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

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たり、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経営の重要性が言われています。勿論、官公庁や自治体でも同じことが言えます。

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4月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。

認定NPO法人 日本システム監査人協会（SAAJ）

目 次

監査とは

監査とは、企業や自治体などあらゆる組織体について、経営や業務の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ついて、
内　容	経営や業務の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。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、企業株主の利益を損なわないことを目的とした会計監査の場合は、決算書などが適正に作成されていることを外部の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言えるでしょう。

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よう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。

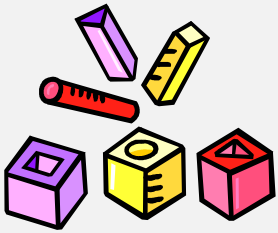
監査を切り口の違いにより整理したのが、下の表です。

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

監査をする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、現状を放っておくと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になります。

このような大事件にならないよう小さな傷のうちに間違いを発見することや、更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、監査することのメリットと言えるでしょう。



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、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

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。

（システム監査基準―2018年4月改訂版―より）

システム監査の実施に当たっては、監査の目的に基づいて監査の範囲を定め、監査テーマを設定します。

システム監査テーマの例

ライフサイクルの監査	・システム企画フェーズの監査 ・システム設計開発フェーズの監査 ・サービス開始、効果検証の監査 ・運用段階における効率性の監査　など
テーマ別監査	・情報システムのガバナンスの監査 ・情報システムのマネジメントの監査 ・情報システムの有効性（目的適合性、投資対効果など）の監査 ・情報システムの可用性監査 ・情報セキュリティ管理体制の監査 ・個人情報保護体制の監査 ・外部委託開発・運用・保守の監査 ・AI、IoT、RPA等新技術対応監査　など

情報システムのライフサイクルを対象とする場合、企画段階から、開発段階、移行段階、運用段階、保守段階などの監査を行います。この場合は、監査のタイミングが重要です。開発が終わってからでは、開発段階の監査は効果が少ないし、システム稼働後に、企画段階の監査をしてもあまり意味がないことになります。

特定テーマのシステム監査では、個別のテーマに絞って重点的な監査を行います。その中でも、情報セキュリティ監査は、脅威の高まりから特に重要な監査テーマとされており、経済産業省から情報セキュリティ監査制度として、監査基準や管理基準が出されています。情報セキュリティ監査については、別項で詳しく述べます。その他、正確な処理が行われていることを確認するシステムの信頼性の監査や、個人情報保護体制の監査なども重要なテーマとして注目されます。

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。「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。一方、「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主な基準には表のようなものがあります。これらから、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年改訂）
■システム管理基準（経済産業省2018年改訂）
■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）

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年改正） ■クラウド情報セキュリティ管理基準（JASA　2014年9月改定）
■情報システム安全対策基準（経済産業省1997年9月最終改定）
■内部監査基準（日本内部監査協会2014年6月1日適用開始） ■内部監査基準実務指針（日本内部監査協会2017年3月または5月）
■専門職的実施の国際フレームワーク（IPPF） （内部監査人協会2017年11月25日初版）
■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指針(改訂第3版)　（FISC2014年3月版） ■金融機関等のシステム監査指針(改訂第3版追補)(FISC2016年5月版) ■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） （FISC2018年5月版）
■COBIT2019　Control Objectives for Information and related Technology　（米ISACA：2018年11月公表）
■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)
■JIS Q 19011（マネジメントシステム監査のための指針）
■JIS Q 38500（ITガバナンス）
■JIS Q 31000（リスクマネジメント―原則及び指針）
■JIS Q 9001（品質マネジメントシステム）
■JIS Q 20000-1、 JIS Q 20000-2（サービスマネジメント ）
■JIS Q 27001（情報セキュリティマネジメントシステム）
■JIS Q 27014（情報セキュリティガバナンス）
■JIS Q 27017（クラウドサービス管理策実践規範）
■JIS Q 22301（事業継続マネジメントシステム）
■JIS Q 15001（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年と2004年の2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、独立したシステム管理基準として制定されました。

