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
～情報社会では、システム監査が不可欠～

現代は情報社会と言われています。例えば、“会社に着いて、一日の仕事の最初にすることは自分のパソコンの電源を入れること、一日の仕事の終わりはパソコンの電源を切ること”という毎日がそのことを示しています。つまり、今日の仕事は情報システム無しではあり得ないということです。

一方、世の中ではその仕事を対象にいろいろな監査が実施されています。例えば、会計監査、業務監査、経営監査、監査役監査、監事監査、個人情報保護監査、環境監査・・・。

これらの監査においては、監査対象や監査人の視点は異なりますが、多くの場合、情報システムの基盤の上で行われている仕事（業務・ビジネス）のありようをその対象としており、**どの監査においてもその監査対象を支える情報システムにも目を向けなければならないことは明らかです。**例えば上場企業に法律で義務付けられている会計監査では、会計情報システムの評価（IT統制監査と言います）が欠かせないのはその典型的一例です。

こう考えると、システム監査（システム監査と銘打って実施される場合の外、他の監査の中でその一部として行われるシステム監査を含む）は、今日の情報社会に不可欠な監査であると言えます。

2016年よりマイナンバー制度が始まり、マイナンバーはIT（情報技術）によって利活用されていきます。ITは、仕事（業務・ビジネス）の世界から広がって一般市民の生活にかかわってきています。システム監査は、企業、団体さらに社会が、ITの利活用においてリスクに応じたコントロールを適切に整備・運用しているか、また情報システムがその目的に照らして有効であるかを監査し、経営者や責任者の方へ報告を行う役割を担っています。

しかしながら、システム監査には馴染みの無い方も多いようです。そこで、ここにシステム監査をご理解いただくための小冊子を作成しました。ご一読いただき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。

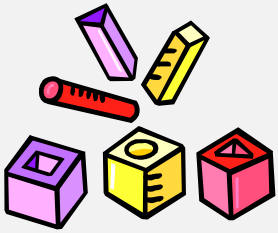
一方、企業内部で不適切な業務処理が行われ、大きな損失が発生することがないように行われる業務監査は、不適切なところを指摘して改善を促す助言型監査になり、一般的には内部監査として行われます。

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。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

システム監査とは、業務で使用されている情報処理システム（以下、情報システム）を対象に、経営に役立っているか、または組織体内外に対して信頼性が維持されているかなどを監査することです。

その結果として組織体の「ITガバナンス」の実現や情報システムにまつわる「リスク」に対する「コントロール」が適切に整備・運用されていることの説明責任を果たすことに寄与することになります。リスクに対するコントロールの目的は、「システム監査基準」に次のように示されています。

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

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です。

システム監査の目的

システム監査の目的は、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、独立かつ専門的な立場のシステム監査人が検証また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にある。　（システム監査基準―2004年版―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	• システム開発段階の監査 • 運用段階における効率性の監査　など
テーマ別監査	• 個人情報保護体制の監査 • 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 • 外部委託による保守体制の監査　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、開発段階の監査はできません。システムが稼働してから、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、近年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、次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。

情報セキュリティ監査とは

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。

上に述べたように、情報セキュリティ監査は、情報資産の管理・活用に責任を負っている組織体が、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。

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も多いことから、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。

監査手続きにも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、従来は、コンピュータを使った監査手法は、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、ネットワークセキュリティ検査やWEBアプリケーション検査を行う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。

たとえば、WEBアプリケーション検査では、クロスサイトスクリプティング、SQLインジェクション、セッション管理、バッファオーバーフロー等の診断などを行います。

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、経済産業省が発行している「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監査人の行為規範（倫理規定）、②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。

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次頁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。

システム監査のためのもしくはシステム監査に利用できる主な基準
■システム監査基準（経済産業省 2004年改訂）
■システム管理基準（経済産業省 2004年策定）
■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月策定）
■情報セキュリティ監査基準（経済産業省 2003年策定）
■情報セキュリティ管理基準（経済産業省 2015年改定案公表） ■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）
■コンピュータウイルス対策基準（経済産業省 2000年12月改定）
■コンピュータ不正アクセス対策基準（経済産業省 2000年改定）
■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 2015年3月改定）
■金融機関等のシステム監査指針（FISC 2014年3月改訂） ■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 （FISC 2015年6月改訂）
■COBIT5：Control Objectives for Information- related Technology （米ISACA 2012年4月公表）
■JIS Q 19011（マネジメントシステム監査のための指針）
■JIS Q 9001（品質マネジメントシステム）
■JIS Q 27001（情報セキュリティ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 15001（個人情報保護マネジメントシステム）
■JIS Q 38500（ITガバナンス）
■JIS Q 27014（情報セキュリティガバナンス）
■JIS Q 31000（リスクマネジメント―原則及び指針）

