東京海上リスクコンサルティング（株）
リスクコンサルティング室
主席研究員　指田　朝久
E-mail: t.sashida@tokiorisk.co.jp

危機管理の新常識

（日経情報ストラテジー2002 年 12 月～2003 年 5 月連載）

目次

第１回　内部告発への対応　法令違反！あなたはどうする
求められる「内部告発」への誠意ある対応

１，内部告発は悪だろうか

牛乳による大規模食中毒事件以来、日本の企業や自治体・官庁の事件や不祥事はまさに目白押しとなっています。事件が発覚するきっかけの多くは、取引先あるいは企業内部の人間による当局やマスコミへの告発です。なかでも国が実施したＢＳＥ（牛海綿状脳症、狂牛病）対策を悪用した牛肉ラベルの偽造事件では、ついに上場企業が解散に至りました。ある弁護士は「上場企業ほどの体力があれば、事故や災害で倒産することはまずありません。しかし、法令違反を起こせば企業は倒産します」と話します。企業の総務部門の責任者と話をすると、「内部告発が悪である。これをなんとか防ぎたい」という意見を良く聞きます。しかしこの発言は本当に正しいのでしょうか。良く考えてみましょう。

本当に防がなければならないのは内部告発ではなくて、その根本にある法令違反のはずです。ところが、違反自体は棚に上げて、内部告発が悪いという声は少なくありません。「内部告発をして会社がつぶれてしまっては、どうしようもないではないか」「内部告発を抑えきれなかったのは現場の管理職の問題だ」「内部告発は派閥争いや人間関係の恨みが原因。それさえなければ、たとえ不正があっても漏れるはずがない」「内部告発によって俺たちの一生が台無しになった、告発者は許せない。」―――

どうでしょう。読者の皆さんも真剣に考えて下さい。自分の会社がそのような事態になったとき、どう感じますか。法令違反をした人が悪いのでしょうか。法令違反が起きやすい風土を放置しておいた会社が悪いのでしょうか。それとも内部告発をした人が悪いのでしょうか。

マスコミ関係者から、最近の内部告発者の心理が変わってきていると聞きました。以前は派閥争いや人事の不満による告発が多く、マスコミもそれほど注目していませんでした。しかし最近は、企業に法律を守って信頼される存在になって欲しいから告発するのだというケースが増え、マスコミも真剣に取り上げるようになってきているそうです。この背景には様々な要因があると考えられますが、特に大きいのは価値観の変化でしょう。

従業員にとって、現在務めている企業が人生のすべてではなくなってきています。１９９０年ごろ、つまり日本経済の頂点である豊かな時代から始まったとされる、企業の論理より個人の倫理観を重視する流れが底流にあります。その後の不況時代に、相次ぐリストラによって終身雇用が揺らいでいることを目の当たりにして、なおさら個人の倫理観を重視する流れが加速しているのではないかと考えられます。

２，組織的犯罪はなぜ起こるのか

組織的な法令違反はどうして起きるのでしょうか。関西経済連合会が実施した企業倫理に関するアンケート調査によれば、２６～３５歳の年齢層で「良心に反することでも、それが会社の方針であれば従わざるを得ない」という傾向が飛び抜けて高くなっています。これは企業の実働層に対して「組織の暗黙の圧力」が強く働いていることを意味します。上司の命令により、法令違反と知りながらそれに荷担してしまう。そして、その良心の呵責（かしゃく）の持って行き場がない場合、企業外への告発となっていくのです。法律に抵触する行動を皆無にすることが理想ですが、企業には多くの従業員がいるのですから、現実的には困難です。では、企業、そして多くの無実の従業員にとって、どういう方法で法令違反の被害をくい止めればいいのでしょうか（「図　良心に従って行動できますか」参照）。

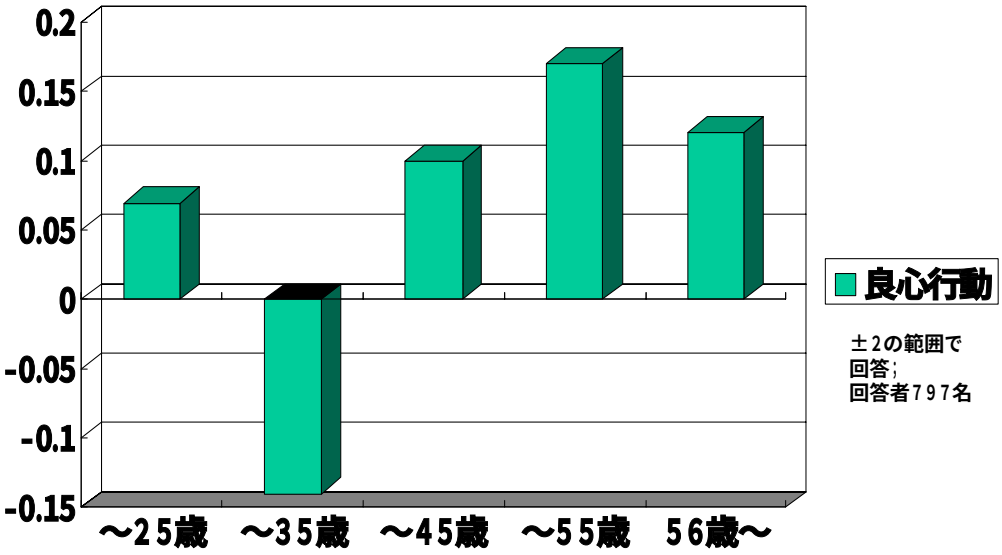

図　良心に従って行動できますか

出典；関西経済連合会「企業倫理の実践に関する調査報告書」より、良心に従って行動する良心行動のグラフ（倫理法令マネジメントシステムの構築：高巌著；タリスマン１９９９－９号）

