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～

特定非営利活動法人 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”という毎日がその実際を示しています。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。

しかしながら、システム監査にはなじみのな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。

特定非営利活動法人日本システム監査人協会（SAAJ）

目　次

入門編

✓ 監査とは 1

✓ システム監査とは 3

✓ システム監査に適用される基準とは 5
～システム監査における判断の拠りどころ～

✓ システム監査人に求められる能力とは 7

✓ システム監査人の思考回路（一例） 9
～チェックリストを超える柔軟さを身近な事例から～

✓ システム監査人を目指すということ 10
～システム監査経験を通じ、将来の能力発揮場面を拓く～

応用編

✓ システム監査への期待 11

✓ 身近な“システム障害管理” その目的を今一度 13
～システム監査の視点で、経営に貢献する障害管理へ～

✓ システム監査による経済的メリット 15
～東日本大震災の教訓は、具体的な実践になっている～

✓ システム監査は、世の不正とも戦えるでしょうか？ 17
～システム監査の知られざる力～

✓ システム開発プロジェクトの成功にシステム監査を 19
～価値観も方法論もPMが実現したいものと合致～

✓ 組織から独立した外部監査の有効活用 21
～大手証券会社の誤発注事例から学ぶ外部監査の必要性～

✓ 個人情報保護とシステム監査 23
～開発と運用の両面で厳しい監査が求められる時代に～

✓ システム監査人の新たな活躍の場としての 25
プライバシー・バイ・デザイン

✓ 情報漏えい防止に有効なシステム監査 27
～自分たちでは気が付かない情報漏えい 防止対策がある～

✓ 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 29
～SaaSを利用したビジネスプロセスの整備にもつながる～

✓ 組織内のシステム監査人へ、SAAJからの応援メッセージ 31
～情報システムの点検や改善に取り組むすべての方へ～

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。

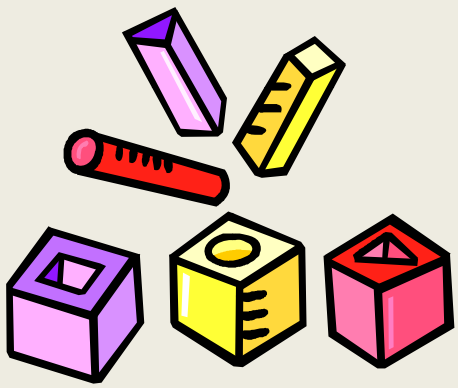
例を挙げれば、企業株主の利益を損なわないことを目的とした会計監査の場合は、決算書などが適正に作成されていることを外部の株主に保証する必要があることから、保証型監査であり、外部監査が望ましいと言えるでしょう。

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。

監査の種類	監査主体による分類	内部監査、外部監査
	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、情報システムの有効性・信頼性・安全性などが検証されて、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ます。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することができることです。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しれません。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を作ることが、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、業務処理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。

システム監査には「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。このようなリスクにつながる脅威として、システムの故障、運用上のヒューマンエラー、自然災害、その他事故があります。

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 ・情報セキュリティ監査 ・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。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。

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。なお、「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。

