払拭し、システム監査は組織体自身が自分たちのために実施しているんだということを理解してもらうことが重要です。

次頁にシステム監査に対する被監査部門からの質問を想定したQAをまとめました。参考にしてください。

情報システム監査実践マニュアル

システム監査の実施に当たっては、情報システムの知見と監査スキルのあるシステム監査人が担当します。しかしシステム監査人が様々な分野の情報システムの様々な場面を把握し、短期間で監査目的を達成することは大変難易度の高い作業になります。この小冊子にもいくつかのヒントがあります。こうしたシステム監査人にはSAAJが監修している「情報システム監査実践マニュアル」（第3版）が参考になるはず。本書は、システム監査の導入からフォローアップに至る業務を、事例を交えて実践的に解説して、高い評価をいただいている、システム監査人の必携書（通称赤本）です。以下の特長があります。

- テーマごとに監査（管理）のポイントを詳説
- 監査書類・監査チェックポイント集のダウンロードデータ付き
- 経験豊富な執筆陣



<https://www.saa-j.or.jp/shuppan/index.html>（割引き購入注文書）

システム監査へのQA

～監査にご協力いただくために～

システム監査を実施するに際し、被監査部門にご理解いただきたい点をQA形式でまとめました。場面に応じてアレンジしてお使いください。

Q.システム監査実施の意義はどんなものですか？

A.システム監査は組織の健康診断です。

システム監査はよく健康診断にたとえられます。組織の現状を客観的に把握し、組織の運営が適切に行われていることを確認するとともに、見つかった問題点に対処することを目的に行われるためです。監査を外部監査人に委託することもあります。外部監査では、専門性のある監査人が監査することで、より客観的・専門的に監査を実施できます。

Q.システム監査は専門の監査人に任せれば十分ですか？

A.システム監査の主体は自組織です。

経済産業省「システム監査基準」では、システム監査は、組織がそれを通じて組織の目標達成に寄与することを目的として実施すると定義されています。

このように監査は組織目標達成のための手段であり、組織が自らのために行うものです。その点、他者により行われる検査や審査とはその主体が異なります。システム監査人に任せれば済むということではありません。

Q.システム監査の目的は何ですか？

A.実態を把握し、問題点を改善することが目的です。

「システム監査基準」では、システム監査は情報システムにまつわるリスクに適切に対処しているかを点検・評価・検証することを通じて、組織の経営活動の効果的な遂行や変革を支援する、としています。システム監査人は組織の業務・システムの調査を通じて実態を把握し、評価することで問題点を抽出します。



Q.監査で指摘する問題点とは何ですか？

A.問題点とは組織のあるべき姿と現状のギャップ です。

「問題とは、あるべき姿と現状のギャップである」とよく定義されています。「あるべき姿」については、世の中で一般的に使われている共通の基準（ものさし）を使いますが、組織の「あるべき姿」は、共通の基準ではなく組織の方針に鑑みて評価することになります。

Q.何故現状把握が必要なのですか？

A.現状（＝実態・事実）が把握できてこそ、そのギャップである問題点がわかります。

監査は実態・事実を把握することから始まります。そうすることで初めてギャップが見えてきます。したがって、実態・事実を把握・確認することが非常に重要になります。そのために業務・システムの調査に重点を置きます。

情報システムを使用した業務においては、使用上・管理上のルールや仕組みがあるか、ルールに即した業務がなされているかを調査します。それらの実情をより把握・確認するために、規程・手順書等の文書や各種記録・資料の収集・閲覧、インタビュー、現場視察などをします。監査人には守秘義務があり、調査した内容を外部に漏らすことは監査人の倫理違反となります。

Q.問題点が発見されたら、現場の担当者の責任になりますか？

A.問題点は個人の問題ではなく組織の問題です。

監査により検出された問題点は、組織としての問題点です。個人へのインタビューや、個人が分担されている業務上で問題点が検出されても、それは個人の問題ではなく、組織の問題です。監査は個人の責任を問うものではなく、組織上の問題点を抽出することが目的です。

Q.システム監査とコンサルティングはどう違いますか？

A.監査人は組織と独立性を保ち、客観的基準により意見表明をします。

システム監査でもシステムのコンサルティングと同様、組織の問題点に対し、改善の助言（提案）を行うことがあります。外形的には似ていますが、システムコンサルティングでは依頼者の立場で、コンサルタント独自のノウハウを発揮し、依頼者に適した改善提案を行うのに対し、システム監査では被監査部署と独立の立場のシステム監査人が、客観性のある監査基準に則り、業務や情報システムを総合的に点検・評価・検証をして、意見表明をします。また、副次的に改善のための助言を与えることもあります。

システム監査に適用される基準とは

～システム監査における判断の拠りどころ～

システム監査は、納得性のある基準に照らして監査対象の状況を監査することから、どの基準に基づいて監査するかを明確にしておく必要があります。

システム監査の代表的な基準には、経済産業省が公表している「システム監査基準」と「システム管理基準」があります。

「システム監査基準」は、①システム監査人の行為規範（倫理規定）、②システム監査手続きの規制（守るべきルール・手続き）を規定するものです。一方、「システム管理基準」は監査人の判断の尺度を規定するものと言えるでしょう。あわせて、「システム管理基準」は、システム管理者がシステムのライフサイクルを有効に管理するための基準にもなります。

システム監査の実施体制を整備するうえでは、公表されている基準やガイドライン・規格などを基に、組織体としてのシステム監査基準を作成し、監査テーマに合わせて個別のチェックリストを確定させる必要があります。システム監査のための基準もしくはシステム監査に利用できる基準、ガイドライン等の主なものには表のようなものがあります。これらを含めて、システム監査の目的、テーマに合った基準を選定し、利用します。

システム監査に役立つ主な基準等

- システム監査基準（経済産業省2018年4月改訂）
- システム管理基準（経済産業省2018年4月改訂）
- システム管理基準 追補版（財務報告に係るIT統制ガイダンス）
（経済産業省2007年3月）
- 情報セキュリティ監査基準（経済産業省2003年）

システム監査に役立つ主な基準等(つづき)

- 情報セキュリティ管理基準(経済産業省2016年3月改正)
- クラウド情報セキュリティ管理基準(JASA2016年改定)
- 内部監査基準(日本内部監査協会2014年6月改訂)
- 内部監査基準実務指針(日本内部監査協会2017年3月および5月)
- ISMAP管理基準(ISMAP運営委員会2021年6月改定)
- ISMAP情報セキュリティ監査ガイドライン
(ISMAP運営委員会2021年6月改定)
- 地方公共団体における情報セキュリティ監査に関するガイドライン
(総務省2018年9月改定)
- 金融機関等のシステム監査基準 (FISC2019年3月)
- 金融機関等コンピュータシステムの安全対策基準・解説書(第9版令和2年3月版)
(FISC2020年3月)
- COBIT2019 Control Objectives for Information and related Technology
(米ISACA2018年11月)
- サイバーセキュリティ経営ガイドラインVer2.0
(経済産業省2017年11月)
- JIS Q 19011:2019(マネジメントシステム監査のための指針)
- JIS Q 38500:2015(ITガバナンス)
- JIS Q 31000:2019(リスクマネジメント—指針)
- JIS Q 9001:2015(品質マネジメントシステム)
- JIS Q 20000-1:2020、20000-2:2013(サービスマネジメント)
- JIS Q 27001:2014(情報セキュリティマネジメントシステム)
- JIS Q 27002:2014(情報セキュリティ管理策の実践規範)
- JIS Q 27014:2015(情報セキュリティガバナンス)
- JIS Q 27017:2016(JISQ27002に基づくクラウドサービスのための情報セキュリティ管理策の実践規範)
- JIS Q 22301:2020(事業継続マネジメントシステム)
- JIS Q 15001:2017(個人情報保護マネジメントシステム)

システム監査基準

～システム監査人の行為規範～

システム監査基準は、1985年に、コンピュータシステムの効率性・信頼性・安全性を総合的に点検評価し、もって情報化社会の健全化に資する目的で、当時の通商産業省によって制定されました。

その後、情報システムを取り巻く環境の進化に伴い、1996年、2004年、2018年の3回改訂が行われました。2004年の改訂では、従来の実施基準の主要部分を抜き出して、システム管理基準として独立させました。

2018年4月、進化し続けるIT技術環境への適合、システム監査の知識経験のない中小企業での自己診断や監査への対応などシステム監査ニーズの多様化、ITガバナンスの実現への貢献、情報セキュリティ監査基準・管理基準との補完性などの今日的課題を克服する狙いで、システム監査基準とシステム管理基準の改訂が行われました。

システム監査基準は「システム監査業務の品質を確保し、有効かつ効率的な監査を実現するためのシステム監査人の行為規範である」と位置付けられました。このため、「誰が、何を、どのように」が判り易く明記されています。

システム監査基準は、前文と5種12基準で構成されています。前文では、システム監査の意義、目的、システム監査基準の意義に加えて、「情報システム」についても定義されています。また、留意事項として、

- ・情報セキュリティ監査基準や内部監査基準を参照する
- ・中小企業や官公庁などで利用できる
- ・判断尺度として、システム管理基準をカスタマイズしたものや独自の諸規定を利用できる

などと、汎用性を持たせたものであることがうたわれています。

12の基準は、それぞれ

基準本文：すべきことを「しなければならない」と記述

主旨：基準の説明

解釈指針：実務上の望ましい対応、基準の補足説明、留意点から成っています。「すべきこと」と「することが望ましいこと」が明確に判るようになりました。さらに、従来の「一般基準」「実務基準」「報告基準」の体系が、5種に括られました。

- i. システム監査の体制整備に係わる基準
- ii. システム監査人の独立性・客観性及び慎重な姿勢に係わる基準
- iii. システム監査の計画策定に係わる基準
- iv. システム監査実施に係わる基準
- v. システム監査報告とフォローアップに係わる基準

