

月刊「ビルメンテナンス」2001 年 8 月号 42 ページの掲載記事

「ビジネス」を進化させるための IT とセキュリティ

国を上げての IT (情報通信技術) 革命が進行しているという。

我々は、その意味を的確に理解し、取り組んでいるだろうか？

The business of America is business.

(アメリカの本務はビジネスだ！)

- Calvin Coolidge (30th U.S. President, 1872-1933)

に代表される「彼らのビジネス」に対抗すべき我々の戦略、戦術、業務遂行について考える！

冒頭に掲げた第 30 代アメリカ大統領 Calvin Coolidge の言葉にあるように、彼らは 1900 年代初頭から既にビジネスで世界をリードするべく準備を始めて、今日に至っている。

彼らのビジネス論については、別の機会に考えることにして、彼らがビジネスに使おうとしている IT とは何かを知ることは大変重要なことだと私は考える。

ここでは、IT の基本をまず紹介したい。

そして、それを戦略的に使う (言わば、攻めの IT) の一例としての CRM (Customer Relationship Management : 顧客指向システム) の考察を行った後、守る側の情報セキュリティについて解説したい。

IT (情報技術) とは...

4,5 年前までは、企業経営における資源といえば、「人・物・金」と答える方が大半だったと記憶している。

昨今は、これに 4 つ目の資源である情報が当然のごとく語られ、この情報資源を活用することが企業の優劣を決するといっても過言では無くなってきている (図 1)。

では、この情報とは何なのか？

私がこの業界に入ってまもなく、さる経営コンサルタントから情報とは「なさけのしらせ」「なさけにむくいる」という表現をお聞きしたことがある。

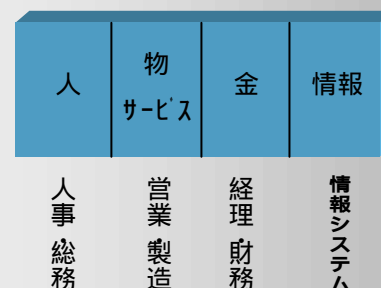
その方は「経営者が、あーよかった、これが知りたかった、というものが情報なのですよ！」と教えてくれた。

本当にこれでいいのだろうか？と、その禅問答的な回答に対してすっきりしないまま思い続けてきた私は、2 年前に知ったカナダ、ブリティッシュコロ

ンビア州立大学のインターネット授業を受けて、自分の考え方をかなり整理することができた。

ここで、その一部について英文を交えて紹介したい。

図1
企業活動に必要な4つの資源と主要部門の関係



北米の大学一年生が勉強する「Introduction to Information Technology」では、広義の意味において「情報」を以下の1行で説明している。

In the broadest sense, information is data that has a context.

この文章の最後にあるコンテキストとは、周囲の状況や時間の経過等、その意味を明確化できる状態、あるいは関連した出来事である。

情報とはデータがコンテキストを持ったものである。

なんと分かり易い表現ではないか！

誤解がないように一言言わせて頂くが、「米国は低コンテキストの労働文化であり、取引は当事者たちが電子メール、手紙、電話、その他のコミュニケーション手段を通じて明示したことに基づいて行われる。一方、ヨーロッパやアジアの文化の多くはそれとは対照的に高コンテキストの文化であり、暗示されているものも同じく重要である」という馬越恵美子氏（NHK やさしいビジネス英語、土曜サロン）の分析にあるように、私は“高コンテキスト文化”を持った日本人の一人であることを誇りに思っている。本題に戻るが、前述にある北米の大学生が勉強するITテキストでは、情報システムとは、データを扱い、保存して、それを処理し、アウトプットとして情報を提供するシステムであると述べた後で、このシステムに関して私達が身近になればなるほど、我々の考え方を創造的にしてくれる利点に気付くだろう、と説明している。

さらに、日本では既に過去のもののよう扱われているMIS (Management Information System : 経営情報システム) を次のように説明している。

MIS refers to a system that gathers, condenses, and filters data until they become information, and then makes it available on time, and in a useful forms, for use in decision making at various levels of management within an organization.

MISとは、データが情報となるまで、そのデータを集め、要約し、フィルタリングして、組織の様々なレベルで意思決定をするために、その情報を欲しい時に、役に立つ形式で提供する仕組みである。その後で、ITについて以下のように言及している。

Information Technology - a collective term for the computer and communication hardware and system and application software - to make their employees more productive and their business more effective and efficient.

