緊急対応24時、有事における3場の原則と危機管理
―個人情報漏洩事件後の実務対応事例を踏まえて―

AIGコーポレートソリューションズ株式会社
ディレクター
白井 邦芳

1．リスクマネージメントと危機管理

（1）はじめに

リスクマネージメント（Risk Management）とは「今後発生するであろう損害･損失を最小限のコストで効果的に防御する事前手法」であり、一方、危機管理（Crisis Containment）とは「予想外の、あるいは予想を超えた問題事案の拡大防止や、それに伴う風評被害、ブランド劣化から発生する損害･損失の極小化による利益確保のための事後対処」である。

リスクマネージメントは、「リスク移転」、「リスク回避」、「リスク保有」、「リスク防御」（図表1）の4つの手法を巧みに利用して、ある種のリスクを全くなくしてしまったり、軽減させることが可能である。そうした意味ではリスクマネージメントは周到な計画と緻密な頭脳によって管理される知的なしくみであると言える。一方、危機は防ぐことが不可能であり、一度発生すれば損害･損失を無にすることはできない。危機の発現から拡大までのスピードはリスクマネージメントにかけた時間とは比べものにならないほど短く、早ければ3時間でピークを迎える。また、その状況変化は千差万別であり、経験と応用力に長けた実務家と訓練された組織こそが不可欠である。彼らのミッションは軍隊における戦術行動（Maneuver）と等しい。また、英語で危機管理をCrisis Containmentと訳すのは、Contain=Keep to controlの通り、一度発生すれば同時多発的に各種の「危機」が企業を襲い、全ての「危機」に適切な対処を取り続けなければ企業は破綻することに由来する。たった一度の管理（Management）ではすまないのが「危機」である。

医療の分野で言い換えれば、「人間ドック」がリスクの洗い出しを行うリスクマネジメントであり、「救命救急センターによる治療」が危機管理である。予め人の体の脆弱性を予想し、決められた手法で特定の病巣を洗い出す方法はリスクマネジメントの典型的な考え方であるが、突然の事故で頭部外傷、内臓破裂、大腿骨の開放性骨折といずれも重篤な症状を一瞬の間に被った人間を救うには、その道のプロ達が全ての傷害に対する措置を適切に成功させて初めて生命を繋ぐことが可能となる。どれ一つ失敗できないことに危機管理の難しさがある。

（2）緊急事態は時を選ばず！

仮に一般企業の就業時間を午前9時から午後6時と設定した場合に、残業時間を考慮しても午前8時から午後8時位までが通常の業務時間帯と思われる。『緊急事態』はその時間枠を超えて発生するものが全体の30％程度存在する。30％がそれほど多くないとお考えになる企業も残業時間帯に移る午後6時以降を含めた場合の合計発生確率が46％であるとお聞きになれば、安心してもいられないはずである。AIGはこの15年の間に1300近くの上場企業の危機と呼ばれる事態に遭遇し、対処してきたが、その多くがこの「魔の時間帯」に発生している。構えている時と異なり、人は無防備な状態で危機に遭遇すると、一種のパニック状態に陥ることがある。その場合、一般的に見られる兆候は、「泣く」「喚く」「沈黙する」などいずれも通常人とは明らかに異なる態様を呈する。経営層に伝達される頃にはそのパニックは増幅されて人事不省となる場合すらある。企業を取り巻く周辺の状況も同様に一変する。否応なく危機の現場に到来するのは『3場の原則』である。

（3）『3場の原則』が経営者を襲う！

修羅場－広がる動揺、色濃い悲壮感、指揮命令系統を失った組織が最初に経験するのは『修羅場』である。怒号、号泣、沈黙相乱れて迷走する企業人は、危機に遭遇して初めて命綱のない崖淵に立たされることになる。向かうべき方針を見失った企業人の痛ましさが浮き彫りにされる。

土壇場－最初に始まった危機はすぐに形を変えて新たな危機に変貌する。危機の連鎖である。危機の怖さとは、実はこの連鎖にある。既に最初の危機で倒れんばかりのダメージを与えられた企業あるいは企業人は、休む間もなく次々に新たな危機の連鎖に遭遇することになる。お客様窓口における担当者の対応の失敗は、それがインターネット上で掲載、話題となった瞬間にもはや一担当者の問題ではなくなり、企業ブランドすら崩壊させる危機的状況を呈することになる。さらなるマスコミへの稚拙な対応、情報開示の失敗、経営者層の不遜な態度など、いずれも危機の連鎖は続いていく。

