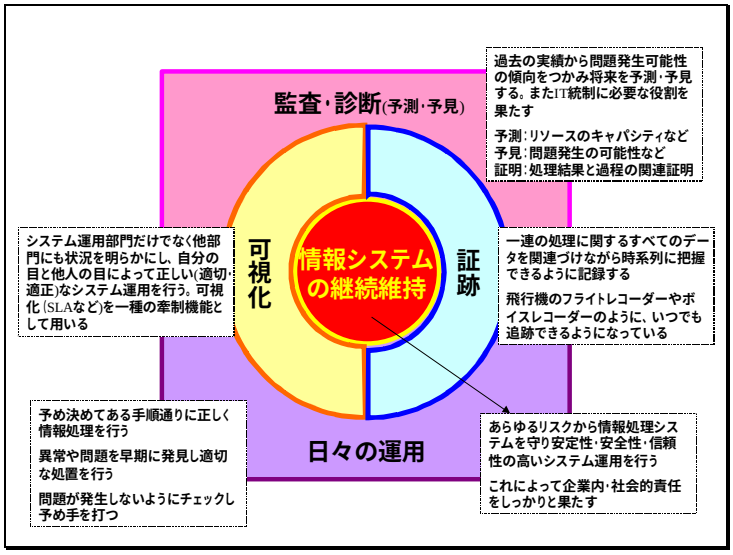
システム運用「人としくみ」

最近、日本版 SOX 法や内部統制、そして、IT 統制という言葉が、マスコミなどでも日常的に聞かれるようになってきました。情報システムを司るそれぞれの部門や企業でも、これらの事柄には非常に大きな関心を抱いていると同時に、実質的な取り組みを始めている企業も多く出始めています。

これからのシステム運用

システム運用における IT 統制(後)

前回は、図－２８を用いて、システム運用の果たすべき責任「継続的な情報処理システムの維持」の、日々の運用と監査･診断について述べてきました。今回は、可視化と証跡について考察していくことにします。



（図－２８）システム運用の IT 統制

情報処理システムの継続的維持を行なうための監査ができるようにはどのようにしなければならないか。それは、次に述べるような可視化と証跡という２つの側面から捉えていく必要があります。

1 つは可視化です。システム運用部門だけでなく、他部門にもシステム運用の状況を明らかにして、自分の目と他人の目によって、正しい(適切･適正)なシステム運用を行っ

ていくことが大切なことです。すべての部署、ここに、システム運用の状況を明らかにしていくことによって、システム運用部門にとって一種の牽制機能ともなります。

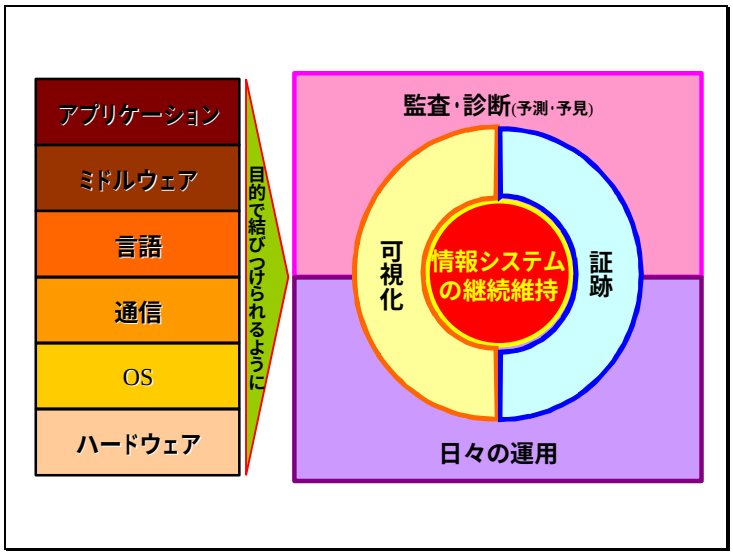
また、システム運用部門が、自部門の責任を全うしているかどうかを、SLA(service level agreement)という目に見える形にして、それを公表していくことも大切なことです。SLA を用いて、一種の、システム運用部門と業務部署･企業との契約事項とするわけです。そのことによって、システム運用が単なる作業ではなく、ビジネスを行っていることを明らかにしていくことができます。そこに、責任というものが生まれてきます。あるいは、責任を尊重するという風潮が生まれてくるはずです。

もう 1 つの面は、証跡という面です。一連の処理に関するすべてのデータを、何らかの目的に関連づけながら、時系列に把握できるように記録しておく必要があります。つまり、これは、監査の時、あるいは、診断の時、一つの業務処理について、すべての関係を明らかにしていくことです。そうすると、その業務処理が、正しく行われている、あるいは、誤った処理が行われている、あるいは、データの関連づけがどうなっているか、そういうものを明確に示すことができます。

そのための記録をとっていく必要があります。しかし、ただ単に記録をとればよいというものではなく、これらがある目的に沿って、正しく結びつけられていることが大事です。

飛行機のフライトレコーダーやボイスレコーダーも、飛行機事故が起こったときに、まずそれが、原因究明、あるいは当時の状況を明らかにする、大きな手がかりになります。それによって、事故はなぜ起きたのか、この原因を明らかにすることができます。この記録は、事故があっても壊れてはいけないようになっています。つまり、何者にも侵されることなく、安全に保存されるようになっています。そして、いつでも追跡できるようになっています。

これらのデータは、図－２９にあるように、ハードウェア、OS、通信、言語、ミドルウェア、アプリケーション、それぞれの中から発生してきます。それらを、監査などのある目的で結びつけられるように証跡･蓄積されていく必要があります。



