《株式会社東芝 セミコンダクター社》

グローバルな半導体ビジネスを支えるSCMシステムとリスクマネジメント

1999年に社内カンパニーとして誕生した株式会社東芝 セミコンダクター社（以下、セミコンダクター社）は、IT（Information Technology：情報技術）を活用した経営改革を推進し、Global-Oneと呼ばれるSCM（Supply Chain Management）システムを2001年から運用しています。

Global-Oneは、同社が今までに運用してきた各種需給システムを統合した仕組みであり、半導体製品の余剰在庫を抱え込むリスクを防ぎつつ、お客様への確実なデリバリーを実現しました。同社のオンデマンドビジネスに向けての一つの布石ととらえることもできるでしょう。

今回のインタビューでは、Global-Oneの構築・運用に当たって、どのようにリスクアセスメントやビジネス影響度分析を実施し、具体的な対策を立てていったのかというお話を中心に、同社におけるリスクマネジメントの基本方針について伺いました。

Interview with IBM Customers ❷ Semiconductor Company Toshiba Corporation

An SCM System and its Risk Management Support a Global Semiconductor Business

TOSHIBA Semiconductor Company which was born as an in-house company in 1999 has advanced management innovations by utilizing information technology (IT), and has been running a Supply Chain Management (SCM) system called 'Global-One' since 2001.

Global-One is a mechanism which has integrated various demand and supply systems which were operated in the past, and it made on-time deliveries to Toshiba's customers possible while preventing the risk of being saddled with excessive inventory of semiconductor products. It can be perceived as a strategic move toward the company's on demand business.

In this interview we heard the company's basic policy for risk management with a central focus on how risk assessment and impact analysis were conducted to work out concrete measures on the occasion of the development and operation of Global-One.

社内カンパニー制とセミコンダクター社

株式会社東芝（以下、東芝）は、130年の歴史を誇るわが国屈指の総合電機メーカーであり、エレクトロニクスやエネルギーの分野を中心にさまざまな商品やサービスを送り出してきたグローバルカンパニーです。

同社では、1999年4月から社内カンパニー制を導入し、各カンパニーがそれぞれ独立して経営を進める体制を取っています（**図1**）。社内カンパニーの一つであるセミコンダクター社は、世界一のシェアを誇るディスクリート半導体（トランジスタやダイオードを中心とした汎用半導体素子）をはじめ、システムLSI（Large Scale Integration：大規模集積回路）、メモリーなどを開発・供給する世界的な半導体サプライヤーです。

同社では世界中の半導体需要に対応するためにグローバルに製造／販売拠点を展開することで、効率的なビジネスを進めています。

同社の製造拠点は主に国内・アジアに置かれています。半導体の製造工程は、ウェハーを加工する前工程と、その組み立てを行う後工程に大きく分かれますが、前工程は姫路・大分・北九州・四日市・岩手の国内工場で行い、後工程は日本のみならずタイ、マレーシア、中国、ドイツの各国でも行っています。アジアにおける販売については、香港・シンガポール・上海・韓国・台湾などがその主な拠点となっています。

一方、ヨーロッパ地区ではドイツのデュッセルドルフに地区本社を構え、ヨーロッパ各地にエンジニアリングセンター、デザインセンター、販売拠点を展開しています。また、米国では西海岸のアーバインに地区本社を置き、米国各地のエンジニアリングセンター、デザインセンター、販売拠点が全米の需要をカバーしています。

こうしたグローバル展開によって、生産やデリバリーを効率化するとともに、お客様に近い地域でそれぞれのニーズに合わせたカスタム設計に対応しているのです（**図2**）。