ITとは組織の生産性を高め、ビジネスをより効果的に、効率よく実現させために使われるコンピュータ、コミュニケーションハードウェア、システムおよびアプリケーションソフトウェアの総称である。

グローバル時代の企業モデルとは

前述のようにITは、情報をより正確に、役立つ形で、それが必要とされる時、場所に、必要とするユーザに提供するための「道具」といえる。

英文では、以下ようになる。

By assembling, storing, transmitting, processing, and retrieving data, Information Technology helps make information more accurate and useful, and make it available when and where it is needed.

そのために、情報システム部門はユーザが所属する組織の「ビジネスの本質」を理解することに努め、

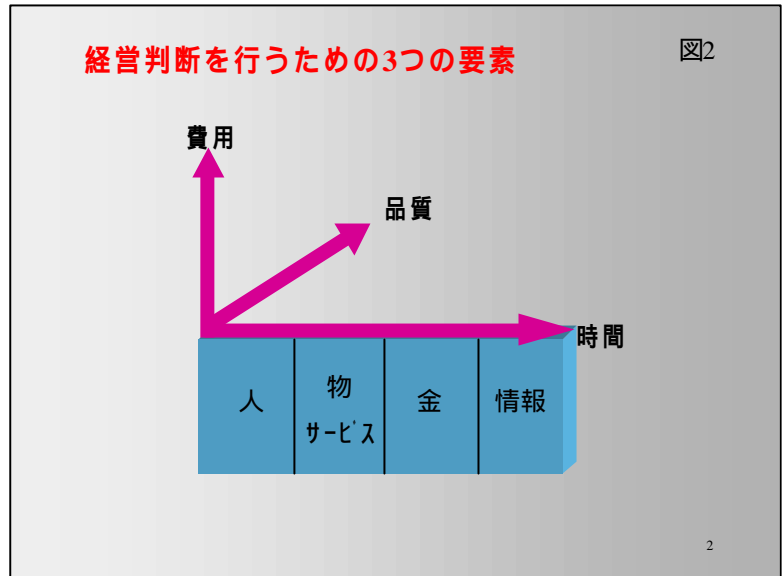
ITによって彼らの「ビジネスを改善する」ことがミッションとなる。そして、ユーザ側の管理者や経営者はITを駆使して、提供された情報によって意思決定を行うのである。

この意思決定に関する私自身の考え方を述べてみたい。

企業経営における意思決定＝経営判断を行う要素は、「時間」「品質」「費用」の3つであると考えられる（図2）。

管理者および経営者は、その企業および組織が保持している「人・物・金・情報」の4つの資源を考慮しながら、上記3つの要素で意思決定を行うのである。

例えば経営者は、手持ちの資金と人材では、この位の時間＝スピードと、この位の品質＝サービスが可能であり、その場合の費用＝コストはこれ位を掛けていいだろう、といった経営判断をしていることになる。

