[連載] ISMS適合性の監査から有効性の監査へ

ISMSの内部監査は、基準への適合性を追求するあまり重箱の隅をつつくような指摘の山になりがちです。もちろん基準への適合性の監査は基本なのですが、これを踏まえ有効性への監査へ一歩踏み出すことにより、それまで気づかなかったリスクを顕在化できます。
情報資産に対する脅威は、情報資産の運用（ライフサイクル）や、情報資産の置かれている環境（ファシリティ）、および情報資産に関連する法令、規制、契約への順守などが関係します。これらを考慮したリスクアセスメントや内部監査を実施しなければなりません。
ISMSの導入目的が継続的に果たされているか、つまり有効であるかどうかを内部監査で確かめていくことが、継続的なビジネスの維持･発展に繋がります。
有効性とは「計画した活動が実行され、目的とした結果が達成された程度」であり、適切な計画と妥当な実施が有効な結果を導きます。
すなわち「ISMSと業務の一体化」そのものです。

ここでは「ISMS適合性の監査から有効性への監査へ」と題して連載します。

1.ISMS内部監査の問題点　―こうして適合性の監査は重箱の隅にたどりつく―

1.1.　基準と事実の関係

ISMS内部監査は、ISMSの運用が、すなわち日常業務で行われているさまざまなことが、情報セキュリティ関連の規格要求事項や社内規定に適合し、かつセキュリティ上有効かどうかを確認する活動です。
ところが、監査員が発見した事実が監査基準に適合しているか否か判断できないことが往々にしてあります。

- ■ 目の前の事実に気付かない
- ■ 事実の見分け方が分からない
- ■ 発見した事実の重要度が分からない
- ■ 事実と監査基準を結び付けられない
- ■ 監査基準の目的が理解できていない
- ■ 監査基準を杓子定規に当てはめる
- ■ 監査基準を自分勝手に解釈している

監査員が目の前のリスクに気づかない、あるいは気づいたとしても対象組織がどのような業務をしているのかを把握していなければ、発見した事実がその組織にとってどのような意味があり、どれくらい重要な事項なのかがわからないため、是正を求める指摘をしてよいのかどうか迷うことがあります。

> 確かに、監査は発見した事実が監査基準を満たしているか否かを判定するものですが、ここで事実の見分け方がわからないとか、基準の目的とするところの認識がずれていたら、せっかくの是正を求める指摘も本来の目的が達成できないままになってしまいます。

1.2.　ことの本質に気づくこと

監査員が、気がついた事実をある基準に照らして、これは適合していないと判断し、「この事実はこの基準に合っていないので是正してください」と指摘したとします。

しかし、たいがいの是正はそれらのさまざまな事象を引き起こしている本質が何かに気づくこともなく、指摘された目に見える事象を取り除くのみに終始してしまいます。

これらの指摘と是正の反復は、ことは違っても同じ原因で似たような事象を発生させることになり、監査員は毎回それらをもぐらたたきのように指摘するという繰り返しに陥ります。

たとえば、必要な記録が残されていなかったとしたら、その原因は業務手順が決まっていないことかもしれませんし、役割が明確でないことかもしれません。そもそもその記録がなんのためになぜ必要なのかを教育などで周知徹底していないためにおろそかにされているとも考えられます。

本質に気づくのは監査員だけでなく、監査を受ける側に気づいてもらわなければ、期待する是正処置が講じられません。

ISMSの運用が進み、規定の運用や情報資産の管理がしっかりとされていればいるほど、監査を繰り返すたびに目に見えるものへの対策は施され、もはや監査で発見できることは重箱の隅の事象となっていくのは必然です。

次のような指摘の本質は何でしょうか。

- 記録に管理者の捺印が無い部分があった
- 規定の改定によって、関連する規定の一部に用語の不統一があった
- 教育・研修で未受講者のフォローが完了していなかった
- プリンターやFAXに出力文書の取り忘れがあった
- 保管期限の過ぎた廃棄資産が残っていた
- 不在者の机の上に書類が積んであった
- マネジメントレビューのインプット項目で、1年間報告事象のない項目があった