ちなみにリスクマネジメントについては、東芝グループ全体で、リスクマネジメントのみならず、法令・社会規範・企業倫理を順守するためのコンプライアンスも

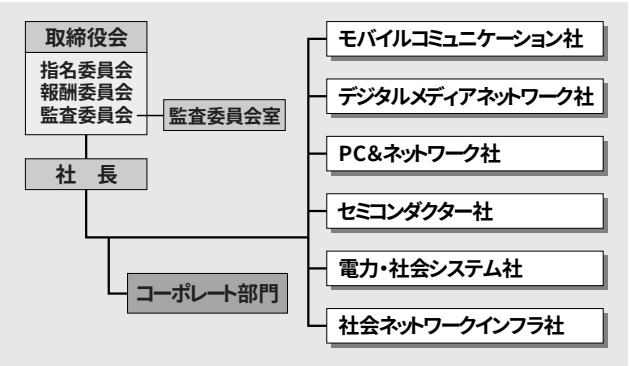

図1. 東芝の組織図

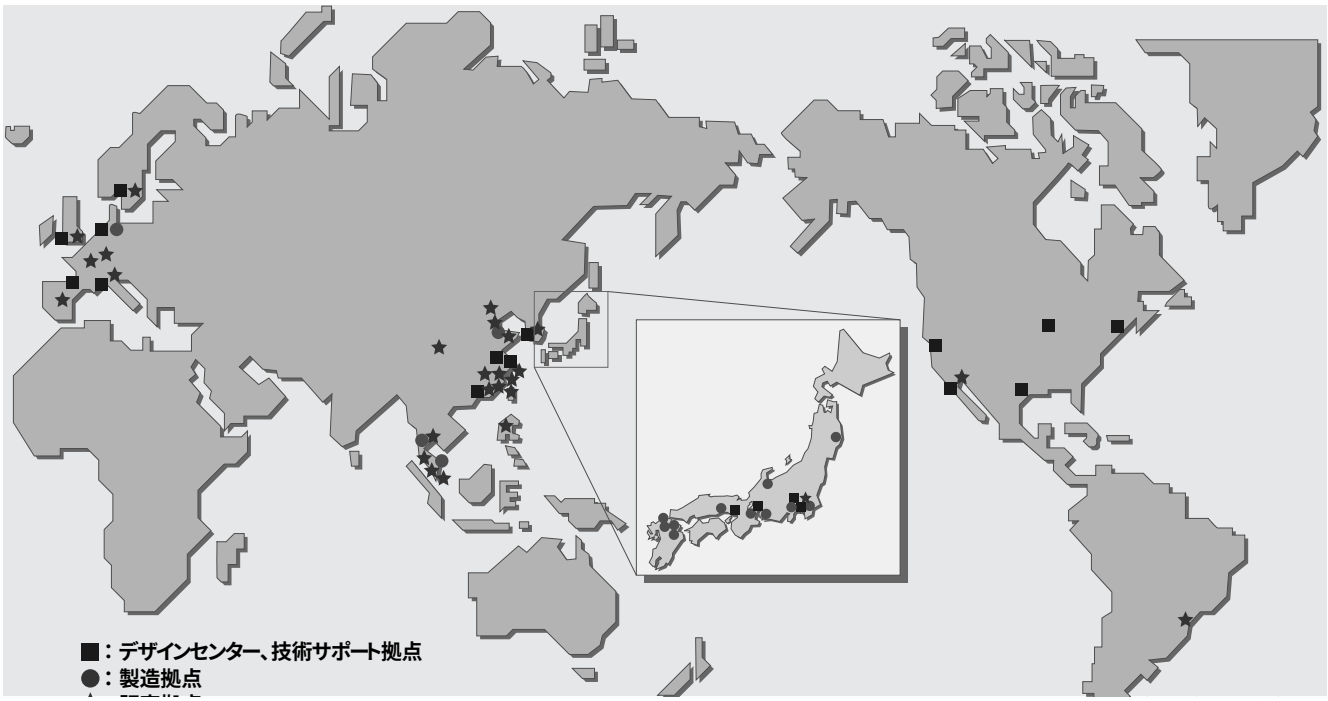

図2. セミコンダクター社のグローバル展開

株式会社東芝 セミコンダクター社
情報統括責任者
遠藤 俊二氏

Shunji Endo
Chief Information Officer
Semiconductor Company
Toshiba Corporation

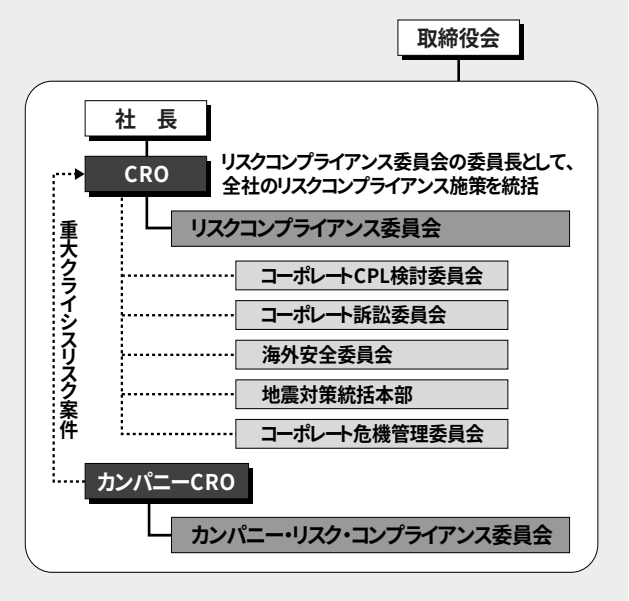

図3. 東芝グループのリスク・コンプライアンス体制

一体化して対応する体制を取っています。リスクとコンプライアンスについての最高責任者であるCRO（Chief Risk-Compliance Management Officer）の下にリスク・コンプライアンス委員会を設置。さらにはセミコンダクター社をはじめとする各社内カンパニーにも、カンパニーCROとカンパニー・リスク・コンプライアンス委員会を置き、東芝グループ全体のリスクマネジメントおよびコンプライアンスとの整合性を取りつつ、各カンパニーの責任において施策を進めています（**図3**）。

ITとMIの両輪による経営改革

1999年4月に社内カンパニーとして誕生したセミコンダクター社は、半年後の10月にITを活用した経営改革をスタートさせました。

セミコンダクター社 情報統括責任者の遠藤 俊二氏は、経営改革におけるITの重要性を、次のように説明します。