2018年4月、その後も進化し続ける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自己監査への対応などシステム監査ニーズの多様化、ITガバナンスの実現性の向上、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。

この改訂で、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となる組織能力である。」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こと
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こと

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部門に回ってく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。

今回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。

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。

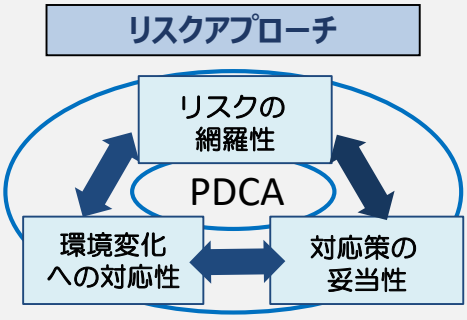
経営者にはシステム監査を経営に活かすという知見が必要ですし、システム監査人はこういった期待に応えることが重要です。

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になっています。

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」では無く、企業の実情及び組織目的に合わせて実施する「リスクアプローチ」をお勧めします。

「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）等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、あくまで組織として行う経営目的を達成するための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としており、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しています。



実践に当たってはまず、組織及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外部・内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及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無くすことが出来ます。

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格やルールなど）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、情報資産台帳、システム構成図、ネットワーク構成図、業務フロー等の整備から始まり、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、情報資産の重要度及び脅威と脆弱性による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。全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及びその影響は“想定内”になり、外部からは企業のリスク対応の**“妥当性”**として評価され、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等も踏まえ着実に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標準規格である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。

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。また、情報セキュリティに関するコントロールは日々変化していくものと見られます。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」が施行され、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。

これらの対策のひとつとして情報セキュリティ監査の役割は重要となっています。ところで、システム監査の中でも、情報セキュリティの監査項目を設定して監査を行います。情報セキュリティに関するコントロールが専門化・多様化していることから、新「システム管理基準」では、情報セキュリティについては、「情報セキュリティ管理基準」を参照するよう、記述しています。

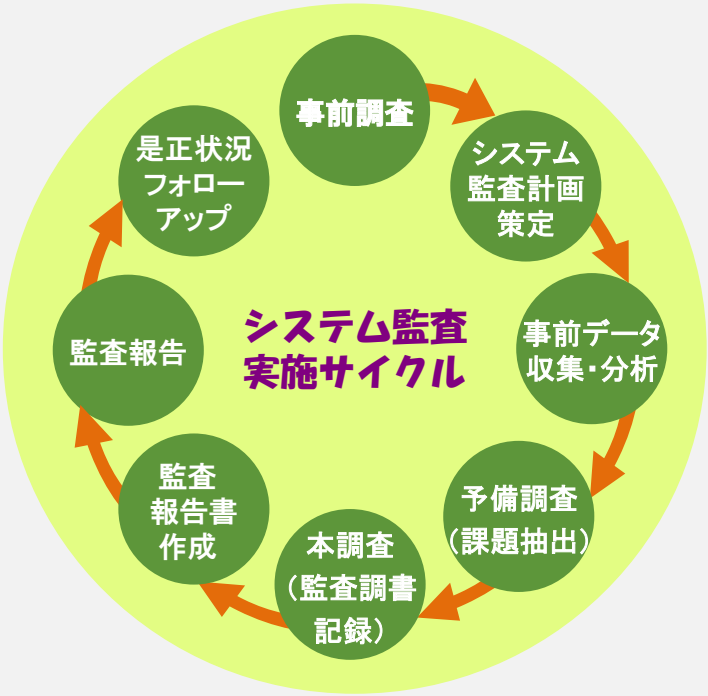
また、2018年2月28日に経済産業省が、「情報セキュリティサービス基準」を公表しました。これは、情報セキュリティに係るサービスが、一定の品質の維持向上が図られていることを第三者が客観的に判断し、公開することで、利用者が調達時に参照できるという制度です。この登録サービスの種類に「情報セキュリティ監査サービス」があります。監査サービスを行う企業や監査を受ける企業は必見です。

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、先方と的確、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。