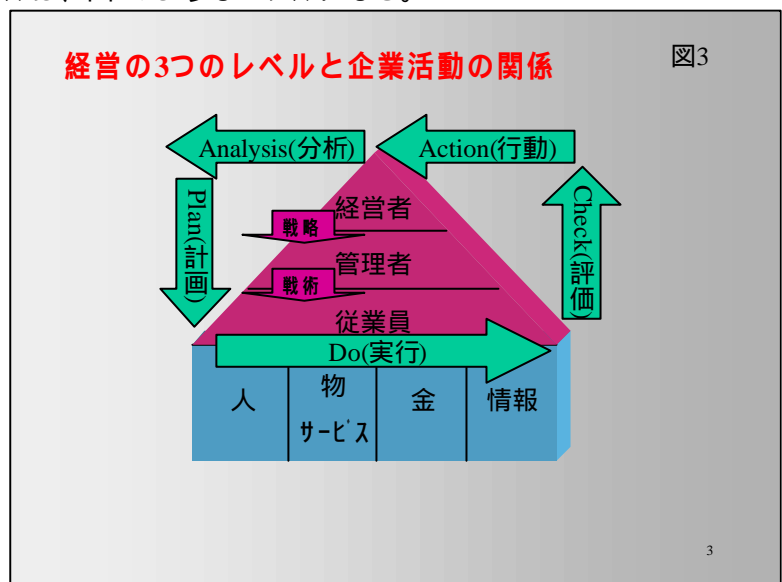


その経営者に、より正確で、役立つ情報が、素早く提供されれば、その意思決定はよりよいものとなることは疑いの余地はない。

一方、一般的な企業における組織のレベルは、図3のようなモデルになる。

この上側にあるピラミッドの3つのレベルでは、経営者が策定した「戦略」に基づいて、管理者が「戦術」を立案し、その戦術に則した日常の業務オペレーションが一般社員によって実行される。この企業活動では、P（Plan）D（Do）C（Check）A（Action）の絶え間ない業務プロセスの反復が行われる。

近年は、このPDCAに加え2つ目のA（Analysis）がDWH（Data Ware House）等のITを使って活発に行われるようになってきた。



しかしながら、世界規模での企業競争の時代を迎えて、これまでのピラミッド型の企業組織では対応が難しくなっている。

図4は、グローバル時代の企業モデルのイメージである。

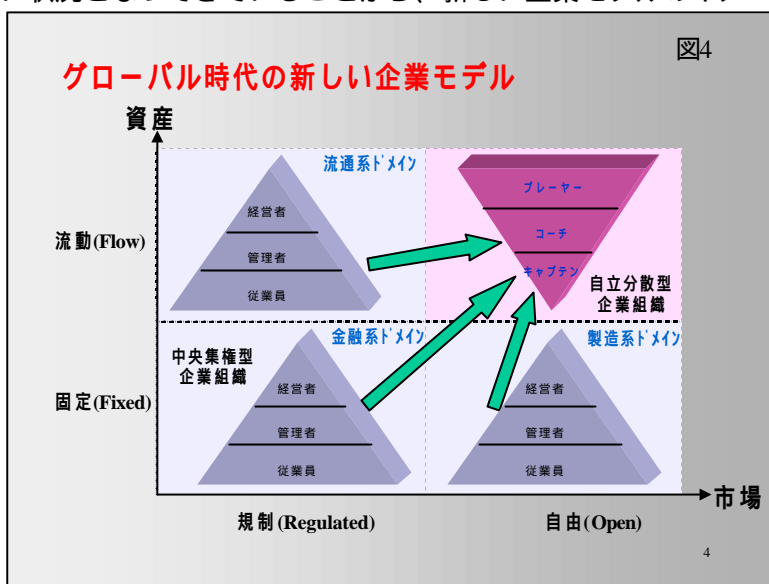
この図では、グローバル時代の「市場」が規制市場から自由市場へと移行する横軸と、企業の価値を評価する「資産」が固定資産から流動資産重視に変化していく縦軸の中で、従来の「中央集権型企業組織」

では企業活動が閉塞していかざるを得ない状況となってきたことから、新しい企業モデルのイメージを考えてみた。

例えば、従来の企業の代表的な業種を、左下ドメイン（規制市場、固定資産重視）の金融系ドメイン、左上（規制市場、流動資産重視）の流通系ドメイン、右下（自由市場、固定資産重視）の製造系ドメインと考えてみて頂きたい。それらのドメインにある企業は全て、右上のドメインへと移行せざるを得ない状況にあると考えられる。

その右上のドメインでは、新しい企業モデルである「自立分散型企业組織」へと変身せざるを得ないと私は考えている。

この図については、数年前にSAP社日本法人の副社長でいらっしゃった住忠明氏からヒントを頂いた。住副社長は当時、アメリカンフットボールのようなダイナミックな企業組織がこれからの日本に必要であり、従業員、管理者、経営者の3つのレベルもプレイヤー、コーチ、キャプテンと呼んでいらっしゃったことに私は感銘したものだ。