「半導体ビジネスは景気の影響を受けやすく、当社の売上高の推移を振り返っても実に大きな波があります。そうした中で、いかにして安定した収益を上げていくかが、グローバルな競争に勝ち残っていく大きなポイントとなります。

そこでITの活用による経営改革を目指して、1999年10月にITPJ（ITプロジェクト）を立ち上げました。社内カンパニーとして生まれ変わったことを契機に、ビジネスの仕組みを刷新し、いわば会社の神経網を根本的に変えることで、グローバル化のニーズに応えていくことになりました。

ITPJでは、まずは半導体ビジネスの要であるSCMにフォーカスし、サプライチェーンの仕組みを全世界で一元化することに取り組みました。というのは、世界的な規模での需給をコントロールするために、以前から世界各地の拠点でさまざまなシステムを運用していましたが、ビジネスのスピードがますます速くなる中で、お客様のニーズに柔軟にお応えするのが難しくなってきたからです。SCMシステムを世界レベルで一元化した上で、技術開発システムや調達システム、品質／環境管理システムにまでスコープを広げ、セミコンダクター社のアクティビティーに関係する仕組みをグローバルに統合していくための切り札が、Global-Oneと呼ばれるシステムです（**図4**）。

このシステムの狙いは、世界中のどのお客様に対しても均質なサービスをお届けすることです。それからもう一つ。開発や製造のパートナーとの協業を、より効率的なものにしたいということもありました。一元化したサプライチェーンの仕組みを回すことで、生産データや販売データ、あるいは歩留まりのデータをリアルタイムに確認し、ダイナミックなマネジメントを展開していこうと考えたのです。