手順に関わる記述はなくなりました。



改訂されたシステム監査基準は、システム監査を「情報システムのガバナンス・マネジメント・コントロールの適切性の保証、または改善のための助言を与える」こととしています。従来は「情報システムのライフサイクル全般にわたるリスクコントロールの適切性の保証、または助言を与える」ことでした。

システム監査の概念にガバナンスが入ったことで、システム監査の対象に、情報システムに係わるリスクコントロールの適切性に加えて、経営層とマネジメント層を対象にしたITガバナンスの適切性も加わりました。

システム管理基準の前文では、「ITガバナンスは経営陣が組織の価値を高めるために実践する行動であり、情報システム戦略の策定及び実現に必要な組織能力である。」としています。このことはすなわち、システム監査の対象が「IT経営」の領域まで拡大することといえます。ガバナンス強化の観点からも、システム監査とシステム監査人への役割と期待は拡大し続けています。

システム監査とITガバナンス

～システム管理基準の有効活用～

ITガバナンスについては、2015年7月に「JIS Q 38500:2015情報技術－ITガバナンス」が制定されました。国際規格としては2008年に「ISO/IEC38500」第1版が、2015年に第2版が発行されております。そして2018年4月改訂の「システム管理基準」にはこれら規格のITガバナンスの考え方を全面的に踏襲しています。昨今、企業の信頼を損ねるような不祥事が散見され、また、ITの運用でも、経営者のモニタリングが十分でなく、問題を深刻化させているケースがあります。そこで、ITガバナンスを経営活動にうまく活かしていくことが重要になります。

JISでは、ガバナンス (corporate governance) とは、“組織を指示し、管理するシステム”であり、ITガバナンス (corporate governance of IT) とは、“組織のITの現在及び将来の利用を指示し、管理するシステム”と定義しています。規格は、良好なITガバナンスのための「六つの原則」（次ページの表参照）を示し、この原則はほとんどの組織で適用できるとしています。

一方、経営陣は三つの主な職務によってITを統制することが望ましいとしています。その職務は、「評価 (Evaluate)」、「指示 (Direct)」、「モニタ (Monitor)」の三つです。また、評価-指示-モニタのサイクルがITガバナンスのモデルであるとし、これをEDMモデルと呼んでいます。

経営陣は、良好なITガバナンスのための「六つの原則」が、組織において実施され運用されるよう職務を遂行します。つまり、事業プロセス (ITプロジェクトとIT運用) に対して、計画及び方針の準備及び実施を指示し、事業プロセスから上申してくる報告や決裁稟議などを評価し、方針への適合及び計画の実績をモニタし、ITを統制します。

良好なITガバナンスのための六つの原則

原則1：責任（Responsibility） -組織内の個人及び部門は、ITの供給及び需要の両面の役割について、その責任を理解して受け入れる等

原則2：戦略（Strategy） -組織の事業戦略は、ITの現在及び将来の能力を考慮する等

原則3：取得（Acquisition） -ITの取得は、適切で継続的な分析を基礎として、明確で透明な意思決定による正当な理由に基づいて行う等

原則4：パフォーマンス（Performance） -ITは組織を支援し、現在及び将来の事業のニーズに合うサービス、サービスレベル及びサービス品質を提供する点で目的に適合する

原則5：適合（Conformance） -ITは、必須である全ての法律及び規制に適合する等

原則6：人間行動（Human Behavior） - ITの方針、指針及び決定は、プロセスにおける人間の全ての現在及び発展するニーズを含み人間行動を尊重する

JIS Q 38500およびシステム管理基準では、先に述べたように、組織の経営陣のために効果的、効率的及び受入れ可能なIT利用に関する原則について規定しています。日本の組織では、“IT”と付くものはすぐにIT部門に回ってることが多いのですが、この規格や基準は、「経営陣にまずしっかり理解して実践して頂きたい原則と枠組み」を示しているのです。

2018年に改訂されたシステム管理基準には、ITガバナンスに関する管理策が多数盛り込まれました。システム監査人はシステムの戦略性や有効性の監査を行うに当たり、ITガバナンスの視点を良く理解し、活用していくことが肝要です。

FISCの各種基準の概要

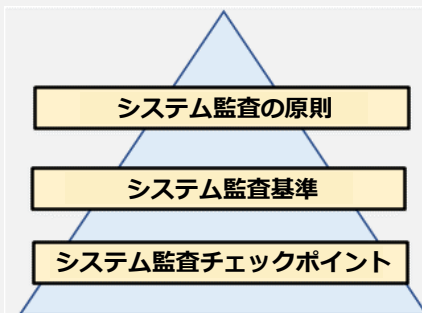
金融機関は、情報システムの活用が不可欠な業界であり、かつそのシステムが社会のインフラにもなっています。そのため、金融機関では、厳格なシステム監査が求められています。

こうした金融機関においてシステム監査を行う際の基準として用いられているのが、公益財団法人金融情報システムセンター（The Center for Financial Industry Information Systems：以下「FISC」という。）が策定した各種の基準です。

ここでは、FISCの基準のうち、「金融機関等のシステム監査基準」と「金融機関等コンピュータシステムの安全対策基準」について、ご紹介します。

「金融機関等のシステム監査基準」

システム監査人が監査を実施する際の「システム監査の原則」、監査人の行為規範である「システム監査基準（全般基準、実施基準、報告基準）」、対象領域ごとの主な着眼点である「システム監査チェックポイント」が示されています。



「金融機関等コンピュータシステムの安全対策基準」

金融機関等が実施する情報システムの安全対策の基準として、①統制基準、②実務基準、③設備基準、④監査基準の4つの基準に分類して、合わせて300余りの基準が示されています。

基準の適用においては、「重要な情報システム」には「高い安全対策基準」を、「それ以外の情報システム」には「必要最低限の安全対策基準」を適用するといったリスクベースアプローチの考え方が取り入れられています。

COBIT2019について

COBIT(Control Objectives for Information and related Technology)

COBITは情報システムコントロール協会（ISACA）が提唱し、初版は1996年にリリースされ、その後版を重ねて、現在はCOBIT2019となっています。その内容も「監査の基準」から「事業体I&Tガバナンス（EGIT：Enterprise Governance of Information and Technology）」に進展しています。

COBIT2019の特徴は次のようになります。

・“ガバナンス”と“マネジメント”のフレームワークは、組織のIT部門に限定せず事業全体が対象で、事業体 I&T ガバナンスを構築することにより、デジタル変革による価値創出の実現、リスク最適化、資源最適化が期待できる。

・ COBIT2019概念は、原則（ガバナンスシステム原則、ガバナンスフレームワーク原則）、ガバナンスおよびマネジメント目標、達成目標のカスケード、ガバナンスシステムのコンポーネント、フォーカス領域、デザインファクターで構成されている。

・ 「COBITコアモデル（ガバナンスとマネジメントの目的の参照モデル）」は体系化されており、ガバナンスには評価・方向付け・モニタリング(5)の目標、マネジメントには、計画（14）、構築（11）、運用（6）、モニタリング（4）の目標がある

・ CMMIベースのプロセス能力方式を採用し、各ガバナンス及びマネジメント目標のプロセスは能力レベル（0～5）で測り、重点領域のパフォーマンスは成熟度レベル（0～5）で測る。

これまで、COBITはIT統制の「**全社レベル統制**」と「**IT全般統制**」の業務方針を策定する上で有効な標準ガイドとなっています。また、現在の「**ニューノーマル**」、「**デジタル社会の到来**」等の状況下では、I&Tを活用した事業戦略が必至であり、I&Tガバナンスの構築、あるいはIT統制等々に、COBIT2019を多岐にわたって活用することで、組織の発展に役立てることが期待されています。

システム監査への期待の変化

～経営を支えるシステム監査～

システムの監査は、コンピュータが企業等の業務に活用されるようになった1970年ごろから出現しました。システム監査の定義の変遷から、社会がシステム監査に求めるものが見えてきます。

「システム監査とは、監査対象から独立した客観的な立場で、コンピュータを中心とする情報処理システムを総合的に点検・評価し、関係者に助言・勧告することをいい、その有効利用の促進と弊害の除去とを同時に追求して、システムの健全化をはかるものである。」

(1977年3月日本情報処理開発協会「システム監査体制確立への道」より)

「監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動」

(1996年1月システム監査基準より)

この年代では、システム監査は「情報処理システム」を点検・評価する活動が主です。しかし、情報技術・ネットワーク技術の高度化に伴い、情報システムの適用は社会システムの様々な分野に拡大し、それに伴い、システム監査への要求は拡大してきています。

「システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが、リスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行う活動である。」

(2004年10月システム監査基準「システム監査の目的」より)

2004年のシステム監査基準の解説では、「情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的」は、次のためとしています。

- ①組織体の経営方針及び戦略目標の実現に貢献するため
- ②組織体の目的を実現するよう安全、有効、効率的に機能するため
- ③内部又は外部に報告する情報の信頼性を保つように機能するため
- ④関連法令、契約又は内部規程等に準拠するようにするため

さて、2018年4月の改訂版のシステム監査基準で、システム監査の目的は次のように述べられています。

「システム監査は、情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする。」（2018年4月システム監査基準「システム監査の目的」より）

リスクに対する対処の視点はこれまでと変わりません。しかし「IT経営」時代を踏まえ、より経営的な視点が強調されています。

例えば、従来のシステム監査では、大規模プロジェクトを監査対象とした場合、工期や品質、費用対効果といった点を監査項目としていました。しかし、最近はこういった観点に加え、経営者の視点として、**このプロジェクトを実施しないときの経営リスクは何か、このシステムのビジネス戦略との整合性は適切か、プロジェクトの推進に当たっての利害関係者とのコミュニケーションに齟齬が無いか**といった点の検証が期待されます。

