システム監査と情報セキュリティ監査の違いと関連　１０のＱ＆Ａ

Ｑ１（目的）：システム監査と情報セキュリティ監査は、目的がどのように違うのでしょうか？

Ａ１：「システム監査基準解説書」では、システム監査の目的を「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、独立かつ客観的な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い、もって IT ガバナンスの実現に寄与すること」と述べています。

一方、「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同じですが、リスクとコントロールの対象が違うといえます。システム監査は情報システムを対象にリスクとコントロールをとらえ、情報セキュリティ監査では情報資産を対象にリスクとコントロールをとらえます。

これは、それぞれの監査の社会的役割の違いということもできます。システム監査は、組織体が社会的使命・責任を果たすうえで情報システムが健全に機能しているかを評価します。健全に機能しているかとは、情報システムが組織体の目的に合致した形で構築・運用されているか、情報システムに対する投資効率が適切か、組織体が活動を行ううえで情報システムの信頼性・安全性・効率性が確保されているかといったことになります。システム監査では“IT ガバナンスの実現に寄与する”ことが最終目的になっており、IT を活用した組織経営・運営に密接に係わるリスクとコントロールの整備への貢献を目的にしています。

一方、情報セキュリティ監査は組織体が管理・活用する責任を負っている情報資産を適切に管理・活用しているかを評価します。情報資産が適切に管理・活用されているかとは、Ｑ３で説明する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ということになります。

組織体の長の立場に立つと、経営資源を投下して構築・運用する情報システムが組織体のためになっているかを評価するのがシステム監査、組織体が情報資産を決めごとに従って目的通りに管理・活用しているかを評価するのが情報セキュリティ監査といえます。

ただし、情報資産の管理に情報システムを利用しており、情報システムを管理するために存在する情報資産を多いことから、両者の境界線を厳密に引くことはできないのが実情といえます。

Ｑ２（範囲・対象）: システム監査と情報セキュリティ監査の範囲はどのように違うのでしょうか？

Ａ２：「システム監査基準解説書」の P.20 に、次のような解説があります。

「システム監査と情報セキュリティ監査の違いは次のとおりである。システム監査は、情報システムのライフサイクルを通じて実施する総合的な監査であるのに対して、情報セキュリティ監査は、情報セキュリティに特化した監査である。」

この解説とＡ１の説明を合わせて考えると、システム監査は情報システムのライフサイクル（情報戦略の策定から、企画、開発、運用、保守）の適切性に対する監査であり、情報セキュリティ監査は、情報資産のライフサイクル（発生・入手から保管、利用、廃棄）の適切性に対する監査であるといえます。

情報資産のライフサイクルを管理するうえで情報システムを利用し、情報システムのライフサイクルを管理するさまざまな情報資産が発生するのは、Ａ１で説明した通りです。

Ｑ３（範囲・対象）:「システム監査基準解説書」にある「情報セキュリティは、情報セキュリティに特化した監査」を、もう少し詳しく説明していただくと、どういうことでしょうか？

Ａ３：情報セキュリティマネジメントシステムの国際規格である ISO/IEC 27001（日本では、JIS Q 27001：2006 として国内規格化されている）では、「情報セキュリティとは、情報資産の『機密性』『完全性』『可用性』が維持されていることを保証すること」と定義しています。

つまり、情報セキュリティ監査は、情報資産のライフサイクル全体における、機密性･完全性･可用性が確保されているかどうかに関する監査ということになります。これが、「情報セキュリティに特化した」の意味です。

なお、システム監査は情報システムのライフサイクル全体において『安全性』、『信頼性』、『効率性』を点検・評価するといわれていますが、情報資産の機密性・完全性・可用性は、情報システムの評価の視点としては『安全性』に分類される（特化している）といえます。

Ｑ４（範囲・対象）:「システム監査と情報セキュリティ監査は同じものだ」という意見がありますが、それは間違いということになりますか？

Ａ４：Ａ１からＡ３で説明してきたように、システム監査と情報セキュリティ監査は目的や対象、範囲が違いますので、同じものということはありません。

それは、経済産業省が「システム監査基準」と「情報セキュリティ監査基準」、およびそれぞれの監査における監査人の判断基準となる「システム管理基準」と「情報セキュリティ管理基準」を分けて公表していることからも、明らかです。

ただし、前述の繰り返しになりますが、両者の境界線が明確に設定できないことも事実です。

Ｑ５（範囲・対象）: では、システム監査と情報セキュリティ監査は、まったく違うものなのでしょうか？

Ａ５：今まで説明してきたように、目的、範囲・対象が違いますので別のものと考えるのが適切です。ただし、両者のオーバーラップする部分が多いことも、説明してきた通りです。

「システム監査基準」の「Ⅳ．実施基準」に「６．情報セキュリティ」があり、「情報セキュリティ監査については、原則として、情報セキュリティ管理基準を活用することが望ましい。」と、書かれています。このことは、システム監査の中で情報セキュリティについての監査を行う場合があるが、その場合には、「システム管理基準」とは別に定めている「情報セキュリティ管理基準」を活用することが有効であるということで、システム監査を実施する中で情報セキュリティに監査を行うことが多々あることを示しています。

同じように、情報セキュリティ監査を行う中で、情報資産の管理を情報システムで行っているので、情報システムの保守業務の信頼性をシステム監査するといったことは当然のこととしてあります。