（図－２９）証跡データの出所

ハードウェアの利用状況をつかみながら、コンピュータが、あるいは、インフラストラクチャーとしてのコンピュータ・システムが寸断することなく、事業が継続するための予測・予見ができるようなデータの蓄積が必要です。

また、オペレーティングシステムについても同じです。OS のバージョンが古い場合、これによる障害発生の可能性がありますから、処理した OS バージョン番号も履歴としてしっかりと記録しておかなければなりません。OS が記録しているデータ管理の情報やシステム管理の情報(SMF に類するもの)などもとりながら、システムの負荷分析を行い、将来の問題発生を未然に防ぐ必要があります。

通信についても同様で、多量なトランザクションが発生し、ネットワークのトラフィックが高くなっている。これをどう解決するか。いまは、ネットワークが企業内すべてに張り巡らされ、目的別の通信ではなくなってきています。すべてが共有される通信構成になっています。

そのために、ある部署で非常に高い負荷をかけた場合、全く業務とは関係ないところで、あるいは、重要性の非常に低い業務で、大きな通信負荷をかけていて、重要業務に影響を与えるということもあります。こうした問題を未然に防ぐためにも、通信のデータも蓄積していく必要があります。

言語。言語については、言語そのものについての問題はないと考えます。しかし、プログラムについては大きな問題が発生する可能性があります。つまり、業務システム

のプログラムが、正しい・新しいプログラムがきちっと配布されているのか、いつ配布されたのか、必要なところにすべて配布されたのか、不必要なものはしっかりと削除されているのか、こういうプログラム管理も情報をしてしっかりと持っておく必要があります。

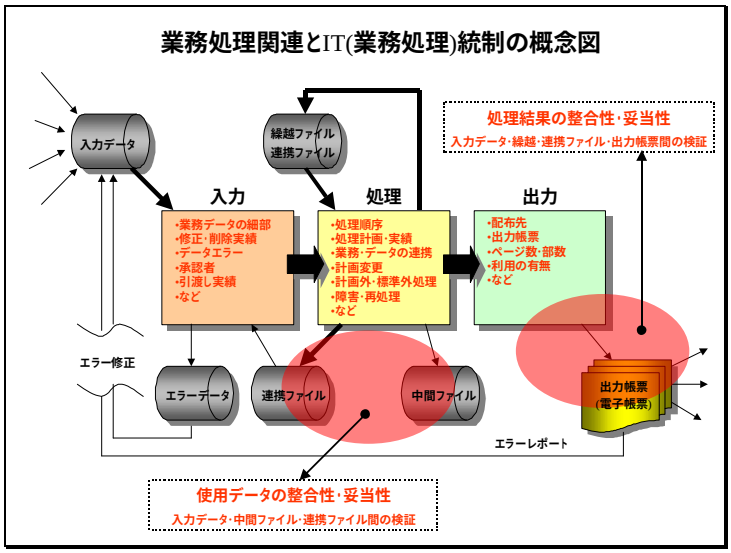
つまり、正しく処理されたということは、正しいプログラムで処理されたということです。その内容についても、しっかりと証明していくことができるようになっていなければなりません。

ミドルウェア。最近ではいろいろなミドルウェアを使うようになってきています。たとえば、ERP パッケージの中にも含まれているし、運用システムにも含まれています。いろいろな処理が、いろいろなソフトウェア・パッケージを用いて行われています。ERP パッケージはアプリケーションとして捉える方が適切と思いますが、運用システムなどのミドルウェアは、そのしくみの中で業務処理が行われていきます。処理手順が正しいかどうか、これを証明するのは、このミドルウェアになります。

アプリケーション。アプリケーションの内部、つまり、プログラムの内部について証明することはできません。しかし、アプリケーションが処理した結果、この論理的な確認は行うことができます。アプリケーションが、どのような手順で処理されたかは、先ほどのミドルウェアで証明することはできますが、処理した結果のデータは、システム運用の中で捉えています。つまり、ファイルや出力帳票として、その処理結果のデータはすべてシステム運用が蓄積しています。これらの論理関係をしっかりと捉えることによって、業務処理の IT 統制を行うことができます。

業務処理統制という考え方もあります。この業務処理統制は、「企業のもつ、個々の業務システムの中に組み込まれたシステムで、情報の入力、処理の指示や処理内容そのもの、および、出力の過程において、会計情報の正確性と信頼性を直接的に保証する統制である」、と定義されていますが、業務システムにおけるデータの入力、処理、出力が正しく行われていることを確かめることができる、という意味に置き換えて考えることができます。

この業務処理統制の考えを概念化したものが図－３０です。これらの、この図－３０で表すようなデータは、すべて、システム運用側で蓄積し維持しています。これを、この監査・証跡という観点から、ある一つの目的で結びつけられるように捉えていく、そういう明確なしくみをもつ必要もあります。



（図－３０）システム運用における業務処理統制

IT 統制は、システム運用部門だけで責任を果たすことはできません。企業として、全体統制を行っていくプロセスの中で、ICT に関する一つの役割を担うに過ぎません。しかし、その一つの役割が欠けてしまうことにより、全体統制は成り立たなくなってしまいます。内部統制の中で ICT が果たすべき役割、IT 部門が果たすべき役割、さらに、その中で、システム運用部門が果たすべき役割、これらのすべてが満足することによって、企業の社会的責任は全うされていくのです。これを証明することができるのです。