以前から東芝グループでは、MI（Management

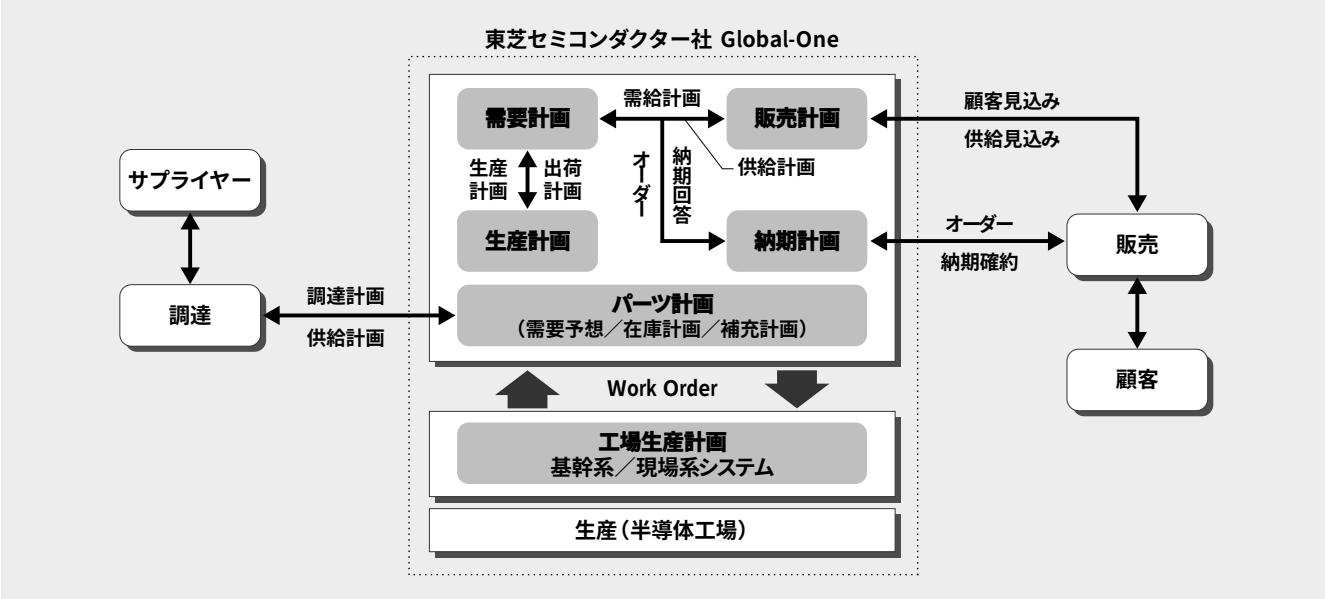

図4. Global-Oneの概要

Innovation：経営改革）を推進するためシックスシグマと呼ばれる手法を導入していましたが、さらにITベースのマネジメントを確立することで、いわばITとMIを車の両輪として、相互に補完しながら改革を進めていくことにしたのです」

Global-Oneの構築と運用

もちろんシステムを構築するだけで、ビジネスを変革することはできません。従来の仕事のやり方やフレームワークにとらわれずに、業務の仕組みも改革しながら、新しいサプライチェーンの仕組みをつくっていくことが大切です。

そこで具体的には、需給関連の情報を全世界から1カ所に集めて管理するセンターを設置。週次で計画を立てて、日次で調整するという需給サイクルを確立し、お客様への納期をリアルタイムで回答すると同時に、生産拠点に対して生産を指示する仕組みをつくり上げました。

世界中の拠点を一元化するシステムの構築ですから、乗り越えなければならない壁が幾つかありました。一つは、用語を含むマスター情報の統一です。もう一つは、それぞれの拠点で時差がありますから24時間365日ノンストップのオペレーションを実現することです。「こうして約2年の月日と約200億円のコストを掛けてGlobal-Oneを構築し、2001年8月から運用を始めました。こうして、当社の新しいビジネスが始まったのです」（遠藤氏）。