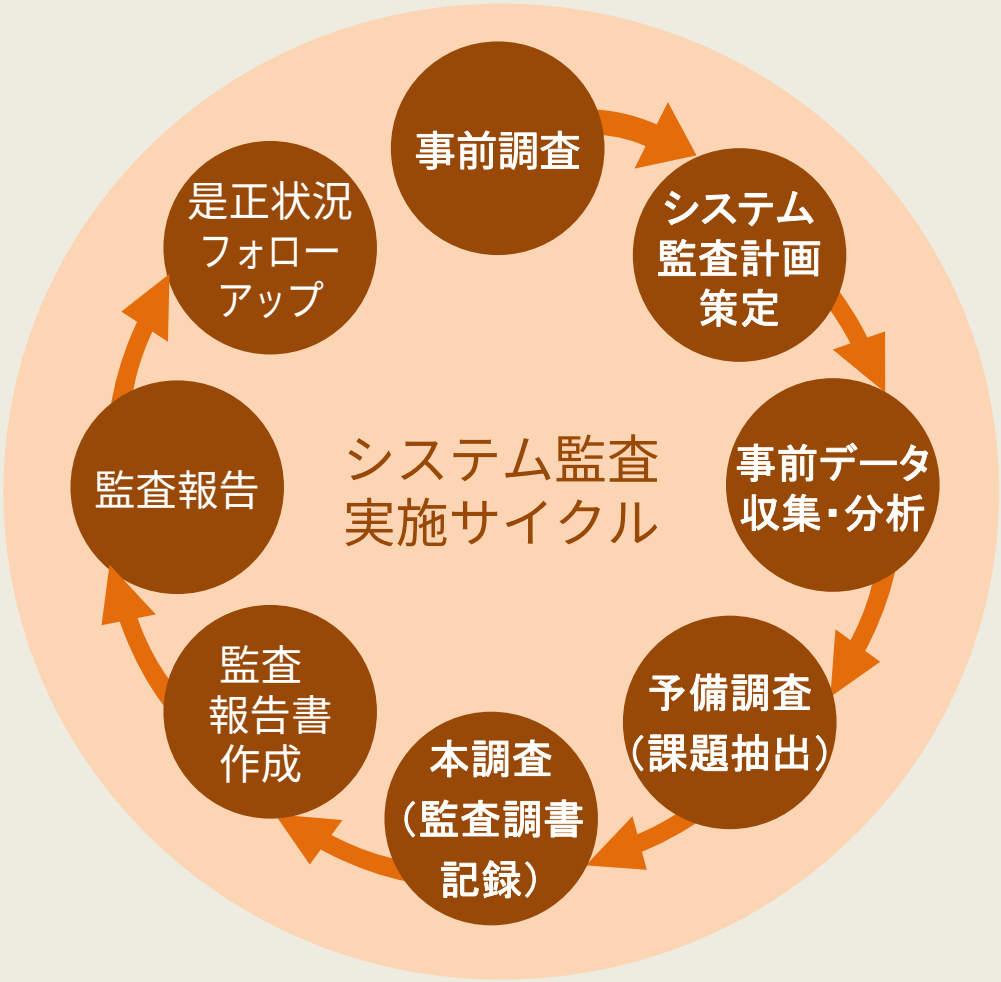
公表されている基準やガイドライン・規格などを基に、組織体としてのシステム監査基準を作成し、監査テーマに合わせて個別のチェックリストを確定させる必要があります。システム監査のために公表されているシステム監査基準には次頁のようなものがあります。これらから、システム監査の目的、テーマに合った基準を選定し、利用する必要があります。

システム監査のための公表されている主な基準
■システム監査基準（経済産業省平成16年改訂）
■システム管理基準（経済産業省平成16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） （経済産業省平成19年3月）
■情報セキュリティ監査基準（経済産業省平成15年）
■情報セキュリティ管理基準（経済産業省平成20年改定）
■情報システム安全対策基準（経済産業省平成9年9月最終改定）
■コンピュータウイルス対策基準（経済産業省平成12年12月改定）
■コンピュータ不正アクセス対策基準（経済産業省平成12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 （総務省平成22年改定）
■金融機関等のシステム監査指針 （FISC金融情報システムセンター平成19年3月版）
■COBIT5：Control Objectives for Information- related Technology （米ISACA：情報システムコントロール協会2012年4月）
■JISQ19011（マネジメントシステム監査のための指針）
■JISQ9001（品質マネジメントシステム―要求事項）
■JISQ27001（情報技術―セキュリティ技術― 情報セキュリティマネジメントシステム―要求事項）
■JIS Q 20000-1（情報技術 ― サービスマネジメント ― 第1部：仕様） JIS Q 20000-2（情報技術 ― サービスマネジメント ― 第2部：実践のための規範）
■JIS Q 15001（個人情報保護マネジメントシステム ― 要求事項）

システム監査人に求められる能力とは

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能力が求められます。

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最も重要な資質は、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。

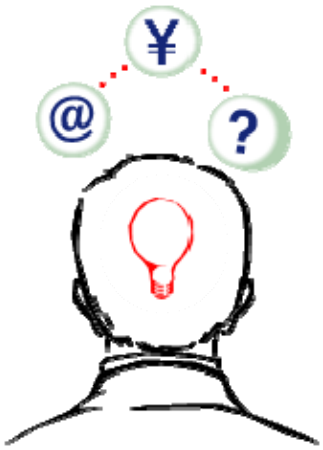
第10条（名誉と信義）システム監査人は、深い教養と高い品性の保持に努め、システム監査人としての名誉を重んじ、いやしくも信義にもとるような行為をしてはならない。

