2007-2-15

混沌とした中から

第62号
発行責任者　稲崎義明

日本版ＳＯＸ法について（３）

内部統制を実施するうえで情報システムは大きな助けとなります。ＥＲＰ、ＢＰＭやワークフローなどのビジネスプロセス系ツールを使い、情報システムへの入力（あるいは情報システムを通じての権限者の承認）無しに業務を進めることができないようにすることによって業務遂行の記録を残すことができるようになります。このほかにも業務の記録や参照を支援するＢＩ及びコンテンツ管理やドキュメント管理ツール、不正アクセスや情報漏洩などを防止するセキュリティ製品やアクセス制御システム、会計などの業務システムの入力値の正確さを確保するための各種チェック機構など内部統制に有効なシステムがあります。

ＥＲＰ：企業全体を経営資源の有効活用の観点から統合的に管理し、経営の効率化を図るための手法・概念のこと。「企業資源計画」。ＥＲＰパッケージとしてＳＡＰ社のＲ／３などがある。

ＢＰＭ：“ビジネスプロセス”に「分析」「設計」「実行」「モニタリング」「改善・再構築」というマネジメントサイクルを適応し、継続的なプロセス改善を遂行しようという経営・業務改善コンセプト。

ＢＩ：　企業内外の事実に基づくデータを組織的かつ系統的に蓄積・分類・検索・分析・加工して、ビジネス上の各種の意思決定に有用な知識や洞察を生み出すという概念や仕組み、活動。

コンテンツ管理：テキストやグラフィックなどのさまざまなデジタル・コンテンツを収集、登録して統合的に管理し、更新・配信する仕組み。

ＩＴそのものについてもシステムダウンや不正侵入などリスクがあり、内部統制の対象として考える必要があり「ＩＴ統制」と呼ばれます。

ＩＴ統制は「ＩＴ業務処理統制」と「ＩＴ全般統制」の2つに大きく分類することができます。ＩＴ業務処理統制は業務プロセスに組み込まれたＩＴ統制で、例えば経理処理をする際に上長承認を必須とするような承認システムの導入です。一方「ＩＴ全般統制」はＩＴ業務処理統制が正しく有効に機能することを保証しようとするもので、前例のような上長承認の場合、成りすましによる承認を以下に除外して確実に本人のみが承認できることを証明しようとするものです。成りすましなどを除外するためにもＩＴ統制では職務掌握とアクセス管理が必須となります。その意味でも本来情報システムの開発環境と運用環境を分離して別の担当者とすることが基本です。これは開発部門担当者が不正プログラムを組み込むことに対する対応策となります。

情報部門として特に注意しなければならないものにシステムの統合的管理があります。これまではシステムによって汎用機、Ｗｉｎｄｏｗｓ、Ｕｎｉｘなどを利用してきましたが、それらをそれぞれで管理するのではなく統合的に管理することを検討する必要があるということです。例えば、分散環境において全般統制であるＩＤ管理を行うことを考えた場合、退職した人のＩＤが残っていないか（ＩＤ削除）、部署異動した人の権限変更が確実になされているか（権限変更）などをシステム毎に確認し評価しなければなりませんが、統合管理されていることによりその評価対象が集約でき内部統制の評価コストダウンになります。また、アクセス管理も重要で、データを入力する人と承認する上長の権限をはっきり分けるということです。つまり承認する上長にはデータの入力する権限を与えてはいけないということでわかると思います。もちろん上長が勝手に入力データを変更することを防止するためです。（次回へ続く）

(今週の情報誌から)

○日経エレクトロニクス　２月１２日号

特集　薄型ケータイを解剖する

→携帯機器の薄型化がヒットの流れとなっている。高機能だから厚くてもいいということはない。携帯音楽端末を初め「薄い」ということが新しさを感じさせる。高機能で頑丈でしかも薄い。その中はどう対応しているか。

○日経パソコン　２月１２日号

検証　詐欺に勝つ

→ネット詐欺は大変にはいろいろなものがある。ワンクリック詐欺、偽ソフト、オークション詐欺、フィッシング詐欺などなど。大体インターネットを接続しているだけでこちらの情報(個人確定情報)がわかるわけがない。また、プロバイダがそのような情報を提供することもない。ワンクリックについては無視が一番。間違っても退会申し込みをするとこちらの情報を教えるようなもの。など、ネット詐欺は大部分がその手口を知っていれば対応することができるが、オークション詐欺のように見破られないものもあるので、そのときはある程度リスクを覚悟しなければならないかもしれない。