Global-Oneの運用がスタートしたことにより、動きの激しい半導体市場における需要・供給を的確に管理し、余剰在庫を抱え込むリスクを防ぎながら、お客様に半導体製品を確実にデリバリーすることが可能となりました。

以下に挙げるような長年の課題を解決することができたのです。

- 世界中のお客様へのダイレクトなデリバリー
- ネットワーク社会におけるe-コマースへの対応
- グローバルな在庫／生産計画の立案
- グローバルな受発注／生産状況の把握

「グローバルビジネスに勝ち残っていくには、ITを経営基盤に組み込むことが今や不可欠です。Global-Oneにより、SCMを中心にCRM（Customer Relationship Management）やERP（Enterprise Resource Planning：統合基幹業務システム）などを経営的視点で統合し、世界中の市場とリアルタイムで対話しつつ、全世界の販売・生産拠点を同期させ、24時間365日体制のグローバルビジネスを回し始めることができました」（遠藤氏）。

半導体ビジネスにおけるリスクマネジメント

同社の半導体ビジネスにとって、Global-Oneは今や不可欠な存在となっています。

逆に言えば、仮に震災などで運用できなくなったときの衝撃は計り知れません。その意味でも、Global-Oneの構築や運用に当たっては、災害だけでなく、どのようなリスクが考えられ、またリスク発生時の対応策について、徹底的に検討しておく必要がありました。

その際には、半導体ビジネスにおけるリスクマネジメントの特異性に十分留意する必要がありました。「よく言われることですが、半導体ビジネスはその特性から、ほかの産業に比べるとさまざまな意味でリスクが高いといわれます。

まず、半導体業界の景気サイクルが激しいことです。半導体製品が産業界において果たす役割は極めて大きく、『産業の米』とまでいわれますが、それだけに各産業界の動向に左右されやすく、需要の急激な変動が大きなリスクになりかねません。もし需要の変化に柔軟に対応できない場合は、過剰在庫が一気に増えて経営を圧迫することさえあります。

また、技術開発のスピードは格段に速く、新製品の登場により従来品は駆逐されてしまうため、受注から出荷までのスピードを上げられないメーカーは生き残ることが困難です。

製造現場におけるリスクも考えておかねばなりません。半導体の生産設備は非常に微細な加工を行うため、センシティブな装置が少なくないのです。地震で少し揺れただけでも装置を止めざるを得ないということがよくありますから」（遠藤氏）。

関東一円の災害を想定し、回復力をシミュレート

そこで具体的に起こり得る災害の一つとして、関東一円に及ぶ大地震を想定して、セミコンダクター社のビジネスにどんなインパクトが発生し、業務ごとにいつまでに回復させる必要があるのかといったシナリオを描き、その対策について検討しました。

【スコープ】

被災時においては、たとえ情報システムをリカバリーできたとしてもが完全に復旧させることは困難でしょう。その点からも、全体の計画の半分以上は人の問題を解決することに力点が置かれます。

・人・ファシリティー・情報

事前に検討しておくべき範囲は、人・設備・情報の各方面に及びます。なぜなら、情報システムをリカバリーできたとしても、運用する施設に障害があったり、実際にオペレーションできる人がいなかったりすれば、業務を再開できないからです。

【シナリオ】

対策をイメージしやすいように、「たら、れば（What if ?）」で起こり得る事態を想像するシナリオベースで検討を進めました。具体的には、最悪のシナリオとして関東一円の広域災害を想定しました。

・停止あるいは縮退する業務の明確化

実際に震災が発生したときに、どの業務を停止または縮退させるのかをあらかじめデザインしておきます。つまり、どんな事態が発生してもフルオペレーションできるような体制を整えておく業務と、機能を縮小したり、レスポンスを落としながらも継続したりする業務を明らかにしておくということです。

