特集

組織の経営戦略に活用される、IT 化・情報化とは

IT 化・情報化が加速する今、組織はどのような観点を持ってその取り組みを進めるべきなのか。今回の ISONET 特集では、組織が注視するべき点や具体的にどのようにして IT 化・情報化を進めていくべきかを緒方 健氏にお答えいただいた。

経営戦略において必要なデータを明確化にすることが重要

―― 多くの組織が「IT 化・情報化」に向けて、現在取り組みを進めていると思いますが、その第一ステップとしては、何が挙げられますか。

「IT 化、情報化に向けて組織の方々の中には書類作成を PC で行うことを取り組みのひとつとして認識されている方もいらっしゃいます。しかし、PC の書類作成用ソフトはあくまで清書用のものなんです。これまで手書きで作成していたものを、PC で作成することで、誰もが綺麗に仕上げることができ、あるいは、時間を短縮できるといったことが可能になりますが、それだけで IT 化・情報化とはイコールにはなりません。

また、建設・設計事業を展開している組織の方でしたら、紙ではなく電子データでの納品などにも取り組んでいらっしゃると思います。しかし、これもまた、IT 化・情報化というより、省スペースという要素が実情としては大きいと思われます。もしくは、データ保存によって、ドキュメントを探し出すための、検索性の向上ですね。そこから一歩先に踏み込むことが、IT 化・情報化の第一ステップと言えると思います」

―― 一歩先と言いますと、具体的にどんな取り組みがあるでしょうか

「データを分析に用いるということです。単純にデータが羅列しているものではなく、ある目的があって、その目的を達成するための手段として、それらのデータから情報をすくい上げ

て、分析・活用するのです。

そのためにも、組織の方々は、まず、自分たちにとってどういう情報が必要かということを、明確にする必要があります。これは階層によって異なるため、それぞれの層にとって必要なデータは何かを洗い出すことが必要だと考えます。

必要な情報を明確にできたら、その情報を得るためのデータをまとめる段階になりますが、ここで重要なのは日常業務の中で具体的にどのように吸い上げていくか。その構築を図ることです。一番良くないのは、そのために新たに別の資料を作成することです。日常業務の中で、自然と必要な情報が蓄積され、分析などに用いられるデータベースが構築されていく。そして必要なときに、その蓄積された情報の中からピックアップする。そうした形が、あるべき姿だと思います」

―― そういう考え方を元に、フォーマットを作って、書類を作るようにすれば、それがデータとして構築されるんですね

「そうです。これは経営にもつながると思いますが、一定のコンセプトがあって、その上で情報化や IT 化といった戦略が出てくるんです。それから、個別の IT システムという発想を入れていきます。つまり、IT 化も情報化も、経営戦略の1つとして考えるのです。だからこそ、経営戦略において、どんな情報が必要かを明確にしなければ、IT 化も情報化も進みません」

―― 事業内容によっては、“職人”の要素が強く、技術やプロセスが組織全体に蓄積されない場合もありますよね

「そうなんです。技術やプロセス、ノウハウが人に溜まって、組織に蓄積されない。つまり、特定の人が現場を離れてしまうと、組織に継承されなくなってしまうのです。そのため、技術、プロセス、ノウハウは『見える化』することが重要なのです。

私は、『システム化』は、見えていないものを見えるようにすることと捉えています。業務プロセスを整理して、どのような指標が必要かを考察し、それをシステムに組み上げていきます。組み上げる際、『IT と人』とのバランスが必要になります。IT は万能ではありません。人の手に頼る方がいい場合もあるのです。そうした意味でも『標準化』が大切です。全てをルール化することは難しいので、原則的な処理と、例外的な処理についても柔軟に対応するために、イレギュラーなものについては、現場でうまく対応できるように遊びを利かせるシステムを構築していくことが、現場の人にとってもスムーズに進行できると考えます」

セキュリティ面において重要なことは、対応すべきリスクの明確化。

―― IT 化・情報化を進めるにあたって『セキュリティ』における課題やリスクは必ず発生すると思いますが、この点についてはどのような課題・リスクがあると考えられますか？

「IT 化・情報化の1番のインフラは社内外のネットワークですから。それらにまつわるセキュリティのリスクや課題は当然、発生します。この点において、組織の方がまず考えるべきは『何か起きた時、自分たちがどこまで対応できるのか』です。具体的な方法としては、まずネットワークを使用することで、業務の効率性がどのように上がるか。あるいは今までできなかったことが、どのようにできるかを考察します。そこから、必要なセキュリティは何かを考えるのです。リスク0は、ありえません。また、リスクを過剰に考えるあまり IT 化・情報化を進めないというのも本末転倒です。だからこそ、自分たちが対応できるリスクの割合を決めておく必要があるのです。そして、そのラインを超えないためにどのようなシステムを構築するかという発想を持たなければ、ネットワークを使った IT の活用はできないと思います。そのため、メールひとつにしても、対応は組織によって異なります。迷惑メールの処理の仕方や管理方法など、それぞれの組織が抱えるリスクに対応するために、どうすれば良いかを考えるのです」

―― セキュリティの取り組みとして、よく見られるのがメールへ添付したデータのパスワードの後送などがありますよね。

「私はよく例えるのですが、メールはハガキのようなものであると考えています。つまりハガキのように他者にも内容が見えますし、また見られたかどうかも分かりません。だから、パスワードを後送しても、間違ったアドレスに続けて送ってしまうと意味がありませんし、もしかしたら他者に見られているかもしれません。そう考えると、リスク回避として役割を果たしているか疑問ではありますね。そうした観点から見ると、パスワードの後送も、例えばメールを送った後に、送り先から『受信しました』と連絡を受けてからパスワードを送るというやり方であれば、誤送信をしたときのリスク対策としての意味もなくはありません。しかし、サーバに残るデータやセキュリティ対策のない無線 LAN の通信等で他者に読まれるリスクは、依然残ります。

前述の通り、セキュリティにおけるリスクをどこまで抱えられるかが大切なので、ハガキはハガキ、封書は封書でそれぞれ使い方を見極める必要があります。ハガキで送ってリスクがあるなら、暗号化をする、オンラインストレージを活用するなどの方法があります。

自分たちの組織を知り、対応できるリスクはどこまでか、その対応方法をしっかり見極めるこ

と。それが、組織にとって意味のあるIT化・情報化へとつながるはずです」

緒方　健氏　プロフィール

おがたコンサルティング代表。情報セキュリティ、個人情報保護、ISO、知的資産経営に関するコンサルティング、監査・認証審査を行っている。

経産省高度情報処理技術者、プライバシーマーク主任審査員、医療情報技師、行政書士などの資格を有し、国の医療系研究プロジェクトのセキュリティアドバイザー等を務める。