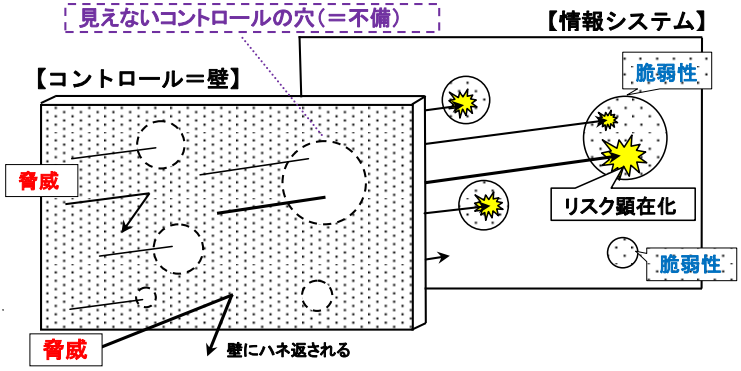
第12条 （自己研鑽）システム監査人は、システム監査を行うのに必要な専門能力および監査技術の向上に努めなければならない。

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

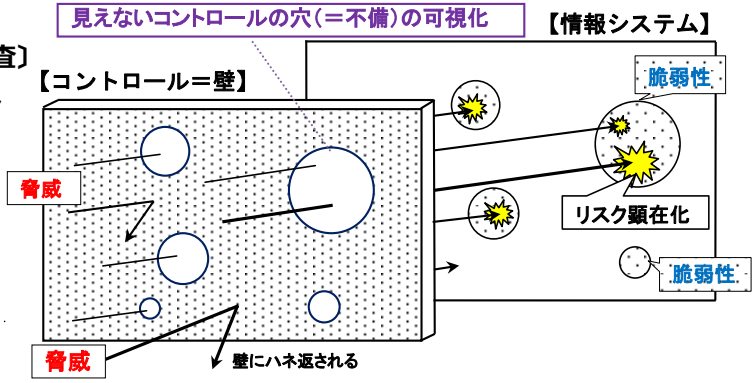
情報システムリスクは、「脅威」（リスクの源泉）と、情報システムの「脆弱性」（リスクの発生を許す弱点）が結びつかなければ、顕在化しません。

〔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]

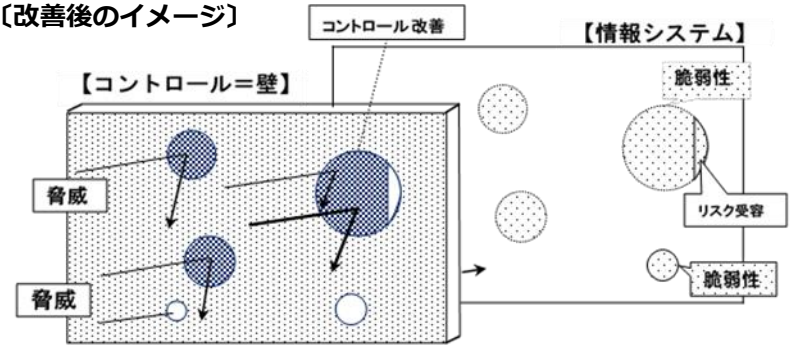


～システム監査人は発見したコントロールの穴を報告します

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)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

〔改善後のイメージ〕



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てくるでしょう。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労も伴うことであり、習得に喜びを持つ人がいる一方、苦労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。