システム監査とＩＴガバナンス
～ JIS Q 38500 の有効活用～

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。ISO では 2008 年に「ISO/IEC38500」第１版が、2015年 2月に第 2 版が発行されております。JISはISO の発行から少し遅れましたが、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昨今、この機会にJIS Q 38500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。

この規格では、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、規格は、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

出典：「JIS Q 38500:2015」本文より抜粋、加工

JIS Q 38500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。

システム監査人にとっても、システム管理基準に準拠してシステムの戦略性や有効性の監査を行うに当たり、指針とするべき規格になります。経営陣、システム監査人ともにJIS Q 38500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
～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分野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。（「システム監査とは」から再掲）

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

つまり現代では、システム監査には、情報システムによる組織体（社会）の目的の実現や情報システムのリスクに対するコントロールを検証・評価することが期待されています。

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**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
- IT戦略としての誤り、コスト回収不足
- 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

システム監査ではこういったさまざまな情報システムにかかわるリスクに対する「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。

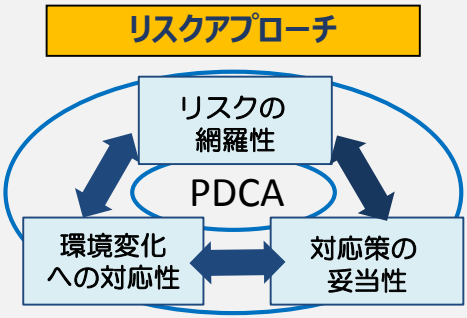
経営者にはシステム監査を経営に活かすという知見が必要ですし、システム監査人はこういった期待に応えることが重要です。

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～

2011年3月11日の東日本大震災から5年になりますが、関連して発生した原子力発電所の事故も含めて、当時は“想定外”との説明が多く見受けられました。しかしながら、企業における財務報告に係る内部統制の構築や事業継続計画(BCP)の作成を通じて、次第にリスクの捉え方がより明確になってくるとともに、リスクの特定・分析・評価や対応策・モニタリングの仕組みが定着してきました。

システム監査においてもシステムリスクへの対応が重要な視点の一つになっていますが、一般的には、システム管理基準等による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」が行なわれています。しかし、企業により置かれている外部・内部環境は異なっており、取るべき対応策の最適解も異なってきます。また場合によっては企業固有のリスクが見過ごされ、“想定外”として発生する可能性があります。

そこで、発生リスクから“想定外”をなくしていくために、あらためて、リスクアセスメント及びリスク対応のプロセスを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。



このプロセスを初めて実施する際には、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、相当な工数と時間を要します。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、適切な対応策が取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、経営者が積極的に関与し、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、経営者としても説明責任を果たせることになります。

また、「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。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事も有効です。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ります。

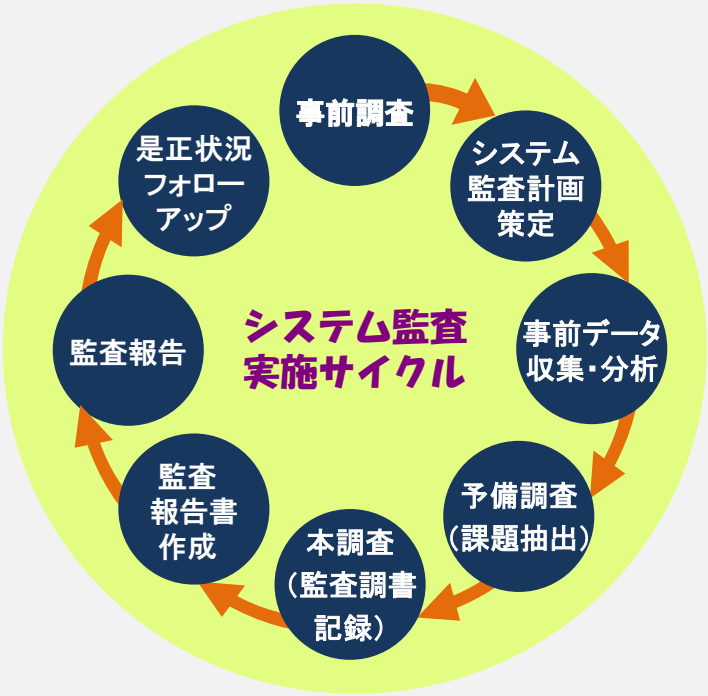
「リスクアプローチ」については、例えば、ISO/IEC 27005（情報セキュリティのリスクマネジメント）やJIS Q 31000（リスクマネジメント－原則及び指針）の解説書等に手順が示されています。これらを参考に、自社に合わせた実行可能な手順を規定していくことが全社的な「リスクアプローチ」の第一歩となります。