正念場－経営トップに押し寄せる危機時の経営判断の波は頭で考えるほど生易しくない。記者会見が始まるまでのおよそ72時間という極めて限られた時間の中で、少なくとも10以上の経営判断を下さなければならないのが有事対応である。頂点を極めた者だけが経験する『正念場』がここに在る。

（4）経営トップの4つの心構え－『4戒』

『危機』とは前述のとおり単発の事故の羅列ではなく、それ自体が引き金となって同時多発的に発生する新たな危機を誘引する起爆剤である。経営トップは、いかなる事態にも動揺せず、また自ら決定した判断に疑いを持たず、自信を持って速やかに行動に移すだけの意思の強さと力量を示さねばならない。今まで経験したことのない張り詰めた緊迫感の中では、行動を共にしている他の役員や社員は、ちょっとした気の緩みから出た経営トップの弱気な挙動や顔色にも敏感に反応し、焦りやあきらめから始まる無秩序な組織行動は一瞬の間に企業を震撼させることになる。以下の『4戒』こそが危機管理組織を支えていく

上での経営トップの基本姿勢となる。

①難事に直面して恐れるな！⇒怖れは人を萎縮させる！
②驚きを顔に出すな！⇒トップが動揺すれば他の役員や社員にまで伝染する！
③部下を信頼して疑うな！⇒疑い出せばきりがなくチームは崩壊する！
④一度判断した指針を疑うな！⇒迷いは大きくなり、訂正報道を繰り返す！

（5）危機管理における重要な５つの工程管理

危機的状況が発生すれば、時間の制約の中で、できることは極めて限られてくる。企業がその存続をかけて行うべきことはおよそ以下の5つと考えてよい。

『アクションプラン』－「危機」発生後、a）どの段階で（When）、b）どの役割･責任を担う者が（Who）、何を目的に（Why）、どの場所で（Where）、誰に対して（Who）、どのようなアクションを（What）、如何なる方法で取るか（How）を予め明示しておく必要があり、一度危機管理組織が動き出せば、現場はその指示に忠実に従わなければならない。指示を出す側も現場に混乱や議論を招くような曖昧な指示を絶対に出すべきではない。

『情報管理』－「危機」はもともと予見されていないか、予想を超えたところで発生するもので、情報不足が常につきまとう。そのような場合、人の判断は偏りがちで、自分の意見に合致する補強的情報を過大に評価し、反証情報を過小評価する兆候が見られる。さらに言えば、限られた情報を基に、迅速な判断を求められると視野狭窄的となり、独断的結論に帰着させる傾向が強くなるため、誤った経営判断が誘引される。『情報管理』とは、危機的状況下における「情報収集」、「事実確認」、「噂の排除」、「機密情報の漏洩対策」など、情報周りの的確な管理を指すものである。

『タイム･マネージメント』－危機的状況下では通常、「事実確認⇒原因究明⇒対応措置⇒責任表明⇒再発防止策の実施」と各工程を順序良く展開していかねばならない。この通過点を時間がないからといってスキップすることは許されない。各通過点の断絶は明らかに説明責任事項のロジックに穴を開け、メディアや消費者を含むあらゆる利害関係当事者に対する情報開示に精彩を欠かせる要因となる。タイム･マネージメントは危機管理の工程管理の基本であり、各通過点は重要管理点（Critical Control Points）である。

『選択肢の合理的分析』－収集された情報は、事実と噂、伝達情報や意見といった複雑な色合いをもったものに細かく分類され、最終的に経営判断チーム（主に取締役会）によってその選択肢が決定される。時間の制約下で、完全な情報収集がなされることは少なく、満足できるレベルまでの情報は得られない。そうした状況下では各選択肢はその解釈や判断の仕方によりメリット･デメリットが混在し、どの選択肢がベストであるかを容易に見極めることができない。法務担当者や外部専門家を入れた分析チームは、これらの選択肢を各方面から多角的に分析し、メリット･デメリットを詳細に検討しておくことが後日判断ミスを追及された場合の経営リスクを回避する防御策となる。

『大胆な経営判断』－大胆と言っても「いいかげん」という意味ではない。経営判断チームは危機のピークと言われる記者会見までの数日の間、少なくとも10～20の経営判断を行う必要性に迫られる。情報がないからという理由で判断を遅らせれば前述の『タイム･マネージメント』が不可能となる。創業者の意思だからという理由で独断先行的な判断を行えば今度は『選択肢の合理的分析』が抜けることになる。危機管理の5つ目のポイントは今までの全ての工程を踏まえて、経営判断を着実かつ冷静に実行することにある。すなわち、適正な情報収集、緻密な選択肢の検討･分析、タイム･マネージメントされた妥当な経営判断は、互いの関係が合理的であり、補完しあって客観的に導き出されてこそ法的価値が見出される。「大胆」とは、この場合、時間の制約下で躊躇なく「英断」することである。