また、情報システムにかかわるリスクには、次のようなものが考えられます。

- ・システム構築の遅延、予算超過
- ・システム運用障害、障害による顧客サービス低下・停止
- ・システムへの不正アクセス、マルウェア被害、情報漏えい
- ・委託先における問題
- ・IT人材確保、人材育成の課題

システム監査にはこういったリスクに対する「コントロール」が有効かどうか、点検・評価することが期待できるのです。

経営者にはシステム監査を経営に活かすという知見が必要です。システム監査人はこういった期待に応えることが重要です。

リスクマネジメントは経営課題

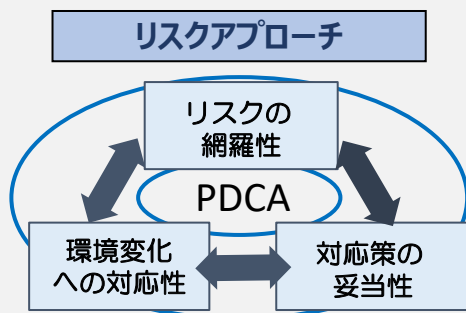
～リスクアプローチの勧め～

「システム管理基準」では、ITガバナンスに責任を持つ経営陣は、ITマネジメントプロセスを評価(Evaluate)し、指示(Direct)し、モニタ(Monitor)することとしています（「システム監査とITガバナンス」の項参照）。このEDMモデルの中で、経営陣がリスクについても評価・指示・モニタ、即ちリスクマネジメントすることが極めて重要といえます。

リスクマネジメントの実務においては、単に一般的な管理策のチェックリストを利用する「ベースラインアプローチ」ではなく、企業の実情および組織目的に合わせて実施する「リスクアプローチ」が有効といえます。

「リスクアプローチ」については、例えば、JIS Q 31000（リスクマネジメント－原則及び指針）などに手順が示されています。JIS Q 31000によれば、リスクマネジメントは、組織が経営目的を達成するために行う経営活動そのものだとしています。従って、リスクマネジメントは全社的で統一的な枠組みの中で運用すべきであり、そのためには経営者の強力かつ持続的なコミットメントが必要といえます。

リスクマネジメントの実践に当たっては、まず、組織および組織の状況の理解が必要です。企業によって置かれている内部・外部環境は異なっており、採るべき対応策の最適解も異なります。リスクアセスメントおよびリスク対応のプロセスを個々の企業に合わせて行うことにより、企業固有のリスクを見逃すことを防ぎ、“想定外”として発生するリスクをなくすることができます。



このプロセスを初めて実施する際には、「組織の置かれている状況の確定」を行います。この段階では解決すべき課題、業務の目的、目指すべき目標、外部の条件（法律、規制、ステークホルダーの要求など）、組織内部の条件（組織構成、役割と責任、経営資源、採用や準拠すべき規程やルールなど）を確認し特定します。

ここでは、情報システム部門での情報資産に対するリスクマネジメントを例に考えてみますが、初期段階では、業務プロセスフロー、情報資産台帳、システム構成図、ネットワーク構成図などの整備から始まり、相当な時間と工数を要します。しかし、本来どれも経営レベルの統治に必要なものであり、これらを利用したリスクの特定により、リスクマネジメントの“網羅性”が確保されます。

次に、リスクの分析・評価を行うとともに、それぞれのリスクに対して、プロセスや情報資産の重要度および脅威と脆弱性を考慮したリスク発生可能性に応じた、適切な対応策が採られることとなります。すべてのリスクに対して、完全に対応することは現実的ではありませんので、経営陣が積極的に関与し、対応策によるリスク軽減効果と対応コストとの関係などから優先順位や中・長期の方針を意思決定することが重要です。このように対処したリスクおよびその影響は“想定内”になり、外部からは企業のリスク対応の“妥当性”が評価され、経営陣としても説明責任を果たせることとなります。

「リスクアプローチ」ではシステム監査の助言なども踏まえ着実にPDCAサイクルを回し、常に外部・内部環境変化へ適切に対応していく“対応性”が求められます。その上でリスクマネジメントの目的・目標達成に向けて、“想定内”の範囲を拡大していく一貫性が重要です。また、リスクの発生を想定した訓練によって、対応策の有効性や課題を把握し、実践力の向上を図っていくことも有効です。訓練によって新たなリスク課題の発見に繋がる効果もあるのです。

情報セキュリティ監査

情報セキュリティ監査は、2003年4月の「情報セキュリティ監査制度(経済産業省)」開始に際し、「情報セキュリティ監査基準」「情報セキュリティ管理基準」という2つの基準が設けられたことにより、監査の分野として明確になりました。

「情報セキュリティ監査基準」では、情報セキュリティ監査の目的を「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うこと」と述べています。

リスクに対するコントロールの整備状況を独立かつ客観的に評価し保証または助言を行うという点は、システム監査と同じです。しかし、システム監査は組織のITガバナンス、ITマネジメントの視点で、経営層から情報システム部門、利用部門までを監査対象とするのに対して、情報セキュリティ監査では情報資産(物理的資産だけではなく、ソフトウェア資産や人的資産、サービスなども含む)を対象にリスクとコントロールをとらえます。情報資産が適切に管理・活用されているかどうかは、情報資産に対する機密性、完全性、可用性が確保されているかを確認することにより明らかになります。

コントロールの基準としては、「情報セキュリティ管理基準」を用いることが推奨されています。



初版の「情報セキュリティ管理基準」は経済産業省が2003年に、情報セキュリティマネジメントにおける管理策のための国際規格であるISO/IEC 17799:2000（JISX5080:2002）を基に、情報資産を保護するためのコントロールを規定するものとして策定しました。その後、ISO/IEC 27001:2005（ISMS要求事項）の発行およびISO/IEC 27001:2013の発行に伴い、2008年及び2016年に国際規格と整合を取る形で見直しが行われています。

また、「情報セキュリティサービス基準」（2018年2月28日、経済産業省）が公表され。これは、情報セキュリティに係るサービスが、一定の品質の維持向上が図られていることを第三者が客観的に判断し、公開することで、利用者が調達時に参照できるという制度です。この登録サービスの種類に「情報セキュリティ監査サービス」があります。監査サービスを行う企業や監査を受ける企業は必見です。さらに「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））（2020年1月30日サイバーセキュリティ戦略本部決定）」が運用されています。

パソコンやスマートフォンの普及、SNSやネットショッピングの利用拡大と共に、情報セキュリティ事件・事故は人々の身近になり、社会におけるセキュリティ対策への関心は急速に高まっています。さらに、インターネット空間のセキュリティについては、「サイバーセキュリティ」と呼び、2015年1月9日に「サイバーセキュリティ基本法」が施行、2018年12月5日に改正されており、国を挙げて情報セキュリティ対策に取り組む時代になりました。

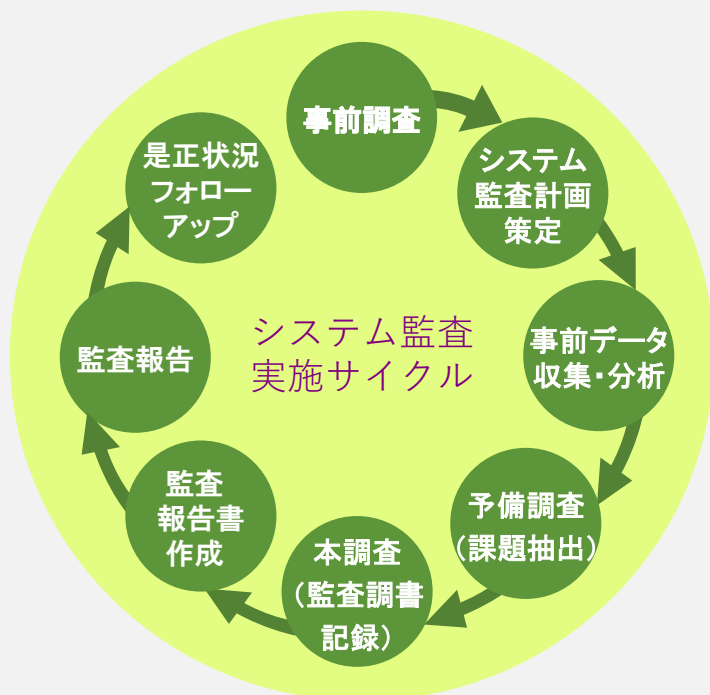
さらに現在は、コロナ禍を経験しての「ニューノーマル」、 「デジタル社会の到来」と認識されおり、デジタル庁創設による国全体のデジタル化主導、デジタル改革の推進、テレワーク/オンライン教育等の進展、厳しさを増す安全保障環境対応、SDGsへの貢献、等々の期待があります。このようなことから増々情報セキュリティ監査の役割は重要となっています。

システム監査人に求められる能力

システム監査人とは、その名のとおりシステム監査を実施する人です。では、システム監査人にはどのような能力が求められるのでしょうか。

システム監査の作業内容と必要な能力を見ていきましょう。

システム監査の作業内容は、以下の通りです。この業務を実施するシステム監査人には、システムと監査に関する専門的な知識が必要です。



さらに、基本的な能力として次の能力が求められます。

状況判断能力

システム監査のテーマ選定では、経営環境、トップの意向、自社のシステムリスク状況、社会環境等を勘案する必要がありますが、これらの要素を総合的に状況判断する能力が求められます。

リスク分析能力

システム監査では、リスク分析結果を監査テーマ選定に利用したり、監査対象にどのようなリスクがあるかを判断する力が求められます。

コミュニケーション能力

システム監査人は、経営トップ、監査役、被監査部門等と監査報告書や口頭にてコミュニケーションをとる必要がありますが、先方との確、簡潔、適時にコミュニケーションする能力が求められます。