・復旧に要する時間の設定

各業務の復旧に要する時間を設定しておきます。セミコンダクター社の需給サイクルは基本的に週次で回っているため、1週間での復旧を一つの指標としています。ただし、例えば東京がダメージを受けても、ヨーロッパやアジアの生産拠点で対応できる場合もありますから、データそのものはリアルタイムで上がってくることを前提に、システムごとに許される停止時間を設定します。

【備え】

実際の災害では、シナリオで想定したものがそのまま起こるわけではありません。当然ながら、すべての災害の状況をシミュレーションすることは不可能です。しかしながら事前に検討しておくことで、被災時の初動を速やかに行ったり、連絡網や重点回復業務の理解などの基本事項を押さえた上で行動できるようになるでしょう。災害時に実際に起こることはすべて応

用編だと心得て、日ごろからのトレーニングで一人ひとりが基本を理解し、行動に移せることが重要です。

・安全確保・要員・業務再開手順

人の安全を最優先しつつ、いかにして要員を確保するかということを検討しておきます。例えば自宅が壊れて避難している社員に、バックアップセンターでのオペレーションを指示することはできません。他地区の要員で業務を再開できる体制を全社的に整えておきます。

・バックアップセンターを遠隔地に設置

Global-Oneについては、海外にバックアップセンターが設置してあり、災害時には代替できる体制が整っています。また各国の販売拠点のシステムについては、他地区との整合性を取りつつ、それぞれの拠点で個別にバックアップする仕組みになっています。

・部材・商品の備蓄

「セミコンダクター社の業務の一部が止まったときに備え、お客様側である程度の部品在庫を確保しておいていただく」という考え方もありますが、基本的にはサプライヤーの責務として、セミコンダクター社側でも一部の部材・商品を備蓄しておきます。

・トレーニング

さまざまな災害に対するシナリオや運用マニュアルを作り、バックアップセンターを設置しても、いざ災害が起こったときに実際に動けないのでは意味がありません。災害時にも対応できるように、システム要員に対して定期的にトレーニングを実施しています。

日本におけるリスクマネジメントの難しさ

セミコンダクター社の専任スタッフとして、情報セキュリティーのグループを率いる川本 栄二氏は、このシミュレーションを実施した際に、日本の企業に特有のリスクマネジメントの難しさが存在することに気付きました。それが「言霊（ことだま）」です。

「わたしが『言霊』というものを知ったのは、歴史物に対する興味から読み始めた井沢元彦氏の著作を通じてです。災害対策のシナリオを描く中で、日本におけるリスクマネジメントを難しくしている理由の一つに『言霊』というものが影響しているのではないかという井沢氏の説に納得したのでした。

株式会社東芝 セミコンダクター社
IT推進部
情報セキュリティ担当
グループ長
川本 栄二氏

Eiji Kawamoto
Group Manager
Information Security Group
IT & Business Transformation
Division
Semiconductor Company
Toshiba Corporation

災害対策を具体的に検討していくには、イマジネーションを働かせて、実際に災害が発生したときにどんなことが起こるのかを徹底的に考えなければなりません。ところが日本人に特有の性癖として、災害のことはなるべくイメージしたくないのです。災害のことを考えるのはそれだけでも縁起が悪く、もし災害が発生したとすれば、それは『誰かが縁起でもないことを言ったから、現実に起こってしまったんだ』といわれてしまうわけです。

実は、当社の情報セキュリティーについて検討したときにも感じたのですが、米国では『もし、それが起こったら、こんなひどいことになるかもしれない』と、最悪のケースを想定してつぶさに検証するのに対し、日本人は『そんなことは考えたことはない』、もっといえば『考えたくもない』となってしまうのです。

確かに、阪神・淡路大震災のような災害を想像するのはつらいことです。しかしイマジネーションを働かせてあらゆる状況を考え抜いておかないと、的確に対応することはできません。ましてや、そういった状況における対策を、経営陣やお客様に説明することは困難です。まずはそういったマイナスの発想から抜け出すことが大切なのではないでしょうか」

リスクマネジメントは、情報システムのことだけを考えても実効性がないといわれますが、人・設備・情報のみならず、「心」の方面までカバーしておくことが大切であり、リスクがもたらす被害について、冷静に思