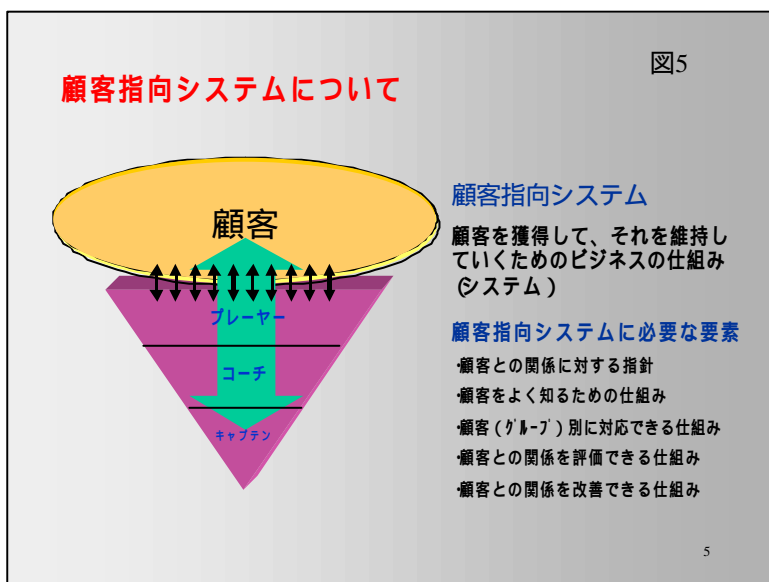


戦略的な情報の活用

このピラミッドが逆さまになった「自立分散型企业組織」のモデルは、CRMを説明するにも非常に都合がよい組織形態といえる（図5）。

一般的には、顧客との日常のコミュニケーションはこのプレイヤーによって行われている。

CRMを一言で表現するならば、CRMは「顧客を獲得して、それを維持していくためのビジネスの仕組み」であるといえる。



紙面の関係から、顧客指向システムのアーキテクチャーについては割愛するが、結論としてのCRMのイメージは図6ようになる。

この図において、管理者および経営者は、図2、3で説明した企業活動の関係を理解して、図4、5で述べた新しい企業モデルのイメージにおいて、Plan Do Check Action + Analysisのサイクルで粘り強く、徹底的（Radical）にCRMを実践していく必要がある。

そのためには、戦略的経営のツールとしてITを活用していかなければならない。

では、その戦略的経営とはどういうことなのだろうか？

数年前までのMISは、受注入力や在庫管理といった業務系取引の処理に重点がおかれていた。その後、ビジネスが発展するに伴い、グローバルな競争と複雑さが増加する中で、経営に対する新しいデマンド（要求）が起こってきた。

前述のITテキストには「この新しいデマンドに上手に適応するために経営者は戦略を明確に述べ、計画して、実行

しなくてはならない。その戦略とは、変化、競合、および不確かなことに対処するためにデザインされたアクションプランである」と書かれている。以下にその英文を紹介する。

To cope successfully, management had to place more emphasis on formulating, planning, and executing **Strategies**, which are plans of action designed to cope with change, competition, and uncertainty.

そして、戦略的に情報を使うことは経営者に以下のことを考えることを要求している、と結んでいる。

- (1) Where the organization is heading.
- (2) How the competitive environment in which the organization operates is changing.
- (3) The consequences of those changes to the organization.

直訳すれば、1) その組織はどこに向かっているのか。2) その組織の業務において競合環境はどのように変わっていくのか。3) その組織にとって変化することの結果は…。

We must change. あるいはYou must change.という掛け声をよく聞く。

では、具体的にどう変わっていけばいいのか、また自分達が変わったらどうなっていくのか、そのことを経営者はきちんと語り、率先して範を示すべきである。

珈琲ブレイク：Computer Literacy

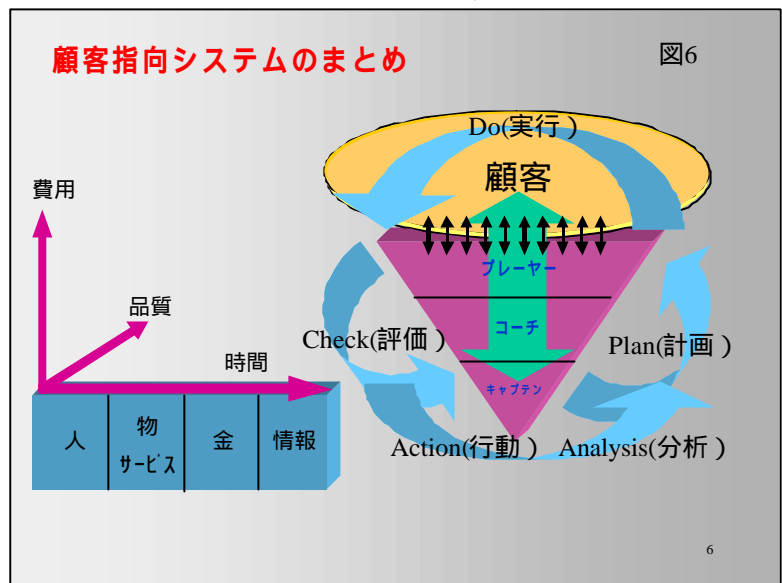
ITを使いこなすためには、コンピュータに関するリテラシーが必要だ、とよく言われる。