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でしょう。

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IT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、ITリスクの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。

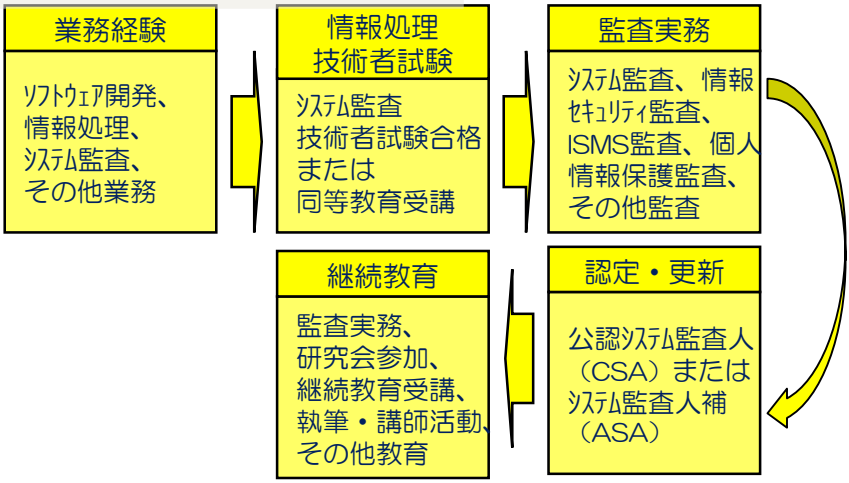
- システム監査技術者試験合格者もしくは同等の能力を有し、且つ一定の実務経験を重ねた者をSAAJが認定。実務経験については小論文と面接で審査します。
- 資格継続には、継続的な実務及び教育受講が必須です。
- 認定制度は１９９９年通商産業省（現経済産業省）の産業構造審議会・情報化人材対策小委員会の提言を受け誕生しました。

「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い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」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、

- 委託元に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

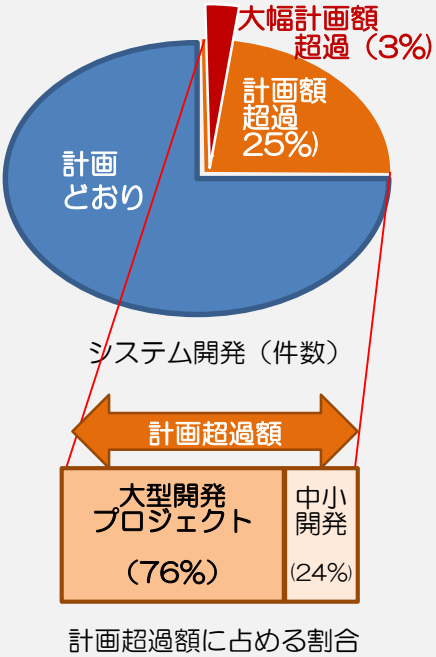
- **外部委託管理の監査では、委託元、委託先の双方に対して調査が必要である。**
- **外部委託で問題があれば、委託元、委託先双方に問題があると考えた方がよい。**
- **外部委託は、委託元、委託先双方が基本的行動をとることから始まることを、双方に理解してもらうという観点での改善指摘が重要である。**

システム監査の効果的活用
～システム開発プロジェクトマネジメントの監査～

ある調査によると、情報システム開発プロジェクトの25%が計画額を超過し、超過額の76%を大型開発プロジェクトが占めているそうです。トラブルプロジェクトでは超過額が億円単位になることも珍しくないので、その撲滅は、会社全体の収支改善の重要課題でもあります。

