2007 年 4 月号

# マネジメントニュース

株式会社マネジメントセンター
茨城県水戸市住吉町 68-1
ＮＥＷ108－202 号室
http://www.isommc.com/
Tel029-246-4671　Fax029-246-4672
編集責任者：松本幸雄

今月号のニュース　＜日本版ＳＯＸ法とは？＞
２．日本版ＳＯＸ法とＩＳＯの関連性について
（前回のつづき）

## 日本版SOX法とは？

前回の続きとして「日本版ＳＯＸ法」についての内容です。特に今回は、「日本版ＳＯＸ法」と「ＩＳＯ」との関連について考えてみます。

### １．「日本版ＳＯＸ法」とＩＳＯの関連性について

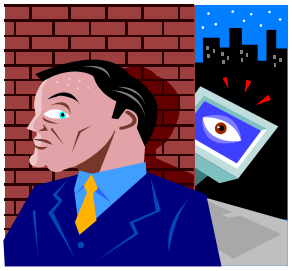
**「日本版ＳＯＸ法」の求めるもの**

前回ご紹介した「日本版ＳＯＸ法」の概要では、「米ＳＯＸ法」との関係や、「日本版ＳＯＸ法」全体についての内容でした。

その中でも、特に重要視されているのは「内部統制」の仕組み作りです。「内部統制」とは“企業の経営そのもの”とも言われ、各項目への対策が注目されています。

しかし、米国のＳＯＸ法と、日本のＳＯＸ法については、考え方の違いがあるようです。米国のＳＯＸ法の場合は、企業経営の健全性を求めるため、ガラス張りの仕組みとし経営者そのものも管理していくという考え方です。

それに対して日本版ＳＯＸ法の観点は、企業の経営者を中心に、自社のリスクを認識しそのリスクを管理することが求められています。



これら米国と日本との考え方の違いはありますが、企業トップへの信頼度が損なわれており、「内部統制」の仕組みを使い企業そのものの管理を強化することに変わりはありません。

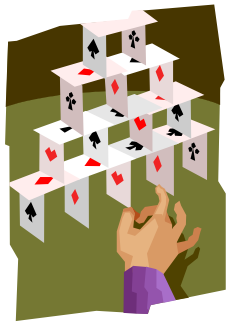
**「内部統制」への対応と「ＩＳＯ」**

前回も紹介させて頂きましたが、「内部統制」は以下の 6 項目で構成されています。

（１） 統制環境
（２） リスクの評価と対応
（３） 統制活動
（４） 情報と伝達
（５） モニタリング
（６） ＩＴの利用

各項目の具体的な対応と、ＩＳＯとの関連について幾つか取り上げてみます。

**（１）統制環境**



統制環境とは「組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えるとともに、他の基本的要素の基礎となるものをいう。」との定義です。
前述の（２）～（６）までの各項目の基本となる要素と言えます。

その中の具体的な確認事項としては、次のようなものが挙げられます。

- 経営方針・経営戦略が会社に浸透しているか
- 職務権限や、職責が規程などで定められているか
- 従業員の雇用、研修などに関する手順は定められているか

これらは一部ですが、ＩＳＯなどのマネジメントシステムを構築している企業では、聞き慣れた内容ではないでしょうか。

例えば「経営方針が会社に浸透しているか」は、ＩＳＯ9001 の要求事項『5.3 品質方針』などとの共通事項です。（環境・情報に関するＩＳＯにしても同様）

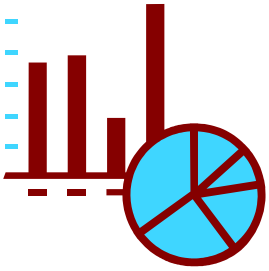
また、「職務権限」については、『5.5.1 責任

及び権限』での要求事項と同様の内容です。更に「従業員」に関する事項は『6.2 人的資源』の考え方が十分当てはまります。

## （２）リスクの評価と対応

リスクの評価と対応とは「組織の達成に影響を与える全てのリスクを識別、分析及び評価する事によって、当該リスクへの対応を行う一連のプロセスをいう。」と定義されています。

ＩＳＯ9001 では、『8.4 データの分析』などの対応がなされたり、ＩＳＯ27001（情報管理のマネジメントシステム）では、『4.2.1ＩＳＭＳの確立』の中でリスクの特定方法を定めたり、その結果特定されたリスクの分析及び評価までの仕組みを要求されています。



## （３）統制活動

統制活動は、「経営者の命令及び指示が適切に実行されることを確保するために定める方針及び手続きをいう。」となります。

この項の具体的な確認事項としては、次の内容が含まれています。

・ 方針や手続きが文書化されているか
・ 承認などが規程どおりに実施されているか

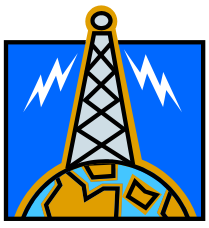
これらは、各ＩＳＯのマネジメントシステムにおいて共通している文書の管理方法が効果を発揮するのではないでしょうか。

## （４）情報と伝達

情報と伝達とは「必要な情報が組織や関係者相互間に、適切に伝えられることを確保することをいう。」となっています。

具体的な確認方法としては、“ 外部情報、内部情報の両者が入手できるシステムが構築されているか ” が挙げられます。

これについては、ＩＳＯ9001 では『5.5.3 内部コミュニケーション』、ＩＳＯ14001 では『4.4.3 コミュニケーション』、ＩＳＯ27001 では『管理策 A.6.1.6 関係当局との連絡』や『A.13.1.1 情報セキュリティ事象の報告』での対応が可能となります。



## （５）モニタリング

モニタリングとは、「内部統制の有効性を継続的に監視及び評価するプロセスをいう。」となっています。

その内訳は、次の 4 点に分類されます。

① 日常的モニタリング
② 独立的評価
③ 評価プロセス
④ 内部統制上の問題についての報告

これらの活動は、日常的な『監視及び測定』の活動と、ＩＳＯの各規格で要求されている『内部監査』及び『マネジメントレビュー』のインプットと言えるでしょう。

## （６）ＩＴの利用

ＩＴ（情報技術）の利用とは、「内部統制の他の基本的要素が有効かつ効率的に機能するために、業務に組み込まれている一連のＩＴを活用することをいう。」と定義されています。

これは、ＩＴ環境に対応した情報システムに関連する内部統制を、整備及び運用することを言っています。

具体的な対応の一例として、

・ 経営者は経営目的達成のため、積極的にＩＴの利用を考えているか
・ ＩＴのセキュリティレベルやアクセス権限が適切であり、その対策も万全か

などがあります。

このような内容は、ＩＳＯ27001 の『5.1 経営陣のコミットメント』や、『管理策 A.11 アクセス制御』の要求事項に含まれているものです。

以上のことからもお判りのように、「日本版ＳＯＸ法」で重要視されている「内部統制」の考え方は、ＩＳＯの各マネジメントシステム（品質・環境・情報）などと共通項も多くあります。

その中でも、今後は『ＩＳＯ27001 情報セキュリティマネジメントシステム』が最も注目される規格になることは間違いありません。

**㈱マネジメントセンターへの、ご意見、ご質問をＦＡＸ又はメールでお寄せ下さい！**
**ＦＡＸ：029-246-4672**
**Mail：info@isommc.com**