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～

（改定第４版）

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

目次

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。

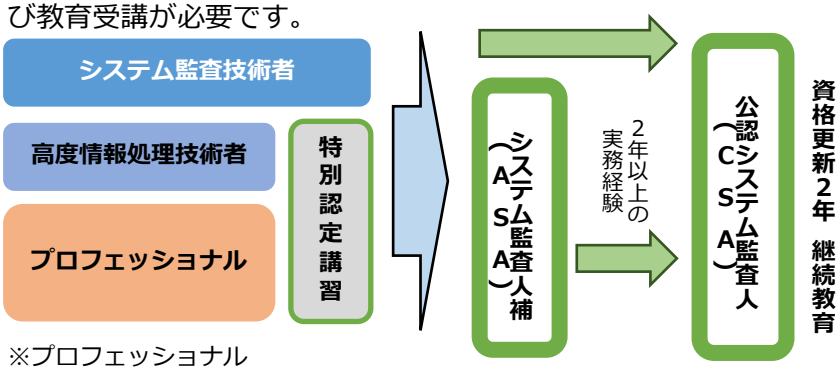
・認定制度は1999年通商産業省（現経済産業省）の産業構造審議会・情報化人材対策小委員会の提言を受け誕生しました。

「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へのステップ

・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かつ2年以上の実務経験者が申請できます。書類審査、面接試験を経て資格認定されます。

・認定後は2年毎に資格更新が必要です。資格維持には継続的な実務及び教育受講が必要です。



※プロフェッショナル

公認会計士、米国公認会計士、中小企業診断士、技術士、ITコーディネータ、CISA（公認情報システム監査人）、内部監査人（CIA,CCSA・・・）、QMS主任/エキスパート審査員、公認情報セキュリティ監査人、プライバシーマーク主任審査員、ISMS主任/エキスパート審査員、PMP（Project Management Professional：PMIが認定するプロジェクトマネジメントの資格）※2023年追加

公認システム監査人資格を保有することの期待

・社会での信用力向上と活躍の場の拡大
・専門知識や技能の更なる向上
・人的ネットワークやビジネスチャンス
・キャリアアップ（社内、転職）　等々

詳細は当協会のHPをご参照ください。

はじめに

～重要性を増すITガバナンスを対象にしたシステム監査～

今日の社会では、様々な組織において、ITシステムの利活用※によって、組織体の価値を向上させるサービス、製品及びプロセスを生み出し、改善する取組が加速しています。また自社で保有する情報システムだけでなく、広く外部のサービスを利用して事業を推進する組織体が多くなってきています。

※2023年改訂のシステム監査基準では「ITシステムの利活用」は、IT の利活用だけではなくデータの利活用も含み情報システムの計画、調達、外部委託、設計、統合、検証、移行、運用、保守及び廃棄、さらには外部のIT サービスの利用も含まれると定義されている。

システム監査は、ITシステムの利活用に係るガバナンス（ITガバナンス）やマネジメント（ITマネジメント）等について、信頼性、安全性、効率性等の観点から検証や評価を行い、組織体におけるITに関するリスクを軽減させるためのアプローチの一つとして、その役割を果たしてきました。そして、リスクコントロールの対象としては、組織体に直接損害をもたらすリスクだけではなく、変化する事業環境に適応できないことによるビジネス機会の損失リスク等も含まれています。全社的リスクマネジメントにおいてITガバナンスが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りました。

上記のように「信頼性・安全性が高くかつ有効なITシステムの利活用（以下、適切なITシステムの利活用）」の実現は、あらゆる組織と個人の活動において必要不可欠となりました。SAAJは、ITシステムの利活用に係る検証・評価（システム監査）並びにその実現の支援等を通じて「適切なITシステムの利活用」を広く社会に普及させることを目指しています。そのために「システム監査・管理ガイドライン」等、広く外部に対して「適切なITシステムの利活用」に関する情報を提供していきます。

その一環として、本小冊子は、新たな役割を担うシステム監査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、システム監査についてご理解を深めていただければ幸いです。

認定NPO法人 日本システム監査人協会（SAAJ）

監査とは
～経営や業務活動を健全な態勢に導く～

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かを、法令や規定に照らして点検・評価し、その結果が適切でなければ、正しい方向へ改善を促すことです。会計監査の場合などでは、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かを、法令や規定などに照らして点検・評価し、
目　的	点検・評価の結果、その活動が適切でなければ指摘を行い、正しい方向へ改善を促すこと。会計監査に代表される一部の監査（システム監査を含む）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類としての内部監査と外部監査、監査対象による分類としての業務監査と会計監査など、さらに目的による分類としての助言型監査と保証型監査があります。

例を挙げれば、株主の利益が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た結果、大きな損失が発生することを防ぐために行われる業務監査は、不適切な箇所を指摘し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。

助言型監査と保証型監査については、別項（5~6ページ）でより詳しく述べています。

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、組織体にはどのようなメリット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効率性・利便性などの面で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大事件や大被害になることを未然に防止できることです。何億円も使いこみをされると企業によっては存続に関わることになり、最悪、倒産という結果に陥り、取引先や従業員に多大な迷惑をかけることになるかも知れません。

こうした事態にならないよう小さな事象のうちに誤りを発見すること、さらには、そもそも誤り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
～経営に資するITシステムの利活用を目的に～

■システム監査の定義

「システム監査基準」（経済産業省、2023年改訂版）では、『監査人が、一定の基準に基づいてITシステムの利活用に係る検証・評価を行い、ガバナンスやマネジメント等について、一定の保証や改善のための助言を行うものであり、システムの信頼性等を確保し、企業等に対する信用を高める重要な取組である』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システムの利活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、ITシステムの利活用のガバナンス（IT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期待できます。あるいは、システム監査にはたとえば、「保有する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」が期待できます。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

「システム監査基準」では、システム監査の目的は、『ITシステムに係るリスクに適切に対応しているかどうかについて、監査人が検証・評価し、もって保証や助言を行うことを通じて、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、及び利害関係者に対する説明責任を果たすことである。』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。

7～8ページ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が、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）が参考になるはずです。

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
◯経験豊富な執筆者陣

https://www.saaj.or.jp/shuppan/（割引き購入注文書）

保証型システム監査
～システム監査のさらなる深化に向けて～

■保証型システム監査とは

保証型システム監査とは、被監査組織の代表者から提示された言明書（IT統制のための要求項目が、どのようにコントロールされているかを具体的に記述し、責任者がその要求に対する達成度合いを表明した文書）の内容に基づき、監査対象である情報システムのコントロール状況が、一定の判断基準により監査手続を実施した限りにおいて適切であるか否かを監査報告書で表明する監査のことです。

■助言型システム監査と保証型システム監査の違い

助言型システム監査は、主にIT統制の改善のために実施され、保証型システム監査は、主に利害関係者への説明責任を果たすために実施されます。その他の違いは次の通りです。

	助言型システム監査	保証型システム監査
監査目的	判断基準に照らし問題点を指摘し改善を促す	判断基準に照らし適切であることを保証する
言明書	必ず要るわけではない	必要
可監査性要求レベル	低い	高い
被監査組織の成熟度レベル	低～中程度で効果的	中～高程度で効果的
報告内容	改善提案	保証意見
監査人の立場	組織内部の内部監査人でも良い	組織外の専門システム監査人

■保証型システム監査を実施するための条件

(1) 言明書があること　（監査証拠の範囲を決める）

システム監査人は前述の言明書で表明されている事項について監査し、妥当であると判断したときに保証を与える監査意見を表明することができます。

(2) 保証型システム監査が実行可能であること　（可監査性）

監査依頼の内容確認において、被監査組織の可監査性が確保できているかを関係者へのヒアリングなどにより確認します。その結果、言明書の内容に沿うコントロールおよび監査証拠の存在が確認できれば、保証型システム監査の実施についてシステム監査人と依頼者が合意し、監査計画の策定に進みます。