業務関連法令に関する知識

システム監査においては、外部委託等において、民法、個人情報保護法、著作権法等業務に関連する法令知識が求められます。

そして、システム監査人が備えるべき重要な資質は、高い倫理性と言えます。SAAJではシステム監査人の倫理規定を定めています。

システム監査人倫理規定（抜粋） '02/2/25 日本システム監査人協会制定

- 第 2 条（使命）システム監査人は、情報システムの信頼性・安全性・効率性・有効性を高めるため、その専門的知識と経験に基づき誠実に業務を行い、情報化社会の健全な発展に寄与することを使命とする。
- 第 3 条（責務）システム監査人は、情報システムを総合的かつ客観的に点検・評価し、関係者に助言・勧告するものとする。
- 第 6 条（守秘義務）システム監査人は、正当な理由なく業務の遂行に伴い知り得た機密情報を他に漏洩し、または窃用してはならない。
- 第 7 条（独立性）システム監査人は、常に独立の立場を堅持しつつ、適切な注意と判断によって業務を遂行し、特定人の要求に迎合するようなことがあってはならない。
- 第 8 条（公正不偏）システム監査人は、業務を誠実に果たし、常に公正不偏の態度を保持しなければならない。
- 第 9 条（社会的信頼の保持）システム監査人は、自らの使命の重要性に鑑み、高い社会的信頼を保持するよう努めなければならない。
- 第 10 条（名誉と信義）システム監査人は、深い教養と高い品性の保持に努め、システム監査人としての名誉を重んじ、いやしくも信義にもとるような行為をしてはならない。
- 第 12 条（自己研鑽）システム監査人は、システム監査を行うのに必要な専門能力および監査技術の向上に努めなければならない。

システム監査人を目指すということ

～システム監査経験を通じ、

将来の能力発揮場面を拓く～

システム監査に取り組む皆さんに関する副次的な効用について考えてみます。

社会における情報システムの役割は大きく、システム監査のように情報システムの安全性、信頼性、効率性、有効性、正確性を点検・評価する必要性は増大し、システム監査人の活躍の場は益々増加するでしょう。類似した業務である業務監査、システム検査、個人情報保護の監査、各種審査、レビューなどの形態も含めると場面はもっと増えます。

ところが、情報システムなどを客観的に点検・評価することが出来る人材はまだ希少です。そこで皆さんのシステム監査実務経験は大変貴重で、努力次第では皆さんにはこのような業務の担い手として、あるいは将来第2の職場への転身など、活躍の場がたくさんでくるでしょう。とは言っても、システム監査人の能力は、ただ単に経験すれば良いというわけではなく、情報システムに関するさまざまな知識・技術などが要求されます。目安として、システム監査技術者試験で公表されているシステム監査人に求められる知識要件が参考になります。

情報処理試験制度 システム監査技術者試験「期待する技術水準」は独立行政法人情報処理推進機構（IPA）の以下の情報処理試験のページの「試験要綱」から参照できます。

http://www.jitec.ipa.go.jp/1_08gaiyou/_index_gaiyou.html

知識や能力を習得することは努力と苦勞も伴うことであり、習得に喜びを持つ人がいる一方、苦勞を歓迎しない人もいるかもしれません。しかしここで習得した知識、能力は、応用場面が多く、かつ新しい活躍の場を広げることに有効なのです。

システム監査は実学といわれ、机上の知識以上に経験が重要です。システム監査を実施できる機会があれば、将来を見据えて積極的に取り組み、人生設計の目標の一つに設定し、新しい活躍の場を拓いてください。

システム監査人の新たな活躍の場

～AIの世界とシステム監査～

(SAAJ会報216号より再編転載)

～最近注目されている分野も、システム監査人の新たな活躍の場になるでしょう

ICTの革新とインターネットの普及により、多くの機器がネットワークに接続されるIoT化が進展しています。これらの機器がビッグデータを産み出し、AI技術によるデータの利活用に繋がっています。

モビリティの分野では自動運転車の実用化が目前です。スマートシティ・スマートハウス分野でもエネルギー管理やIoT家電などにより、新たなライフスタイルが提案されています。さらに、ウェルネス分野では、健康志向の高まりもあり、様々な機器が出現し身近なものになっています。また、医療分野におけるビッグデータを活用したAIによる診断なども社会を変えることになるでしょう。

社会は早晚SFのような世界に突入するかも知れません。しかし、“古手のシステム監査人”の眼から見ると、たとえばAIが提供するサービスの保証、事故や障害に至るプロセスの解明といった視点で、監査項目や監査証跡はどのようなものになるのか、見当がつかないことも多くあります。

～これからのシステム監査人は未知の領域に踏み込む覚悟が必要でしょう

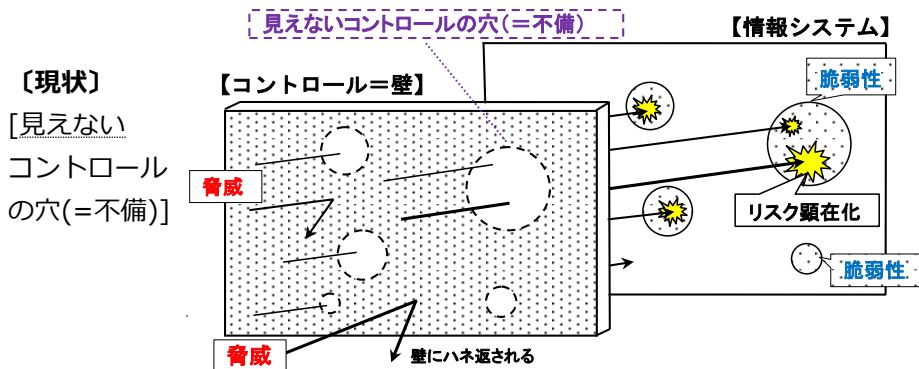
技術革新に対してシステム監査で何ができるのか、システム監査人はどうあるべきなのか、ここでは答えは出せません。しかし、AIが進化する中で、システムの品質は人命や社会にこれまでにない影響を与えかねず、システム監査の重要性、システム監査人への期待は増大の一途でしょう。新技術に対応するスキルがあれば、システム監査人の新たな活躍の場となります。

システム監査の役割と効果

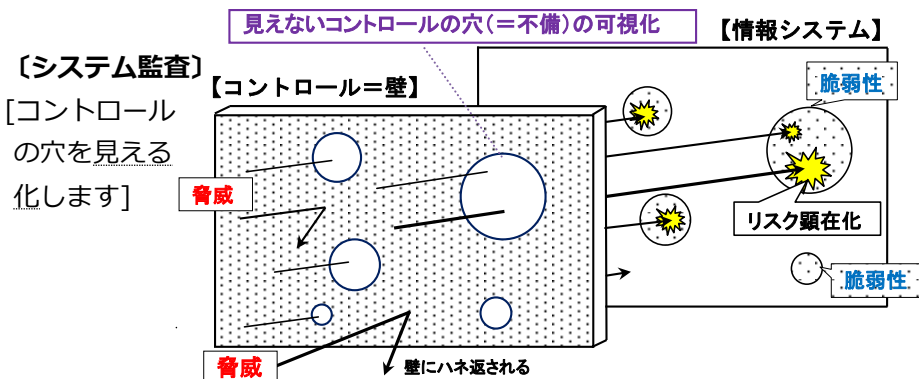
～（図解）システム監査～

～システム監査とはいわばコントロールの穴（＝不備）を見える化すること

情報システムリスクは、「脅威」（リスクの源泉）と、情報システムの「脆弱性」（リスクの発生を許す弱点）が結びつかなければ、顕在化しません。



脅威と脆弱性が会わないように、脅威を「コントロールの壁」で遮断することが大切です。システム監査はコントロールの見えない穴を見える化します。

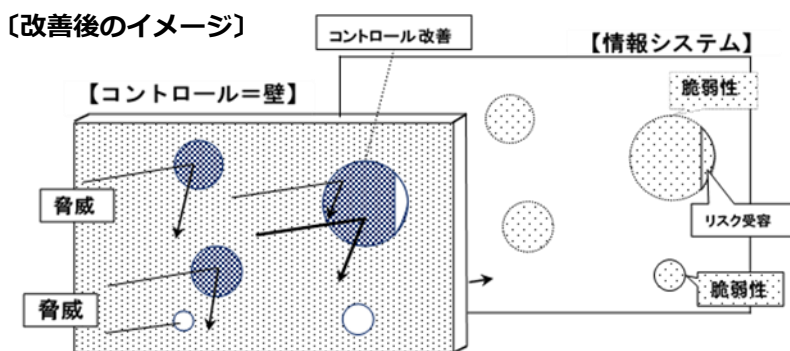


～システム監査人は発見したコントロールの穴を報告します

システム監査人は、

- (a) リスク評価（評価基準としてシステム管理基準などを用います）というフィルターを通して、
- (b) 情報システムにまつわるリスクを低減する管理策である「コントロール（の壁）」が、適切に整備・運用されているか点検・評価し、
- (c) コントロールに「不備（＝穴）」がないか検証（＝不足しているコントロールの問題点指摘）して、
- (d) 「コントロールの穴（＝不備）」の「見える化（＝可視化）」を行ない、
- (e) 監査報告書で、コントロールに関する指摘事項・改善提案を作成・提出します。

～監査で見える化した穴を被監査部門が改善により塞ぎます



システム監査の指摘事項・改善提案に基づき、不足しているコントロールを改善（リスク受容する箇所を除いて）することで、「コントロールの穴（＝不備）」を塞ぐことができます。

