

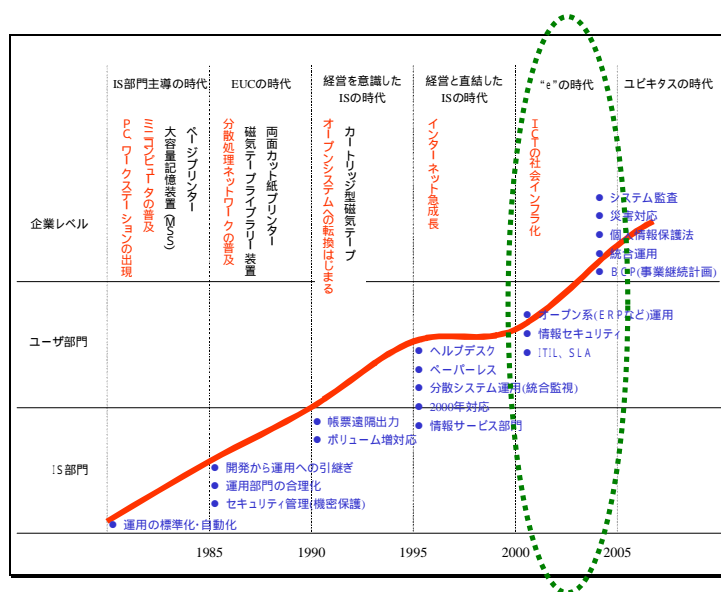
システム運用「人としくみ」

システム運用は長い歴史の上に成り立っています。コンピュータが採用されはじめた初期のころは、運用担当者の作業効率を上げることが主目的とした運用改善が行われていました。その後、年を経るごとに内から外へと運用改善の目的が広がり、今では、企業経営そのものを支える盤石な情報システムのインフラ運用にまで至っています。こうしたシステム運用は、どのように進化してきたのか、その歴史を5回に分けて振り返ってみます。今回はその5回目(最終回)です。

これまでのシステム運用

システム運用の歴史【5】

前回は経営と直結したISの時代について説明しましたが、今回は“e”の時代(2000年～2004年)について、図-16(前回レポート図-14と同じものです)を用いて振り返ってみます。



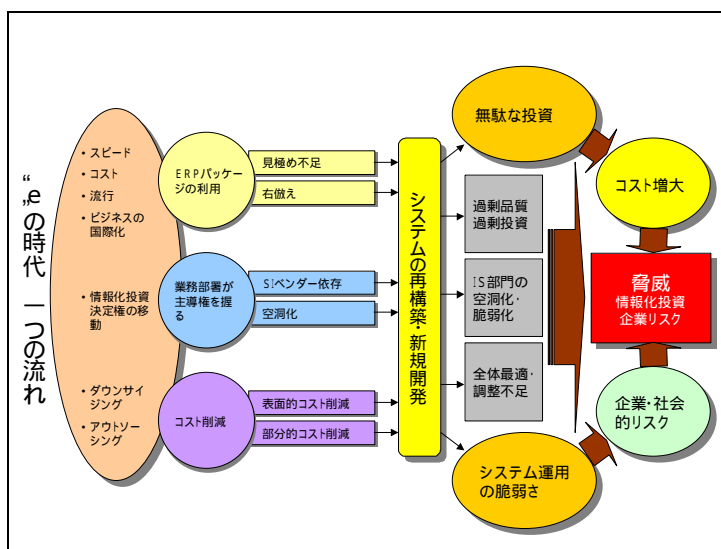
(図-16) システム運用の歴史

2000年～2004年の“e”の時代は、ある意味ではいまの時代ともいえますが、ICT革新がどんどん先に進んでいることを考えれば、“e”の時代はもうすでに過去の時代であるといえます。

