いま、米国企業でCSOが注目される理由
―CSOによる総合的な企業セキュリティ統括の重要性

株式会社ジュリアーニ・セキュリティ & セーフティ・アジア
代表取締役会長兼CEO　齋藤ウィリアム

セキュリティを統括するCSO

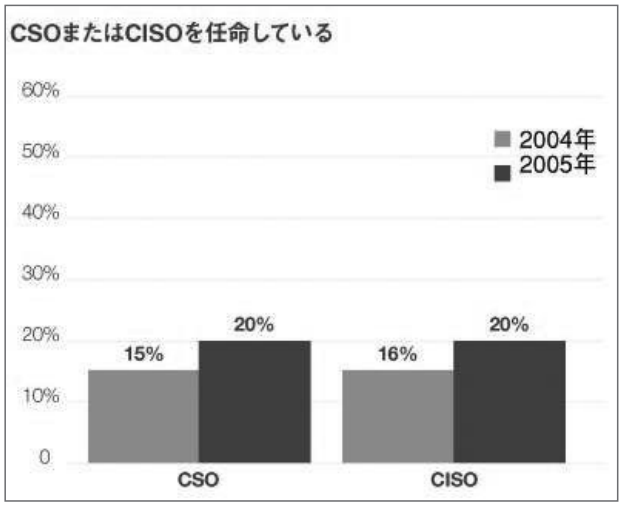
ここ数年、米国企業においてCSO（Chief Security Officer= 最高セキュリティ責任者）に対する認識が急速に高まっている。

日本でセキュリティ責任者といえばIT部門のセキュリティ担当者をイメージする場合が多いが、これはCISOであってCSOとは異なる。

CSOが担当するのは狭義のITセキュリティだけではない。物理セキュリティ、組織セキュリティまでふくめた総合的な企業セキュリティ、危機管理全般を統括する役職がCSOである。また、CSOは企業セキュリティ全般に対して単独で責任を持つ役職でもある。かりに企業がなんらかの災害(サイバーテロ、物理テロ、自然災害など）に見舞われて企業活動にダメージを受けた場合、予防策をふくめたすべての対策・事後処理など全プロセスに対して責任をとるのがCSOである。当然ながら米国企業でのCSOの地位は高く、CEOの元、CFOとならぶ役職と見なされるケースも少なくない。

● CSO任命企業の増加率

米国では、セキュリティ専門職を任命するケースが増加している



Source:CIO Magazine 米国版「情報セキュリティ動向調査 2005」

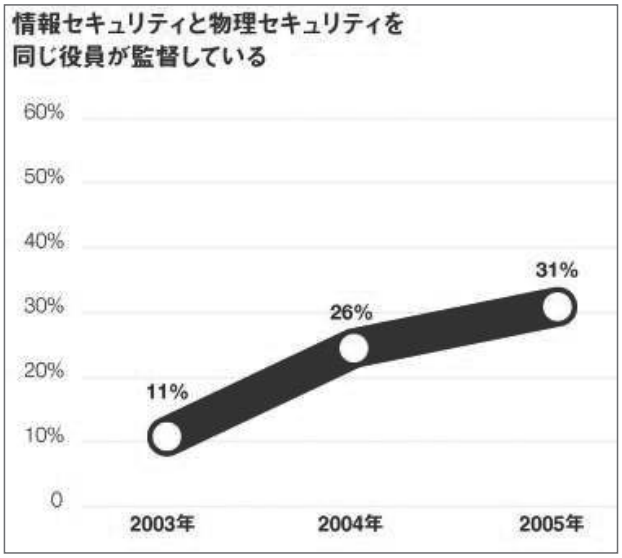
ではなぜCSOという役職が必要とされているのだろうか？

第一には「責任の所在を明確にする」という意識である。企業セキュリティには多くの部門が関係する。ところが、日常の対策や運用ルールについては個別部門ごとにボトムアップで決定されている場合がほとんどだ。たとえば、パスワード運用やノートPCの持ち出し規定についてはIT部門が決め、入退室カードの手配は総務が担当し、社員のセキュリティ教育については人事が受け持つ、といった具合。このような状況では、何か事件が起きたとしても誰も責任を取ることができない。

かりに退社した社員が、退社後、パスワードを悪用して企業の情報システムに侵入し重要な顧客データが流出したとする。このケースで責任を取るべきなのは誰だろう？IT部門の担当者？あるいは人事の担当者だろうか？予防策を講じるべきだったのはどの部門だろう？