* システム監査の役割は、「情報システムの健康診断」に当たります。

情報システムリスクにおけるコントロールの不備対処への処方箋は示せますが、処方箋の薬を飲む（＝提案した改善案を実施する）のは、患者の方次第です。

システム監査の勘所

～チェックリストを超える柔軟さを身近な事例から

システム監査人は、既存の基準やチェックリストだけに頼ることなく、監査対象の状況、業務遂行形態・環境などによって、評価・判断尺度を自ら形成して監査します。このように説明すると、システム監査人はあらゆる知識と経験を兼ね備えた万能な人間かという、そうではありません。

身近なサーバの管理状況を例に、災害などによる停電対策を点検する場合で説明します。この場合UPS（無停電電源装置）のバッテリーの点検には、次のようなチェック項目が考えられます。

- ・バッテリーの日常点検は行われているか？
- ・バッテリーの交換時期管理は適切か？
- ・停電時の供給能力はサーバの安全停止に十分か？



この監査で特別な専門知識は必須ではありません。マイカーのバッテリー交換の経験を参考にしているのです。バッテリー上がりは急に発生することや定期的に交換しなければならない、という常識的な感覚を持つ柔軟性が監査では役立ちます。上記チェック項目3点もその常識から導き出せます。仮に『このバッテリーは高性能なので交換は不要だ』と説明されても、そんなことはあるのか、自動車にもそのようなバッテリーはあるのか、というように今度は逆にこだわって真偽を点検します。その上でマイカーとUPSの相違点を考えます。常識的な感覚をもとに時に柔軟に、時にこだわって確認します。

このような思考から意外なリスクが事前に発見されることも少なくありません。

～システム監査の視点で、経営に貢献する障害管理へ

システム障害管理はシステムの信頼性・安全性にかかわる基本であり、多くの方が経験している業務と思います。

例えば、障害を記録する「障害管理一覧表」のようなものがほとんどの組織にあると思います。この「表」の作成目的は何でしょう。対処漏れを防ぐためでしょうか、それとも社内報告用でしょうか。「何のため？」の質問に対してどのように説明しますか。

システム監査では、システムリスク管理に必須の「表」と即答します。障害が発生したことは残念ですが、**その障害を糧にリスク低減に取り組む**ための重要な「表」と位置付けています。それは、リスク低減に積極的に使うものだからです。

つまり、障害原因を分析・評価して、障害の再発防止と予防に役立つための「表」です。そのためには、分析・評価に役立つ「表」でなければなりません。そのポイントは、原因を二つの側面から究明しておく必要があります。それは、障害が起きてしまった原因と、それを防ぐことができなかった原因です。ここがシステムリスク管理の勘所になります。

具体的には、この「表」を定期的あるいは随時にシステム別、原因別、製造元別などで集計・分析して、その傾向により対策を実施することで。例えば、頻発した委託先や製品がある場合にはその対処をし、軽微な障害でも類似ケースで多発なら重度障害発生と同様に扱うなどです。このような分析と対策が「未来志向の障害管理」になります。

システム監査では、障害個々の現象よりも障害発生が防止できなかった仕組みや態勢をリスク管理の視点で分析し、今後実施しなければならない改善点を明らかにします。これにより、システム障害管理業務が、その日その日の対処に終始する**単なる失敗の後始末**などではなく、**経営に貢献する管理業務**となるのです。

システム監査と“学び”

～新技術のシステム監査にどう取り組むか～

システム監査人が日進月歩で変わる情報技術（IT）に関するシステム監査を行なうには、やはり、その技術に関する知識が必要です。システム監査人が新技術について学ぶのは大変ですが、2018年4月に改訂されたシステム管理基準にそのヒントがあります。

新しくなったシステム管理基準には、用語集があり、「情報システム」の概念が定義されました。これによれば、ITは、情報システムを構成する物質的人工物です。システム監査の対象は情報システムですが、それを構成する物質的人工物の技術そのものを監査するわけではありません。つまり、情報システムの構成要素として、その技術の特徴と情報システムでの使われ方、それを使うことのメリットとデメリットを最低限知っていればよいわけです。メリットはITガバナンスへの貢献、デメリットはリスクと捉えることができます。

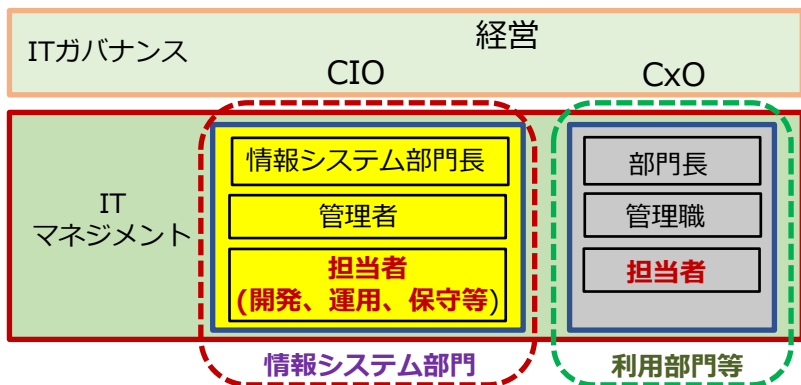
情報システム

組織体の活動を支えるデータ・情報の収集、蓄積、処理、伝達、利用に関わる仕組み・体系の総称である。情報通信技術、人間、制度・ルールなどで構成される。

考えてみれば、システム監査人は情報システムに関する全ての業務を経験しているわけではありません。過去の経験や知識をもとに予備調査を行い被監査部門の状況を知ると共に、その業務を理解します。その業務で新技術を使っても、この監査手続は同じはずです。

また、新しくなったシステム管理基準を読んで気づくのは、管理項目が<主旨>と<基準>に分かれ、何のために何をするかがとてもわかりやすくなったこと。その理由は、前文4.システム管理基準の前提となる組織構成にあります。ここでは、その組織体制を図で示しており、この図には、業務の担い手である担当者が明記されています。

ITガバナンスに基づくITマネジメントの中で、実際に管理項目の内容を実施するのは担当者ですから、実務としてそれを行なう人にわかりやすく書き直されたといえます。もし、あなたが担当者ならば、試しにご自分の業務に関する管理項目を読んでみてください。これは実施している・していない、とチェックできるのではありませんか？



担当者の皆さんは、特に、情報システム部門の担当者（開発、運用、保守等）は、新技術を踏まえ、業務を遂行しています。それは、新技術に合わせて管理項目を使いこなしているのと同じこと。そう考えたとき、システム監査人が新技術を学ぶのと、実務として新技術を使っていた人がシステム監査の知識を学ぶのと、二つの道が見えてきます。

しかし、新技術は次々と出てきますから、どちらの道も学び続けることに変わりはありません。では、どうやって学んだらよいのでしょうか？ SAAJの「月例研究会」や「CSAフォーラム」では、新技術に関する第一人者の方を講師としてお招きしています。単に技術概要だけでなく、システム監査の視点などからもお話をお願いしており、講師の方に質問することもできます。書籍やウェブ上の情報とは違った学びの場があります。また、業務経験を活かしシステム監査人になろうという方には、「事例研究会」の「システム監査実務セミナー」などがあります。

私たちと一緒に学びませんか。

システム監査人の体験から

～外部委託管理の監査では、
委託元・委託先双方に対する調査が必要～

～以下はSAAJの公認システム監査人（CSA）が、実際に体験した、システム監査事例の紹介です。

業務システムの開発を外部委託している企業（委託元）から、委託先が行っている開発および開発管理の信頼性について調査して欲しいという依頼がありました。

委託元は、本来、自ら、委託先の開発プロセス・開発管理における信頼性、契約書に従った業務遂行の適切性を確認する必要がありますが、この委託元では、人的パワーや調査スキルが不足している状況から自ら調査を実施することがむずかしいので、システム監査人である私に調査を行って欲しいという依頼でした。また、委託元には、外部の専門家から問題点を指摘してもらうことで、委託先がより真摯に開発及び開発管理に取り組むだろうという期待もありました。

勿論、委託元と委託先の間で、調査権（というと高圧的になるので、委託先の業務執行状況を現地で確認するという程度の表現で）について合意いただいた上で調査を行いました。

なお、この事例では、委託元と委託先はグループ会社であり、グループ内での位置付け的には委託元が上位の立場になるという関係でした。

以上の状況で監査を実施しました。監査目的は「委託先における開発および開発管理業務の信頼性の確認」、監査対象は委託先の開発プロジェクト、監査テーマは「開発および開発管理手順の妥当性」、「開発における要員管理・文書管理の適切性」、「開発に係る委託元との契約履行の順守性」に置きました。監査テーマを監査チェック項目に落とし込み、委託先に対するヒアリング、現場確認、関連文書類の入手と閲覧などの手続きで調査を進めました。

委託先に対する調査を進めるうちに、委託元と委託先とのコミュニケーションがほぼ皆無であることが分かってきました。委託先は自分たちのやり方で開発・開発管理を進めており、委託元への報告は、月次の形式的な進捗報告だけでした。また、委託元は委託先からの進捗報告に対する確認をほとんど行っていない状況でした。表現はよくありませんが、委託元の「丸投げ」、委託先の「丸受け」に近い状態でした。

そこで、私は、当初の監査計画にはありませんでしたが、委託元の責任者に話をし、委託元の現場に対するヒアリングを実施することにしました。委託元の現場では、当初、自分たちが監査ヒアリング対象と想定していませんでしたが、私は、委託元・委託先双方がそれぞれの役割を果たすことで、はじめて外部委託が成功するという説明を行い、委託元の責任者にご理解をいただきました。

結果として、

- ・委託元は委託先が行っている業務（委託元の業務システムを開発している）に対する確認が弱い
- ・委託先は、委託元に対する報告が不十分である
- ・一言で言うと、委託元と委託先とのコミュニケーションが機能していない