それには、法令違反を防ぐ組織的な仕組みが必要です。万一、法令違反が発生した場合でも、外部に告発される前に企業内部で適切に違法行為を解消する事が求められているのです。

最近はコンプライアンス（法令順守）が大切だといわれていますが、本当に企業風土になじむようにするには相当な努力が必要です。例えば、麗澤大学の高巌教授が主導して提案されている「倫理法令遵守マネジメントシステム規格ＥＣＳ２０００」を導入するのも良いでしょう。先進的な企業では、法令違反の駆け込み寺として社内に企業倫理室を設置したり、あるいは顧問弁護士へのホットラインを設ける企業も出てきました。ある大手企業では１年で３０件以上の相談案件があったと、その効果を認めています。最近はやりの業績評価についても、法令違反がないことを条件にするなど人事制度の改革も必要です。また社会的にも内部告発者を保護する法制度の検討も始まっています。

いずれにしろ、企業が真剣に取り組まなければ意味がありません。今まで当然と思われてきた業界の慣行も見直しが必要です。企業の取り組みのなかでも、最も重要なのは企業トップの姿勢です。「企業利益は追求する。しかし法令違反をしてまで利益は要らない」と明確に、繰り返し、本気で問わなければ意味がありません。

皆さんの企業では、すでに企業倫理やコンプライアンス構築のための活動が開始されていますか。もしまだでしたら、皆さんは自分自身の身を守るためにも一刻も早く提案する必要があります。

最後にもう１度問いかけます。内部告発は悪ですか、法令違反をした人が悪ですか、それとも放置している会社が悪ですか。

日経情報ストラテジー2002 年 12 月号

第 2 回　危機発生時の情報共有　「工場長！それは本当か」
クライシス・コミュニケーション体制を構築せよ

１，社長は何も知らされない

「工場長、それは本当か」―――。記者会見の席上、新たな事実が工場長から説明されました。そして思わず社長が発した言葉がこれです。今までマスコミに対して説明してきたことが、すべて嘘になってしまった瞬間です。これと同じ発言が、他の企業の記者会見でも繰り返されました。

また、ある企業は記者会見で「そのような事実はございません」と大見えを切った次の日、「実は昨日の発表には誤りがありました。事実はこれこれで、誠に申し訳ございません。おわびして訂正いたします」という釈明をしています。どうしてこのようなことが繰り返し起きるのでしょうか。実は社長にとって、真実を知ることは本当に困難なのです。

多くの事件・事故の発生や発覚は、突然やってきます。そして極めて短時間で、いったい何が発生したのか、これから何が起きようとしているのか、何が原因で、責任はどこあるのかなどを、消費者、株主、取引先、行政、従業員といった多くのステークホルダーに説明しなくてはなりません。つまり、最高責任者が真実をいかに迅速に把握するかという「時間との闘い」なのです。

事件が発生したことは分かります。ところが、その本当の原因、企業に与える影響、責任の所在は容易にはつかめないことが多いのです。情報収集に当たる従業員に対して、思わず社長が叫びます。「本当のことを言ってくれ」―――。

事件や事故は、人間のほんのわずかなミスや思い違いから起こります。ところが人間は弱いものですから、責任を追及されないようにと、自分の落ち度を小さく報告しがちです。同じ企業の中でも部門をまたがる事故になると、部門間で責任が問われてきます。ましてや他の企業や個人が事件や事故の当事者になると、それぞれの言い分がどんどん食い違ってくるのです。複数の報告者が皆、違ったことを言ってきます。どちらが本当に正しいのでしょうか。

危機発生時の情報共有の問題はもう１つあります。

事件や事故の発生を知るのは通常、第一線で働いている従業員です。そこからどれだけ早く情報が企業のトップに伝わるでしょうか。

問題を発見した従業員が上役に報告しました。上役はさらにその上司に電話で連絡しようとしました。ところが、上司は不在です。現場では事件対応に追われています。そこで伝言を頼み、指示を待ちました。ところがいくら待っても指示が届きません。

そうです。残念ながらこの伝言は上司の書類の山に埋もれ、上司が事件を知ったのはすでに大事になった後だったのです。

２，報告した瞬間から責任は上司にある

事件や事故は何も営業時間中にだけ発生するものではありません。休日や夜間でも発生します。そのとき報告者が、「上司を夜中に起こすと怒鳴られるから、様子を見ながら明日に報告しよう」と思ったことが、企業にとって取り返しのつかないことになるかもしれません。そのような事態が起こったとき上司は必ず次のように言います。「どうして起こしてくれなかったのか」「なぜ、もっと早く伝えてくれなかったのか」。

従って部下は、上司のご機嫌をおもんぱかる必要はありません。むしろ夜中でも、ゴルフ場にでも伝えるべきです。

ところで、情報を早く上司に伝える良い仕組みがあります。いつもは批判の対象となる官僚組織ですが、情報伝達に限って言えば、参考になる仕組みがあるそうです。それは「上司に伝えたときから上司

の責任」というもので、問題がある場合、情報を止めた人が最も重い責任を問われるというのです。自分が責任を逃れたいのであれば、できるだけ早く上司に伝えた方が良い。これで上司に早く情報が上がるというわけです。この仕組みは企業でも取り入れているところがあります。その企業では、事件や事故の責任以上に、情報伝達を遅延させた罪が問われます。