(3) 言明書の基となるシステム管理基準が作成されていること

保証型システム監査では、言明書に記載された要求レベルをより適正に反映したシステム管理基準の存在が重要となります。システム監査は、言明書に記載された要求レベルの統制内容が適正に実施されているか、システム管理基準や規定、マニュアル等と照合しながら実施します。

(4) 適切なシステム監査人チームを組織化できること

保証型システム監査の場合、外部に対して監査意見を示すことが多いことから、外観上の独立性を確保するため、当該組織外部のシステム監査人で監査人チームを組成することが適切です。

■保証型システム監査の４分類

保証型システム監査を誰が主導して実施するかで分類すると下図のようになります。システム監査人はその違いに留意して対応する必要があります。

分類	依頼者	監査結果の利用目的	言明書の作成	被監査組織
経営者主導方式	経営者(CIO他)	自組織の管理レベルを評価するため	自組織が考える独自なレベルで依頼者が作成	自組織
委託者主導方式	委託者	委託先の管理レベルを評価するため	委託者の要求レベルで受託者が作成	委託先(受託者)
受託者主導方式	受託者	委託元へ管理レベルを報告するため	委託者の要求レベル等で受託者が作成	受託者
社会主導方式	経営者(CIO他)	取引先や社会に対して、自組織の管理レベルを表明するため	一般に周知されている高レベルの基準等に基づいて依頼者が作成	自組織

■実践的な解説本「保証型システム監査の実践」（同文館出版）

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が、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ITシステムに係るリスクに適切に対応しているかどうかを検証・評価することを通じて、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。
　IT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、現場視察などをするのです。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ITシステムの利活用を総合的に点検・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、妥当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。

■システム監査の基準・ガイドライン

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ます。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であり、システム監査における判断の拠りどころになります。

また、経済産業省以外の官公庁や各監査団体等でも先に紹介した「情報システム監査実践マニュアル」をはじめとした監査の基準やガイドライン等を公表していますので、監査対象となる業界や法人等の特性に応じた監査を行う際に参考とすることができます。

■組織体としてのシステム監査基準等の整備

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2023.４改訂)
システム管理基準(経済産業省2023.４改訂)
システム監査基準ガイドライン(日本システム監査人協会2023.8)
システム管理基準ガイドライン(同上)
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2024.12改訂)
情報システム監査実践マニュアル第3版(日本システム監査人協会2020.6)
情報セキュリティ監査基準(経済産業省2003年)
情報セキュリティ管理基準(経済産業省2016.３改正)
クラウド情報セキュリティ管理基準(日本セキュリティ監査協会2016年改定)
IT監査の国際的ガイド（GTAG）(Global Technology Audit Guides)（内部監査協会2009.1～2015.3）
内部監査基準(日本内部監査協会2014.6改訂)
内部監査基準実務指針（同上　2017.3／5）
ISMAP管理基準(ISMAP運営委員会2023.7改)
ISMAP管理基準マニュアル(ISMAP運用支援機関2023.7)
ISMAP情報セキュリティ監査ガイドライン(ISMAP運営委員会2022.4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2022.3改定）
中小・地域金融機関向けの総合的な監督指針（金融庁2022.5）
金融機関等のシステム監査基準(金融情報システムセンターFISC 2024.3)
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（同上）

システム監査に役立つ主な基準等
金融機関等におけるコンティンジェンシープラン策定のための手引書（FISC 2024.1）
金融機関等におけるセキュリティポリシー策定のための手引書(FISIC 2008.6）
金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書（FISIC 2018.3）
COBIT 2019 フレームワーク(米ISACA 2018.11）※COBIT:Control Objectives for Information and related Technology
COBIT 2019 デザインガイド(同上)
COBIT 2019 導入ガイド（同上）
サイバーセキュリティ経営ガイドライン Ver3.0(経済産業省／情報処理推進機構2023.3)
JIS Q 15001:2023(個人情報保護マネジメントシステム)
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）
ISO/IEC 38500:2024（ITガバナンス）
ISO/IEC38503:2022(ITガバナンスのアセスメント)
JIS Q 31000:2019（リスクマネジメント）
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 27001:2023（情報セキュリティマネジメントシステム）
JIS Q 27002:2024（情報セキュリティ，サイバーセキュリティ及びプライバシー保護）
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)

システム監査基準
～システム監査人の行為規範～

■システム監査基準改訂の経緯

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、2023年の4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年の改訂は、進化する情報技術環境への適合、中小企業へ自己診断やシステム監査への対応、国際動向であるITガバナンス、情報セキュリティ監査基準・管理基準との補完など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。

そして2023年4月、ITガバナンスの国際基準の改訂やITの進展を踏まえ、システム監査基準・管理基準の改訂・見直しを実施し、変化に合わせ監査が速やかに可能となるよう、実施方法の「実践部分」は切り離して、基準ガイドラインとして、関係団体と共同で策定・改訂して、日本システム監査人協会において公表しています。

■システム監査基準のポイント

システム監査基準は、前文と3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、目的に加えて、監査人の倫理とし監査人が守るべき4つの原則（基準5から独立）を謳っています。

主な改定として、

・監査人が意識すべき倫理に関する部分については基準と切り離す構成とし、守るべき原則として①誠実性、②客観性、③能力 及び正当な注意、④秘密の保持 を明示する

・システム監査人のみならず、組織としての対応の在り方、デジタル技術・システム開発手法の変化によるリスクアプローチ等を追記する等があげられます。

■システム監査基準の構成

12の基準は、従来の5種の体系が３種に括られ、それぞれ「基準・主旨・解釈指針への主な追加点」と「ガイドラインへの主な移行点」から成っています。

［１］システム監査の属性に係わる基準
【基準1】システム監査に係る権限と責任等の明確化 【基準2】専門的能力の保持と向上 【基準3】システム監査に対するニーズの把握と品質の確保 【基準4】監査の独立性と客観性の保持 【基準5】監査の能力及び正当な注意と秘密の保持
［２］ システム監査の実施に係る基準
【基準6】監査計画の策定 【基準7】監査計画の種類 【基準8】監査証拠の入手と評価 【基準9】監査調書の作成と保管 【基準10】監査の結論の形成
［３］システム監査の報告に係わる基準
【基準11】監査報告書の作成と報告 【基準12】改善提案（ 及び改善計画）のフォローアップ

本基準は、組織体の監査役（会）等（監査役設置会社の監査役会及び監査役等）や内部監査部門等が実施するシステム監査だけでなく、組織体の外部の第三者に依頼するシステム監査においても適用又は参考にされます。また、取締役や経営者、管理者がガバナンスやマネジメントの視点から ITシステムの利活用を監視、監督、あるいは点検や確認等を行う際にも参考になるものです。

■今後のシステム監査について

IT関連のリスクは経営や事業における多種多様なリスクと関連します。システム監査は会計監査、業務監査、コンプライアンス監査、環境監査などの内部監査との連携を強化する必要があります。これは統合的な監査、即ち総合監査Enterprise risk management (ERM)監査への展開も考えられます。

目次

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、国内規格として、「JIS Q 38500情報技術－ITガバナンス」、国際規格としては、「ISO/IEC 38500 Governance of IT for the organization」があり、ISOは2024年に改定されましたが、2023年4月改訂の「システム管理基準ITガバナンス編」は、ISOの規格との整合性が図られています。