という監査意見、及び具体的な改善指摘を行いました。

委託元の当初の意図とは違う形にはなりましたが、報告後には、委託元の責任者の方からも、大事なことを気づかせてもらった、という声をいただきました。

事例を通して再認識した、外部委託管理の監査で留意すべきこと

- ・外部委託管理の監査では、委託元、委託先の双方に対して調査が必要である。
- ・外部委託で問題があれば、委託元、委託先双方に問題があると考えた方がよい。
- ・外部委託は、委託元、委託先双方が基本的行動をとることから始まることを、双方に理解してもらうという観点での改善指摘が重要である。

成功に導くプロジェクト監査

～システム開発成功の鍵～

■ **決め台詞** 人気医療ドラマの決め台詞「私 失敗しないので！」
自信たっぷりのその根拠は《卓越した技術とあらゆることを想定した周到な準備》でした。ではシステム開発ではどうでしょう…

■ 失敗しないシステム開発の鍵

《卓越した技術と周到な準備》と《プロジェクトマネジメント》が鍵です。そのポイントは次の6点です。

(1)	PM	全員のベクトルを合わせ一丸にする（最重要ミッション）
(2)	体制	業務を熟知した設計者を揃え、経営陣も参画する
(3)	計画	成功に導く「プロジェクト計画」を緻密に立てる
(4)	仕様	外部仕様を早期確定する（確定遅延は大トラブルに直結）
(5)	品質	レビューを徹底し、高品質を作り込む（特に設計品質）
(6)	リスク	重要リスク3つを確実にコントロールする（早期発見/早期対処の仕組みが廻れば他のリスクにも対処できる）

■ しかし！ しっかりマネジメントしても「大トラブル」に！

そのような悲惨な例が沢山あります。巨大な基幹システム開発でも、継続的に機能追加してきた安定したシステムでも大トラブルが起きて、数十億、数百億の損害が出たりします。

■ どうするか？

『成功に導くプロジェクト監査』を受ける



これが、開発を成功させる肝です。

開発の当事者は「渦」の中にいます。プロジェクトのことは誰より熟知して、最大限の努力をしています。でも直近の課題に目が行きがちで、大きな抜けが出ます。周りから正しい情報が上って来ないこともあります。利害関係があるからです。そうすると責任者は誤った判断を下し、トラブルが拡大します。

でも、監査人は、渦の外から、大所高所から冷静に見るので、トラ

ブルの本質や抜本的な解決策が見えます。開発の真の目的は何だったか？何が一番重要か？など根本に立ち戻って見るので、本質が見えるのです。

■専門の監査人は……

沢山のプロジェクトを見て来ているので、「この先こうなる」がはっきり見えます。例えば「外部設計は後2ヶ月では終わらない、あと半年かかる」とか「設計品質が悪いので試験工程で大トラブルになる」などです。

監査人は、監査結果を所見にまとめ、抜本改善の助言もします。監査所見に真摯に向き合って改善すれば、プロジェクトを成功させることができます。

■プロジェクト監査の基本

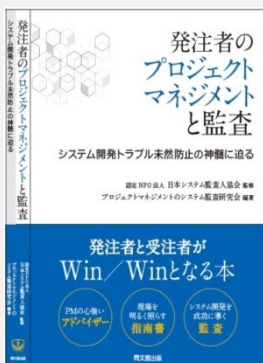
「早め早めの監査で是正する」これが基本です。

プロジェクト企画計画時、外部仕様設計時、試験計画時などに監査を受けて、問題に抜本対策すれば、成功させることができます。

作業終わり頃の監査は、「問題が無いことの確認」です。工程毎の終了判定事前監査、リリース判定の事前監査などがそれです。これらの監査で、経営者や責任者の判断やマネジメントを支援します。

■2冊の実践的なガイドライン本

プロジェクト監査研究会では、開発を成功に導く2冊の本を上梓しました。具体的なトラブル事例で根本問題を解説しています。また、プロジェクトマネジメントと監査について、工程毎に詳しく説明し、詳細な点検項目を満載しています。Excel版でも提供しています。開発や監査の現場で直ぐに活用できます。ぜひご活用下さい。



(2018年3月 同文館出版)



(2020年7月 同文館出版)

<https://www.saaj.or.jp/shuppan/index.html> (注文書 2割引き)

効果的かつ安心してクラウドサービスを利用 するためのシステム監査 ～第三者評価も活用したシステム監査の実践～

クラウドコンピューティングサービスの利用は、利用者にとって、ITコストの削減だけでなく、データ管理、さらには業務改革にも効果があるということで、広く普及しつつあります。また昨今では、より迅速なシステム対応が必要となるDX推進において、システムリリースまでの対応期間短縮を目的とした活用も広がりつつあります。

一方で、クラウドサービスを利用するということは、重要な業務データをインターネット経由でクラウドサービス事業者のサーバとやりとりすることになります。そのため、データ送信上及びクラウドサービス事業者のサーバ上でのデータ管理における安全性が確保されていなければ、利用者は安心してクラウドサービスを利用できないという問題を抱えています。

クラウドサービス事業者はビジネスとしてクラウド事業を行っているわけで、上記の問題に対して万全な安全対策を講じていることを利用者との契約書で謳っており、利用者はそれを信用するしかないのが実情で、そのため、不安を抱く利用者が多いことも事実です。

これらの不安を解消すると同時に、利用者側に課せられる外部委託先管理に関する説明責任を果たすための手段としてシステム監査を活用することが有効です。実際のシステム監査の実施方法については、次頁にあるガイドライン等を活用し、システム監査人が直接クラウドサービス事業者を監査する方法の他、第三者評価の仕組みも活用した監査を実施する方法もあります。いずれの方法においても、システム監査を実施することで、一定程度信頼

してよい安全対策（内部統制）と、必ずしもクラウドサービス事業者任せられない安全対策が具体的に認識できるようになり、利用者としてどのような活用ができるか、どこまで活用してよいかという判断をする上での有効な情報を得ることができるようになります。

なお、現時点で比較的活用が容易なクラウドサービスに関する第三者評価の制度には、ISMS、CSゴールド認定、SOC2保証報告書その他、2020年より開始された国が定めるセキュリティ評価制度としては我が国初となる「政府情報システムのためのセキュリティ評価制度（ISMAP）」等があります。

クラウドセキュリティに関する規格、ガイド、基準など

規格、ガイド、基準などの名称	発行・公表機関	状況・備考 (2021/10現在)
ISO/IEC 27017	ISO/IEC	ISO/IEC 27001のクラウド対応版、2015年発行
ISMAP管理策基準	ISMAP運営委員会	2020年6月発行
<ul style="list-style-type: none"> クラウド情報セキュリティ管理基準 クラウド情報セキュリティ管理基準利用ガイド クラウドサービス（IaaS）の技術的評価ガイド 	日本セキュリティ監査協会－クラウドセキュリティ推進協議会	<ul style="list-style-type: none"> クラウド情報セキュリティ管理基準2013年度改訂版（2014年9月発行） ガイド：2014年8月発行 評価ガイド：2016年3月発行
クラウド・セキュリティ・ガイドランス (*CSA:クラウドセキュリティアライアンス)	国際団体 CSA(*)	ガイダンス V4.0 日本語V1.1版 (2018年7月24日発行)
<ul style="list-style-type: none"> ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項 ISMSユーザーズガイド追補～クラウドを含む新たなリスクへの対応～ 	一般社団法人情報マネジメントシステム認定センター（略称：ISMS-AC）	<ul style="list-style-type: none"> 2016年8月1日発行 2018年3月30日発行

ISMAP制度

～政府情報システムのための セキュリティ評価制度～

2018年6月に、政府情報システムは、「クラウド・バイ・デフォルト原則」、すなわち、クラウドサービスの利用を第一候補として、その検討を行うものとするの方針が発表されました。各府省はこれらを踏まえ、民間クラウドサービスを含め、クラウド技術の積極的な活用を図り、また、国が直接保有・管理する必要がある政府情報システムについては、標準化・共通化を図るとともに、投資対効果の検証を徹底した上で、政府共通プラットフォームへの移行を推進してきています。

この際、大きな課題の1つとして、クラウドサービスの安全性をどう評価・担保していくのかというものがあり、クラウドサービスの統一的な安全性評価の必要性が認識されました。これを受けて同年、「クラウドサービスの安全性評価に関する検討会」が立ち上げられ、約2年の検討・協議の後、2020年6月に「政府情報システムのためのセキュリティ評価制度（通称：ISMAP）」が発表されました。

「ISMAP制度とは」

ISMAP制度を一言で言えば、『国が定めた基準への対応状況をクラウド事業者自身が言明し第三者の評価を受け、その言明内容をISMAP運営委員会が審査のうえ、政府が求めるセキュリティ要求水準を満たしていると判定されたクラウドサービスが「ISMAPクラウドサービスリスト」に登録され、サービス名が公表される。各政府機関（2021年10月時点では中央省庁のみが対象）は原則としてこのISMAPクラウドサービスリストに登録されているクラウドサービス事業者の中から入札先を選定する』という制度です。

したがって、今後政府関連の入札に参加しようとするクラウドサービス事業者にとっては、必須の対応になります。実際の

影響という点では、それに限りません。本制度においては、審査を通過したクラウドサービス事業者については、対象サービスと共に、言明内容が公表されます。この情報は政府機関に限らず広く閲覧することが可能であるため、例えば民間企業が、利用しようとして検討しているサービスが当該リストに掲載されているか否か、掲載されている場合はどのようなセキュリティ対策を実施しているのかについての情報がある程度までは得ることができるため、民間を含め、広くクラウドサービスに関するセキュリティ状況の確認に活用されることが想定されています。

「監査機関による第三者評価」

本制度の特徴の1つとして、言明書に記載された内容については、監査機関による情報セキュリティ監査を受けたうえで、その監査結果（実施結果報告書）を添えてリスト登録の申請を行う必要があります。