“e”とはいったい何を言うのでしょうか。本来は Electronic の頭文字をとったものだろうとは思いますが、どうやら通常の電子的(Electronic)という意味ではなさそうです。従来の企業内・企業間ネットワークというものではなく、もっと広範囲なネットワークとしてインターネット技術を利用したものを、“e”という言葉で使い分けているようです。

このような、とくにインターネット技術を活用した ICT が社会のインフラとなって定着しはじめたのが、この 2000 年からの“e”の時代です。“e”はさまざまなものに影響を与えるようになりました。企業ビジネスそのものにも大きな影響を及ぼすようになりました。新しいビジネスもどんどん立ち上がってきました。とくべつ、施設・設備・人をそれほど必要としないということから、仮想商店・仮想企業のような新しいビジネスも増えていきました。まさに、情報を動かすだけでビジネスになる(儲かる)時代となってしまったのです。

このような“e”の時代になって、システム運用は混沌とした状況の中に入ってきました。いままでのように綿密に設計された情報システムだけではなく、短期間で立ち上げる情報システムも多くなりました。そのため、図 - 17 にあるように、システム運用にはさまざまな問題や課題が山積するようになってきました。



(図 - 17) “e” 時代に噴出した問題

とくに、1990 年代の後半から急増した ERP などのオープン系システムは、当初は部分最適化が計られ、それなりに満足のいくものとして評価されていました。しかし、その数が増し、あるいは、本格的に利用されるようになってからのコンピュータ資源

の増加が、企業全体から見たコスト(総コスト:TCO)をかなり押し上げていることに、企業自身も気づきはじめてたのです。そして、オープン系システムの存在が、その業務部署に留まらず全社に影響を及ぼすようになり、いままでのメインフレームによる基幹システムとなんら変わらないほど重要な位置づけとなってきました。メインフレームは基幹システム、オープン(分散サーバー)は情報系システム、などとはいえない状況になってきました。ERP パッケージを用いたシステムは明らかに基幹系システムとなっていたのです。

そのため、システム運用に関しても、それぞれのオープン系システムの部分最適がなされた上で、企業としての全体最適がなされるべきとの主張も強くなってきました。これは、コストの問題のみならず、システム運用の如何が企業リスクに大きく影響を及ぼすことが懸念されたからです。

こうしたことを背景に、“e”の時代に入ってから、ERP などオープン系のシステム運用のあり方、そして、いままでのメインフレームのシステム運用との統合化などを模索するようになってきました。もちろん、その前からも議論は行われていましたが、ERP システムにしても、まだ、企業経営に直結したものの受け止め方は少なかったため、そのうち困るのではないかという程度のとらえ方でした。

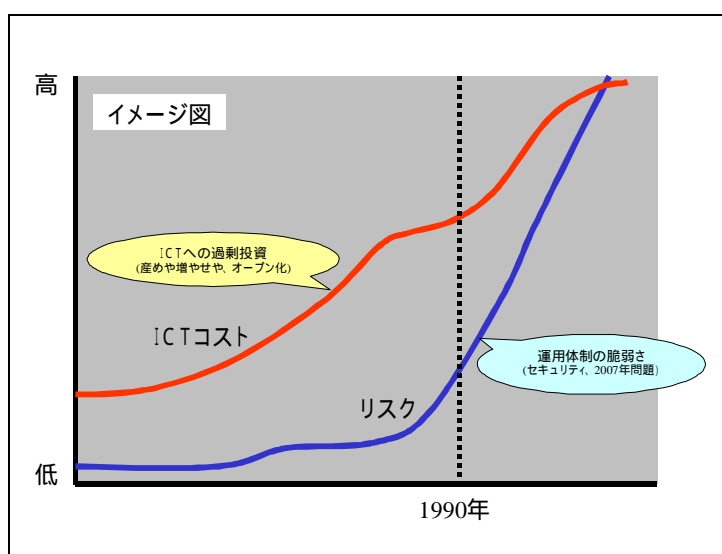
コンピュータが、一般の企業で使われはじめてから 50 年近くなるとういうのに、システム運用に関する理論は整理されないままでした。メインフレームを扱うシステム運用の技術者は、オープン系のことには自信がありません。オープン系を扱う人たちは、システム運用とはどんなものかを知りません。オープン系の人たちはシステム運用のことを知らないのだから、メインフレームの技術者がシステム運用を教えてあげればよいのではないかと、思うのですが、オープン系とメインフレームとは別なものだと思っているし、システム運用理論たるものもあるわけではないのです。