なお、上司は真夜中に起こされた場合でも決して不機嫌になってはいけません。「よく伝えてくれた。ありがとう」と報告者をねぎらいましょう。また、結果的に、一大事にならなかった場合でも、「こんなことでいちいち報告するな」などと決して発言してはいけません。この一言が、後で情報が入ってこない原因になりかねないからです。

このように情報が早く正しく最高責任者に入る仕組みは、危機発生時の情報共有、つまり「クライシス・コミュニケーション」のとても重要な要素です。すべての従業員は事件や事故の情報を把握したら、素早く上司に伝えます。もし上司が不在なら、その上の上司に伝えます。直接、危機管理事務局や事案担当役員に連絡することも認めます。状況によっては社長に直接連絡しても良いとするのが、早期警戒態勢の基本です（「図　早期警戒態勢の構築を急げ」参照）。

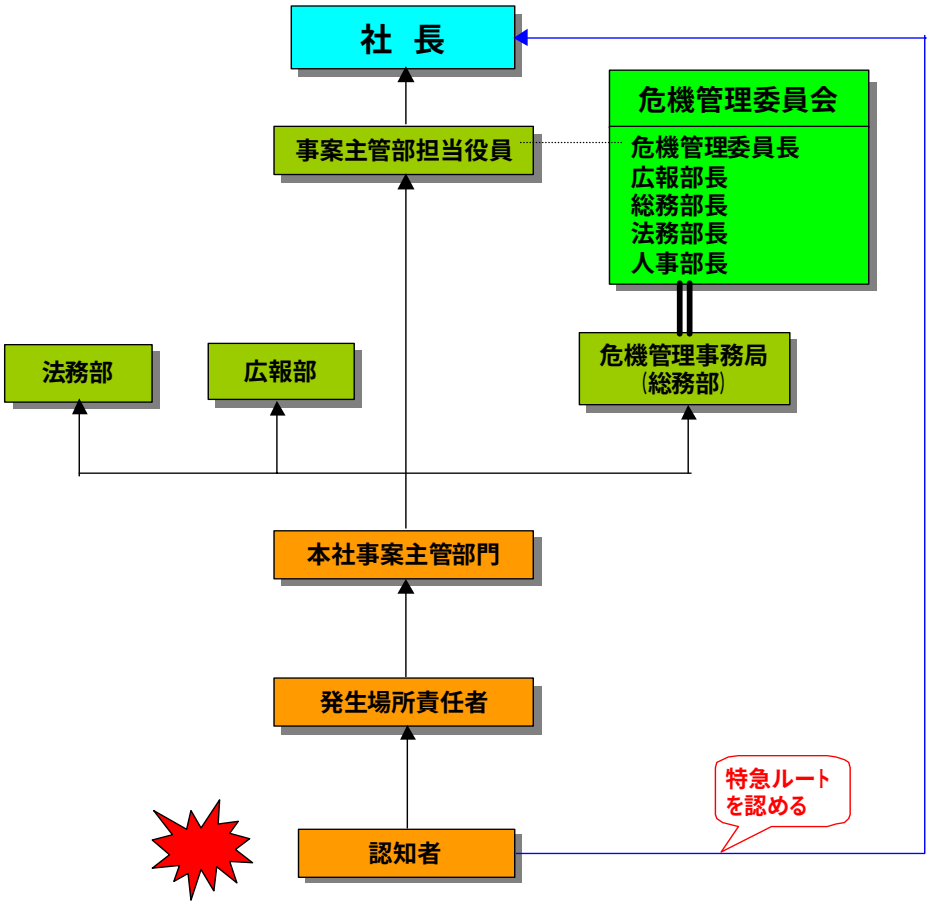

図　早期警戒態勢の構築を急げ

また、事件や事故の真の姿を早くつかむことが大切です。米国の大企業では、危機管理の要点は情報収集であるとも言っています。実際、事態が発生するとすぐさま３０人規模の情報収集班を構成します。真実を早くつかむには、それぐらいの人数が求められます。ここで重要なことは、素早く情報を伝えるようにすべての従業員が教育されていることです。

最後に、たとえ誤報であっても、悪い情報の入手を尊ぶ社長の日常の姿勢が求められます。

日経情報ストラテジー2003 年 1 月号

第３回　業務復旧計画の構築　災害！そのとき業務を復旧できるか
業務復旧計画の必要性と構築法

１，バックアップも役立たず

いつも通り出勤の身支度を整え、朝食を取りながらテレビを見ていると、ビル火災のニュースが目に飛び込んできました。良く見ると見覚えのあるビルが、ヘリコプターからの撮影で放映されているではありませんか。なんと我がオフィスが火災に遭ったのです。朝食もそこそこに出掛けると、ビルは現場検証の最中でロープが張り巡らされ、立ち入り禁止になっていました。ビルの外見はそれほど燃えているようには見えませんでしたが、割れた窓ガラスから垣間見えるオフィスは、黒焦げの書類やコンピュータ端末が無残な姿をさらけ出し、消火用水が床一面を浸しています。これでは、オフィスは機能しません。大切なお客様への提案書が入ったパソコンも使えそうもありません。さあ、どうすれば良いのでしょうか。