Ｑ６（範囲・対象）:「システム監査基準解説書」の中に「システム監査は・・・総合的な監査である」という記述がありますが、「総合的な」とはどのような意味なのでしょうか？

Ａ６：「システム監査基準解説書」の P.52 に、「システム監査は、企画・開発・運用・保守という情報システムのライフサイクルに従って、特に情報システム構築・運用の全体最適化を目的とした監査であり、・・・」という解説があります。

例を挙げてみると、システム企画の内容が経営目的と合致しているか（有効性）、システム開発が標準化された手順に従って実施され品質の高いソフトウェアを実現しているか（信頼性）、システム運用に無駄がなく適切なコストで行われているか（経済性）、システム保守手続きが明確になっておりタイムリーかつ確実にシステム修正が行われているか（効率性）、など、システム監査の対象は広範囲であることが分かります。こうした広範囲の視点で情報システムを監査したうえで、その結果を踏まえて助言あるいは保証意見を述べることを「総合的」といっています。

このことは情報セキュリティ監査よりも明確であり、システム監査の視点は「総合的」、情報セキュリティ監査の視点は「特化」といえます。

Ｑ７（範囲・対象）：システム監査は情報システムだけを対象にし、情報セキュリティ監査は情報システム以外も対象にする、という意見がありますが、どういうことでしょうか？

Ａ７：経済産業省が情報セキュリティ監査制度を立ち上げたときの説明資料にもありましたし、「システム監査基準解説書」の P.52 にも、同じ解説が書かれています。
情報システム以外とは、紙媒体の情報、人などが対象になると思いますが、これらがシステム監査の対象でないとは、いいきれません。たとえば、経営者が定め明文化した経営戦略が情報システムに関係がないかというと、上述の有効性をシステム監査で確認しようとすれば、経営戦略を監査対象にしなければなりません。
また、仕事で PC をまったく使っていない作業員も、情報システムから提供される資料や情報を使って仕事をしていれば、監査対象でないとはいいきれません。
情報システムが業務活動を支える重要なインフラとなっている現在、「情報システム以外」という考え方は、あまり意味をもたなくなってきているといえます。

Ｑ８（手続き）：システム監査と情報セキュリティ監査では、監査手続きに大きな違いがあるのでしょうか？

Ａ８：監査手続きに大きな違いはありません。「システム監査基準」に、システム監査を実施するための手順と留意点が書かれています。また、「情報セキュリティ監査基準」に、情報セキュリティ監査を実施するための手順と留意点が書かれています。その両者の内容に大きな違いはありません。
あえて違いを上げるとすれば、システム監査はヒアリングや文書確認を中心にした準拠性監査の手続きが比較的多く、情報セキュリティ監査は現地確認や記録確認などの実証性監査の手続きを比較的多く採ります。また、伝統的なコンピュータを使った監査手法（CAAT）は、システム処理の正当性を確認する目的でシステム監査で用いられることが多かったのですが、最近では、ネットワークペネトレーションテスト、ログ分析、デジタルフォレンジックなど、情報セキュリティ監査における IT 活用も増えてきています。

Ｑ９（基準）：システム監査で評価・判断するための基準は「システム管理基準」、情報セキュリティ監査で評価・判断するための基準は「情報セキュリティ管理基準」ということでしょうか？

Ａ９：システム監査、情報セキュリティ監査で評価・判断のために利用できる基準は、いろいろと公表されていますが、ご指摘の経済産業省が公表している２つの管理基準は、もっとも多く用いられている基準といえます。
これらの基準をベースに、他の基準も参考にして、自社としてのシステム監査、情報セキュリティ監査の基準を作っておくことが重要です。
また、注意しなければいけない点として、これらの２つの基準の主目的は、システム管理者が有効なシステムライフサイクル管理を行うための基準、情報セキュリティ管理者が有効な情報セキュリティマネジメントシステムを構築・運用するための基準であるということです。したがって、望ましい姿は、情報システムのライフサ

イクルが「システム管理基準」に従って管理されている、情報資産のライフサイクルが「情報セキュリティ管理基準」に従って管理されている、という状況の下で、システム監査人、情報セキュリティ監査人は同じ基準を判断尺度にして、それぞれの管理状況の適切性を評価することです。
そのことを理解したうえで、システム監査人、情報セキュリティ監査人が、これらの基準を利用することが重要です。

Ｑ１０（監査人・監査体制）: システム監査人、情報セキュリティ監査人には、まったく違う知識・スキルが要求されるのでしょうか？また、システム監査と情報セキュリティ監査で監査体制に違いがありますか？

Ａ１０：要求される知識・スキルの違いは、それぞれの監査の範囲・対象をカバーできるかどうかということです。一般的にいって、システム監査人には情報システム全般についての幅広い知識と監査スキルが求められ、情報セキュリティ監査人には技術的な分野も含めた情報セキュリティについての深い知識と監査スキルが求められるといえます。システム監査人で情報セキュリティ監査のできる人もいますが、システム監査の中で情報セキュリティの監査を行う場合には、情報セキュリティについての知識をもった専門家の力を借りることもあります。そのことは、システム監査基準の実施基準「５．他の専門家の利用」でもいっていることです。
技術的スキルについてはお互いに補完し合う姿勢が大事です。
監査実施体制において、それぞれの監査で特別に考慮しなければならないことはありません。