システム管理基準では、「I. ITガバナンス編」が設定され、ITガバナンスの実践例と活動例が多数盛り込まれています。
システム管理基準では、「ITガバナンスとは、組織体のガバナンスの構成要素で、取締役会等がステークホルダーのニーズに基づき、組織体の価値及び組織体への信頼を向上させるために、組織体における ITシステムの利活用のあるべき姿を示すIT戦略と方針の策定及びその実現のための活動である。」と定義しています。
また、ITガバナンスの達成目標として「１．効果的なITパフォーマンスの実現」、「２．責任あるIT資源管理の実施」、「３．組織体における倫理的行動の確保」を掲げています。

■取締役会によるITガバナンスの活動

活動	内容
ステークホルダーへの対応 (Engage stakeholders)	ITシステムの利活用に関するステークホルダーを特定し、協議し、そのニーズを明確にして反映する
評価（Evaluate）	ITシステムの利活用に関し、現在及び将来のあるべき姿を、十分な情報に基づいて評価し、判断する
指示（Direct）	責任と資源を割り当て、期待効果を示し、リスク対応を指示し、ITマネジメントの実践を指示する
モニタ（Monitor）	IT戦略目標の達成、IT方針の遵守、ITパフォーマンスの達成状況に関する情報を収集し、確認する

■取締役会等が行うITガバナンスのための「実践」と「実践を支える活動」

ITガバナンスの実践と実践を支える活動	
実践のための直接的活動	1．経営戦略とビジネスモデルの確認
	2．IT戦略の策定
	3．効果的なITパフォーマンスの確認と是正
	4．実行責任及び説明責任の明確化
実践を支える活動	1．ステークホルダーへの対応
	2．取締役会等のリーダーシップ
	3．データ利活用と意思決定
	4．リスクの評価と対応
	5．社会的責任と持続性

取締役会等が、組織体のITシステムの利活用に関して責任を負う領域がITガバナンスであり、経営者がITシステムの利活用について責任を負う領域がITマネジメントです。つまり、経営者（ITマネジメント）に対して、計画及び方針の策定及び実施を指示し、ITマネジメント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ガバナンスを実践します。

日本の組織では、“IT”と付くものはすぐにIT部門に回ってくることが多いのですが、システム管理基準は、「取締役会等及び経営者が役割に応じて、ITガバナンスの目的を理解して実践して頂きたい枠組み」を示しているのです。

ITガバナンスを対象としたシステム監査では、システム管理基準のITガバナンス編や、アセスメント規格として発行された「ISO/IEC 38503:2022 情報技術－ITガバナンスのアセスメント」（JIS発行予定）等を参照することが有効です。

システム監査人はITシステムの利活用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。

システム管理基準
～ITマネジメント編～

■想定する組織

取締役会等が決定したITガバナンスの方針等に基づいたIT戦略の各目標を経営者（ITマネジメント）が達成するために、ITシステムの利活用に関するコントロールを実行し、状況を報告する体制を整備・運用していきます。本基準が想定する組織体の体制は、IT関連の業務執行部門が対象です。その中で、IT戦略委員会は経営者とIT部門長、IT利用部門部門長等で構成されます。その下にIT部門、IT利用部門などがあります。ITエコシステムとして、ITベンダー、外部サービス提供者、外部委託先、取引先、行政機関などがあります。この基準は、これらの組織と担当者を想定して作成されています。個別の組織が複数の機能を有する場合は、行動時にどの項目を適用しているかを意識します。分離すべき管理は、機能別に担当者を分けます。

■ITマネジメント編の構成

ITマネジメント編は、大きく4つに分かれています。「推進・管理体制」「プロジェクト管理」「ITの企画から開発・運用・保守・廃棄まで」「その他の管理」です。

基準はツリー構造をしています。大項目の下に小項目があり、その下に、＜達成目標＞と＜管理活動＞があります。例えば、「Ⅱ.5運用プロセス」の下に、「Ⅱ.5.1運用体制の整備」から「Ⅱ.5.8運用の評価と報告」までに分かれています。さらにその下にⅡ.5.1では＜達成目標＞が3つと、＜管理活動の例＞が7つ例示されています。本基準では、システムライフサイクルにおける基本となる活動に基づいて細分化したプロセス毎に記載されているため、その組合せによって、様々なプロセスモデル（ウォーターフォール/アジャイルモデル等）や情報システムの導入形態（パッケージソフト/クラウドサービス等）に応用可能となっています。

■活用方法の例

システム管理基準（ITマネジメント編）はシステム管理を体系的に、かつ、実践的な視点で作られています。従って、例えば次のように利用できます。

１．組織のITマネジメントレベルを上げる。

組織のITマネジメントレベルを向上させるためには、過不足なく、網羅的に管理項目を確認することが役立ちます。マネジメントレベル向上活動は、長期的に継続すると効果的です。例えば、2年間をかけてプロジェクト管理全体を見直す、次の2年間で保守プロセスを見直すというときに必要な項目を網羅的に確認するための基準として利用できます。

２．ITの課題に対する解決の視点を探す。

例えば、「業務システムが止まると長期間復旧しない。どうしたらよいか」という課題があるときに、組織内部か外部かにかかわらずITの専門家に相談をします。この時に、どの管理の検討をしているのか、そして、それで漏れがないか、解決しても残るリスクは何かを確認する手段が必要です。システム管理基準は俯瞰的に全体像を示していますので、これと比較することにより、確認ができます。同時に、専門家は専門用語にとらわれすぎずに、利用者に基準に記載されている文章で説明できるため、十分な意思疎通ができます。この事を土台にすると、適切な解決を進められます。

３．ITマネジメントの学習に利用する。

ITの全般的な管理者として広く網羅的に管理を知るために、全体を精読します。基準には、原則、主旨、解釈指針、達成目標、管理活動の例が載っています。また、システム管理基準ガイドラインには、基準の実施方法、管理活動の例の着眼点（必要な観点や留意事項）実施・書式の例などが掲載されています。読者が具体的な事例を思い浮かべながら学習できます。

目次

システム監査基準・管理基準ガイドラインの活用
～ 基準の実践的有効活用のために～

■システム監査基準ガイドラインの概要

本ガイドラインは、「監査基準」とその主旨、解釈指針が示す事項をより具体的に説明し、留意事項や監査の際に用いる手法や各種記載事項を例示することにより、「監査基準」を利用するに当たってより実践的な参考となるように策定されています。

システム監査にとって普遍的な内容は「監査基準」に記述し、本ガイドラインでは、ITシステムやシステム監査を取り巻く環境の変化に対応するべき事項や、「監査基準」のより具体的な内容を取り扱っています。