●情報セキュリティと物理セキュリティの統合化率

米国ではここ数年、CSOが情報セキュリティと物理セキュリティ双方を監督する割合が増加している



Source:CIO Magazine 米国版「情報セキュリティ動向調査 2005」

「共同責任は無責任」という言い方があるが、これは企業のセキュリティ対策にもあてはまる。縦割りの各部門がボトムアップで連携するだけでは限界がある。企業が総合的なセキュリティを確保するためには、強力な権限を持つ CSO がすべての部門を鳥瞰し横断する形で統括する必要がある。

言うまでもなく現在では、データ流出などのセキュリティ侵犯事件が株価をはじめとした企業価値の下落に直結する。事故が起きてからでは遅い。米国企業で CSO の役割が重要視される背景には、企業自らが実効性あるセキュリティ対策を講じようとする意識の高まりがある。

BCP が企業を救う

前述したとおり CSO は、IT セキュリティだけでなく、物理セキュリティ、組織セキュリティもふくんだ総合的な企業セキュリティを統括する役職でもある。ここには近年注目されている BCM あるいは BCP への取り組みという意味合いも強く反映している。

BCM とは Business Continuity Management、BCP とは Business Continuity Plan の略語である。それぞれ「ビジネス継続マネジメント」「(実効性ある) ビジネス継続プラン」の意味を持つ。自然災害、人為的災害、環境災害、政治的災害、さらにはウイルス感染などの情報システム災害等が発生しても、企業の根幹となるビジネス機能を停止することなく、主要な企業活動を継続可能とすること。そのためのマネジメントが BCM であり、具体的対策や手順の取り決めが BCP である。

人為的災害であれ偶発的な災害によるものであれ、企業活動の停止や中断は、以後長期にわたって企業業績に大きな影響を与えてしまう。どのような災害に対しても、基幹部分の企業活動を継続できるよう対策を講じておくこと。これが BCM の基本的な考え方である。数回にわたって物理的なテロを経験した N.Y. の企業を中心にして、1990 年代後半からこの BCM の意識が非常に高くなっているのだ。

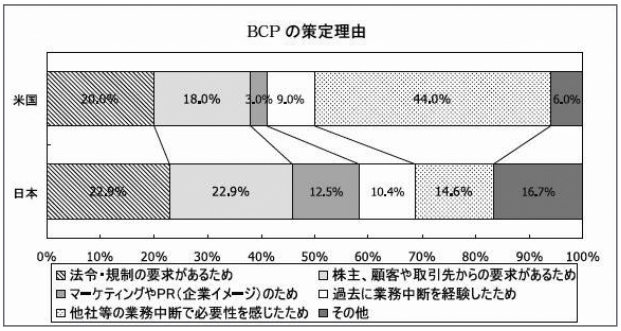
具体的な例をあげよう。

WTC（世界貿易センタービル）に本社を置いていたある薬品会社の例である。この薬品会社では 1993 年の爆弾テロの経験から、自主的に BCP の策定に着手した。1993 年 2 月の爆弾テロの際、本社機能が完全に停止し、世界中の支店をはじめとして社外社員からの連絡がまったく取れなくなってしまったのである。この企業では本社業務を一からすべて見直し、基幹業務については完全なバックアップサイトを構築した。このコストは何十億ドルとも言われ、一時は株主からも「本当に必要な対策なのか ?」と苦言を呈されたほどである。

しかし、この取り組みの有効性はすぐに証明されることになった。N.Y. では 1990 年代前半、2 回の大規模停電をはじめとして、大雪での交通ストップ、タクシー会社のストライキなどが頻発した。ところが BCP に取り組んでいたこの薬品会社では、まったく業務に影響を受けなかったのである。と同時に、BCP による予想外の効果も手にしている。業務の全面見直しによって無駄が削減され、日常的な業務の運用効率が改善されたのである。この企業で BCP に投資されたコストは、2 年以内にほぼ回収されたと言