（6）『3分』－風評発生までの時間はあまりにも短い！

危機的状況が始まれば、48時間以内に公表の方法を決定し、情報開示の手続を進めなくてはならない。仮に「社告」による公表で翌日の新聞に掲載することを決定した企業は、前日の昼12時迄にPR会社に社告内容を電子データの形式で送り込むのが一般的である。そのまま何もしなければ翌日の朝刊の社告欄に掲載された後、マスコミの取材攻勢が予想されることになるが、社会ネタとなる事件では、社告掲載を決めた新聞社の編集デスクから社会部へ社告内容が伝わり、社告掲載の前日から取材が開始されることはもはや常識である。

危機管理広報の専門家が入る場合は、そのような状況下では、社告前日に記者クラブへ投げ込み（プレスリリース）を行うのが一般的となった。投げ込みのタイミングは夕刊やタブロイド紙の締切を意識して夕方4時以降に設定される。これによって当日の公表内容を報道する媒体としては概ねテレビ局一本に絞られることになる。

仮に午後4時ジャストに投げ込みを行うとどんなことが起きるだろうか？　3分後には幾つかのテレビ局の番組内でテロップ形式で速報が流されることになる。これは、記者クラブの中に新聞社だけではなく、テレビ局が加盟していることから発生する事態である。この段階では企業の従業員すらほとんど知らされていない状況下で、すでに公知となる可能性が出てくる。投げ込み開始から30分も経過すると、記者クラブの幹事会社から「レクチャー」もしくは「記者会見」のいずれかの対応を求められる。「お願い」ではなく、「強い要求」である。投げ込みから1時間から2時間程度の間に設定されることがほとんどである。開始される段階では、すでにテロップで大まかな内容が公表されているから、テレビ局を含めたメディア関係者のほとんどが押し寄せることになる。

（7）記者会見は最初の15分を乗り切り、60点以上を目指せ！

社会事件の場合の最初の記者会見では開始早々の15分が山場である。テレビ局ニュース番組内の論調がここで決まり、翌日の朝刊の見出しやインターネット上でも、これに関連する言葉が踊ることになるからである。「組織的隠蔽」「経営トップの判断の遅れが致命的」など、最初の15分程度で矢継ぎ早に行われる質問の中で判断されてしまうことが今までの記者会見の一般的な『流れ』である。

記者会見の質疑では外せない説明事項として以下のものがある。

①何が起きたのか？（現状説明）
②なぜ起きたのか？（原因説明）
③どのように対処するのか？（対応措置説明）
④誰の責任なのか？（責任表明）
⑤同様の事件はもう起こさないか？（再発防止策説明）

原因究明がなされず質問の回答に窮して、いきなり「責任を取ります」と責任表明した事例をよく見かけるが、社会通念上、事実を明らかにしないままの謝罪は、企業倫理を問われ、更に風当たりを強くさせるだけで、なんら危機管理の観点から見ればメリットがない。

想定される質問はおよそ100～150、時間にして2時間～3時間、企業のスポークスパーソンはかつてない試練に立ち向かうことになるが、満点を狙うのではなく、60点以上を取る気持ちでQ＆Aを準備すればよい。

2．実例、個人情報漏洩事件を参考に･･･

（1）漏洩事件の発覚は突然一本の電話から！

午後8時55分、ある会社Aのお客様相談室に一本の電話が入った。そのお客様は2つの企業に自分の個人情報を開示しているという。1社はB、もう1社は当該会社Aである。二週間前から突然、不審な電話や郵便受けにも記憶にない請求書が入りだしたというこの苦情はただちに個人情報保護管理責任者に伝えられ、調査が開始された。一方、同様に会社Bのお客様相談室にも同じ人物から連絡が寄せられ、役員に伝えられていたが、こちらの動きは若干違っていた。「過去に同様の苦情が寄せられたか」との役員からの質問にお客様相談室長は「初めての事例で戸惑っています」と回答していたため、調査は開始されなかったのである。結局、二週間様子を見るということでこの苦情に対する対応は終了していた。