では、どうやって撲滅するか？

PM教育、PMO※充実、開発標準の徹底など、やるべきことはいろいろありますが、「システム監査」の実施は、特に効果があります。監査すると、「危ないな、このまま行くとトラブルになる」ということが見えるからです。



※PMO:Project Management Office

トラブルプロジェクトの多くは、トラブルになるべくしてトラブルに陥っています。無理な計画、リスク対策不足、外部設計の品質問題、プログラム品質の問題、プロジェクトマネジメントの問題等々、原因は様々ですが、トラブルに陥るプロジェクトと計画通り成功するプロジェクトでは、明らかな差があります。

システム監査で、それらの問題を早く炙り出して、早く対処すれば、立て直すことが出来ます。

トラブルを未然防止する鍵は≪早期発見・早期対処≫です。“火事は小火のうちに消せ”と同じです。これが、システム監査の効用です。

計画超過額の7割以上を占める大型開発については、特に、システム監査を実施する必要があります。大型開発でのトラブルは、超過額も巨額に上るからです。このようにシステム監査を徹底し、大トラブルの発生を撲滅したことで、会社全体で大幅な黒字を計上した例もあります。

では、システム監査を誰がいつやるのか？

システム監査は「プロジェクト当事者以外の第三者による監査」が原則です。出来れば、公的資格をもった専門家による監査をお勧めします。たくさんのプロジェクトを見てきた専門家には、そのプロジェクトの危うさ／大丈夫さのレベルを見抜く力があります。

監査の時期はプロジェクトの特性により、決めます。トラブルを未然に防止するには、開発終了時に監査するのでは遅すぎるので、計画段階や作業途中段階で監査し、改善点を提言するのが良いでしょう。先手先手で監査し改善点を見出す必要から、あらかじめ計画に組み込み、多忙なプロジェクトメンバーに過度の負担をかけない工夫が必要です。

監査の指摘事項、是正指示に真摯に対処することで、プロジェクトは成功に向かいます。プロジェクト計画の監査や、主要な工程ごとの監査で、≪早期発見・早期対処≫することで、プロジェクトを成功に導いて欲しいと思います。

組織から独立した外部監査の有効活用
～大手証券会社の誤発注事例から学ぶ外部監査の必要性～

ヒューマンエラーを排除することは難しく、ときに一人のミスが事業継続を脅かすような大事故に繋がることがあります。2005年に起きた大手証券会社による大量誤発注問題では、担当者の入力ミスが原因で、短時間に企業に400億円もの損害を与えました。

2005年12月、東証マザーズ市場に新規上場した某社の株式売買において、証券会社の担当者が1株61万円の売り注文を、誤って61万株1円とコンピュータに入力しました。その時、異常を知らせるメッセージが画面上に表示されましたが、担当者はいつものことと無視をして注文を完了させました。これにより大量の売り注文が発生し株価は急落。鵜の目鷹の目のトレーダーは見逃すはずはなく、大量の買い注文を入れました。証券会社では誤りであることに気付き、慌てて注文取消を行うも、証券取引所の株式売買システムに不具合があり受付けられず、止む無く証券会社は発注した全株式の買戻しを行いました。この間わずか16分、証券会社は一瞬にして400億円もの損害を被ることになりました。また事故後、証券会社と証券取引所が損害賠償額責任などをめぐり最高裁まで持ち込み争っていた裁判は、2015年9月にやっと判決が確定しました。

この事故では、株式価格と数量を反対に入力してしまい、それを未然に発見し、阻止することができませんでした。

もし、1円という異常な注文をブロックする仕組みがプログラムに組み込まれていれば、また、一定の規模を超える注文は管理者が承認する手続きになっていたなら、この事故は起こらなかったかも知れません。一方で、証券会社内には売買手続きを、できるだけシンプルにして取引スピードを上げたいという強いニーズもありました。さらに、ITを駆使した高速取引などにより株式市場が変化するなか、誤発注リスクも日増しに大きくなっていましたが、ルールや手続きを変更できないという内部事情があったようです。

このような時こそ、**組織から独立した外部のシステム監査人の活用をお勧めします。**今までのリスク対策で十分かどうか、システムの利用・管理態勢を第三者の目線で評価し、必要な改善点について助言を受けることができます。

