

システム運用「人としくみ」

企業の情報システムは、この近年、社会からの強い要請にも応えなければならない責務を負っています。法律を遵守するだけでなく、企業ビジネスのインフラストラクチャーとしてのシステム運用に関して、情報処理の継続性、および、情報処理のプロセスを証明するための透明性(可視化)、という責任がつよく求められています。

企業ビジネスとシステム運用

システム運用と社会的責任

情報処理システムは、いまや、企業ビジネスの根幹を担っていますが、この中でも、企業情報システムの HUB 的な役割にあるシステム運用は、大きな社会的責任を負っているといっても決して過言ではありません。

情報システムあるいはシステム運用が負うべき社会的責任とは、ここでは「情報処理システムを通じて社会に不利益を与えないこと」と定義します。情報処理システムが、企業を通じて、広く国民・国家にまで影響を及ぼしていることは、最近のいろいろな報道でも十分知ることができます。

このように、「社会に不利益を与えない」という、その社会とは、国民・企業・国家(の威信)ということになります。また、不利益とは、こうした社会に対して、何らかの損害を与えることをいいます。つまり、社会的責任とは、社会に不利益を与えないということですから、いいかえれば、社会に対して損害を与えないようにすることといえます。

情報処理システムの場合、損害を与えるといっても、そのほとんどは直接的なものではありません。何かを破壊するとか、いわゆる物理的なものではありません。しかし、間接的あるいは心理的に悪影響を及ぼすことが多いために、それは、安心・信用・威信を覆すことにつながってしまいます。こうした心理的な問題は、いちど発生すると、これを回復するには相当な時間・期間を必要とし、最悪の場合は回復不能という状態にまで至る危険性があります。

例えば、最も多く報道されているのがデータ漏洩の問題です。最近は、情報開示が徹底されていることもあってか、それは、それは、報道を通じて多く耳にします。デー

データ漏洩が直接的に被害をもたらしたということを実証するのは難しいかもしれませんが、少なくとも、国民に対して不安感を与えていることは事実です。とくに、個人情報に関しては、それが、どこで、どのように悪用されるかもしれないという不安がつきまといまいます。また、電子マネーやネット通販が一般的になって、預金口座やクレジットカードなど、個人財産への危険性も拭いきれません。

データ漏洩の中でも、最近とくに多いのが、個人情報、つまり、住所・氏名・生年月日・家族構成・年収・口座番号・クレジットカード番号などの情報が入った名簿などの持ち出しが多いのですが、今後は、情報処理の履歴を記録したログの漏洩も気になる場所です。内部統制の一環としても、情報処理プロセスのすべてを記録することも傾向としてありますが、こうした情報にはいろいろな要素が含まれていますから、その利用の善悪には紙一重の危険性があります。

こうしたことへの対応は、一般的には、セキュリティ対策として数々の手が施されています。そして、それを具体的に企業姿勢として示す方法として、ISMSなどの各種認定制度を利用している企業が多くなっています。それぞれの企業のホームページにもセキュリティポリシーを掲げ、CSR(企業の社会的責任)やコンプライアンス(法令順守)を謳うことが一般化さえしています。

社会への不利益を考えると、このデータ漏洩などによる社会・国民への不安のほか、いくつかの要素を含んでいることがわかります。そして、これらが、直接的・間接的にかかわらず、かなりシステム運用に関係していることもあらためて認識させられます。

もう、過去のニュースですが、東京証券取引所で、株の売買数に制限を持たざるを得ない状況に陥ったことが報道されました。コンピュータのキャパシティの問題だったようですが、これもシステム運用が関わっている大きな問題でもあるわけです。結局、こうしたトラブルで、国家としての威信が低下したことは否めない事実です。