会社Aは担当役員からの要請に基づき、調査責任者が当該苦情者である個人情報がどこに保存されていたかを究明し、その情報主体を含む近辺の個人情報をもとにリストを作成して、コールセンター長へ渡した。コールセンター長はオペレーターに事前に用意していたコールスクリプトを渡して30分程度で均一のサービスが提供できるようオペレーター訓練を実施した。その後、ひとまず50人をランダムに選別し、電話による確認作業に入った。結果としてこの50人からはなんら同様の不審な電話や郵便物に対する苦情は聞かれなかった。会社Aは念のため、さらに50人を追加して電話による確認作業を継続したが、幸いなことにやはり被害は認められなかった。会社Aは自社の個人情報漏洩を懸念して、調査を開始したが、ログ検証からも情報漏洩した可能性は見つけられず、電話による情報主体への検証も被害が確認されなかったことから「情報漏洩なし」との判断に至り、本件の収束を宣言した。

一方、会社Bはどうなったか？　二週間の待機を命ぜられたお客様相談室長は、その期間を待たずに重篤な危機的状況に対応せざるをえなくなる。10日程度過ぎた頃、一斉にお客様より問合せが入り始めた。その人数は50人を超え、またその内の数人には詐欺被害の兆候が確認された。次々と寄せられる苦情の嵐に対応は後手後手となり、原因の究明や是正が行われなかったために、その後も2次流出や新たな詐欺被害者からのお問合せが相次ぐことになる。この状態に至って初めて役員は自社からの個人情報漏洩に気がつくが、もはや危機的事態から逃れる術はなく、対処療法しか思いつかない。行政への報告やマスコミへの公表に対する対応も同様に判断の遅れが目立ち、危機管理計画はほぼ機能しないまま、社会問題視される事態を招く段階まで二週間とかからなかった。

（2）情報漏洩事件、それは最も難解な危機対応の連続である！

一般に不祥事件が発生すると、最も企業が危機的状況に陥るのは、マスコミに自ら公表またはリークによってマスコミに察知されるタイミングであると言われている。社会ネタになりやすい、しかも話題性の高いイシューであればその記事になった場合のインパクトは計り知れず、危機管理広報の専門家も、そのときこそ最も専門性を発揮し、またスポークスパーソンも重要な責務を負うことになる。

個人情報漏洩事件ではどうであろうか？　「情報漏洩の対象者は最大60万人、但し、現在判明している確実な情報漏洩数は1800人」というような歯切れの悪い社告や記事が展開される。これは、多くの企業においてログ検証などによる調査結果が短期間に確定できず、事件の社会的影響を考慮し、かつさらなる詐欺被害の抑止を目的として速やかに公表に踏み切る積極的な企業の開示姿勢であるため、言わばやむをえない事態であると考えねばならない。

当然ながら、公表後の風評はかなりのものになるが、その後も「詐欺被害は止まらず！」「こんな詐欺手口まで登場！」「詐欺被害額うなぎのぼり！」「企業を恐喝する者まで登場！」「集団訴訟がついにスタート！」と数ヶ月に渡り、キャンペーン期間中のように報道され続けることになる。しかも、この悪いタイミングで反社会的勢力を通じてマスコミの一部に全ての紛失されたとされる個人情報データが受け渡されることが発生し、最も懸念される危機的事態となっている。企業は事態の重さを認識し、発覚から数ヶ月ないし約1年程度を費やしてあらゆる危機管理対策を取り続けるが、度重なる報道によるブランド劣化に打ちのめされ、収束宣言ができないまま、株主総会等においても経営者が攻撃される場面が相次ぐことになる。経営者の首をいとも簡単に刈り取ってしまうリスク、それが個人情報漏洩事件である。

（3）現在の企業実態を考察する！

2004年7月22日、経団連会館においてJASDAQアフタヌーンセミナー第11回「個人情報漏洩の実際と危機管理」というテーマで小職が講演を行い、多数の参加企業があったが、その際、個人情報保護の観点から収集したアンケート調査結果が図表2である。興味深いのは、約96％の参加企業が「個人情報漏洩はガバナンスの重要課題である」と考えている一方で、外部からの不当なアクセスからの不安（約79％）、外部業者のリスク管理の不安（約81％）、社内の持出しリスクの不安（約89％）など、社内対策の遅れから企業内での不安が広がっていることがうかがわれる点である。「すでに情報漏洩が発生しているのではないか」との不安に駆られている企業も約63％あり、悲愴感すら感じとれる。現在、AIGでは個人情報保護に関して一日あたり数社から多いときで10社を超えるお問合せをいただいているが、未だ体制作りはこれからとなっている企業がほとんどではないかと推察される。残された時間から考慮するとかなり厳