■システム管理基準ガイドラインの概要

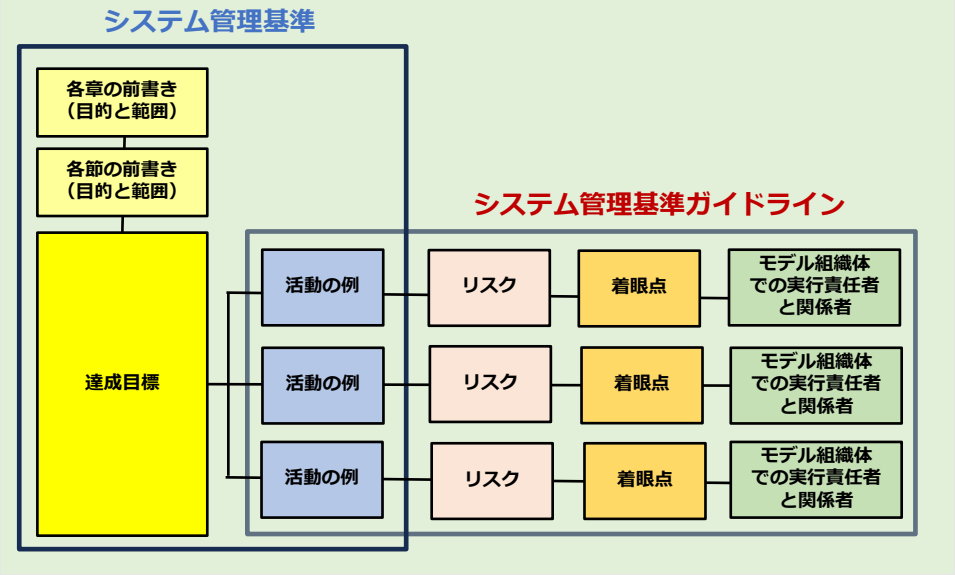
本ガイドラインは、今後の技術革新や社会情勢の変化等に伴って、改訂が必要となる実践的な内容について策定されています。本ガイドラインは「管理基準」を利用するにあたって、より具体的なITガバナンスやITマネジメントに関する着眼点等を例示することにより、システム監査を実践する際の参考とすることを目的としています。

本ガイドラインでは、「管理基準」の「活動の例」に紐付けて「リスク」と「着眼点」を示し、実行責任者の具体例を「モデル組織体での実行責任者と関係者」として示しています。

（基準とガイドラインの関係は次図をご参照下さい。）

■システム監査基準ガイドラインの活用

本ガイドラインでは、監査の際に用いる手法や留意事項を例示などで具体的に説明しています。これはシステム監査の計画策定に役立つことに加えて、システム監査の専門的能力向上の教育研修にも役立てることができます。



■システム管理基準ガイドラインの活用

本ガイドラインは、システム監査を実施する際の参考となるよう、システム監査の判断尺度である「管理基準」の具体的な評価基準を例示しています。また「リスク」には、「活動の例」に示した活動が行われない場合に、達成目標を阻害するどのような影響が生じるかを記載しています。システム監査で不備の指摘を行う際に、その不備によりどのようなリスクが生じているかを示す参考になります。

本ガイドラインは、監査の実施以外に、システム管理の具体策の検討や、IT部門などへの教育研修にも役立てることができます。

■システム監査・管理基準テーマ別ガイドライン

システム監査・管理基準に関して、「テーマ別ガイドライン」として基準運営委員会（日本システム監査人協会、システム監査学会、日本内部監査協会、日本公認会計士協会、経済産業省で構成）で計画し、進めています。

作成中または検討中のテーマ別ガイドラインは以下の通りです。（2024年11月現在）

・DevOpsに関するガイドライン/アジャイルに関するガイドライン
・リスク・アプローチによる監査計画の策定方法
・ITガバナンスのアセスメント・監査
・IoTシステムの監査　他

FISCの各種基準の概要
～金融機関以外の組織体でのシステム監査でも有効～

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の実施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余りの基準項目が示されています。

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。

なお、両基準とも、金融機関以外の組織体でのシステム監査でも、大いに参考になる内容となっています。

目次

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。（COBIT2019では「ITガバナンス」から「I&Tガバナンス」へと用語を変更）

”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。

これまでも、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。

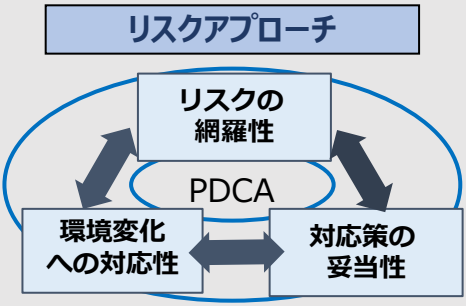
リスクマネジメントは経営課題
～リスクアプローチの勧め～

■リスクマネジメントの重要性

「システム管理基準」では、ITガバナンスに責任を持つ取締役会等は、ステークホルダーへの対応と、ITマネジメントの成果を評価し、計画の策定や実施を指示し、パフォーマンスをモニタ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ITガバナンスモデルにおいて、取締役会等がリスクについても、常にステークホルダーの動向を踏まえて評価・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ってきます。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過ごすことを防ぎ、”想定外”として発生するリスクをなくすことができます。

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」を行いますが、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。

■リスクマネジメントの例

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になります。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になります。

「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。

目次

情報セキュリティ監査
～わが国の情報セキュリティ監査への取組と動向～

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。

最新版は「JIS Q 27001:2014及びJIS Q 27002:2014」に基づいて整合し作成された2016年版が用いられています。

なお、元となる規格の 「JIS Q 27001:2023及びJIS Q 27002:2024」が発行されており、これに対応した「情報セキュリティ管理基準」の改正が予定されています。

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）が公表されています。これは、情報セキュリティに係るサービスにおいて、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。

情報セキュリティ脅威と対策
～サイバーセキュリティ対策の視点～

■情報セキュリティ脅威の動向

サイバー攻撃の手法が高度化・巧妙化して、個人情報や機密情報を狙った攻撃が蔓延しています。フィッシング詐欺、ランサムウェア、ゼロデイ攻撃等の攻撃手法は日々進化しています。また、多くの組織がデジタル化を進めていく中で、サプライチェーン、IoTデバイス、VPN機器なども攻撃者に狙われ、データの漏洩・暗号化による業務停止など、経済的損失が増大しています。

具体的な事例と効果的な対策については、IPAが毎年発行する情報セキュリティ10大脅威の記載が参考になります。

■サイバーセキュリティ対策とシステム監査人の視点

サイバーセキュリティ対策には技術的な対応も重要ですが、システム監査人には、組織体がサイバーセキュリティをリスクマネジメントの一部として捉えているかどうか、の視点が必要になります。

経済産業省の「サイバーセキュリティ経営ガイドライン」では、次の経営者が認識すべき３原則を提言しています。

経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
平時及び緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

さらに、次ページに挙げた法令、ガイドライン、白書など、また、各専門機関から発信される施策、活動報告など、日常的にかつ俯瞰的に情報を捉えておくことが重要です。

■参考となる法令、ガイダンス、各種資料など

■法令及び法令に準ずる文書：サイバーセキュリティ基本法、不正アクセス行為の禁止等に関する法律 、個人情報の保護に関する法律 、電子署名及び認証業務に関する法律 、情報通信ネットワーク安全・信頼性基準、特定電子メールの送信の適正化等に関する法律、不正競争防止法、営業秘密管理指針、電気通信事業法、特許法、著作権法、輸出貿易管理令、など

■ガイドライン：政府機関等のサイバーセキュリティ対策のための統一基準群、重要インフラのサイバーセキュリティ確保に係る安全基準等策定指針、サイバーセキュリティ経営ガイドライン 、IoTセキュリティガイドライン、クラウドセキュリティガイドライン、医療情報システム安全管理に関するガイドライン、テレワークセキュリティガイドライン、IoT セキュリティ対応マニュアル 産業保安版、AI・データの利用に関する契約ガイドライン、など

※この他に各業界別ガイドライン： 医療、航空など、各業界において、それぞれに特化した情報セキュリティガイドラインがある。
（本書の「システム監査に役立つ主な基準」も併せて参照。）

具体的な活用については、サイバーセキュリティ関係法令 Q&A ハンドブック （NISC）（付録１「サイバーセキュリティ関係法令・ガイドライン調査結果」）、インターネットの安全・安心ハンドブック（NISC）を参考に

■白書： 情報セキュリティ白書（IPA）、情報通信白書（総務省）、科学技術・イノベーション白書（文部科学省）、警察白書（警察庁）、防衛白書（防衛省）、など。AI、IoT についてはIPA、総務省、文部科学省の各白書を参考。