そこに、ITIL(Information Technology Infrastructure Library)というものが出はじめてたのです。どうやら ITIL は、システム運用を体系化した一つの理論をもっているようだ、誰も彼もが ITIL を研究しはじめました。ITIL と名がつくセミナーはいつも超満員でした。書籍もずいぶん出版されました。それだけ、“e”の時代のオープン系システムについては、システム運用に対する関心や問題意識が高かったのです。これは 2005 年以降のいまの時代でも続いています。

もうひとつの大きな問題は企業リスクの問題です。情報漏洩など、情報セキュリティ上の問題が発生すると、いまでは強い社会的批判を受けるようになります。そして、

これが、企業の存続を脅かすことになってしまう、企業倫理の欠如によって受けるダメージと同列の非常に深刻な問題です。

図 - 18 は、企業リスクの増加を表したイメージ図です。従来のメインフレーム時代とは異なり、オープン化はさまざまな環境にさらされますから、それだけに情報化による企業リスクは増大していくものです。そして、この企業リスクを回避するための手段として、もっとも重要視されているのが情報セキュリティによる対策です。



(図 - 18) 増え続ける企業リスク

情報セキュリティに関しては、どの企業でも最優先の課題として取り組んでいることのひとつです。しかし、この問題に関してはイタチゴッコの感があります。セキュリティを犯す手段は日々変化していきます。新たな技術が出はじめると、それを追うように新しい手がつくりだされるからです。このような情報セキュリティに関して、大きくは2つの考え方が必要です。つまり、内部から外部へもたらされる情報(情報流出)と、外部から内部へ侵入し情報が持ち出されたり情報が改竄されたりするという問題です。

このうち、外部からの侵入に関しては、ハードウェアやソフトウェアなどの組み合わせ(システム構成)、あるいは、ウィルススキャン・ワクチンなどのウィルス対策ソフトの導入などで、ほとんどの企業が何らかの対策を講じています。しかし、次から次へと新たなウィルスが発生するために、今後も決して万全な対応といえる策はとることができないと考えられます。結局は、後手の対策をとらざるを得ないことになってい

るのが現状です。

社内のセキュリティに関しては、一般的にはユーザ ID とパスワードによる運用が多いようです。これは、まだインターネットが普及しはじめるずっと以前から用いられている方法です。ユーザ ID によって、情報へのアクセス権限を制限するやり方も、今までのオンライン処理に見られた方法となんら変わってはいません。

社内セキュリティを徹底して行うということは、基本的には、利用者にとって情報システムを使いにくくすることでもあるわけです。できるだけ使いにくくすることで、簡単・容易に情報にアクセスできないようにすることです。実際、この時代のセキュリティ管理は、何重にも張り巡らされた関所(パスワードによるチェック)を通らなければなりませんでした。とにかく使いづらいのです。そうであっても、“e”時代の情報セキュリティにとって、もっとも重要な課題への対策としてとらざるを得ない手段でした。

しかし、情報セキュリティのなかでも、とくに情報漏洩については、結局は社員のモラルの問題です。どんなに厳しいセキュリティのしくみを用意したとしても、許可されたものによる犯罪は防ぎようがありません。事実、情報漏洩など多くの問題は、内部のものによるところがほとんどなのです。こうしたことから、モラル維持のための教育を行い、PC などの操作記録を保持し分析するなど、こうしたことがせいぜい打てる手のすべてとなっていました。