システム運用「人としくみ」

最近の ICT に関する話題のひとつに BCP があります。BCP は Business Continuity Plan の略ですが、日本語では事業継続計画と訳されています。BCP。とても目新しい言葉のように思えますが、経営責任から考えればごく当たり前のことです。ただ、経営・ビジネスそのものが ICT に非常に大きく依存するようになり、企業が社会的責任を果たす上でも、いまや欠かすことのできない 1 つの課題であるといえます。そうしたことから総合的かつ体型だったしくみが求められているのではないでしょうか。

これからのシステム運用

システム運用と事業継続

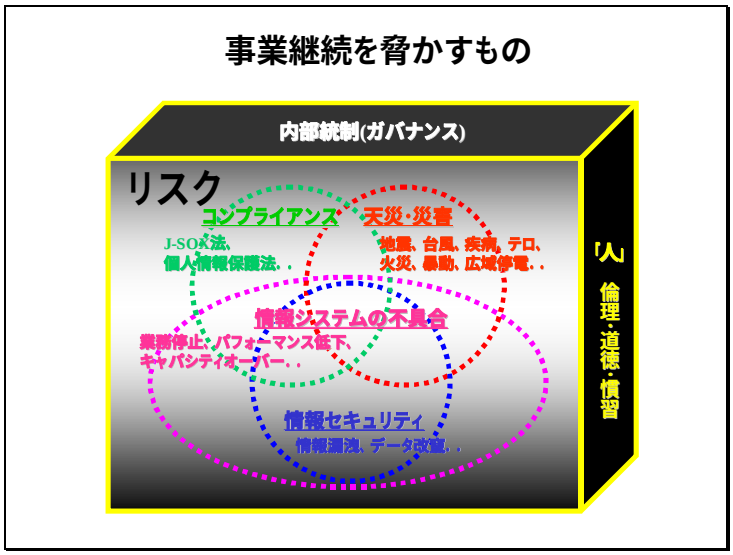
内閣府が発行している「事業継続ガイドライン 第一版 平成 17 年 8 月 1 日」によると、事業継続計画（BCP）を次のように定義しています。

企業は、災害や事故で被害を受けても、取引先等の利害関係者から、重要業務が中断しないこと、中断しても可能な限り短い期間で再開することが望まれている。また、事業継続は企業自らにとっても、重要業務中断に伴う顧客の他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守る経営レベルの戦略的課題と位置づけられる。こうした事業継続を追求する計画を「事業継続計画」（BCP） と呼ぶ。

「事業継続ガイドライン 第一版 平成 17 年 8 月 1 日」は、内閣府 防災担当 企業評価・業務継続ワーキンググループの「民間と市場の力を活かした防災力向上に関する専門調査会」が発行したものです。

他の文献にもいろいろな定義がありますが、おおよそは上の定義と同様の内容となっています。しかし、いままでにも、私たちは危機管理やリスクマネジメントという取り組みをしてきており、これらとどういう関係になるのかを明らかにする必要がありそうです。また、重要業務を中断させる可能性のあるものは、災害や事故の被害によるものだけか、ということに対しても考えていく必要があります。

いずれにしても、事業継続を追求することは、企業経営にとって、必要・不可欠な戦略的課題であることには違いありません。図－２７は、企業の事業継続を脅かすものにはどのようなものがあるかを概観したものです。



（図－２７）事業継続を脅かすもの

システム運用から見ても、事業継続を脅かすリスクには非常に多くのものが含まれます。とくに最近では、ICT が企業経営の根幹をなしていることからも、こうしたリスクを真っ正面から捉えていかなければならなくなってきています。BCP の定義にあるような災害や事故によるものだけではなく、図－２７にあるような、法令違反や環境破壊、あるいは、情報システムの不具合など、事業継続を脅かすものは多岐にわたっていると考えるべきです。

いままでにも述べてきたように、コンプライアンス(法令遵守)に関しても、企業の存続を脅かす大きなリスクを負っています。いまは、企業が、単独で社会に存在することは非常に希になってきました。どんなに小さな企業でも、その顧客をはじめ取引先など多くのステークホルダーが存在し、そういう中で経営が成り立っていることを考えると、一企業の責任だけで物事を考えることはできないわけです。