このリテラシーとは、問題解決のためにコンピュータを使う知識やスキルを意味する。

このコンピュータリテラシーに対する一般的なアプローチは、以下の3つである。

- 1) コンピュータについて読むこと
- 2) コンピュータを使うこと
- 3) アプリケーションを開発すること

リテラシーとは、読み書きする能力（語学力）であり、語学力があるからと言って、全ての人が小説を



書くわけではなく、読者の立場のほうが圧倒的に多い。そのレベルは全ての人に一律に要求されるものではない。

しかし、コンピュータは楽器と同じように表現のメディアと言えるので、より有益なツールをいかに使うかを学ぶことは、そのコンピュータの表現力の恩恵を最大限に享受することになる。

以下にその英文を紹介する。

But in many ways, computers are like musical instruments in that they are a medium of expression.

Learning how to use the more advanced tools allows you to take full advantage of the computer's expressive power.

情報セキュリティについて

ここまでは、使う（攻める）側の立場で、ITを考えてきた。

ここからは守る側の立場の「情報セキュリティ」について解説したい。

一般的には、企業における第4の資源「情報」の主管部署は情報システム部門であり（図1参照）以下の3つの役割を担っている。

- 1．ITインフラの整備・維持
- 2．システムの導入・開発およびその運用・管理
- 3．情報管理

上記1、2については、ITの知識とスキル、および業務経験等のノウハウを駆使して構築・運用されるものである。

では、3の情報管理とは一体どのような業務であろうか？

情報システム部門の情報管理とは、「**情報を保存するコンピューターシステムの安定した、安全な稼働を保証する**」ことであり、その業務は以下の3つに集約される。

- 1．障害対策

情報が保存されているシステムの無停止化対策と障害が発生した場合の復元対策

- 2．性能

情報がとりだせるようなパフォーマンスを適正に維持

- 3．セキュリティ

情報の安全を侵す危険・脅威から守る

この3．セキュリティについては、インターネット利用の拡大とともに、最近特に注目されるようになってきた。

コンピュータとネットワークを使いこなせば使いこなすだけ、企業活動において電子データは増加の一端をたどる。

この電子データには顧客、製品、仕入先、経理、経営などの機密情報が含まれている。

しかし、電子データゆえに、簡単に破壊、改ざんされたり、瞬時にコピー、漏えいされてしまうことがある。

そのため、コンピュータ・セキュリティとは「許可されていない参照および露出、改竄、破壊からデータや情報を守ること」といえる。

図7は、そのセキュリティを4つのレベルに整理したものであり、セキュリティが破られた結果としての脅威（危険性）は下から順に大きくなっていく。

情報システム部門のセキュリティも、このレベル毎に実装することになり、各々のレベルの代表的な対応策は以下になる。

レベル1：建物内への侵入

- ・マシンルーム施錠・入退室管理
- ・PC起動時のパスワード設定

レベル2：外部ネットワークからの侵入

- ・ネットワークログイン
- ・FireWallの設置
- ・不正侵入検出システムの導入
- ・VPNの導入、One-Timeパスワードの利用

用

レベル3：システムに対するログイン

- ・NTサーバへのログオン、メインフレームへのログイン等
