[連載] ISMS適合性の監査から有効性の監査へ

3. ビジネスの維持･発展のための監査とはなにか ―有効性監査の実際―

3.1. 適合性の3要素と仕組み

マネジメントシステムの有効性は、基準に適合していることが大前提です。基準に適合し、かつその結果が有効であるという状況はどのようなものでしょうか。これを図示します。

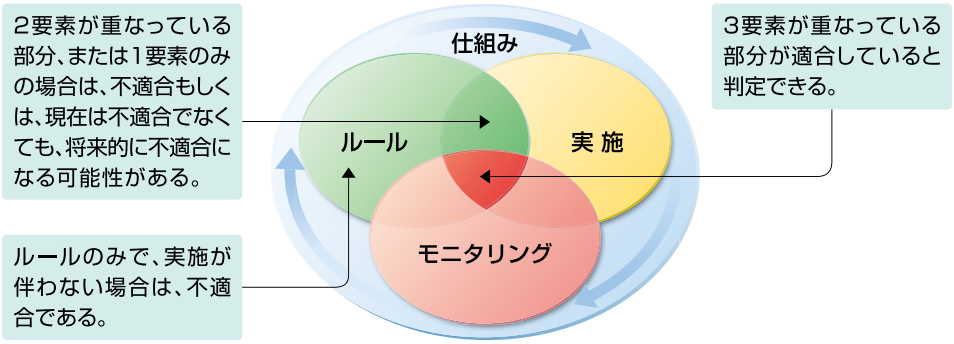

図 3-1 適合性の3要素と仕組み

1. ルールがある

ルールのみで実施していない場合は不適合です。

2. 実施している

実施しているがルールがない場合は改善の機会です。

3. モニタリングしている

ルールがあり実施している場合でも、その状況をモニタリング、すなわち確認していなければ、本当に実施されているかは不明です。実施されていても、どこかの時点で実施されなくなったら検知する手段がありません。

4. 仕組みがある

ルールがあり、実施し、モニタリングしていると適合していると判断できます。それを確実にするのは「仕組み」です。内部監査では、「できている」という状態がどのような形で実現されているか、継続的に維持される仕組みがあるかを確認します。

> 内部監査で確認しなければならないのは、ルールがあり、実施され、モニタリングされているかということと、それを維持している「仕組み」です。

3.2. 有効性監査の視点

その次に内部監査に求められている重要な役目は「マネジメントシステムの導入目的が継続的に果たされているか、すなわち有効かどうか」を監査することです。

> マネジメントシステムの有効性の定義:
> 計画した活動が実行され、計画した結果が達成された程度

これとは反対に、計画した活動の結果が達成されていないとはどのような状況でしょうか。

■計画が適切でない
的はずれの計画で目的や目標を達成できない

■活動の質も量も不十分である
計画に対する活動に漏れや抜けがあり、また十分な時間を割り当てられない

■達成された程度を測る尺度が曖昧である
有効性の測定のための管理指標・目標値、測定方法が具体的でない

■結果が有効でない
その状況が少しも改善されていない、もしくは根本的な原因に対処していない

これはマネジメントシステムに限ったことではありません。日々の業務やプロジェクトにおいても、期待した結果を得られなければそれは有効ではないのです。ビジネスの維持・発展は望めません。

> ビジネスの維持・発展のための監査では、ビジネスの安全性を脅かす事象（機密性・完全性・可用性の3つの分野が対象）が適切に管理されていることを確認しなければなりません。したがって「適切に管理されている」とはどのような状態であるかを知らなければ有効性の視点で監査できません。

3.3. ISMSの有効性

ISMSにおける有効性に関してプロセスアプローチの視点から考えてみましょう。

1. **「計画した活動が」**
   リスクアセスメントの結果、採用した管理策を具体的なリスク対策として実施した内容です。したがって、計画した時点で、その管理策が実施されればリスクを低減すると評価しています。適切な計画が望まれます。
2. **「実行され」**
   管理策が採用したリスク対策として実施されていることです。計画された妥当なコストや日程での実施が望まれます。
3. **「計画した結果が達成された状態」**
   管理策の目的は「リスクの低減」です。リスクの低減とは、「インシデントの発生を予防」していることです。計画された有効性評価方法で評価します。

組織のISMSの目的や目標の達成とインシデントの発生が受容水準以下であれば、ISMSの有効性、および管理策の有効性を評価することができます。

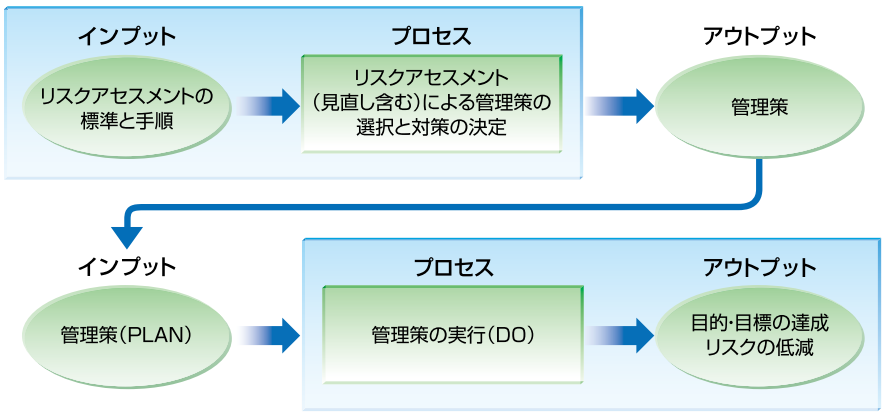

図 3-2　ISMSの有効性の評価

アウトプットとして選択された管理策が適切かどうかは、管理策そのものからは分かりません。インプットとプロセスを確認することで間接的にこれを評価できます。

1. インプットであるリスクアセスメントの標準と手順が論理的で納得性があるかどうか
2. プロセスとして、その標準と手順に従ったリスクアセスメントが実施され管理策が選択されたかどうか

プロセスアプローチの要素（インプット、プロセス、アウトプット）は、他の2つの要素を確認することで評価できます。

> ISMSの有効性では、最初にリスクアセスメントによって、適切な管理策が選択され実装されていなければなりません。そしてその管理策が実施され、その目的·目標を達成することが有効性の指標です。

4. まとめ

限られた時間で実施する内部監査で、すべての部署のすべての情報資産の適合性は確認できません。内部監査には常に不確実性が伴います。対象組織のマネジメントシステムが有効かどうかを確かめるために、いくつかの情報資産の適合性とそれを維持する仕組みを確認します。

対象組織のマネジメントシステム、すなわちPDCAが適切に回され、その結果が有効であればその組織のISMSの目的·目標は達成され、受容レベルを超えるインシデント発生の可能性は低いと考えられます。

以上