組織の仕組みは一度確立されると変えづらいものです。一方で環境変化は絶えず起きており、殊にIT技術の発展は止まる所を知りません。AI技術の進歩により機械が自ら考える時代もすぐそこにきています。時流を把握した外部の監査人が、組織のしがらみのないところで意見を述べることで、組織変革の大きなきっかけになることもあるのです。

システム監査人の新たな活躍の場としてのプライバシー・バイ・デザイン

最近注目されている、システム監査人の新たな活躍の場のひとつを紹介します。

「プライバシー・バイ・デザイン」とは、カナダ・オンタリオ州のプライバシー・コミッショナーであるアン・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、情報システムの設計段階から個人情報の保護を検討し、必要な機能を実装するという考え方です。

近年急速に重要性が増してきた個人情報保護の問題は、それに対する配慮なしに開発されてきた既存のシステム、あるいは、その延長上にある新規システム開発において、事後的に生じた問題であるために、システムを開発し運用する事業者の側からみると、後発的に生じたリスクであり、これらの対処はコスト増という認識しかなく、できれば、避けて通りたい問題でありました。一方、個人情報を提供する消費者（個人）の側から見ると、自身の個人情報が不当に取り扱われる、例えば提供した当初の利用目的外の利用をされる、あるいは無断で第三者に提供されるという不安に怯えつつも、自身の個人情報を提供しないと必要なサービスが受けられないので、やむなく提供するというのが実状でした。

プライバシー・バイ・デザインは、これら消費者（個人）と事業者双方に「WIN-WINの関係」を実現しようというものです。

つまり、システムやプロセスの設計段階でテクノロジーを活用し、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取り入れることによって、消費者（個人）にとっては無用な負担なく、かつ、安心して個人情報が提供でき、必要なサービスの提供が受けられるようになります。

また、事業者にとっては、管理すべき個人情報を必要最小限に抑え、無用な手続きを無くし、かつ、高度な利用ができるということになります。この実現のためには、システムのプライバシー影響評価（PIA：Privacy Impact Assessment）が必要になります。

PIAは、システム開発の早い時期、すなわち、開発・設計段階で個人情報の保護に関するシステム上のリスクを洗い出し、その対策を検討・評価するものです。ここに、**システム監査における開発フェーズの監査の技法が活きてきます。**

なお、2016年1月1日から本格的に運用が開始されたマイナンバー制度を規定する法律、番号利用法（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年五月三十一日法律第二十七号、2015年9月9日改正））には、PIAの考え方が取り入れられていて、その第28条に、行政機関の長（市町村長等）は、マイナンバーを含むデータが記録されているファイルを保有しようとするときは、当該ファイルを保有する前に、影響評価を実施しなければいけない旨が規定されています。「プライバシー影響評価」という文言そのものは用いられておりませんが、趣旨は同じものです。この条文にもとづき、各自治体では、すでにPIAを実施しております。

デジタルネットワーク社会の進展にともない、プライバシー・バイ・デザインの考え方は、いずれ間違いなくシステム開発における基本的なコンセプトとして普及していくでしょう。プライバシー・バイ・デザインが普及した暁には、その重要なプロセスである**PIAは、システム監査人の新たな活躍の場になると思われます。**

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～

2015年９月９日に改正された新個人情報保護法では、新たに、「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利用のため、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、同時期に改正された個人番号利用法に基づき、個人のライフサイクルのあらゆる分野で個人番号の取り扱いがはじまりました。自治体における文書の取り扱いが簡略化されるに伴い、情報システムの安全性がより厳しく求められています。

欧米社会で提唱されている「プライバシー・バイ・デザイン」の考え方は、日本においては、 現在「医療情報システムの安全管理に関するガイドライン」、「金融機関等コンピュータシステムの安全対策基準」等で示されています。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。

また、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）が経済産業省の指導により1998年4月1日から運用を開始した制度で、現在の規格は「JIS Q 15001 個人情報保護マネジメントシステム要求事項：2006」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）を維持していくことにより、自社の個人情報の取り扱いが適切なものであることを、広く社会にアピールすることができます。

PMSのプロセスのうち、「C＝点検」としての内部監査では、PMSがJIS Q 15001に準拠していることを監査するとともに、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。