この監査機関についても、あらかじめ要件を充足した法人（現時点では個人は不可）が制度に申請の上、監査機関としての認定を受けることが必要となっており、2021年12月時点では5法人が登録されています。特にその中心となる「**業務執行責任者**」および「**業務実施責任者**」については、累積で10年以上の外部監査経験を有すること、特定の情報システム・セキュリティ監査に関する資格（2021年10月時点では、**公認システム監査人**、公認情報セキュリティ監査人、公認情報システム監査人、システム監査技術者の4資格のいずれか）を有すること等、非常に厳しい条件が課されており、一定水準以上の知見・スキルを保有する監査人が確認をしているという点で、言明内容の正当性を担保する仕組みとなっています。

なお本制度で利用される評価基準（ISMAP管理策基準）や制度運営に関する各種規則については、ISMAPポータルサイトから確認することができます。

ISMAPポータルサイト <https://www.ismap.go.jp/csm>

IT統制監査

～財務報告に係る内部統制の 評価及び監査の基準とIT統制監査～

上場会社については、金融商品取引法に基づき、財務報告に係る内部統制の経営者による評価と公認会計士等による監査が義務づけられています（内部統制報告制度）。



内部統制の目的は、①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全の4つです。内部統制は、それらの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいいます。内部統制の基本的要素として、①統制環境、②リスクの評価と対応、③統制活動、④情報と伝達、⑤モニタリング（監視活動）の5つの要素に並んで、⑥IT（情報技術）への対応があげられています。

「ITへの対応」

ITへの対応とは、組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のITに対し適切に対応することをいいます。

ITへの対応は、他の基本的要素と必ずしも独立に存在するものではありませんが、組織の業務内容がITに大きく依存している場合等には、内部統制の目的を達成するために不可欠の要素として、内部統制の有効性に係る判断の規準となります。ITへの対応は、①IT環境への対応と②ITの利用及び統制からなります。

「IT環境への対応」

IT環境とは、組織が活動する上で必然的に関わる内外のITの利用状況のことであり、社会及び市場におけるITの浸透度、組織が行う取引等におけるITの利用状況、及び組織が選択的に依拠している一連の情報システムの状況等をいいます。

IT環境に対しては、組織目標を達成するために、組織の管理及び範囲において予め適切な方針と手続を定め、それを踏まえた適切な対応を行う必要があります。

「ITの利用及び統制」

ITの利用とは、組織内において、内部統制の他の基本的要素の有効性を確保するためにITを有効かつ効率的に利用することであり、いわばITによる統制です。ITの統制とは、組織内において業務に体系的に組み込まれてさまざまな形で利用されているITに対して、組織目標を達成するために、予め適切な方針及び手続を定め、内部統制の他の基本的要素をより有効に機能させることです。

SAAJ監修「J-SOX対応IT統制監査実践マニュアル」

本書は、「IT統制」に関する理解を深めるとともに、内部統制報告制度に必要な「IT統制」を中心に解説し、またIT統制に関する監査（IT統制監査）の進め方や手法を紹介し、IT統制監査に役立ててもらうことを目的としています。

本書では、本文に出てくる様式、各様式の記述作成例、監査・評価ポイントをCDに収めて提供しているので、IT統制に関する監査計画書、監査チェックリスト、監査報告書などを効率的に作成することができます。



「IT統制監査実践マニュアル」（森北出版）

<https://www.saaaj.or.jp/shuppan/index.html>

官民一体化！2021個人情報保護法

～GDPR十分性認定の法的根拠～

2021年5月19日「デジタル社会の形成を図るための関係法律の整備に関する法律」(法律第37号)第50条、第51条により「個人情報の保護に関する法律」が改正されました(以下保護法2021と呼ぶ)。国の行政機関、独立行政法人、地方公共団体、地方独立行政法人(以下機関と呼ぶ)について、全体を内閣統一下の組織とみなし、民間を対象としていた「個人情報保護法」(2020年6月12日法律第44号)をベースに一本化するとともに、所管が個人情報保護委員会に一元化されることになりました。

従来の「個人情報保護法」の用語である「個人情報」「個人識別符号」「要配慮個人情報」「仮名加工情報」「匿名加工情報」及び「個人関連情報」は引き継がれ、行政機関個人情報保護法で使用されていた「行政機関」「行政機関の長」「保有個人情報」「個人情報ファイル」「行政機関等匿名加工情報」及び「行政機関等匿名加工情報ファイル」についても「保護法2021」において用語の解釈運用を踏襲しています。

「保護法2021」の成立の背景としては、EU「一般データ保護規則(GDPR: General Data Protection Regulation)」が2018年5月に適用され、日本が、2019年1月23日にEUからの十分性認定を取得し、これにより官民を含めた法的根拠を、国際的に示すことが必要になったことにあります。これにより「保護法2021」では、例えば外国にある第三者への提供の制限について、第28条(民間)、第71条(機関)にそれぞれ規定され、いずれも、“あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。”と、GDPRの規則に沿うことになりました。

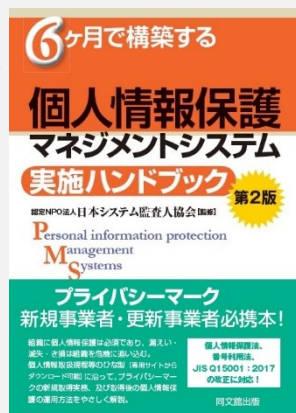
※ 民間の個人情報取扱事業者等の義務については、条文番号が変わったことに注意する必要がありますが、従来の保護法と大きく変わりはありません。

GDPR第25条に「Data protection by design and by default」が明記されています。いわゆる「プライバシー・バイデザイン」のことで、プライバシー侵害が発生する前にそれを予防するため、システム内に最初から安全管理措置を組み込むことを第一義とすることとしています。このキーワード自体は「保護法2021」に規定されてはいませんが、呼応する安全管理措置として、第23条(民間)、第46条(匿名加工情報)、第66条(機関)を規定し、さらに個人情報保護法ガイドライン通則編には、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、及び情報システムを使用する場合の技術的安全管理措置について、具体的な手法を例示しています。

EUから日本への「GDPR十分性認定」の根拠の一つである「プライバシーマーク制度」は「JIS Q 15001:2017個人情報保護マネジメントシステム(PMS) 要求事項」の適格性を認証するものですが、「保護法2021」はこの「JIS Q 15001:2017」の附属書Aに非常に近い内容となりました。「プライバシーマーク」認証取得事業者は、引き続き法令順守を維持できるものとなっています。

個人情報保護監査研究会では2019年7月に「6か月で構築する『個人情報保護マネジメントシステムハンドブック』第2版(同文館出版)を刊行しました。購入者にはPMS構築に不可欠な規程類や様式(約85文書)のダウンロードを提供し、法令等の改正にあわせて随時更新するとともに、購読者向けの監査サービスも実施しています。

<https://www.saa-j.or.jp/shibu/Kojin/kojin.html>



産業用オートメーションのセキュリティ対策

～社会・産業基盤を支える制御システムが狙われる～

産業用オートメーションは、社会・産業基盤で重要な役割を担っています。電力・ガス・石油等のエネルギー分野や、鉄鋼・化学等のプラント、鉄道・航空等の交通インフラ、電機・機械・食品等の生産ライン、商業施設・オフィスの設備管理などに欠かせないものです。

このような産業用オートメーションでは、制御システムなどに数多くのコンピュータが使われています。従来、これらのシステムは独自仕様のもので多く、セキュリティリスクは小さいと考えられていました。しかし、近年ではIT技術の進展でシステムのオープン化が進み、一般的な情報システムと同じようにサイバー攻撃の脅威に晒されています。

ところが産業用オートメーションの運用環境を見ると、セキュリティへの問題意識が低く、対策がとて遅れているのが現実です。システムの特異性から、ウイルス対策ソフトやセキュリティパッチの適用ができないケースも少なくありません。ランサムウェア等のサイバー攻撃が、大規模かつ広範囲に影響するリスクをはらんでいるのです。

サイバー攻撃から重要インフラを守るのは国家レベルの対策が必要とのことから、2014年11月6日に「サイバーセキュリティ基本法」が衆議院で可決・成立しました。同法第14条には、「重要インフラ事業者等におけるサイバーセキュリティの確保の促進」という規定があり、重要インフラ事業者等に当たる企業は、積極的なサイバーセキュリティ対策が求められています。重要インフラ事業者等に関係する事業者も準じた対応が必要となるでしょう。

こうした中、日本では2014年、世界に先駆けてCSMS*認証制度が始まりました。CSMSは、IEC 62443-2-1の規格番号で示される国際標準であり、規格にはIACS**に対するセキュリティマネジメントの要求事項を定めています。認証制度を運用しているISMS-AC***は、認証のメリットを「CSMSの構築・運用を通じて、企業内のリスクマネジメントに対する理解が進むとともに、セキュリティに対する目的意識の高い取組みが期待でき、CSMSに基づくセキュリティ対策を実施することで、サイバー攻撃に対するリスクを低減することができる。」としています。

今後、CSMSを構築・維持・改善するためのセキュリティ監査を、広く産業分野へ浸透させる必要があります。さらに言えば、IACSに対するガバナンスや事業リスクのコントロールを検証・評価する、「システム監査」が重要になるのです。産業用オートメーションのリスク低減にシステム監査を活用することが、社会・産業基盤の高い安定性と信頼性の確保につながるはずです。

*CSMS (Cyber Security Management System,
サイバーセキュリティマネジメントシステム)

**IACS (Industrial Automation and Control System,
産業用オートメーション及び制御システム)

***ISMS-AC (一般社団法人情報マネジメントシステム認定センター、
2018年4月JIPDECから独立)



日本が世界初としてスタートしたCSMS認証

CSMS認証は、CSMS (IEC 62443-2-1) に基づいた第三者認証制度。情報セキュリティマネジメントシステムであるISMS適合性評価制度を運営するJIPDEC (一般財団法人日本情報経済社会推進協会) により、CSMS適合性評価制度として2014年にスタート。経済産業省が国際的に通用する認証基盤の確立のために実施した、「グローバル認証基盤整備事業」の一環。