● BCP 策定理由 : 日米比較

米国では44%もの企業が「過去の業務中断の経験」をBCP策定の動機にあげている。企業自身の切実な危機意識がBCPの取り組みにつながっている。



Source: KPMG ビジネスアシュアランス BCP サーベイ 2004/2005

われている。もちろん、9.11 テロに際しても本社機能を一切停止することなく、企業活動を続けることができた。

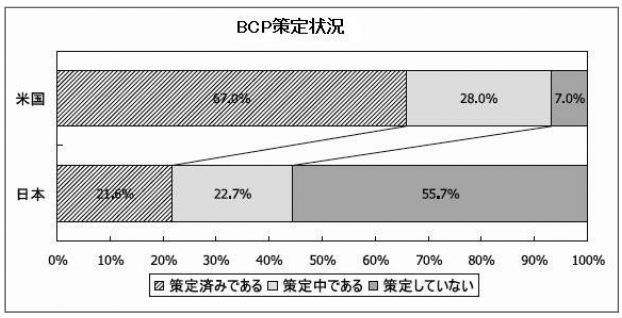
もう一例あげよう。NYSE（ニューヨーク証券取引所）は、9.11 テロに際して 3 日で業務を再開している。これは 1990 年代後半から CSO を任命して BCP に取り組んだ成果だと言われている。同じように、事前に BCP に投資して対策を講じていた証券会社は、テロ後もごく早期に業務を再開している。逆に BCP 投資を怠っていた証券会社は 3 か月以上も業務が停止し、以後、長期にわたって企業業績を大きく落ち込ませてしまった。

これらの例が示すのは次の 2 点である。BCP を背景とした総合的なセキュリティ対策の有無が、災害に際して企業存続のキーポイントとなること。

そして、実効性あるセキュリティ対策にかかるコストはけっして無意味な投資ではなく、災害時はもちろん、日常の業務においても副作用的なコストメリットを生じ得るものだということである。

● BCP 策定率 : 日米比較

策定済み・策定中を合計した割合では米国93%に対して、日本では約45%。対策の遅れが危惧される。



Source: KPMG ビジネスアシュアランス BCP サーベイ 2004/2005

JSOX 法はセキュリティ改革の好機

日本ではいまだに「セキュリティ対策はコスト高」という漠然とした印象が一般的である。

事実、企業の各部門が別個にセキュリティ対策に取り組んだ場合は、そうなる可能性が高い。総務、人事、情報システム部がそれぞれに企業部門のセキュリティポリシーを策定し、運用しているとすれば、重複した無駄なコストがかさむだけでなく、結果として実効性を伴わない形だけの対策になってしまう。これではまったくの無駄な出費である。

しかし、全体の業務の流れをセキュリティという観点から見直して分析し、有効な対策を講じていくことで、企業活動はセキュアにもなり、また日常的な業務のコストダウンにもなり得る。CSO 職の存在意義とは、セキュリティという観点からの業務見直し効果を企業にもたらすものでもある。

米国企業の CSO が統括するセキュリティの範囲は幅広い。IT 系の日常的なセキュリティポリシーはもちろん、採用社員のバックグラウンドチェック、退社時の手続き、災害時の業務システムの構築、移行の手順、またそれらについての社員教育、あるいは事件発生後の的確な情報公開の対応まで。情報システム、人事、総務、広報といった各部門を横断した、総合的な対策の策定と日々の運用に責任をもつのが CSO の役割である。

逆に言えば、CSO というポジションを置かなければ、こういった総合的なセキュリティ対策は難しい。CSO に適切な人材を割くことで、各部門はセキュリティの責任から解放され、企業全体としては真に実効性をもつ総合的なセキュリティ対策を手にすることができる。このような判断が、米国企業での CSO 職への注目につながっている。

日本では先の 6 月 7 日、参院本会議で「金融商品取引法（投資サービス法）」が成立した。メディアではインサイダー取引の罰則強化など金融系の話題ばかりがクローズアップされたが、この法案はもともと

準備段階から米国企業改革法（SOX 法 = サーベンス・オクスレー法）の日本版とされてきたものである。SOX 法は企業の内部統制ルールの強化を目的とした法案であり、BCP の策定とも強い関連性がある。BCP 策定を怠った経営者は、SOX 法の規定によって刑事罰が課せられる可能性すらある。かりに関東近辺での大地震によって本社業務が停止して株価が暴落した場合、BCP 策定をしていない経営者は内部統制違反に問われることも考えられる。

このため、今後は日本企業においても、BCP をも視野に入れた企業セキュリティポリシーの総合的な見直しが迫られることになるはずだ。

この機会を企業のセキュリティ対策の抜本的な改革期として前向きに対応するか、たんに面倒な規制として消極的に対応するか。企業は選択を迫られている。

本稿で述べたとおり、総合的なセキュリティ対策はけっして各部門の片手間で実現できるものではない。逆に、真に実効性をもつセキュリティを求めるならば、その結果として得られるメリットは予想以上に大きいものでもある。

企業を取り巻く環境が複雑さを増している現在、企業の安定的な発展と存続のためには、実効性あるリスクマネジメントが不可欠である。CSO 職によるトータルなセキュリティ対策。これこそが今後の災害多発時代の企業価値を決定する、ひとつの大きな要因となるはずである。