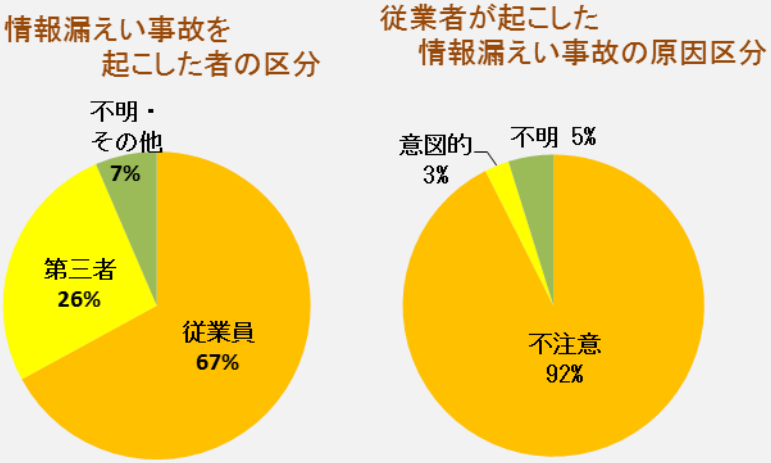
個人に取り返しのつかない被害が及ばないよう、開発と運用の両面で、個人情報保護の観点での厳しい監査が求められる時代となってきました。今後個人情報保護の法整備が行われる中で、システム監査人は、個人情報保護の知見が陳腐化しないよう、日々の研鑽が必要なことは言うまでもありません。

※SAAJの個人情報保護監査研究会では、「情報システム開発の監査チェックリスト」を用意しており、システム構築における個人情報保護の監査に役立てることができます。以下はチェックリストの例で、目的に沿って、適宜変更して用います。

8.2 本人の権利・利益の保護（6）	
(1) 個人情報システムは、個人情報の取得に当って、利用目的を明示し、利用目的の偽りなどにならない措置を講じること。	① 個人情報システムは、個人情報を取得する画面の利用目的の表示が、偽りの表示になっていないこと。
	② 個人情報システムは、個人情報を取得する画面の利用目的の表示が、正しくかつできるだけ具体的な表示、例えば、その取り扱う事業内容を勘案して顧客の種類ごとに利用目的を限定して示すなど、本人にとって明確な表示になっていること。
	③ 個人情報システムは、個人情報の取得元又はその取得方法（取得源の種類等）を可能な限り具体的に表示していること。

情報漏えい防止に有効なシステム監査
～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。下図の消費者庁のデータを見れば、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。



出典：2014年度個人情報の保護に関する法律施行状況の概要
（消費者庁、2015年10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。

効果的かつ安心してSaaSを利用するためのシステム監査の実施
～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、大きな注目を集めています。

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。**

明確な選定基準に基づく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（2016/01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	日本セキュリティ監査協会ー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
クラウド・セキュリティ・ガイダンス	国際団体 CSA（クラウドセキュリティアライアンス）	ガイダンス V3.0日本語版（2013年5月発行）
クラウドセキュリティ認証の要件、ガイドライン等を整備	JIPDEC	2016年夏予定

SAAJの今後の取り組み
～情報システムの改善に取り組むすべての方へのSAAJからのメッセージ～

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）の認証を頂き、2015年6月には東京都のNPO法人審査を得て、認定NPO法人に認められました。また、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輩出しているところです。

一方、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。

◎社会制度の変化：

J-Sox制度、マイナンバー制度、電子政府・電子自治体の推進、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

◎サイバー攻撃の多様化：

標的型攻撃、Webサービスからの機密情報搾取など、ますます複雑化・多様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、それに伴うBYOD（Bring Your Own Device）の普及、など

そこでSAAJでは、システム監査を核にした“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、以下の活動を進めて参ります。

- ITの構築、運用及び利活用などの評価、助言、コンサルティング
- ITガバナンスなどに関する経営者や管理者への評価、助言
- ITに関する各種監査；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、ISO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、システム監査人補を認定
●2015年に認定特定非営利活動法人（認定NPO法人）化

主な部会・研究会

- システム監査基準研究会 ：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
- 月例研究会 ：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実施
- 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
- プロジェクトマネジメントのシステム監査研究会：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
- CSAフォーラム：公認システム監査人（CSA）の交流のための場
- 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実施

〒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

2014年2月21日 初版発行
2016年2月22日 改定１版発行

発行者　認定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、法人部会