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。

システム監査人の思考回路（一例）
～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、既存の基準やガイドライン、チェックリストだけに頼ることなく、監査対象システムの状況、業務遂行形態、置かれた環境などによって点検項目を選択し、評価・判断の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と誤解されてしまいますが、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？

このような点検をする場合に特別な専門知識は必ずしも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って点検する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。

システム監査への期待

情報システムと監査の係わりは、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ﾌﾟﾚｽ発表
「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）

この時代のシステム監査の定義では、監査は「コンピュータを中心とする情報処理システム」あるいは「情報システム」そのものを点検･評価する活動がメインです。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の中で、「 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、

◇情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため

◇ 情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため

などの点を挙げています。

つまり現代では、システム監査には、情報システムの経営とのかかわりや組織体（社会）の目的の実現を検証・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。

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必要です。

身近な“システム障害管理”　その目的を今一度

～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。今更ですが、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。

具体的な方法を少し説明します。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。

皆さんのシステム障害管理が、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、未来志向の分析による**経営に貢献する障害管理**の実現に向けて、皆様に役立つ改善点をシステム監査が示します。

システム監査による経済的メリット
～東日本大震災の教訓は、具体的な実践になっている～

経営者、CIO、システム部門、リスク管理部門、電気・機械設備の担当者などが東日本大震災から多くのことを学び、身近で避けられない喫緊の問題と認識しつつも、どのような施策をどのように具体化すればいいのか、その取り掛かりに苦慮している状況がうかがえます。この背景には、過剰投資でなく身の丈にあった対策を決めかねていることや、現状にどのような問題が内在しているのか、新たな対策を実施しなければどのような事態が発生するのか、等々の検討要素が多いことがあるからと思います。

ここで、**システム監査がそのソリューションの一つ**であることに気付いていただきたいのです。災害対策の大きな柱は情報システムの対策です。電気、水、建物、室などのインフラは人間にとってのライフラインですが、情報システムもまたそれがなくては動けません。

システム監査で情報システムの災害対策を検証し改善点を明らかにすることは、情報システム以外にも共通する多くの効果を生みます。情報システムの災害対策には、システム部門だけでなく、設備管理部門、電気機械管理部門、リスク管理部門、企画部門なども含めて検証する点に実行面の困難さがあると思いますが、**システム監査では関連部署を横断的に点検するため、バランスのいい課題抽出が可能**となるのです。

東日本大震災とその前の阪神淡路大震災から得られた具体的な教訓を少し紹介します。

・緊急連絡網が形だけで、必要要員の漏れや業務委託先の連絡先が最新でないなど、緊急連絡網に実効性がない。
・サーバラックや什器の床固定が不十分で、転倒や暴走などで被害を大きくした。
・PCなどの転倒防止策が一定規模以上の揺れには効果がなかった（業務復旧必須機器はそれなりの対応が必要）。
・応急的にPCを補充したが初期設定処置が自前で出来ずPCが使えなかった。
・バックアップデータを確保していたが、手順が不明でリストアできなかった。

基本的な災害対策の遅れは不要な損失を発生させるだけでなく、予想外の経営的ダメージを与えます。東日本大震災などの教訓の取入れは、今や社会的責任になっているのではないでしょうか。皆様の実態に即した災害対策は経済的メリットも大きいはずです。

システム監査は、
世の不正とも戦えるでしょうか？
～システム監査の知られざる力～

システム監査はもちろん情報システムを対象にしている訳ですが、そのことをもう一度考えてみましょう。と言いますのは、世の中の業務・仕組み・成り立ちの多くは、情報システムによって構成されているからです。

企業等において発生する各種取引、金銭の動き、その関係者、そしてデータ入力者など経済活動の多くは情報システムの中で動きそして記録されています。ビッグデータのような途方もない情報のことではありません。これは、ごく身近な個別の取引データのことです。