■NIST サイバーセキュリティフレームワーク2.0（NIST Cybersecurity Framework：NIST CSF）：サイバーセキュリティリスクに対応するためのフレームワーク。世界中の様々な組織で活用 ※NIST（米国立標準技術研究所）

■「ATT&CK」データベース（知識ベース）（ 米国MITRE社）：
CVE（共通脆弱性識別子）を基に、標的型サイバー攻撃の手口、戦術、手法、緩和策をまとめたフレームワーク。世界中の様々な組織で活用

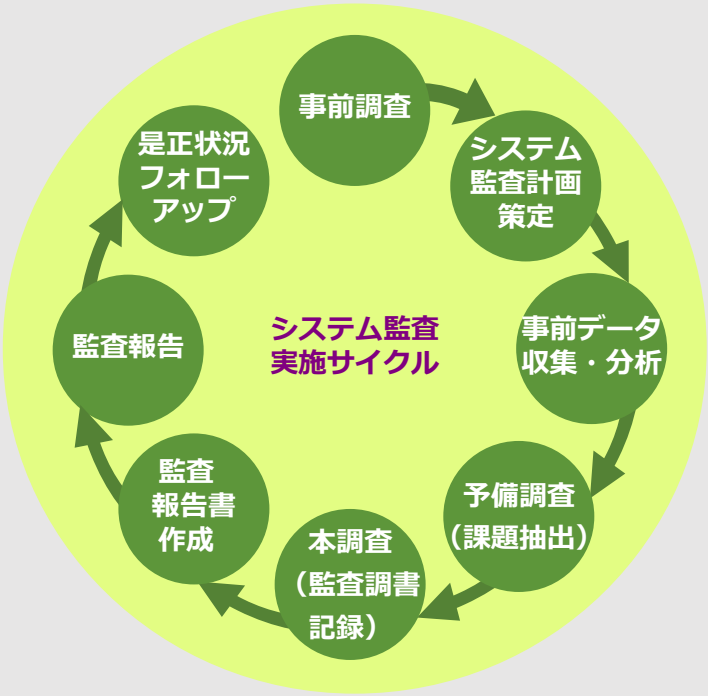
■施策、活動報告書：経済産業省、総務省、金融庁、警察庁、IPA（情報処理推進機構）、JIPDEC（日本情報経済社会推進協会）、NICT（情報通信研究機構）などの発行する様々な報告書

システム監査人に求められる能力
～システム監査人の倫理に注目を～

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、先方と的確、簡潔、適時に実施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。

柔軟性・適応能力

システム監査人は、新しいアイデアや技術の動向を把握し状況や環境の変動に対応できる能力が求められます。

システム監査人の倫理

システム監査人が備えるべき重要な資質に高い倫理性があります。システム監査基準では、４つの原則（誠実性、客観性、監査人としての能力及び正当な注意、秘密の保持）を明示しています。SAAJでは2002年に倫理規程を定めています.

システム監査人倫理規定　　2002/2/25　日本システム監査人協会制定

第 1条 （目的）この規定は、システム監査人が最低限遵守すべき職業倫理の規範を定めることを目的とする。

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４条（監査基準・手続き）システム監査人は、システム監査の基準、手続きを明らかにし、それに基づきシステム監査を行わなければならない。

第５条（監査報告）システム監査人は、監査結果の報告にあたって、知り得た全ての重要な事実を明らかにするものとする。

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11条 （システム監査人間の規律）システム監査人は、みだりに他のシステム監査人を誹謗し、名誉を傷つける等の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意義
～デジタル社会推進におけるキーパーソンとして～

情報システムは、企業内における業務を対象とするだけでなく、複数の企業間の業務もカバーし始めています。さらには、Society5.0で述べられているような、社会のあらゆる主体間が結合されデータ連携やサービス連携が行われる世界も、情報システムによって遠くない未来に実現することでしょう。**すでに情報システムなしには、日々の生活もビジネス活動も成立しなくなっています。**一方、金融機関、通信会社等、私たちの生活に大きな影響を与えるような大規模なシステム障害も報道等でよく目にします。これは、情報システムの機能そのものが従前に比べて複雑になってきていること、複数の情報システムが有機的に融合し始めていること等が背景にあると考えられます。さらには、情報システムへのサイバー攻撃が増加傾向にあることも見逃せません。

このような不確実性の高い環境のもとで、**情報システムが健全な状態を保ち続けるために、システム監査が重要な位置づけにあることは間違いありません。**同時に、システム監査人にはより重大な責務が発生してくるでしょう。

デジタル技術の発展は留まることを知らず、必要となるスキルやノウハウはこれからも日々変化し続けていきます。システム監査人は、いつも新しいことにチャレンジし、環境変化に応じて必要となるスキルを主体的に学び続けるような心構えを持たなければなりません。さらに、生成AI等の利活用が進むにつれて、ビジネス面だけの評価に留まらない、ELSI（倫理的・法的・社会的課題）といった側面からの見識も、システム監査人に求められてくるでしょう。

今後のデジタル社会推進において、**より一層重要な役割を担うことになるシステム監査人をぜひ目指してください。**

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～

■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

デジタル技術の革新により、様々な機器がネットワークに接続され、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。また、昨今では生成AIが注目され、ビジネスや社会生活の様々な分野に利用されつつあります。

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は、リアルタイムなデータ収集や遠隔操作により新たなライフスタイルが提案されています。ウェルネス分野では、ウェアラブルデバイスの活用が進み予防医療に寄与しています。また、医療分野では、遠隔診療、画像診断の精度向上、薬剤開発の加速等に貢献しています。生成AIは生産性向上やクリエイティブ産業の変革等を引き起こすとされ、これらは社会を変貌させることになるでしょう。

社会は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、例えば、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

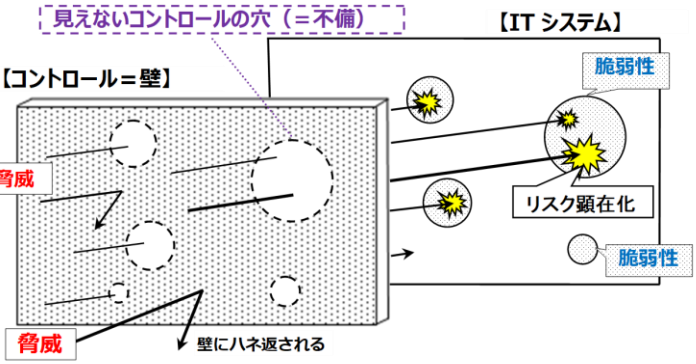
技術革新に対してシステム監査で何ができるのか、システム監査人はどうあるべきか、答えは様々でしょう。しかし、一ついえることは、AIが進化する中で、システムの品質は人命や社会にこれまでにない影響を与えかねず、システム監査の重要性、システム監査人への期待は増大の一途といえるでしょう。新技術に対応するスキルを身に付けることができれば、システム監査人の新たな活躍の場となるに違いありません。

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

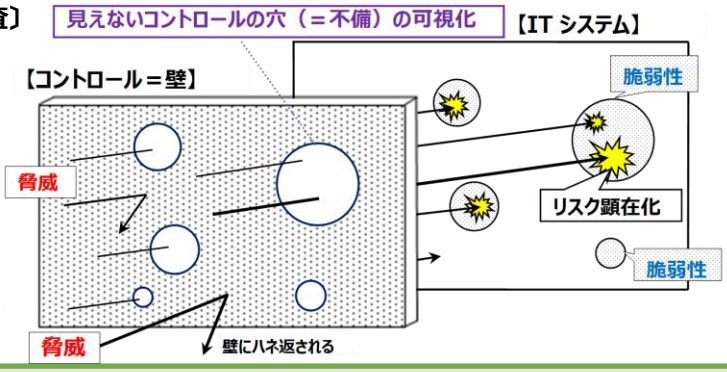
ITシステムリスクは、「脅威」（リスクの源泉）と、ITシステムの「脆弱性」（リスクの発生を許す弱点）が結びつかなければ、顕在化しません。