などなど

> つまり適合性だけをみていけば、重箱の隅にたどりついてしまうのです。単に指摘の数が減ったからといって情報セキュリティのレベルが上がったと判断できるでしょうか。

1.3.　経営陣の疑問

情報セキュリティは投資費用効果の見えにくいものです。多くの内部監査員の育成、リスクアセスメントの実施、内部監査の実施、マネジメントレビューなど、コスト的に多くの人件費がかかります。

果たして、当社の情報セキュリティは有効なのだろうか。そんな疑問が浮かんで当然です。

- 内部監査で特に指摘が無いが自社の情報セキュリティは完璧なのか
- 年に1回の監査で、監査員の力量（実力）は向上しているのか
- マネジメントレビューでは「事件・事故は発生していない」という報告だが、報告漏れや隠蔽はないのか
- 情報セキュリティの投資は軽視できない金額だが、自社のISMSは有効なのか

> 情報セキュリティは投資費用効果の見えにくいものです。

1.4.　適合性から有効性への転換

リスクの受容レベルを一定とすると、監査で発見される順守違反は時間とともに減少し、適合性に関するリスクは受容可能レベルを越えなくなります。しかし、その指摘は重箱の隅レベルになります。

一方、リスク対策自体は、これを放置すると状況の変化によるリスク増加に対応しきれず、その適切な状態を保つことができなくなります。有効性への転換点は、このリスク対策の放置がリスク受容可能レベルに近づく部分です。

適合性から有効性への転換点を以下に図示します。

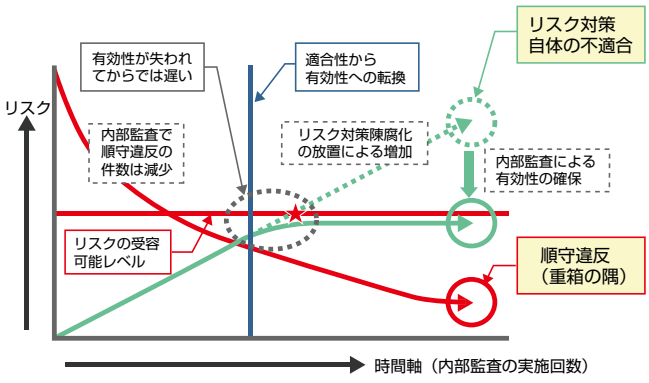

図1-1 適合性から有効性への転換点

監査の有効性が確保できなくなると目に見えないリスクがインシデントとして顕在化するまで対策が放置されてしまうのです。

1.5.　発見した事実の重要性

監査員が監査対象部署の業務を熟知していない場合があります。本来であれば時間を掛けて被監査部署の業務を確認し、重要な業務とそれに関連する情報資産の情報セキュリティを確認し、重点的な監査を計画するのが望ましいのです。

現実的には業務を阻害しないなどの理由により、短時間で監査しようとするため、十分な確認ができないまま表面的な監査になりやすいのです。

組織のISMSでPDCAを繰り返して回していくにしたがい被監査部署も理解を深めていき、表面的な監査の指摘では納得しなくなります。「なぜ指摘されるのか」、「どのレベルまで是正しなければならないのか」、「費用対効果は考えなくて良いのか」などが納得できないと「いい加減な監査で仕事の邪魔をしている」と反発されることもあります。

PDCA：Plan（計画）、Do（実行）、Check（評価）、Act（改善）のプロセスを順に実施するマネジメントサイクル

監査所見での指摘は、被監査組織の「業務内容に照らしたリスクの存在」をしっかり明示し、その指摘事項を放置するとどのようなインシデントが起きてしまう可能性があるのか説明し、理解してもらう必要があります。このプロセスが適切に実施されると、被監査部署はリスク対策に関する有効な指摘を得られたと納得してくれます。

もちろん、些細な違反であっても「守るべき」社内ルールがないがしろにされているようでは問題があります。リスクは低いが、放置してはいけない改善事項についてもその程度によって監査所見とすべきでしょう。

組織の実態を把握していない監査員は、発見した事象を全て同じレベルで判断しようとしますが、組織の特徴を理解していれば、発見した事実の重要度が判断できます。

次回は「2.見えないものには対応できない　―情報セキュリティリスクの可視化―」です。