反社会的な法令違反や巨額不正経理事件、長期粉飾事件など社会の耳目を集める出来事が過去ありましたが、その後も後を絶たない状況にあると思います。これらに対してシステム監査は無力ではありません。システム監査では、情報システムが業務に適合しているか、有効に利用されているかなどいわゆる「有効性監査」を大きな役割の一つにしています。

例えば、お金の移動や取引を処理する一般的な業務システムでは至極当然のことですが、以下のような異常取引を検知・承認するためのドキュメントをシステムで作成し必要部署に出力しています。このドキュメントの管理は部署の責任者の職責になっています。

・多額取引発生一覧表
・内部取引一覧表
・例外取引管理表
・期限経過管理表　　など

こういったドキュメントに印字された内容が日々の業務管理の中でどのように扱われて、どのように承認され決裁されているかを点検することによって多くのことが明確になります。重要な情報が特定の個人の扱いに任されていてはガバナンスは機能しません。

実は、こういったドキュメントは特定の階層以上が扱うもので一般の職員は知らないことがありますが、情報システムの仕組みを理解しているシステム監査人は、このようなことにも目を付けることができます。

システム監査では、業務システムの有効性やシステム機能の有用性評価などへの監査アプローチにおいて、上記のようなドキュメントにかかわるシステムを監査の対象にすることがあります。この監査を通じて、**情報システムがコンプライアンスの観点の要件を充足していることを点検・評価するのは、システム監査の本分です。**

異常取引を検知・承認するためのドキュメントは作成されているか、そのためのデータは正しく管理されているかなど、**システム監査が扱う領域と役立つ範囲は幅広いのです。**

システム開発プロジェクトの成功にシステム監査を

～価値観も方法論もPMが実現したいものと合致～

現実問題として、システム開発プロジェクトの運営は難度が高く予定通り完了（品質に満足、工期/予算が予定通り）のケースは数少ないと、いくつかの調査報告が示しています。また、システム開発プロジェクトにシステム監査を採り入れている事例はさらに少ないようです。

ひるがえって、情報システムの信頼性、安全性、有効性、効率性等に着眼するシステム監査は、完成後のシステムを対象とするより完成前のシステムに対して一層その役割を果たすことができます。

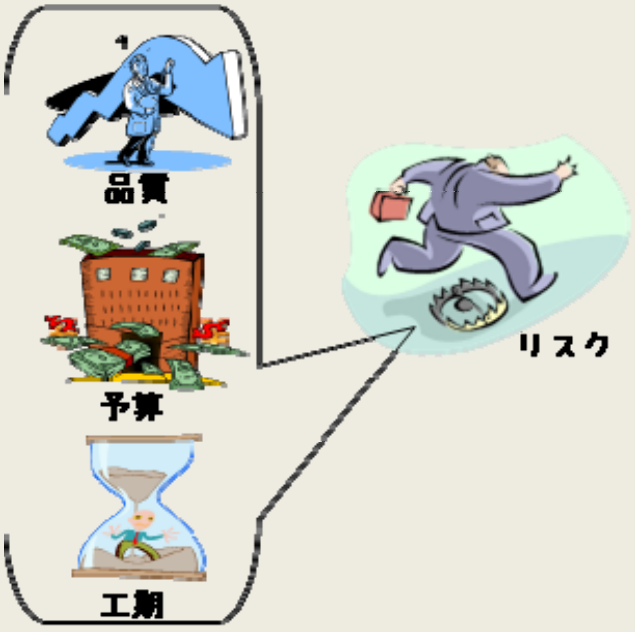
システム監査の役割は端的に言って「組織目標の実現に貢献すること。リスクコントロールの適切性向上に寄与すること。」であり、これはプロジェクトマネージャー（PM）がもっとも意を払う部分でもあります。PMは品質管理、予算管理、工程管理、要員管理など、多様なマネジメントの中で多くの不確定なリスクに向き合っています。しかしながら、これらの視点を有するシステム監査をプロジェクト遂行に活用・利用しようとする動きは極端に少ないようです。例えば、作業実態の把握と現況からのリスクの洗い出しや、次工程の着手判断材料の抽出などにシステム監査は使えると思います。