公認システム監査人資格の取得

～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

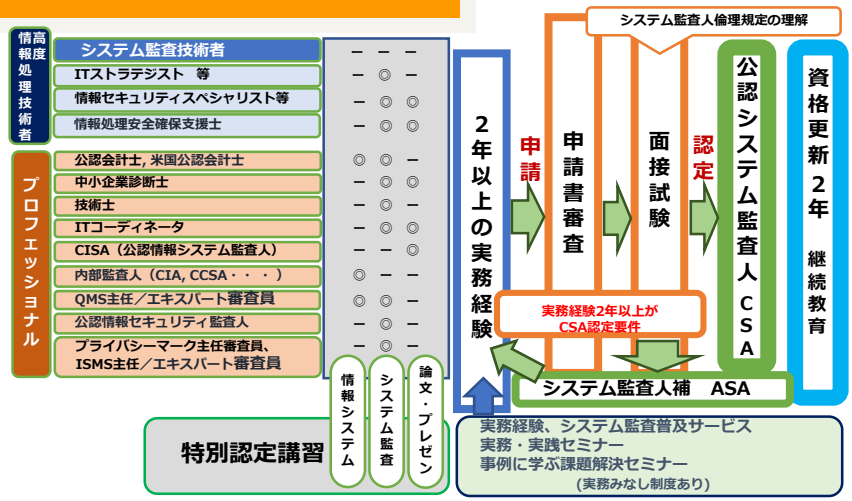
・資格継続には、継続的な実務及び教育受講が必須です。
・認定制度は1999年通商産業省（現経済産業省）の産業構造審議会・情報化人材対策小委員会の提言を受け誕生しました。

「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



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と、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。

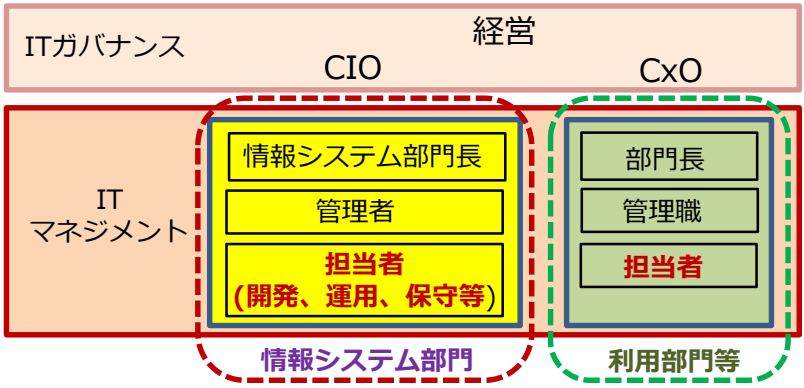
新しくなったシステム管理基準には、用語集があり、「情報システム」の概念が定義されました。これによれば、ITは、情報システムを構成する物質的人工物です。システム監査の対象は情報システムですが、それを構成する物質的人工物の技術そのものを監査するわけではありません。つまり、情報システムの構成要素として、その技術の特徴と情報システムでの使われ方、それを使うことのメリットとデメリットを最低限知っていればよいわけです。メリットはITガバナンスへの貢献、デメリットはリスクと捉えることができます。

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いても、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、講師の方と直接お話しもできます。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「システム監査実践セミナー」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の問題などから自ら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）について合意して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。監査テーマは「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、監査基準は「システム管理基準（2004年版）」の開発業務、共通業務の中のドキュメント管理、進捗管理、品質管理、人的資源管理、委託・受託に置きました。

監査基準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て、委託元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、自分たちも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。**

プロジェクト監査
～システム開発を成功させる鍵～

人気の医療ドラマでの「私　失敗しないので！」、自信たっぷりの女医の”決め台詞”、格好良いですね。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。システム開発もこうありたいものです。しかし実際の開発では、用意周到に準備しても、しばしば大トラブルになります。数十億円、数百億円の損害が出る事もめずらしくありません。優れたＰＭ、優れた開発チームであっても起きます。プロジェクト管理を徹底しても起きます。機能追加開発を高品質に続けてきたプロジェクトでも起きます。ではどうしたら良いか？

専門の監査人による「プロジェクト監査」をお勧めします。沢山のプロジェクトを診てきた監査人には、「このままでは外部設計は終わらない、半年は遅れる、抜本対策〇〇が必要」というように、プロジェクトの未来の姿と対処すべき事が見えます。

この監査レポートと助言を参考に、プロジェクトとして《先手先手》で対処すれば、大トラブルを防ぐことができます。«早期発見・早期対処»が成功の鍵です。プロジェクト監査はこれを支援します。