情報システム部門では従来から、コンピュータの一時的な故障に備えてデータやプログラムなどのバックアップを定期的に取得しておくことが習慣となっています。コンピュータの発展の初期には機械故障の発生率が高く、コンピュータや記憶装置の故障、テープの読み取りエラーで、大切な情報が失われることも多かったからです。データやプログラムのバックアップを取得しておけば、データの消失を防げます。

また、プログラムにはバグがつきもので、万一のプログラムミスにより誤ったデータを作成し、貴重なデータベースを壊してしまうこともありました。作業のやり直しを円滑にするためにも、元情報のバックアップを取っておくことは常識です。しかし、これらのバックアップは故障や誤作動への対応を主な目的としていたため、復旧作業をしやすいように、バックアップの対象となる機器と同じ場所に保管されている場合が多いのが実情です。

今は情報機器も小型化し、オフィスのなかにサーバーやデスクトップ端末、モバイル端末が数多く存在しています。そのなかに企業経営に不可欠なデータやプログラムがいっぱい詰まっています。これらのバックアップは、どこにあるのでしょうか。大抵は、フロッピーやメモリーカードあるいはＣＤ－Ｒで皆さんの机の引出しに保管しているはずです。

オフィスのＬＡＮなどで文書管理ツールが導入されていると、各端末のデータのバックアップをサーバーに保存・管理しているところもあるでしょう。しかし、その場合でも、サーバーは同じオフィス内にあることが多いのです。

さて、そこにオフィスの火災です。これらのバックアップは利用できるでしょうか。耐火金庫の中にバックアップを保存している場合はまだ可能性がありますが、オフィスとともに重要なデータも消失してしまったら、果たして企業は存続できるのでしょうか。

２，業務復旧計画のポイント

地震・洪水・火災などのように、企業の経営に大きな影響を与える事故や災害に対して、どのように業務を継続させるのか、どのように業務を復旧させるのかをあらかじめ定めた計画を「業務継続計画」あるいは「業務復旧計画」と呼びます。まだ記憶に新しいニューヨークのワールド・トレード・センターに対するテロ事件では、オフィスを喪失しながらも、業務復旧計画を実際に発動して、代替オフィスに幹部社員が移動し、データや情報システムをバックアップから復旧させ、業務を継続して、経営に与える影響を最小限にとどめた企業が数多くありました。

日本でも金融機関を中心に業務復旧計画を策定していますが、まだ一般的ではありません。ＫＰＭＧビジネスアシュアランスの調査によると、日本でこれらの計画を持っている企業は２１％にすぎないのです（「図　業務復旧計画を持っている日本企業はわずか２１％」参照）。

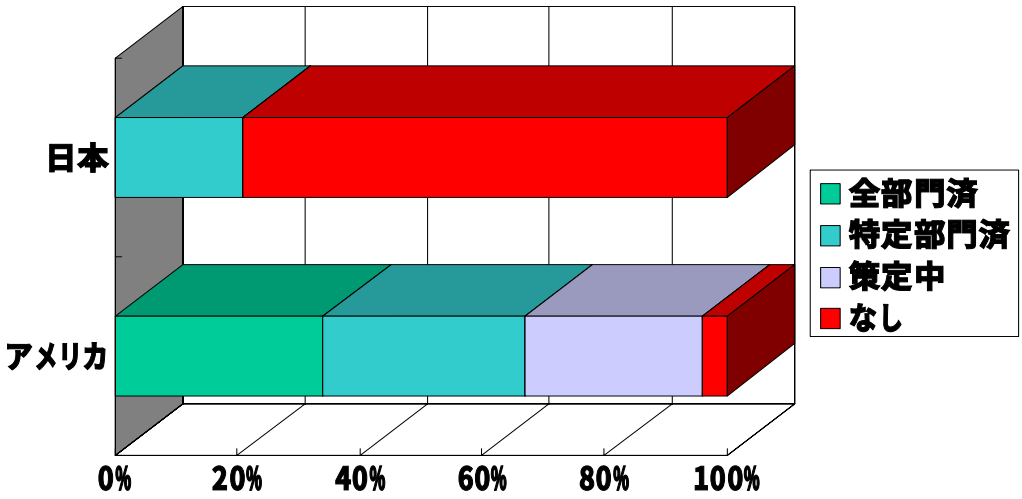

図　業務復旧計画を持っている日本企業はわずか２１％
出典；ＫＰＭＧビジネスアシュアランス
「ビジネス継続マネジメント（ＢＣＭ）サーベイ２００２」

業務復旧計画を作成するには、いくつかのポイントがあります。まず第１に、業務復旧計画の対象とする被害想定を行います。本店などオフィスが長期間使えず、またシステムを使用できないという厳しい状況を設定します。

第２に、企業経営に不可欠な情報を選定します。例としては、売掛金、買掛金、原価計算データなど経理や決算のデータがまずあります。製造業では顧客情報のほかに、ＣＡＤ（コンピュータによる設計）の設計図、品質管理検査数値、工程表、部品品番など様々なものがあります。この情報が失われた場合、手作業で復旧できるのは何日分が限界かを検討し、バックアップのサイクルを決定します。そして、このバックアップをできれば遠隔地に保管します。保管先は専門の業者に委託しても良いし、自社の工場や支店でもかまいません。

第３に、企業経営に必要な業務とそれを支援するシステムに優先順位を設定します。通常、事故災害に備えて用意できる人員、機器、オフィスなどには限りがあります。そのため、すべての業務を復旧することは困難です。優先順位の高いものからいくつかの業務に絞り込みます。