〔現状〕
[見えないコントロールの穴(=不備)]



脅威と脆弱性が出会わないように、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。

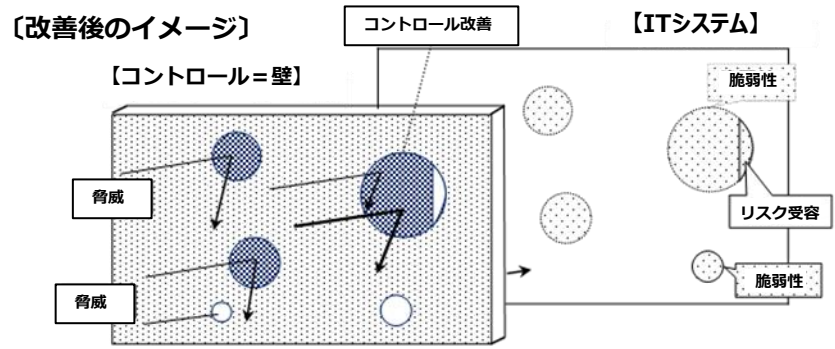
〔システム監査〕
[コントロールの穴を見える化します]



■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) ITシステムに係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、「ITシステムの健康診断」に当たります。
IT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
～システム障害管理を例に～

■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を実施します。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のように思われますが、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？
・停電時のバッテリー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よいのです。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も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。常識的な感覚を基に、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だと思います。

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、**その障害への対応の経験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てるための「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す。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行い、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。

DX推進施策とシステム監査人
～ レガシーシステムの見極めと デジタルガバナンス・コードの活用 ～

■「2025年の崖」という課題

DX（デジタル・トランスフォーメーション）は、業種や組織規模を問わず、あらゆる企業の経営において共通的で重要なテーマとなっています。

DXの推進において大きな障害になっているのが「2025年の崖」と呼ばれている課題です。これは経済産業省が2018年に取りまとめた「DXレポート」で述べられたもので、企業等が保有する情報システムが過剰なカスタマイズが行われたことなどにより、複雑化・ブラックボックス化した結果、DXの推進が困難になるという課題です。これを克服できない場合、国全体として年間12兆円もの経済損失が生まれるといわれています。

複雑化、ブラックボックス化し、結果として経営の足かせになっている情報システムのことをレガシーシステムと呼びます。レガシーシステム化の原因としては、使われている技術が陳腐化したことだけでなく、システム開発のノウハウが開発担当者の退職等によって散逸してしまっていること等が挙げられます。

この課題が厄介なのは、社内にレガシーシステムが存在していること自体を自覚しにくいことです。システムの中身が誰にも分からなくなっているシステムであっても、日常的に使う時には業務上全く問題は発生しません。そのまま放置し、大きな仕様変更を行ったり、ハードウェアの入替えをしたりするときに始めてレガシーシステム化していることが判明するのです。

企業の情報システムが、レガシーシステム化していないかを確認し、必要に応じて対応を行うことを促すことも、これからのシステム監査人の役割の一つになりそうです。

■ＤＸ推進のための指針「デジタルガバナンス・コード」

デジタルガバナンス・コード（以下、コード）は、企業が価値向上に向けてDXを円滑に推進していくために、経営者に求められる実践すべき事柄について、経済産業省がとりまとめたものです。これを活用して、経営者がDX推進に関して投資家や顧客、社員等のステークホルダーと積極的に対話を行うことで、資金や人材、ビジネス機会が集まる環境を整備していくことを目指すものです。

コードは、「経営ビジョン・ビジネスモデルの策定」「DX戦略の策定」「DX戦略の推進」「成果指標の設定・DX戦略の見直し」「ステークホルダー」の５つの柱で構成されています。経済産業省は、これからDXを進めていくための準備が整っている企業であることを示す「DX認定制度」や、DX推進に関して業種を代表するような優れた取組みを行っている企業を表彰する「DX銘柄制度」を運用しています。これらの制度においても、コードの内容が評価基準として活用されています。

また、コードの内容は、「社会全体のシステムの利用状況やデジタル技術の発展状況を勘案し、おおむね二年ごとに再検討し、必要に応じて更新する」ということが、情報処理促進法において定められています。

2024年に行われた更新においては、①企業におけるデータ活用、企業間等におけるデータ連携の重要性、②デジタル人材の育成・確保について、デジタルスキル標準を参照したスキルの可視化や、経営層・管理職の意識改革、キャリア形成支援等の重要性、③高度化・複雑化しつつあるサイバーセキュリティリスクについて、第三者監査やサプライチェーン保護に向けた対策の重要性という３つの項目が、コードの中に新たに盛り込まれました。

企業のDX推進状況について、デジタルガバナンス・コードを活用して客観的に評価し、必要に応じたアドバイスを行うことも、これからのシステム監査人に求められることになるでしょう。

目次

成功に導くプロジェクト監査
～「失敗しない」システム開発の鍵～

■**失敗しない……**女医さんの人気ドラマの決め台詞「私 失敗しないので！」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。システム開発でも同じです。「卓越した技術と周到な準備」をした上で、次の**６つのポイントを外さずにマネジメント**すれば"失敗しない"で、開発を成功に導くことができます。

①ＰＭ	**全員のベクトルを合わせ一丸にする（PMの最重要ミッション）**
②体制	**業務を熟知した設計者に設計させる（高い業務スキルが必須）**
③計画	**プロジェクト計画を緻密に立てる　（成功に導くシナリオとする）**
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する）**
⑤品質	**レビューを徹底し、高品質を作り込む　（高品質に設計する）**
⑥リスク	**最重要リスク３つを確実にコントロールする（その早期発見/早期対処ができるなら,他のリスクにも対応できる）**

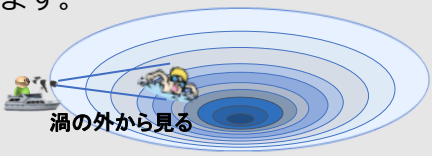
■**しかし……それでも「大トラブル」になることがある！**

百億円超の損害も出ます。きちんと準備し、しっかりマネジメントしても起きています。では、どうしたらよいのでしょう？

■**開発を失敗させない**

プロジェクトの当事者は、誰よりも考え、成功に向けてあらゆる努力をしています。しかし、開発という"大きな渦"の中で、目前の課題解決に追われ、抜本対策が遅れたりします。正しい情報が直ぐに上がらず、判断を誤ることもあります。

しかし、第三者のプロジェクト監査人は、渦の外から大所高所から冷静に見ますので、危険を早く察知し、回避することが出来ます。



トラブルの本質や抜本解決策が見えるので、開発を失敗から救うことが出来ます。これが**《成功に導くプロジェクト監査》**です

■成功に導くプロジェクト監査

プロジェクト監査人は、これまで多くのプロジェクトを見ていますので、「このままだと外部設計は終わらない、少なくともあと半年かかる」とか、「設計品質が悪いので、このままではテストで大トラブルになり、稼働出来ない」等、この先こうなる…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、プロジェクトの課題・問題点を監査所見に示し、抜本改善の助言もします。