SAAJでは、「トラブルを未然防止するプロジェクト監査」をテーマにした研究会で、3年かけて「発注者のプロジェクトマネジメントと監査」という本を発刊しました。

この本のキーワードは、「システム開発トラブル未然防止」「発注者と受注者がWin/Winとなる」「PMの心強いアドバイザー」「現場を明るく照らす指南書」「システム開発を成功に導く監査」です。

開発現場で直ぐに活用できるように、詳細な図表を沢山載せ、具体的な事例等でトラブル未然防止のポイントを解説しています。プロジェクト監査の具体的な観点も豊富に掲載しています。

なお、SAAJでは、プロジェクト監査研究会を中心に、プロジェクト監査のガイドラインや詳細チェックリストについても研究を進めています。

「発注者のプロジェクトマネジメントと監査」
＜本の構成＞

導入部
- 1章　トラブル事例と教訓
- 2章　トラブル未然防止の基本
- 3章　受/発注それぞれの役割

発注者のプロジェクトマネジメント
- 4章　企画/要件定義/調達
- 5章　プロジェクト計画
- 6章　外部設計（仕様凍結が鍵）
- 7章　実装設計（高品質設計）
- 8章　プログラミング～結合テスト
- 9章　総合テスト～サービス開始
- 10章　実践的品質管理
- 11章　＜発注者視点＞のプロジェクトマネジメントの基本

成功に導く「プロジェクト監査」
- 12章　なぜプロジェクト監査が必要か
- 13章　企画フェーズの監査
- 14章　設計開発フェーズの監査
- 15章　サービス開始、効果検証の監査

参考：「発注者のプロジェクトマネジメントと監査」（同文館出版）
https://www.saaj.or.jp/shibu/130801PRJM2018Chirashi.pdf

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
～SaaSを利用したビジネスプロセスの整備にもつながる～

クラウドコンピューティングサービスの一形態であるSaaS（Software as a Service）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。

一方で、SaaS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SaaS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SaaS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SaaSを利用できないという問題を抱えています。

SaaS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。

SaaS事業者が講じるべき安全対策については、次ページの「クラウドセキュリティに関する規格、ガイド、基準など」に示したとおり、経済産業省が発表しているガイドラインをはじめとするいくつかの文書に記載されていますが、SaaS事業者が作成する契約書の内容とともに、利用者にはなかなか理解しにくいのが実情です。また、SaaS事業者だけでなく、利用者がやるべきこともあります。

そこで**お勧めしたいのが、SaaSの利用に関して、システム監査を実施することです。**

明確な基準に基づくSaaS事業者の選定、SaaS事業者と取り交わす契約書の内容、SaaSを利用する中での利用者とSaaS事業者との手続きや入手すべき情報などに関してシステム監査を実施し、クラウドサービス利用に関する知見をもったシステム監査人の客観的な評価、アドバイスを受けることです。安全面での不安を払拭し、安心してSaaSを利用できるだけでなく、SaaSを利用した効果的なビジネスプロセスの整備にもつながります。

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（2019/01現在）
ISO/IEC 27017	ISO/IEC	ISO/IEC 27001のクラウド対応版、2015年発行
クラウドセキュリティ認証（STAR認証）規格	イギリス BSI	STAR認証を受ける日本企業も現れている
クラウドサービス利用のための情報セキュリティマネジメントガイドライン	経済産業省	改訂版2013年版発行済
クラウドセキュリティガイドライン活用ガイドブック	経済産業省	初版2013年版発行済
・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） ・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 (*)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）
・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）	・2016年8月1日発行 ・2018年3月30日発行

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～

2006年6月に成立した金融商品取引法により、上場会社を対象に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（内部統制報告制度）、2008年4月１日以後開始する事業年度から適用されています。内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の４つ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、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及びIT（情報技術）への対応の６つの基本的要素から構成されます。

「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、内部統制の他の基本的要素と必ずしも独立に存在するものではないが、組織の業務内容がITに大きく依存している場合や組織の情報システムがITを高度に取り入れている場合等には、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、IT環境への対応とIT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、組織の管理が及ぶ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の利用及び統制とは、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、並びに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をいいます。