そして第４に、この優先順位の高い業務を復旧するために、危機管理本部長の指名、対策本部の設置場所の決定、サーバーや端末などの機材の入手方法、復旧作業のための手順書やシステム停止時の事務処理マニュアルの作成、連絡網の整備などを行います。

さらに重要なことは、手作業によるデータ復旧を含め、実際に訓練を行うことです。火災への備えは避難訓練や保険だけではありません。情報消失への備えも怠りなく。

日経情報ストラテジー2003 年 2 月号

第 4 回　情報漏洩と日常管理　顧客情報が漏れたとき
情報漏洩の防止は日常の従業員教育がカギ

１，頭隠して尻隠さず　機密情報も筒抜け

ある日、中堅百貨店のお客様相談室に１本の電話がかかりました。「最近、聞き覚えのない企業からダイレクトメールが届くのです。引っ越しをしたばかりなのになぜ分かるのか不思議に思い、いろいろ調べると、新しい住所を書いたのは御社の会員カードに加入したときだけなのです。情報が漏れていると疑うわけではありませんが、念のために調べてもらえないでしょうか」――。

システム部の調査では、ウイルスやハッカーの可能性はほとんどないことが分かりました。一方、社内の情報管理体制を調べると、驚くべき状況が浮かび上がりました。

情報システムが苦手な営業本部長のパソコンには、ご丁寧にパスワードが張り付けてあります。ゴミ箱の中に古い顧客リストの一部が捨ててあります。「社外秘」と赤マークを付けたフロッピーが机の上に放置されています。さらに、顧客名簿の管理状況を尋ねると、鍵をかけていないガラス戸棚に「禁帯出」と書かれたファイルを並べ、担当者が自由にコピーして使用しているとのこと。これでは顧客情報に限らず、「機密情報をどうぞご覧下さい」というありさまです。

情報管理規程はあるはずですが、守られていなければどうしようもありません。

「至急、改善策が必要だ」との認識に至ったとき、営業本部から連絡がありました。顧客情報流出の原因が分かったのです。営業部のある社員がダイレクトメールを使ったマーケティングを企画したとき、自宅で仕事をしようとして顧客リストのフロッピーディスクを封筒に入れて持ち帰り、それを電車に置き忘れたのでした。その顧客リストのなかに、電話をかけてきたお客様も入っていたわけです。

情報流出の原因というと、まずハッカーを最初に挙げる風潮があります。しかし現実には冒頭の事例のように、身近なところで情報が流出していることが多いのです。情報の流出だけでなく、情報の消失や破損、改ざんなどを総合的に防止する仕組みがあります。それが「ISMS（情報セキュリティ・マネジメントシステム）」です。

ISMS では情報を守るために 10 の大項目を定めています(「図　企業が最も重視するのは情報セキュリティポリシーの確立」参照)。各項目の概要を順に説明しましょう。

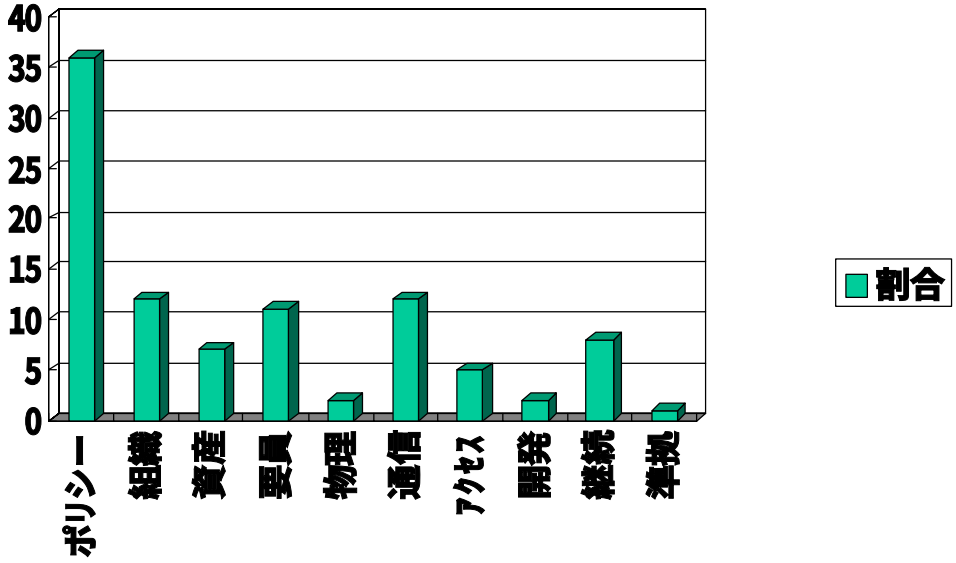

図　企業が最も重視するのは情報セキュリティポリシーの確立
出典：財団法人日本情報処理開発協会
「わが国における情報セキュリティの実態」(2002 年 3 月発行)

まず初めに「情報セキュリティポリシー」です。ここでは企業の情報セキュリティに関する方針や守れない場合の罰則、実施プロセスを明確化し、経営者が全体をレビューするサイクルなどを定めます。「情報セキュリティ組織」では責任者の決定、推進組織の構築、アウトソーシング契約での責任範囲などを明確化します。「情報資産の分類整理」は各情報の重要度や脆弱性を分析し、守るべき情報をランク分けすることです。「人的セキュリティ」とは従業員の守秘義務や、事後対応を含む教育の制度作りです。「物理的環境的セキュリティ」では入退室管理、防火地震対策、パソコンなどの持ち出し管理といったルールを定めます。「通信および運用管理」の柱は機器の操作基準やウイルス対策などです。利用者責任を明示し、パスワードやアクセス権限の管理を確立するのが「アクセス制御」です。「システム開発メンテナンス」は開発時のセキュリティ要件を開発会社との間で合意したり、開発環境のセキュリティ対策などをしっかり決めておくこと。「事業継続計画」は前回お話した大災害時の業務復旧への備えで、最後の「準拠」は法律の順守やシステム監査の実施を指します。