プロジェクトが、**監査所見と助言に真摯に向き合って、抜本対策すれば、成功します。**これが**「失敗しない開発の鍵」**です。

■基本は「早め早めの監査」

成功の基本は、**「早めに監査を受け、早く是正する」**です。

例えば、企画計画、外部設計、試験計画、品質評価などについて、早めに監査を受け、是正する……これが**成功させる基本**です。

■経営者の判断を支援

開発完了判定前の事前監査では、プロジェクトオーナー又は経営者が判定を誤らぬように、プロの眼で監査し、監査所見を出します。もし問題があれば、計画を延長して対処要…など、助言します。

■2冊の実践的なマネジメントとプロジェクト監査の本

プロジェクト監査研究会は、開発を成功に導くマネジメントと監査の本を出しています。

事例、根本問題、工程毎の監査項目、マネジメントの勘所を豊富に載せています。また、読者には1200項目を超える詳細な監査項目表をExcel版で提供いたします。監査と開発の現場で活用下さい。

（2018年3月　同文館出版）
ISBN978-4-495-20711-3

（2020年7月　同文館出版）
ISBN978-4-495-21011-3

https://www.saaj.or.jp/shibu/Projectkansa/130804PJAChirashi.pdf（注文書　2割引き）

目次

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～

クラウドサービスは、DXの普及により、引き続き活用が拡大しています。

一方で、その利用に際しては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課題への対応が一層求められるようになっています。

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等で謳っており、利用者はそれを信用するしかないのが実情です。そのため、未だに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としては、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を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に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、クラウドサービスをどのように活用できるのか、どこまで活用してよいの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、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、「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

	発行・公表機関	状況・備考 （2024/07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 2024年7月改訂
・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	・クラウド情報セキュリティ管理基準2013年度改正版（2014年9月発行） ・利用ガイド：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・ガイダンス	国際団体 CSA(*)	ガイダンス V4.0日本語 V1.1版：2018年7月発行

(*)CSA:クラウドセキュリティアライアンス

実際のところ直接確認が難しいクラウドサービスの評価については、これら第三者評価を活用していくのが現時点では現実的な対応となりますが、注意点もあります。

ほとんどの第三者評価においては、評価対象となる組織・システム・内部統制等は言明書等の文書に明記されており、監査人はここに記載されている事項が事実に照らして適切か否かを評価します。逆にいえば、**言明書等に記載されていない事項については全く評価されません**。したがって、第三者評価を利用する者は「認証を受けているから大丈夫」ではなく、言明書等に記載されている内容を閲覧し、自らが要求する内容を充足しているかを確認した上で、第三者評価を利用することが必要です。

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、政府情報システムに関しては、「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との方針が政府から発表されました。

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監査機関の評価・ISMAP運営委員会の審査を経て、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・公表され、各政府機関は原則としてこの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。

本制度において、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（対応しているセキュリティ対策内容の概要）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、利用しようと検討しているサービスが掲載されている場合、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をある程度までは得ることができるため、政府機関のみならず民間を含め、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。

2022年11月には相対的にリスクの低い業務に利用するSaaSサービスを対象として、評価負担が軽減されたISMAP-LIU（Low Impact Use）制度が追加されました。

また、情報セキュリティ監査の負担が大きい等、制度開始後に判明した課題や、環境変化等に適時に対応するため、2023年10月より2024年にかけて、制度改善が継続的に実施されています。

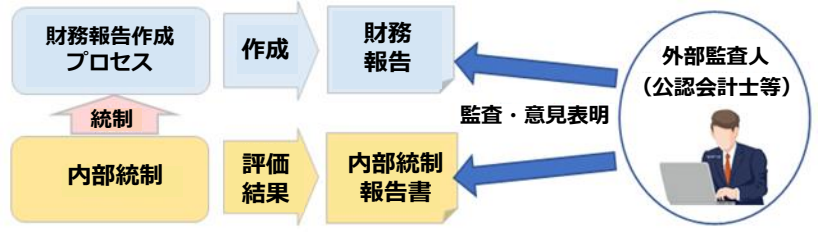
「監査機関による第三者評価」

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、2024年9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（2024年9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
～内部統制において重要な役割を担う～

上場会社に対しては、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。内部統制とは、それらの目的が達成されているこ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は、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）、⑥IT（情報技術）への対応の６つとなっています。

システム監査と関係の深い「ITへの対応」について説明します。

■「ITへの対応」

ITへの対応とは、組織目標を達成するためにあらかじ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なく、組織の業務内容がITに大きく依存している場合などには、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、組織が活動を行う上で必然的に関わる内外のITの利用状況のことであり、社会および市場におけるITの浸透度、組織が行う取引などにおけるITの利用状況、およ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などをいいます。

IT環境に対しては、組織目標を達成するために、組織の管理が及ぶ範囲において、あらかじ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、ITによる統制です。ITによる統制とは、組織内において業務に体系的に組み込まれて様々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、あらかじ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。

■「財務報告に係るIT統制ガイダンス」

経済産業省は、「システム管理基準」をIT統制で活用するためのガイドラインとして、「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 」を、2024年12月に公表しました。

■SAAJ監修「J-SOX対応IT統制監査実践マニュアル」

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、IT統制に関する監査（IT統制監査）の手順や手法等を紹介しています。

個人情報保護法改正の経緯と JIS Q 15001:2023

～『個人情報保護マネジメントシステム実施ハンドブック』第3版を刊行～

2020年6月12日「保護法2020」の改正の主たる理由は、**個人情報の保護及び有用性の確保に資するため**、としており、以下の①～③を掲げていました。（条番号：現行の保護法2021）

①個人情報の**漏えい等が生じた場合**における報告及び本人への通知を義務付け。（第26条：漏えい等の報告等）

②**個人情報等の外国における取扱い**に対する個人情報の保護に関する法律の適用範囲を拡大。（第28条：外国にある第三者への提供の制限等）

③個人情報に含まれる記述等の削除等により他の情報と照合しない限り特定の個人を識別することができないように加工した**仮名加工情報の取扱い**についての規律を定める。（第41条：仮名加工情報の作成等、第42条：仮名加工情報の第三者提供の制限等）

さらに、以下が規定されました。

④**個人関連情報**として、提供元では個人を特定できないが、提供先で個人が特定できる情報の取扱いを定める。（第31条：個人関連情報の第三者提供の制限）

⑤**罰則の強化**　行為者（拘禁刑又は50万円以下）と法人（一億円以下の罰金刑）に対する両罰規定　（第184条）

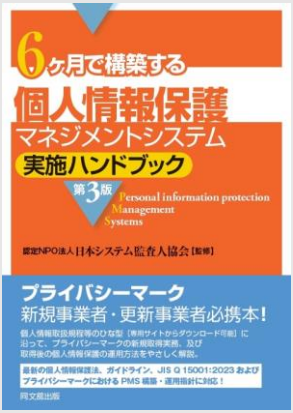
１年後の2021年5月19日に「デジタル社会の形成を図るための関係法律の整備に関する法律」に基づき「保護法2021」も改正され、国の行政機関、独立行政法人、地方公共団体、地方独立行政法人（以下行政機関等と呼ぶ）は、全体を内閣統一下の組織とみなし、民間事業者とともに所管が個人情報保護委員会に一元化されました。

なお、国立大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者は「学術研究機関等」と呼ばれ、原則として民間事業者の規律に従うとされています。

「保護法2020」及び「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した。

2023年9月20日に「**JIS Q 15001:2023** 個人情報保護マネジメントシステム(PMS）要求事項」が公表されました。もともと「保護法2020」は、「JIS Q 15001:2017」を参考にしていることから、保護法とJISは類似を増してきていますが、冒頭に掲げた①～④についての要求事項も、整備されることになりました。

これらの法改正および2023年版JIS改正を受けて、個人情報保護監査研究会では、2024年5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実施ハンドブック**』第3版<R版>を刊行しました。