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.saaj.or.jp/shuppan/index.html

個人情報保護とシステム監査
～開発と運用の両面で厳しい監査が求められる時代に～

2017年5月30日に全面施行された新個人情報保護法では、「要配慮個人情報」として、人種、信条、社会的身分等について、より慎重な取り扱いが要求されるようになりました。一方、国の発展と生活の利便性向上に欠かせないビッグデータの活用のため、一定のルールに従って匿名加工した個人情報については、必ずしも本人の同意を得なくてもよいとの原則が明確にされています。

また、グローバルな情報流通社会の中で個人情報の自国外への移転も制約を受けます。新法では第24条（外国にある第三者への提供の制限）を設けています。EUでは「一般データ保護規則（GDPR）」が2018年5月に適用され、EU域外への個人情報移転について、厳格な制限が規定されています。同様にAPEC加盟国もそれぞれ法規制を持ちますが、電子商取引の活性化のための環境整備を目的に、APEC参加国・地域がAPEC/CBPR認証システムへの参加を同意し、CBPR認証を受けた事業者について個人情報の移転の適合性を認証するという仕組みが運用されています。

このように、個人情報に係る事件・事故が急増しその影響が計り知れない社会にあって、個人情報の安全な取扱いが、国際的に、且つ法的にも技術的にも厳しく求められています。

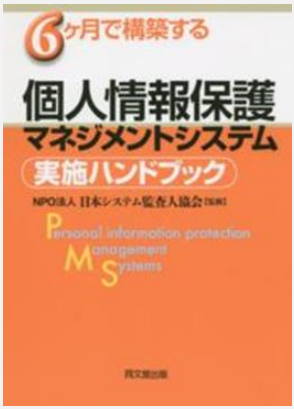
一方、個人情報を取扱うシステムの構築には、「プライバシー・バイ・デザイン」が求められます。この手法は、カナダのアン・カブキアン博士が1990年代から提唱しているコンセプトで、システム内に最初から個人情報の取扱いに関する高度な仕組みを織り込むことによって、利用者は安心して個人情報が提供でき、必要なサービスが受けられるというものです。個人情報の利用において、正確性と効率性が確保されるとともに、厳密かつ十分な安全性が確保されるべきであるという考えはすでに当たり前になっています。

さて、日本には海外でも高く評価されている「プライバシーマーク制度」があります。これは現在の一般財団法人日本情報経済社会推進協会（JIPDEC）が1998年4月に開始した制度で、認証要求規格は「JIS Q 15001個人情報保護マネジメントシステム要求事項」です。この規格に適合していると認証された事業者はPMS（Personal Information Protection Management Systems）を維持することにより、自社の個人情報の取り扱いが適切であることを、広く社会にアピールすることができます。

PMSのPDCAプロセスのうち、「C＝点検」としての内部監査では、PMSのJIS Q 15001への準拠性や現場の運用状況について監査します。特に情報システム運用面の監査では、個人情報の取り扱いについて、例えばアクセス制限、ログの管理、データの保管場所、保存期間等についてチェックします。最近は特に「授受記録」「廃棄・消去記録」の証跡に加え、サーバーのOSの入れ替え、委託先のデーターセンターの評価についても、安全性が確保されているかを厳しくチェックします。

個人に取り返しのつかない被害が及ばないよう、個人情報保護が重要な経営課題となっています。
そのためPMS構築と継続的な改善が必要です。

SAAJの個人情報保護監査研究会では2014年に右の書籍を刊行しました。
購入者には最新版の文書や様式のダウンロードを提供しています。ダウンロードには「監査チェックリスト」なども用意しシステム監査の一助としています。



「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』」（同文舘出版）https://www.saaj.or.jp/shuppan/index.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・オフィスビル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が多く、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、対策がとても遅れているのが現実です。システムの特殊性から、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