い描くことから始めることで、有効な災害対策が立案できるということです。

お客様とのリスク管理ポリシーの共有を

こうして災害対策を具体化していった経験から、遠藤氏は、リスクマネジメントのポイントの一つとして「お客様とのリスク管理ポリシーの共有」の重要性を強調します。

「企業にとってのリスクはさまざまですが、その一つに地震などによる大規模災害があり、いつ、どのように発生しても対応できるように備えておく必要があります。当社は半導体のサプライヤーとして、組み立てメーカーのお客様に確実に部品を供給する責任を負っています。災害が発生したとしても、お客様に安定したデリバリーを提供するという前提で、対策を考えておかねばなりません。

具体的な達成基準としては、当社の供給の遅れが原因でお客様の製造ラインを止めないことが大切です。そのためには、お客様とサプライヤーである当社との間で、リスク管理ポリシーを共有化しておきます。

例えば、海外のお客様に半導体製品を毎日デリバリーしていたとして、東京地区で大規模な災害があり、出荷機能が止まってしまったとしましょう。その際にお客様は供給の再開をいつまで待っていただけるのか、ということです。一つの考え方として、当社の生産設備の復旧に1週間かかる場合、お客様には万一に備えて1週間分の在庫を持っていただくということが考えられます。これがリスク管理ポリシーの共有化です。

そのためには、当社がどのようなリスクマネジメントを行っていて、どのレベルまでコミットできるかということを詳しく説明し、お客様にご理解いただくことが大切です。

阪神・淡路大震災や米国の9.11テロをはじめ、予想もできないような事態が次々と起こる中で、サプライヤーにはお客様に対して自社の災害対策について説明責任があるということです。これは今後のビジネスにとって、とても大切なことです」

リスクマネジメントにおける「見直し」の重要性

一方、川本氏は「技術の進展」という観点から、リスクマネジメントにおける「見直し」の重要性を訴えます。

「IT関連の災害対策というと、当社でもやはり阪神・淡路大震災が一つの大きなきっかけになり、全社的に地震対策の見直しを行いました。

当然ながら、その時点でそれなりのシナリオは描いたわけですが、問題は、当時のITと今日のITを比べると、その仕組みや、ビジネスにおける役割が大きく変わってきている点です。例えば、当時は自動化が難しくて人間系で行っていた業務の多くが、今日ではITを用いるようになっています。

これはIT以外にもいえます。工場やオフィスなどの建物についても、10年前には免震技術はあまり普及していなくて、ほとんどが耐震だったはずです。それが今日では、一般住宅でさえ免震技術を用いるまでになっています。こうした技術や環境の変化を確実にとらえ、災害対策を見直していかねばなりません。

また、災害の種類・範囲も変わってきています。9.11テロ以前は、多くの企業がテロへの対応を想定していなかったでしょうが、対策の検討対象に含める必要が出てきました。サプライヤーとして災害対策についてお客様に説明責任があるという話がありましたが、その観点から、当社ではお客様に対して安定供給の保証とその裏付けについて説明するようにしています。ただし、バックアップセンターの設置場所や、バックアップの詳細な仕組みについては公開していません。これは広い意味でのリスクマネジメントの一つ、という考え方に基づくものです」

「補足しますと、外部からのアタックには、物理的なアタックもあれば情報システムへの攻撃もあるわけですが、データがどこに置かれ、どういう仕組みになっているのかということを非公開にしておけば、それだけでも安全性が高まるということです。

もう一つ。ビジネスの急激な変化に追随するには、システムの一元化・統合化により、効率的な仕組みをつくることが効果的です。その一方で、災害時の安全を図るためにシステムを分散化するという考え方もあるでしょう。一般に、一つにまとめてしまうと災害時のリスクは高まります。卑近な例を挙げれば、ゴルフ