しかも、ICT が企業のインフラとなっていることを合わせて考えると、情報システム、とりわけシステム運用の果たすべき役割がいかに重要であるかがわかります。天災や事故に限らず、あらゆるリスクを完全になくすことはできません。いつ、どのようにリスクが発生するかは誰も予測できないわけです。それだけに、日々の地道なリスク対応活動が非常に重要になってきます。いくら良いしくみを用意したとしても、そのしくみに血を通わせ活動させておかなければ、いざというときに何の役にも立たない結果を招いてしまいます。

事業継続を脅かすもの、つまりこのリスクには、図－２７に示すように、コンプライ

アンス、天災・災害、情報セキュリティ、情報システムの不具合などがあげられます。これらのどれをとってみても、企業の情報システムが寸断される危険性をもっています。また、こうしたことを通じて、企業経営そのものの継続を絶たれてしまう可能性も含んでいるわけです。さらに、社会的責任という観点からも、企業・事業の継続を絶たれてしまう危険性が非常に大きくなってきています。これは、社会から要請される企業の倫理面によるところが大きいと考えます。

いままでにも多くの企業が、さまざまな取り組みを行ってきました。とくに、天災・災害の分野については、日本は地震国ということもあって、その対策には早くから取り組んできた経緯があります。バックアップセンターの建設、地震対策を施した建屋建設、自家発電装置の建設など、多額のコストをかけ大がかりな取り組みを行っている企業もたくさんあります。また、自社では、コスト面から採算がとれないということで、信頼のおけるデータセンターへのアウトソーシングを行っている企業もあります。

このように、個々のニーズによってさまざまな取り組みを行ってはきているものの、それらを１つの考え方に整理した取り組みにはなっていないように思います。危機管理は危機管理、情報セキュリティは情報セキュリティ、コンプライアンスはコンプライアンスというように、それぞれ個々に、時代時代のニーズに合わせた対応となっているのが実態のようです。

最近は、コンプライアンスの面から内部統制の必要性が叫ばれています。そして、ICT に関するものは IT 統制(IT ガバナンス)といわれています。J-SOX 法への対応のための内部統制というような具合です。しかし、ICT の側面からは、事業継続を脅かすリスクから身を守るための内部統制と考える方が理解しやすいし、取り組みやすいのではないかと考えます。図－２７はこうした考え方を表しています。

もちろん、すべてが ICT だけで解決できる、あるいは対応できるわけではありません。企業組織のすべてに関わるものもたくさんあります。しかし、ICT は企業のインフラストラクチャーとなっていますから、少なからず ICT はすべてに関与せざるを得ない状況にあることは事実です。そして、それがシステム運用の果たすべき役割だと考えます。日々の継続した活動からさまざまなリスクを回避することができるからです。あるいは、発生したリスクに速やかに対応できる体制を築くことができるからです。

さまざまなリスクに対応すべく、さまざまなしくみが用意されたとしても、そのしくみを生かすも殺すも「人」次第ということになります。最近発生している災害や事故の多くは、この人によることが非常に多くなっています。ICT とは関係のないことで

すが、2006 年 8 月 14 日に発生した首都圏の停電事故も、クレーン船を操作していた人の問題でした。情報隠しなど、多くの不祥事も人に起因しています。また、情報漏洩やデータ改ざんなども人によるものです。このように、事業継続のための内部統制を行っていくためには、「人」の面を十分考慮していかなければならないのです。

それは、ICT に関わる人だけではなく、企業全体の人を対象にしなければなりませんが、すくなくとも、ICT に関わる人、とりわけシステム運用に携わる人たちには、倫理観、道徳、社会慣習の面からの適切な行動が求められます。そのための教育も必要となります。内部統制もさまざまなしくみから成り立つ 1 つの大きなしくみになると考えますが、このしくみを活かし、企業経営(事業)の継続を守るのは、システム運用、そして、それを担う「人」なのです。