「法令」や「JIS Q 15001:2023」との関係が理解できるよう、例えば項番は以下のように表記しています。

R.A.10 安全管理措置（法第23条）

R.A.13 漏洩等の報告等（法第26条）

また「プライバシーマーク構築運用指針」及び、ISMSなど、他マネジメントシステムにも適合できるよう考慮しました。

第1版、第2版と同様に、購読者登録された方に、PMS構築に不可欠な規程類や各種様式(**約80文書**)のダウンロードサイトを提供し、法令等の改正にあわせて随時更新しています。

https://www.saaj.or.jp/shibu/Kojin/kojin.html

IT-BCPとシステム監査
～実効性のあるIT-BCP/BCP監査～

■企業・組織の目的と事業継続計画の必要性

企業・組織の目的は、組織の事業活動を継続することで企業の社会的責任を果たし続けることです。

経営陣や全社員により、自社の事業活動が「企業の社会的責任（CSR）を果たすため」の活動であることを認識し、重要事業や業務の継続性を阻害する事象を生じさせないように対策を講じることが必要であり、万一、事業の停止があった場合にも速やかに復旧できるよう計画を策定しておく必要があります。大規模自然災害やサイバー攻撃等による事業停止のリスクは高まりつつあり、サプライチェーンを構成する取引先等からの取引条件としてのBCP対応要請も高まりつつあります。

■BCPとは

BCP（Business Continuity Plan、事業継続計画：「ビジネスコンティニュイティ プラン」）は、企業が災害や事故、テロ攻撃などの非常事態に遭遇した際に、重要な事業活動を継続または迅速に再開するための計画を指します。BCPは、リスク管理と危機管理の一環として策定され、企業のレジリエンス（回復力）を高めることを目的としています。

■IT-BCPとは

企業における重要業務のIT依存度は高く、情報システムやネットワークを利用しない重要業務は殆どない状況となってきています。企業のIT部門は全社BCPと整合性のとれたIT-BCPを策定することが必要となっています。

■実効性のあるIT-BCP／IT-BCP監査について

IT-BCPが実効性のある内容となっているかを判断するうえで、監査は有効な手段です。システム管理基準（2023年4月26日改訂）では、取締役会等が組織体のITシステムの利活用に関して責任を負う領域がITガバナンスであり、経営者が IT システムの利活用について責任を負う領域がITマネジメントである」と定義しています。

IT-BCP監査を行う場合「ITガバナンス」「ITマネジメント」の両面から計画の適切性や有効性を確認する必要があります。IT-BCP監査の評価・判断の尺度として、「システム管理基準（2023年4月26日改訂）」「システム管理基準ガイドライン（2023年8月10日公表）」の活用は有効です。具体的な着眼点としては以下が考えられます。

経営者自身が経営戦略／IT戦略と整合性を持つ事業継続計画「全社BCP／IT-BCP」を策定していること **（経営陣の参画性）**
全社BCP／IT-BCPにおいては、自社の中核事業となる事業から優先度を付けた事業継続計画が策定できていること **（事業継続計画における重要業務の優先順位付け）**
全社BCP／IT-BCPの実効性を担保するために、経営陣の指示のもと、継続的な社員教育と訓練を実施し、経営陣による評価がされていること **（事業継続計画の周知徹底と実効性の確認）**
業務に従事する社員全員が全社BCP／IT-BCPを理解し、日常業務における軽微なインシデント発生時においても、自ら判断し、適切な初動が行える等、企業文化として定着していること **（初動対応の意識と運用の定着）**
自組織の事業や情報システムに関する環境変化、時間の経過等により全社BCP／IT-BCPの実効性が低下することが無いよう、定期的な評価と見直しを行うこと **（事業継続計画の継続的改善）**

目次

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拡大を機に、多くの組織がテレワークを採用しました。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、「アフターコロナ」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いわれています。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 第５版：令和３年（総務省）

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」それぞれについて示されており、監査の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整備
- 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得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りませんが、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、1987年12月に設立されました。その後の沿革は54ページの通りです。

システム監査がターゲットとするITの変革には目覚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、生成AIの浸透、 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

◎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
- システム監査・管理基準ガイドラインの公開（経済産業省のシステム監査・管理基準を基に、関連団体と共に現場で実践するためのガイドラインを策定して公開）
- 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

当協会では、そうしたITの変革に応えて、システム監査人のスキルアップを図ることが重要と考えており、システム監査人に対するさまざまな教育・研修の場を提供しています。

■システム監査人のスキルアップ支援

SAAJでは設立目的のひとつである「システム監査人の実践能力の維持・向上」のため、会員サービスとしてシステム監査の基礎知識を習得するためのコースや、システム監査実務の実践を通じて、監査スキルの習得や経験を積んで頂くための各種研修サービスを提供しています。また、一定の実務経験を積んだシステム監査人を認定する「公認システム監査人（CSA）」「システム監査人補（ASA）」の認定機関としての役割も担っています。以下にSAAJ主催の研修・研鑽の機会についてご紹介します。

■月例研究会

本部では豊富な経験と知識を有するシステム監査人やシステム監査に関連する実務に関わる講師による月例研究会を毎月開催しており、SAAJ会員は会員価格で参加できます。

■本部研究会・各支部主催の研究会・勉強会

本部では「システム監査事例研究会」「情報セキュリティ監査研究会」「ITアセスメント研究会」「個人情報保護監査研究会」「プロジェクト監査研究会」「BCP研究会」といった研究活動を行っています。また各支部（7支部）でも研究会や勉強会を開催しており、同様に参加できます。

■システム監査実務セミナー

本セミナーは、当協会のシステム監査事例研究会の「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、ロールプレイを中心とした演習によりシステム監査技術の修を狙いとしたきわめて実践的なコースです。

本セミナーを受講した後、事後課題を提出し、その内容が適切であると判断された場合には、公認システム監査人の認定に必要なシステム監査実務を1年間経験したものとみなされます。

■内部統制監査人セミナー

内部統制評価・監査に関する監査実践能力を修得するための内部統制監査人セミナーを開催しています。当セミナーは、協会が既に30回以上の開催実績を積んだシステム監査実践・実務セミナーを背景に、事例研究会独自の教材を使って行う、ロールプレイ方式を中心としたITに係わる内部統制評価・監査に焦点をあてた極めて実践的なセミナーです。

■事例に学ぶ課題解決セミナー

情報システムの事故・障害で、企業や顧客が損失を被る事例が後を絶ちません。システム監査の専門家が事故･障害の原因を解き明かし、システム監査の観点から見た有効な解決策を示します。事故･障害の原因は報道だけでは分かりません。事故・障害事例をリスクとコントロールの視点で分析して、皆様の課題解決に役立つよう解説します。情報システムの利用者から運営者、経営者から担当者まで多様な階層・職種の方のキャリアアップに、当セミナーを活用頂いています。

■公認システム監査人特別認定講習

当協会では「特別認定制度」により、協会指定の講習カリキュラムガイドラインに沿って講習を実施する機関を認定し、「特別認定制度」に対応する「講習会」の実施を委託しています。公認システム監査人を目指す方で、実務経験が少ない方は本講習を修了することによりシステム監査の「実務経験みなし期間」として申請することができます。

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・研究会等

- ➢ システム監査・管理基準改訂委員会：システム監査・管理基準ガイドラインの策定と公表等
- ➢ ITアセスメント研究会 ：システム監査・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
- ➢ BCP研究会：組織におけるBCPに役立つ情報発信、IT-BCPの研究を行う部会
- ➢ 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/

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
2025年2月21日 改定４版発行、同3月21日訂正版

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