場の更衣室などで、財布やら時計などの貴重品を着替えの上にまとめておくとそれだけで盗まれたときの被害が増大します。リスクを減らそうと思えば、むしろばらばらに置いた方が安全です（笑）。当社の国内の生産拠点は、姫路・大分・北九州・四日市・岩手に分かれています。リスクマネジメントの観点から分散化したわけではないでしょうが、結果的に拠点が分散しているということは、それだけでもある程度のリスクヘッジになっているのです。

情報システムの『分散と集中』についてはさまざまな考え方があるかと思いますが、リスクマネジメントの観点も含めて検討する必要があるのではないでしょうか。

話を戻しますと、いずれにせよ災害への備えは一度考えればいいというものではなく、常に見直さなければなりません。当社では1999年にITPJをスタートして以来、さまざまなシステムを立ち上げ、運用してきましたが、定期的にシステム全体の災害に対する備えを見直してきています。Global-Oneについてもバックアップセンターを設置し、災害に対する世界規模でのサプライチェーンの備えは出来上がってはいますが、これも常に見直しを図っています。環境の変化に対応するということが大切なのです」（遠藤氏）。

IT部門から積極的な提案を

企業が、リスクマネジメントを進めていく上で議論になるのが、そのコストに対する考え方です。災害対策にしろ、情報セキュリティーにしろ、本格的な対策を実施するには何億円・何十億円という投資が必要となります。多くの経営課題を抱える中で、リスク対策を最優先するのはなかなか難しいでしょう。

では、リスクマネジメントの具体的な施策について、IT部門としてはどのように経営陣に提案していくのが効果的なのでしょうか。

「わたし自身の立場で言いますと、情報セキュリティーの責任者だからといって、情報セキュリティーへの投資の必要性を力説して、経営陣を説得しようとは思っていません。説得するのは、わたしの仕事ではないと思っているからです。その代わりに『例えば、こんなリスクが存在します。このリスクは許容可能でしょうか？許容できないとすれば、こんな方法で解決できます』という形で提案します。それを取るか取らないかは、経営の判断ということになります。

例えば、当社が日本アイ・ビー・エム株式会社（以下、日本IBM）の協力を得て情報セキュリティーポリシーを作ったのは1999年ですし、情報セキュリティー部門が専任組織になったのは2000年です。いずれも東芝グループとしては初の取り組みだったはずです。『当社がビジネスを進めていく上で、情報セキュリティーが重要である。それにはこういった施策が考えられる』というわたしたちの提案を、経営陣がいち早く採用してくれたからです。

ある意味で幸運だったのは、当社の場合、半導体ビジネスのグローバル化が進んでいることが考えられるかもしれません。歴代のカンパニー社長をはじめ、海外駐在員や駐在経験のある従業員は少なくありませんし、海外とのコミュニケーションも盛んですから、リスクに対する意識が全般に高かったといえるでしょう。それともう一つ。半導体ビジネスの進め方が大きく変わっていく中で、パートナーといかにして協業を進めるかということが、以前からの課題となっていたことも見逃せません。例えば東芝と日本IBMの関係もそうですが、ある分野ではパートナーでありながら、ほかの分野では競争相手であるという企業間の提携が増えています。その場合、一部の業務のみを協業していく形になりますから、機密管理を徹底しつつ、情報を共有する仕組みが早急に必要だったのです。

いずれにせよ経営陣はリスクマネジメントの重要性を十分に認識していますから、IT部門から積極的に提案していくことが、経営陣の決断を促し、いざというときの備えにつながるのではないでしょうか」（川本氏）。

半導体市場は、産業界全体の動きに敏感で、それだけに素早い動きが要求されるといわれます。だからこそ「さまざまなリスクに対する十分な備えが必要ですが、逆に言えば、そうした環境下に置かれているからこそ、経営トップから社員一人ひとりまでが、リスクに対する意識を強く持っているといえるかもしれません」と遠藤氏は語ります。そうした危機意識の共有こそ、リスクマネジメントを全社的に進めていく鍵となるのかもしれません。