また、データの改ざんによる問題も多くあります。試験データを改ざんして、商品の品質や性能をよく見せようとした例も数多くあります。こうしたものの中には、排ガス、原子力発電など、環境破壊につながる可能性をもったものもあります。もちろん、すべてが企業情報システムで維持しているデータだけではないかもしれませんが、少なくとも、そうした危険性はどこにでも潜んでいるということになります。

データの改ざんというものではないものの、データがうまく活用されていないことによるさまざまな問題もあります。つまり、しっかりしたシステム監査を行っていれば

発見できた問題が眠っているケースも多いのではないのでしょうか。最近の言葉でいえば、データの透明性ということになります。自動車のリコール問題などは、一種のデータの透明性を必要とするものかもしれません。このような、企業や社会の生命に関わるデータは、特定のものだけに秘匿されるものではなく、経営として、少なくとも透明性をもったしくみの中で蓄積・運用されなければなりません。

システム運用の現場では、日々の障害があとを断ちません。バッチ処理の遅延。この遅延による影響は、業務部署や取引先、そして、オンラインの開始時刻の遅れ、場合によっては顧客にまで及びます。そして、それらは機会損失や取引停止に至る可能性をもっています。業務システムのメンテナンス後に発生する、処理の異常終了や処理結果の不具合も、相変わらず続いています。

スケジュールミス、データ投入ミス、コンピュータの操作ミス、処理結果の確認ミス等々、何十年も前から、それら障害の発生する要因はほとんど変化していないのが実情です。そして、これらの回復処理や再処理で起こる二次障害。これらのほとんどは人的障害ですが、完全に取り払うことのできない問題です。

最近では、とくに環境の変化が激しく、さまざまところでその影響も出ています。ネットワーク障害やリソース不足などはその典型でしょう。ネットワークもシステムリソースも、いまでは広範囲にわたっています。そして、捉えどころがないほど変化し続けています。まるで、浮遊物のようです。これに、入力データの多品種・多量化がより加わって、キャパシティもパフォーマンスも、予測がつかないほど複雑になってきています。こうしたことが、先の東京証券取引所で起きたような障害になっていくことになります。

情報処理システムの社会的責任を考えた場合、その責任をシステム運用だけで果たすことはできません。これと同じように、業務システムの開発や保守だけで果たすこともできません。これらが一体となって取り組んでいかなければならない、企業にとって重要な課題です。

最近では、日本版 SOX 法が話題を賑わしています。これも一種の社会的責任を果たす上で重要な法律となりますが、単に財務に関わる業務部署だけの問題にならないことは、いまや常識として知られています。企業内のほとんどの業務はシステム化されており、この業務システムを維持運営している情報処理システムを除いては、なんら解決できないものだからです。

日本版 SOX 法には、いわゆる、財務報告の虚偽記載を防ぐための内部統制が求められているわけですが、この虚偽記載というものを、いろいろな角度から防ぐとともに、これが行われていないということを証明できるしくみが必要です。もちろん、現状の業務システムでは十分対応できているとはいえません。そのため、多くは、日本版 SOX 法への対応と銘打って、さまざまな業務システムへの改修が行われることと思います。しかし、ここにも多くの危険性をはらんでいます。業務システムの改修には障害発生が付きものだからです。

そして、また、業務システムの改修だけでも、日本版 SOX 法への対応は不完全です。企業情報システムは、日々、変化し続けています。経営、ビジネス、商品、取引先、顧客、コンピュータシステムのハードやソフト、法律や規制、こうしたものが刻々と変化し続けています。そして、そのすべてが、何らかの形で企業の情報処理システムに関係しています。このような変化の中で、情報処理システムを安定的かつ安全に維持管理しているのがシステム運用なのです。

その上、システム運用は、企業のほとんどすべての情報を蓄積管理しています。こうした情報を活用する手段ももっています。日本版 SOX 法の対応のために、業務システムを改修するという手段は極力避けるべきです。つくらずに済ませる方法も考えるべきです。企業情報システムの HUB 的役割をもつシステム運用、ここにそのヒントがあります。