注) 現在CSMS認証制度は、ISMS-ACが運営

国のDX提言と推進施策

～DX監査の可能性～

～2018年9月、経済産業省が「DXレポート」を発表

DXは、デジタルトランスフォーメーションの略で、「デジタル技術を駆使して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でしょう。

レポートでは、「DXで大きな成果を出すためには、AIやIoTを活用してだけでなく、足元の既存システムをしっかりとさせなければいけない」、「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、効果も限定的になってしまう」と述べています。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」との問題指摘もあります。

レポートでは「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、単に技術の陳腐化だけではなく、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いること、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を挙げています。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のでしょうか。

～「2025年の崖」

経済産業省は、このままの状況が放置されると、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して試算し、これを「2025年の崖」と名付けています。そして、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ています。

～「DX推進指標」と「デジタルガバナンスコード」

経済産業省ではさらにいくつかのDX推進政策を行っています。「DX推進指標」は企業が自社のDX推進状況を自己認識し、必要なアクションにつなげていくことを目的としたものです。これは、現在の日本企業が直面している課題やそれを解決するために押さえるべき事項を中心に「DX推進のための経営のあり方、仕組みに関する指標」と「DXを実現する上で基盤となるITシステムの構築に関する指標」に関する定性指標から構成されています。企業が自己診断した結果は、IPAが収集し、分析していますが、まだ日本国内の企業のほとんどが「未着手～一部部門の実施」に留まっていることがわかってきています。

また「デジタルガバナンスコード」というものも整理されました。これは、出資者等のステークホルダーに対し、企業が自らのDX推進状況を開示し、そのポテンシャルを理解してもらうためのものです。ちょうどコーポレートガバナンスコードのデジタル版だと考えて下さい。コーポレートガバナンスコードは、①経営ビジョン・ビジネスモデル、②戦略（「組織づくり・人材・企業文化に関する方策」と「ITシステム・デジタル技術活用環境の整備に関する方策」）、③成果と重要な成果指標、④ガバナンスシステムの4つの要素から構成されています。デジタルガバナンスコードに則った行動を行っていて、DX推進の準備が十分にできている（DX-Ready）企業を認定する「DX認定制度」も始まっています。さらに、上場企業全体から特に優秀なデジタル活用の実績が表れている企業を「DX銘柄」として選定することも、経済産業省と東京証券取引所の共同で定期的に行われています。

～「DX監査」の可能性

システム監査基準には、システム監査の目的として「組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること」ということが示されています。この観点から見れば、企業のDX推進状況が健全かつ有効に行われているかを客観的に評価し助言する、いわば「DX監査」もシステム監査のテーマの一つと考えられます。

テレワークを監査する

～どのような視点で監査するか～

新型コロナウイルス感染症の感染拡大防止のため、テレワークを採用する組織が増えています。テレワークには、在宅勤務、モバイルワーク、サテライトオフィス勤務などがありますが、「afterコロナ」でもテレワークが定着し、ニューノーマル時代への移行が言われています。このような、テレワークを対象とした監査の視点を考えてみます。

監査の視点としては①組織のルールや体制整備の状況②人事・労務管理方式③情報インフラの整備状況④教育・コミュニケーションの状況⑤情報セキュリティ対策状況などが考えられます。

テレワークセキュリティガイドライン（総務省発行）

ガイドラインの中に組織の立場に応じた重要な役割が「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」それぞれについて述べられており、監査視点の参考になりますので、抜粋します。

（経営者）

- テレワークセキュリティに関する脅威と事業影響リスクの認識
- テレワークに対応したセキュリティポリシーの策定
- テレワークにおける組織的なセキュリティ管理体制の構築
- サプライチェーン全体での対策状況の把握

（システム・セキュリティ管理者）

- 情報セキュリティ関連規程やセキュリティ対策の見直し
- テレワークで使用するハードウェア・ソフトウェア等の適切な管理
- テレワーク勤務者に対するセキュリティ研修の実施

（テレワーク勤務者）

- 情報セキュリティ関連規程の遵守
- テレワーク端末の適切な管理
- 認証情報（パスワード・ICカード等）の適切な管理
- 適切なテレワーク環境の確保
- セキュリティインシデント発生時の速やかな報告

リモート監査

～監査品質の確保のために～

ニューノーマル時代を迎え、監査業務もリモート化されつつあります。リモート監査には移動日数の減少により、コスト低減や監査の頻度を上げたり、多人数の参加が可能になるなどの利点がある一方、本監査での対面による被監査側への質問や現物の証憑を確認できず、情報機器による閲覧を主とした監査とせざるをえないといったデメリットもあります。

リモート監査に当たり

このことから、監査品質を確保・向上させるために予備調査の段階から、所与の監査目的の達成に必要な証跡が存在するのかを細かく把握することが監査側に求められます。

また、被監査側への質問および観察は、オンライン会議システムを利用することで代替することになりますので、監査側は対面による質問および観察との相違点（微妙な表情の変化がわかりにくい等）があることを認識しておかなくてはなりません。

監査側の対応と工夫

予備調査においては、監査側から問い合わせのあった証跡の有無を被監査側が確認するにあたり、被監査側の対応者は多くの担当者に問い合わせなくてはならないが、被監査側もテレワークのためにすぐに回答できず、回答を得るまでに相当な時間を要することもあるため、予備調査であっても期間に余裕が必要となります。

また、紙の証跡は、すべて判読可能な程度の大きさにスキャナ等で電子化して社内の共有フォルダ等に保存し、リモートで確認できる環境が必要です。

リモート監査の課題

さらに、リモート監査の質の向上や負荷の低減のためには、組織のデジタル化の推進が必須となります。リモートワークに対応したIT内部統制の再編成や業務のペーパーレス化、電子署名・タイムスタンプ等の利用を促進する必要があります。

SAAJのこれからの取り組み

～IT経営の推進に取り組むすべての方への メッセージ～

SAAJはシステム監査の普及啓発を目的として、システム監査技術者試験合格者の集まりが母体となって、1987年12月に発足しました。2002年に特定非営利活動法人（NPO法人）の認証をいただき、2015年6月には東京都の審査を経て、認定NPO法人に認められました。一方、2002年には「公認システム監査人」認定制度を立ち上げ、現在多数の公認システム監査人・システム監査人補を認定し、活躍いただいています。

システム監査がターゲットとするITの変革には目覚ましいものがあります。それにつれ、ITを取り巻く環境や社会的要請は大きく変化してきました。その変化は、次の4つの側面で整理することができます。

◎ 社会環境の変化：

DX、Society 5.0、キャッシュレス決済、暗号資産、働き方改革、ニューノーマル、マイナンバーカードの利用拡大 など

◎ IT特にWebを活用したビジネスモデルの普及：

クラウドファースト、モバイルファースト、インターネットバンキングやネット取引、広範囲なサプライチェーン など

◎ サイバー攻撃の高度化：

標的型攻撃、ランサムウェア、Webサービスからの機密情報搾取など、ますます高度化するサイバー攻撃 など

◎ 情報技術革新：

スマートフォンやタブレットなどモバイル端末の進歩と普及、SNS、IoT、AI、ビッグデータ、RPA、ブロックチェーン など

そこでSAAJでは、システム監査を核にしつつ、“ITアセスメント”を提唱し、ITサービスの提供者と利用者双方における適切な統制を維持・向上させる、以下の活動をこれからも進めて参ります。

- ・ IT構築、運用及び利活用などの評価、助言、コンサルティング
- ・ ITガバナンス、内部統制などの経営者や管理者への評価、助言
- ・ ITに関する各種監査の支援；システム監査、情報セキュリティ監査、各種制度に基づく監査、マネジメントシステムの監査など

認定NPO法人日本システム監査人協会（SAAJ）の概要

設立目的：「システム監査」の普及啓発

- システム監査技術者試験合格者の集まりが母体となり、
1987年12月設立
- 2002年に特定非営利活動法人（NPO法人）化
- 2002年に「公認システム監査人」認定制度を立上げ、
延べ1,200人以上の公認システム監査人（CSA）、システム監査人補（ASA）を認定
- 2015年に東京都認定特定非営利活動法人（認定NPO法人）化

主な部会・研究会

- ITアセスメント研究会：システム監査基準、システム管理基準についての研究部会、基準類のISO化、JIS化活動
- 月例研運営委員会：システム監査に関連するホットなテーマをとりあげ、専門講師による年10回ほどのセミナーを実施
- システム監査事例研究会：システム監査普及サービス及び実務・実践セミナーを実施
- 情報セキュリティ監査研究会：情報セキュリティについての研究部会
- 個人情報保護監査研究会：個人情報保護マネジメントシステム（PMS）の研究部会
- プロジェクト監査研究会：失敗しないプロジェクトのためのシステム監査等の研究部会
- 法人部会：団体会員をメンバーとし、システム監査を専門業として定着させることを目指す活動などの部会
- CSAフォーラム：公認システム監査人（CSA）の交流のための場
- システム監査活性化委員会：SAAJの活動を横断的に議論し、システム監査の活性化を推進する委員会

〒103-0025 東京都中央区日本橋茅場町2-16-7
本間ビル201号室

Tel : 03-3666-6341

<https://www.saaj.or.jp/index.html>



皆様の入会をお待ちしています。

SAAJ 入会

検索

2014年2月21日 初版発行
2016年2月22日 改定1版発行
2019年2月22日 改定2版発行
2022年2月18日 改定3版発行

発行者 特定非営利活動法人日本システム監査人協会（SAAJ）
編集者 SAAJシステム監査活性化委員会

— 禁無断転載 —