- ・サーバへのアンチウィルスソフトウェアの導入

レベル4：ファイルなどのオブジェクトに対する操作

- ・アクセス制限の設定
- ・PCへのアンチウィルスソフトウェアの導入

上記のレベル毎の対応に加え、セキュリティ評価ツールの導入や関連会社も含めた全社的なセキュリティ教育の実施が必要となる。

次に、セキュリティ管理のキーポイントを列記して簡単な解説を行いたい。

1．Create & Implement Policy

セキュリティポリシーの作成、導入と実行は不可欠である。

2．Ongoing Process

セキュリティはワン・タイム(one-time)ソリューションではなく、継続的なプロセスである。

3．Executive Involvement

セキュリティの実現には役員レベルの参加が必須である。

4．User Acceptance

セキュリティが不可欠であることをエンドユーザに納得してもらう。

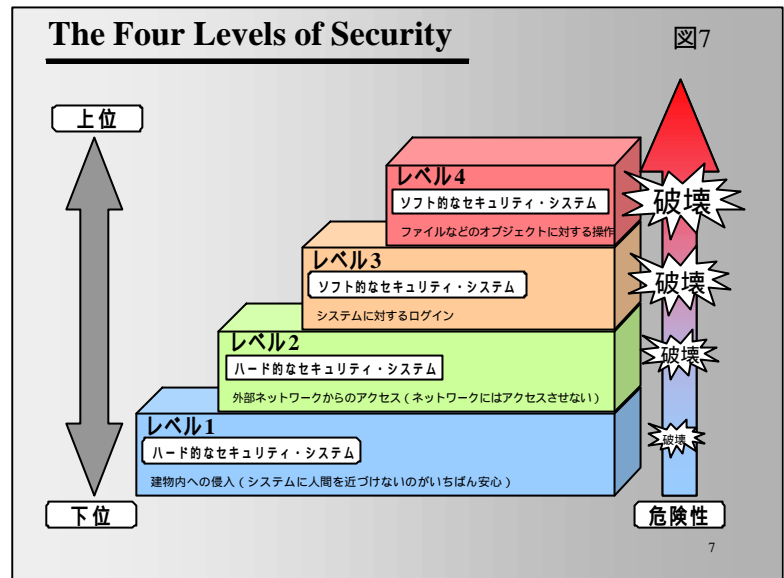
5．User Education

エンドユーザがセキュリティを認知して守るように継続的な教育を行う。

6．Regular Update

今日のビジネスのスピードとITの進化を考えると、セキュリティポリシーの定期的な見直しと更新は必須である。

7．Thoroughness



システム全体の攻撃されやすい個所と実際の侵入を徹底的かつ継続的に監視する。

まずは、セキュリティに関する制度と規則を明記した体系だったセキュリティポリシーの策定に一刻も早く取り組んで頂きたい。

最後に、米国Network Computing誌の記事“ Best Practices in Network Security ”にある「セキュリティに関する新しいグランドルール」を以下に紹介したい。

紙面の関係から、記事の一部を抜粋・直訳したが、原文の意味合いをきちんとお伝えするには難があるので、興味のある方は以下のURLにある記事にアクセスして頂きたい。

<http://www.networkcomputing.com/1105/1105f2.html>

- 1．セキュリティと複雑さは、しばしば逆比例する。
- 2．セキュリティとユーザの使いごちは、しばしば逆比例する。
- 3．実装されない完全なセキュリティよりも現在あるよいセキュリティの方がよい。
- 4．セキュリティに対する間違った考えは、非実装のセキュリティに対する正しい考え方よりも悪い。
- 5．セキュリティは一番弱いリンクと同じだけの強さしかない。
- 6．既知の、あるいは起こりそうな脅威に集中した方がベストである。
- 7．セキュリティは投資であって経費（コスト）ではない。

上記のグランドルールを前提にして、セキュリティポリシーを一度作成すれば、後の作業はセキュリティの実装となる。

前段の「戦略的な情報の活用」でも述べたが、セキュリティにおいても、管理者および経営者は、その企業および組織が保持している「人・物・金・情報」の4つの資源を考慮しながら、「時間」「品質」「費用」の3つの要素で意思決定を行い、Plan Do Check Action +Analysisのサイクルで粘り強く、徹底的（Radical）にセキュリティを実装して頂きたい。

（こまい しのみ/ビジョン クエスト株式会社）

【本記事に関する問合せ】

〒100 0014 東京都千代田区永田町2 17 4

笠松ビル3F

ビジョン クエスト株式会社

コンサルタント 駒井 忍

TEL：03 3580 4913

FAX：03 3580 0922

E-mail：komai@visionquest.co.jp

<http://www.visionquest.co.jp>