２，情報管理のルール　最初は３つでいい

実際に情報セキュリティに取り組んでいる企業は、この 10 項目のうち何を重視しているのでしょうか。日本情報処理開発協会のアンケート調査を見てみると、最も重視する項目として多く挙げられたのが「情報セキュリティポリシー」。その次が「情報セキュリティ組織」「人的セキュリティ」と、人にかかわる取り組みです。情報セキュリティに限らず、企業の事件や事故の防止においては、なんといっても従業員教育が柱です。様々な規程や方針、管理項目をマニュアルに定めたとしても、それを実際に守っていなければ意味がありません。情報セキュリティに関する教育の要点は次の通りです。

第１に、情報の価値や情報が損なわれたときの影響の大きさを認識させます。

第２に、従業員のレベルに合わせて管理項目を徐々に増加させます。少ないと感じられるかもしれませんが、最初は３項目程度を徹底するところから始めることをお勧めします。冒頭に出てきた企業を例にとると、最初に徹底すべき管理項目は次のようなものになるでしょう。

①パスワードを端末に張らない
②顧客情報を打ち出したものは細断して破棄する
③書類棚は施錠する

つい、多くの管理項目を策定したくなりますが、あれこれ掲げて結局どれも守れないより、少数の項目でも 100%実施できるようにするほうがセキュリティ管理においては重要です。

第３に、点検・振り返りを定期的に実施するように指導することです。指示を出しただけでは意味がありません。罰則を含めて、決められたことは必ず守らせることが大切です。施策が定着したところで、管理項目を追加していけば良いのです。

「人は城、人は石垣」。これは情報セキュリティの世界でも通用する教訓です。

日経情報ストラテジー2003 年 3 月号

第５回　情報システムのリスクマップ　ウイルスがやって来た
情報リスクごとの頻度・影響度を把握する

１，リスクマップを作ってみる

「送信者へ、管理者はあなたのメールの添付ファイルにウイスルを発見しました。ウイルス駆除を実施してください」。

突然の警告がメールボックスに飛び込んできます。ウイルス対策ソフトを入れているので感染しないと思っていたのですが、ついにかかってしまったのです。至急、あらかじめ定めた手順通りにパソコンの通信ケーブルを抜き、管理者に連絡し、ウイルス対策ソフトで駆除しなければなりません。このように、ウイルス対策には万全というものがありません。さらに、次々に新種のウイルスが開発されています（「開発」というのがしゃくに障りますね）。この１月２５日には韓国をはじめ多くの国がウイルスに襲われ、その結果、インターネットにアクセスできなくなるなど深刻な影響が発生しました。

また、昨年の情報処理振興事業協会（ＩＰＡ）の情報セキュリティにかかわる事故についての調査では、ウイルスによって全社のシステムが完全復旧するまで休日３日を挟んで６日間もかかり、全社的にシステムが使用できないことによる間接損害は推定で２億円以上と算出された事例が紹介されています。

毎日のようにやってくるウイルスに対し、企業側も「ウイルス対策に全力を挙げよ」と号令します。しかし、それだけを実施していれば情報システムは万全でしょうか。

「ウイルス対策が先だ」「いやいや、オペレーションミスのほうが頻度が多い」――。

「銀行の統合のようにシステム開発の遅延が問題ではないのか」「そんなことより、火事になったら復旧をどうするのか」――。

議論は尽きません。１つひとつのリスクの認識も大切ですが、まずは情報システムにかかわるリスクを把握し、関係者でその情報を共有する事が重要です。

リスクマネジメントの最初のステップはリスクの洗い出しです。一般的には関係者でブレーンストーミングを行い、考えられるすべてのリスクを書き出します。次に、リスクの算定です。洗い出したリスクのそれぞれを、「発生頻度」と「損害の程度」の２つの軸で評価します。損害の程度は、さらに①人的損害、②物的損害、③利益損害、④賠償責任、⑤信用失墜の５つの項目で評価します。

① 人的損害は人の命に関わるもので、医療機器や運行制御システムなどで特に顕著となります。
② 物的損害は大型コンピュータやパソコンなどの機器の損害額です。
③ 利益損害はインターネット・ショッピングや、株式のネット取り引きなどができなかったことによる逸失利益のことです。データの再構築やバックアップシステムの稼働、業務の復旧に必要な費用もこの項目で評価します。
④ 賠償責任は、お客様や第三者に迷惑を掛けた場合の賠償費用の項目です。
⑤ 信用失墜は、事件や事故のために失ったまま戻ってこないお客様の数や、失った売上高、市場シェアなどを評価します。

このようにしてリスクの種類ごとに頻度と損害の程度を評価し、それを１枚の図にまとめたのがリスクマップです。それぞれ個性のあるリスクを地図のように表すことにより、関係者全員が全体像を把握でき、議論がしやすくなります。

２，経営者が対策の優先順位を決める

ここで１つの例を紹介しましょう（「図 情報リスク原因別リスクマップ」参照）。

滅多に発生しないが１度起きると大きな損害をもたらすのがマップ左上の領域で、ここには地震や火災などの災害が当てはまります。さらに、最近の危機管理において注目されている組織的な内部不正などがあります。発生頻度は多いものの、１つひとの損害は限定されるリスクは右下の領域に位置します。