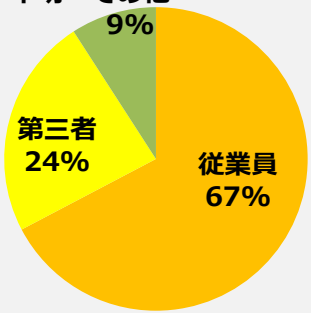
CSMS認証は、CSMS（IEC 62443-2-1）に基づいた第三者認証制度。情報セキュリティマネジメントシステムであるISMS適合性評価制度を運営するJIPDEC（一般財団法人日本情報経済社会推進協会）により、CSMS適合性評価制度として2014年にスタート。経済産業省が国際的に通用する認証基盤の確立のために実施した、「グローバル認証基盤整備事業」の一環。

注）現在CSMS認証制度は、ISMS-ACが運営

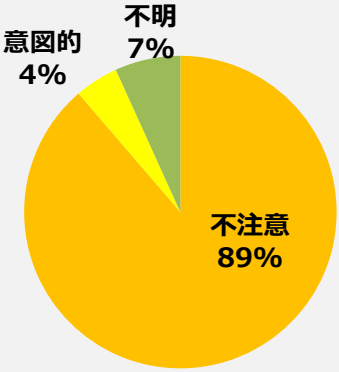
情報漏えい防止に役立つシステム監査
～自分たちでは気が付かない情報漏えい防止対策がある～

情報漏えい事故の原因の多くは、“人”に絡むもの、中でも組織体内部の“人”に絡むものです。下図の個人情報保護委員会のデータを見れば、そのことが明らかです。さらに、「従業者が起こした情報漏えい事故の原因区分」の内訳を見てみると、意図的な漏えい（不正行為）よりも、不注意によるものが圧倒的に多くなっています。ここから、いわゆる不注意のほか、知らなかった、気にとめなかったなど、“人”の無意識な行為による情報漏えいが大半であろうことが推測されます。

情報漏えい事故を起こした者の区分



従業者が起こした情報漏えい事故の原因区分



出典：2016年度個人情報の保護に関する法律施行状況の概要
（個人情報保護委員会、2017年11月）

そうした組織体内部の“人”の無意識な行為による情報漏えいを防ぐための対策には、どのようなものがあるでしょうか？

まずは、予防処置として、重要な情報を取り扱う人に意識や知識をもってもらうための教育や指導が必要です。事故を起こした場合の対処方法を明文化して周知を図ることも、事故の影響を小さく抑えるために、組織体としては必要なことです。

さらに有効な対策が、“人”の無意識な行為が情報漏えいにつながらないための仕組みの整備です。人は間違いを犯す存在であることを前提にした技術的な仕組みを作る必要があるのです。具体的には、アクセス制御、無意識に行った不適切な行為をその場で発見する仕組み、万が一に備えた重要情報の暗号化やバックアップなどです。

こうした技術的対策は進歩が速く、また、組織体の業務環境・情報環境によって効果に差が出ますので、一律に適用することはできません。自分たちは良いと思って適用した対策が最善ではなく、気が付かないだけで実はより効果的で経済的な対策があるというケースも多くあります。

そこで、システム監査の実施をお勧めします。システム監査を実施することで、組織体が行っている、あるいは行おうとしている情報漏えいのための人的対策、運用面の対策、技術的対策が十分か、組織体の実態に則しているか、もっと良い方法がないかなどについて、情報漏えい対策に精通したシステム監査人の客観的な評価とアドバイスを受けられます。

システム監査の実施が、
情報漏えいの防止に有効なのです。

システム監査人の新たな活躍の場
～DXレポートとシステム監査～
（SAAJ会報213号より再編転載）

～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を活用していくだけではなく、足元の既存システムをしっかり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などを挙げています。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に貢献できるといいですね。

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。

社会は早晩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。

SAAJの今後の取り組み
～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、情報処理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、活躍頂いているところです。

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貌してきました。その要請は、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：
キャッシュレス決済、デジタルトランスフォーメーション（DX)、Society 5.0、働き方改革　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

◎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、IoT、AI、ビッグデータ、RPA　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、以下の活動を今後も進めて参ります。

・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２－８－８
共同ビル（市場通り）6階
Tel：03-3666-6341 Fax：03-3666-6342
URL: http://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

目次

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

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