プロジェクトのWBS[注1)]にシステム監査の実施を事前に設定しておくことや、PMO[注2)]の一員に位置づけておくことは有効な手段です。開発プロジェクトにシステム監査を途中から組込むには、忙しい時期に余計な作業が発生するというプロジェクト員の負担感を大きくします。WBSにシステム監査という作業項目を予定項目として明記することで、システム監査が効果的に実施できます。

またPMOの編成については様々な意見がありますが、システム監査人がPMOに組込まれることにより、以下のことが実現できるのです。

-プロジェクトの進行に合わせ、監査実施の適切なタイミングを把握
-監査に用いる文書や体制の理解など、現場の負担を抑えた効率的な監査の実施が可能
-品質や工程の問題などのリスクをシステム監査の視点で評価
-PMの無理な作業遂行や経営の無理な注文などプロジェクトリスクを第三者の立場で摘出

これらの**システム監査活動はPMの仕事をし易くする材料となり、経営者に対してPMが言いにくい報告や要求をも客観的意見としてPMに代わって報告する手段**にもなります。



注1）WBS：Work Breakdown Structure（作業項目一覧表）
注2）PMO：Project Management Office（ﾌﾟﾛｼﾞｪｸﾄﾏﾈｼﾞﾒﾝﾄｵﾌｨｽ）

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年にお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短時間で企業に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、事故から8年たった今でも、証券会社と証券取引所は損害賠償責任などをめぐり係争中です。

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。

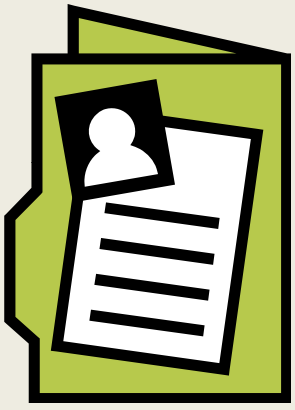
このような時こそ、**組織から独立した外部のシステム監査人の活用をお勧めします。**今までのリスク対策で十分かどうか、システムの利用・管理態勢をリスクベースで評価し、必要な改善点について助言を受けることができます。

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～

米国の2002年電子政府法第208条では、政府関連のシステム開発時に、事前にプライバシー影響評価を実施することを義務付けていますが、日本ではシステム開発時における個人情報保護についての定めは、特に見当たりません。

しかし、2004年4月2日「個人情報の保護に関する基本方針」閣議決定1(1)では、「個人情報は、その性質上いったん誤った取扱いをされると、個人に取り返しのつかない被害を及ぼすおそれがある。」とし、1(2)①には、「情報通信技術の活用による個人情報の多様な利用が、個人のニーズの事業への的確な反映や迅速なサービス等の提供を実現し、事業活動等の面でも、国民生活の面でも欠かせない」と、有用性への配慮を謳っています。

最近、欧米社会から、開発の初期段階における個人情報保護対策の検討が提唱されています。また、日本においても、特に医療情報システム分野では、個人情報保護の安全性への配慮を重視し、情報システムを構築する際に個人情報について十分な安全性を確保することについて意識されています。



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ちます。

また、情報システム運用面の監査では、例えば、個人情報の取り扱いについて、アクセス制限、ログの管理、保管場所、保存期間等について、その規程類と運用について監査します。最近は特に「ID管理簿」「ログ点検記録」「授受記録」「廃棄・消去記録」などについて、それぞれの証跡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、**個人情報保護に関して、開発と運用の両面で厳しい監査が求められる時代となってきた**と言えるでしょう。

「情報システム開発の監査チェックリスト」（例）

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。

注）実際に使用する際には、各システムを充分に調査した上で適宜変更することになります。

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

ここでは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、カナダのアン・カブキアン博士が1990年代から提唱するコンセプトです。プライバシー・バイ・デザインは、情報システムの設計段階から個人情報の保護を検討・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、事後的に取り組んできたために、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たり、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）と事業者側双方にとってWin－Winの関係が実現できるというものです。

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、事業者側にとっては、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、システムの設計段階でプライバシー影響評価（PIA：Privacy Impact Assessment）が必要になります。