ウイルスやソフトのバグ（不具合）、オペレーションミス、不正アクセス、機械故障などが当てはまります。また、発生頻度も高く影響も大きいのが右上のリスクで、情報システムの開発の遅延や計画の失敗がこれに当ります。最後に、発生頻度も低く損害の程度も限定的なリスクに空調故障や停電などがあります。このようにそれぞれのリスクの性格を把握しながら、取るべき対策の優先順位を決めていきます。

どのリスクへの対応を優先するかは、最終的には経営者が判断すべきです。ただ、一般には頻度が高く損害も大きな右上の領域から取り組みます。例えば、情報システム開発の遅延です。システム開発には遅延が付きものと言われますが、対策としてはプロジェクトマネジメントの手法を導入するといったことが考えられます。

右下の領域は発生頻度が高く日常的に起きるため、発生頻度を抑える対策が有効です。ウイルスであればウイルス対策ソフトの導入に加えて、従業員教育なども徹底します。左上の領域は滅多に発生しませんが、起きたときの経営への影響が大きいところです。第３回で説明した業務復旧計画の作成や、保険の手当をします。

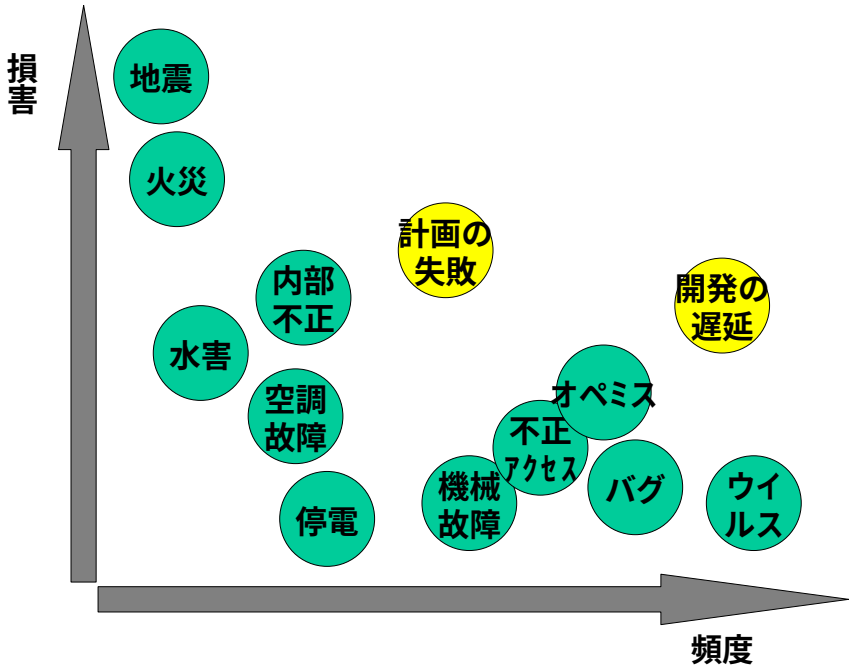

図 情報リスク原因別リスクマップ

リスクは常に変化します。最近、ある企業のアウトソーシング先で、個人情報が入ったテープの盗難が発生しました。同じことが自社にも起きるかどうかと、常に見直す必要があります。

ところで、ウイルスの話をしているうちに私自身がインフルエンザにかかってしまいました。集団風邪のリスクは、マップのどこに位置するのでしょうか。

日経情報ストラテジー2003 年 4 月号

第 6 回　危機管理体制の構築　失敗こそ真の訓練なり
危機管理体制を構築し、評価・改善する

１，危機管理の３つの教訓

朝 9 時、ある食品スーパーの緊急対策本部―――。

営業担当者から物流部長に連絡が入りました。「各店から欠品連絡が相次いでいます。それも１店や２店ではありません。どうも配送している商品が、各店がオーダーしたものと違っているらしいのです。」

大至急、社長に報告し、あらかじめ定めた会議室に要員が参集します。対策本部長に営業統括の執行役員が就任し、早速、集まったメンバーに指示を出します。「すぐ実施するべき項目を挙げよ」「午後の配送をどうするか」「冷凍庫に入庫できずに腐敗する商品への対応策を定めよ」。

集まったメンバーには部長もいれば、管理職が不在のために部下が出席しているところもあります。時間はどんどんたっていきます。早くしないと開店時間です。すぐにも対応策を決めていかなければなりません…。

これは、あるスーパーが実際に行った机上訓練の一場面です。机上訓練はあらかじめ日時を決めておくだけで、訓練に出席する緊急対策要員に課題は事前に知らせません。いわば抜き打ち訓練です。訓練では事務局が次々に課題を与え、短時間で結論を出していきます。あっという間に時間が過ぎます。うまく解決できた問題もあれば、解決できなくて立ち往生してしまうこともあります。また、参加者がマニュアルをよく理解していないために、見当違いの結論を出してしまうことも珍しくありません。今回の訓練では、新聞チラシに掲載した目玉商品が配送されていないことへの対応がうまくできませんでした。

しかし、失敗して良いのです。改善すべき問題はどこにあるかが分かったことが、大変大きな収穫なのです。経営者は決して失敗をしかってはいけません。事務局は訓練を振り返り、参加者の育成とともに対応策やマニュアルの改善に取り組みましょう。

阪神・淡路大震災以降、様々な企業や官公庁・自治体で危機が発生しました。我々がこれらの事例を詳しく分析したところ、３つの教訓が得られました。

①危機管理には経営者の関与が不可欠。②危機に対する日常の予防策が重要。③危機が発生した場合に適切な指揮ができる指揮官の育成が必要―――という 3 点です。冒頭に述べた机上訓練は、この指揮官の訓練に当たるものです。

こうした活動を含めて、組織全体の危機管理に関する枠組みを定めた規格があります。ＪＩＳＱ2001「リスクマネジメントシステム構築のための指針」がそれで、2001 年 3 月 20 日に制定されました。この規格は、品質管理ＩＳＯ9000 シリーズや環境マネジメントＩＳＯ14000 シリーズなどと同様のマネジメントシステム規格の１つです。

２，できることから始めてみる

このＪＩＳＱ2001 は、７つの原則から成り立っています（「図　実施・評価・改善を繰り返してリスクに強くなる」参照)。この活動を繰り返すことによって「今年より来年」「来年よりは再来年」と、リスクに強い企業になるために継続的に体質改善を図ろうという仕組みです。

原則１は「リスクマネジメント方針」です。方針を出すのは経営者。最終責任は経営者にあることを明示することに、大きな意味があるのです。

原則 2 は「計画策定」です。前回説明した「リスクマップ」を作成するなど、企業を取り巻く様々なリスクを評価し、優先して取り組むべきリスクを選定し、その対策を決定します。情報リスクへの対策ならばＩＳＭＳ（情報セキュリティ・マネジメントシステム）の導入はひとつの解決策です。業務復旧計画の策定も重要な対策でしょう。

原則 3 は「実施」です。年間計画で定められたリスクの軽減策や万一の事態に備えた準備をします。

原則４は「評価」です。定めた計画通りにリスク対策を実施できたか、または計画通りリスクは減っているかどうかを評価します。

原則５は「是正・改善」です。点検した結果、なんらかの問題があれば、計画や対策、実施手順などを改善します。

原則６は「経営者のレビュー」です。リスクの変化や対応策の実施状況を見て、次のサイクルの具体的な方針や目標を定め、必要な経営資源（予算や要員）を投入します。この活動を繰り返すことで、少しずつリスクに強い企業へと体質改善できるのです。

これらの活動を支えるのが原則７の「体制・仕組み」です。リスクマネジメントの推進組織の決定や対策要員の選定、リスク情報の開示や関係者とのリスクコミュニケーション、発見したリスクの監視、マニュアルの作成、教育訓練の実施、そして監査などの各項目が掲げられています。

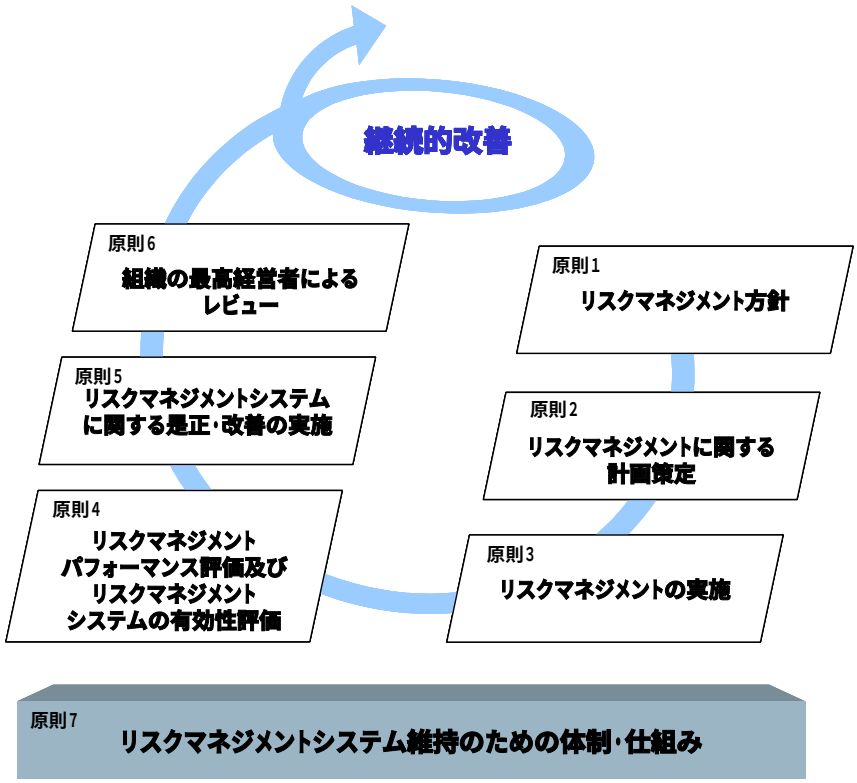

図　実施・評価・改善を繰り返してリスクに強くなる

出典：JISQ2001

このコラムでは法令の順守や危機発生時の情報共有、業務復旧計画、情報リスクへの対応、リスク評価の実践、指揮官の育成など、企業の危機管理のポイントを６回にわたって解説してきました。

最も効果的な危機管理とは、そもそも危機に陥らないことです。そして、その予防策は、満を持して完璧を目指し、なかなか行動が開始できないよりも、できるところから初めの１歩を踏み出すほうがはるかに有効です。「継続的改善」をキーワードに、問題があればその都度直していけばよいのです。

それでは早速、始めませんか。

日経情報ストラテジー2003 年 5 月号

第 27 号（2003 年 6 月発行）