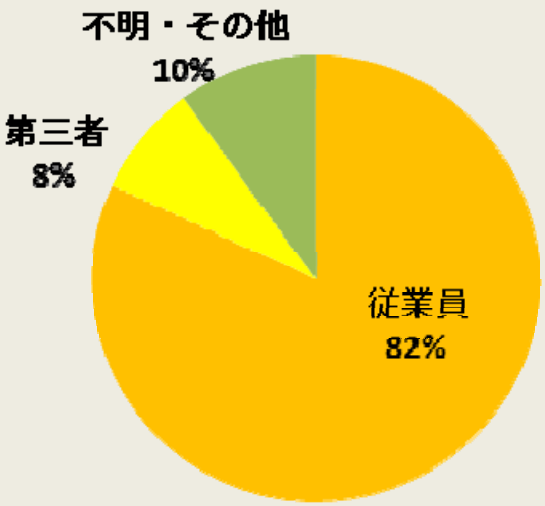
PIAは、個人情報の保護に関し、システム上のリスクを洗い出し、その対策を検討・評価するものです。ここに、**システム監査における開発フェーズの監査の技法が活きてきます。**

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。そこで、プライバシー・バイ・デザイン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。**

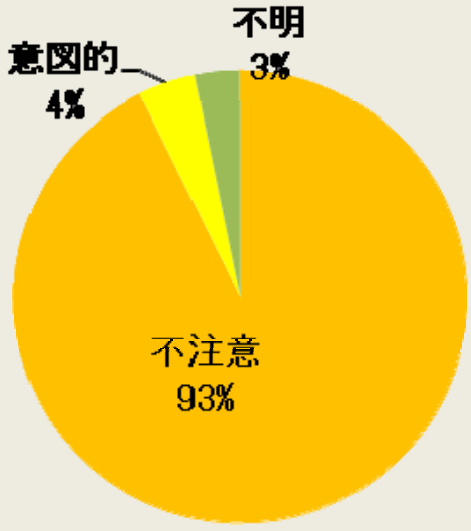
情報漏えい防止に有効なシステム監査
～自分たちでは気が付かない情報漏えい防止対策がある～

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。

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：平成23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、2012年9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、予防機能として、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、データ送信上および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	内容、備考など（状況は2014/01現在）
ISO/IEC 27017	ISO/IEC	ISO/IEC 27001（JIS Q 27001）のクラウド対応版、2015制定予定
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	改訂版策定中
クラウドセキュリティガイドライン利用ガイド	経済産業省	策定中
・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基本言明要件 ・クラウド情報セキュリティ管理基準利用ガイド ・クラウド情報セキュリティ監査技術ガイド	日本セキュリティ監査協会	
クラウド・セキュリティ・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）	

組織内のシステム監査人へ、SAAJからの応援メッセージ

～情報システムの点検や改善に取り組むすべての方へ～

企業等の組織内で、情報システムの点検や改善そしてシステム監査に日々取り組まれている方々は、いろいろなご苦労に向き合っていることと思います。

組織内のシステム監査人などの仕事の重要性を認識し、私どもが皆さんとの情報共有の必要性を考えているのは次のような視点です。

◎システム監査の対象は:

企業等の組織が事業目的を実現するための情報システム

◎システム監査で実現するものは:

事業発展と社会的貢献のための組織内部の課題解決

◎システム監査のあるべき姿は:

組織内に定常業務として根付き機能すること

◎希望の存在、価値ある存在と思うのは:

情報化社会の激変と日々戦い、監査業務を現場 で担い、監査の未来を背負う人材は、組織内のシステム監査人

組織内でシステム監査やシステムの点検･改善活動に携わっている皆さんには、システム監査知識の習得方法やシステム監査に関する社外情報入手、相談相手などにいくつかの制約があり、そのためのご苦労も多々あると思います。私どもは皆さんの日常的な業務改善活動が皆さんの組織を活力あるものにし、組織内にシステム監査が定着することで情報システムがより評価され、さらに情報化社会の健全な発展につながると考えています。何よりも皆さんのやりがいにつながるための取組みが重要と考えています。

特定非営利活動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発足
●設立1987年12月
●2002年に特定非営利活動法人（NPO）化
●2003年に「公認システム監査人」認定制度を立上げ、400人以上の公認システム監査人を認定

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
- 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 ：監査普及サービスおよび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
- 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 ：法人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

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、法人部会