しいものと考えざるを得ない。

（4）危機管理の重要性

図表3に示した通り、一度「危機」が発生すると企業の利益は加速度的に落ち込み、損失が拡大する。対応にかかる直接経費は膨らむ一方で、ブランド劣化などから生じる利益喪失は短期間に一気に進み、潤沢な企業利益ですら枯渇させてしまう。危機管理の重要性は、危機直後の利益落ち込みを抑制し、回復までの期間を短縮させることで、マーケットに対して「危機に強い企業」と印象付けさせることに他ならない。

図表4は、個人情報漏洩事件を例に、危機発生から初期対応までの危機管理体制の簡単なシミュレーションを想定したものである。担当部署別の時系列的な動きを見ると危機管理対策本部を中心に各方面へ指示が出ており、トップダウンによる支配関係が明白である。

通常の危機管理に不可欠な「事実確認」「原因究明」「是正策」「責任表明」「再発防止策」の流れに加え、2次流出や詐欺被害の抑止を目的として行う情報主体に対する通知･警告作業は、他の事例に見ない個人情報漏洩特異なものである。また、利害関係当事者に対する対応を明確にし、時系列的に置き換えることで、取るべき行動計画とこれから進むべき方向性を確認しやすくすることに力点が置かれている。さらに、指示する側からは他の部署におけるオペレーションの遅滞が容易に把握でき、何を今、最優先して行うべきかの判断や決定に効果を与えることになる。

（5）CMT、BCP、DRPとコマンダープログラムの必要性

一般に有事対応を行うには3つの組織とそれらを統率する監視システムが必要と言われている。CMT、BCP、DRPとコマンダープログラムがそれに相当する。

CMT（Crisis Management Team）とは、危機管理計画を実行･監視･是正･運営する組織（情報漏洩後の危機管理組織）で、会社の経営全般の業務に影響を与える能力、権限、役割を有するものである。

BCP（Business Continuity Plan）は、情報漏洩後に付随的に発生するオペレーション障害に対する復旧計画を指すもので、原因部署やその影響下にある関連部署ごとに個別に行動計画を策定して、発生直後から自動的に発動させるものである。

DRP（Disaster Recovery Plan）は、情報漏洩後に付随的に発生するインフラ障害に対する復旧計画を指すもので、システムネットワークが攻撃を受けた場合など、個別部署単位ではなく、企業全体あるいはグループ企業全体で対処すべく、システム関連のバックアップ体制を前提とした行動計画を意味するものである。

コマンダープログラムは、CMTが、タイムマネジメント（時間による統制管理）の中で個別のBCPや企業全体のDRPオペレーションを見渡すための重要な戦略的行動計画である。これらの全体のイメージは図表5に示した通りである。

（6）恐るべき反社会的勢力の実態

AIGが対処した機微情報漏洩事件48事例のうち、実に35事例で企業に対して反社会的勢力と思われる者からの何らかのアクセスが確認された。また、弊社が独自に調査したところでは、詐欺被害を展開するこれらの反社会的勢力のほとんどがコールセンターを所有し、50人～100人近いオペレーターを使って2週間で1億円程度のノルマを課して展開、その様は一般の企業の営業さながらの様相である。さらに驚くべきは、基本情報が1件5円～35円程度であるのに対して、機微情報となると3万円前後で取引されている実態がある。ある企業では従業員が300件の個人情報を売りに出した際に、自ら10社を紹介するよう求め、9000万円を自らの口座へ振り込ませた。果たして20代、30代の若手や中堅社員が、これらの金銭を目の前に示された際に毅然として拒絶できるのだろうか。組織的、人的、技術的、物理的安全管理措置は確実にある程度の効果をあげるはずであるが、意図的･計画的に実行された犯罪行為はどこまで防ぎきれるだろうか。そこには限界があるはずである。また、こうして売買された個人情報は想像できないスピードで反社会的勢力の中に浸透していく。2週間～1ヶ月で数十社から数百社、中には700社を超える反社会的勢力にコピーされ、入手した当日から詐欺被害は展開されていく。その計画性、組織力、手口の巧妙さには舌を巻くばかりだ。

（7）通知と公表がただ一つの抑止効果

個人情報の漏洩のおそれは、明らかな漏洩の他、流出、紛失、盗用、所在不明、不着など色々な実態で報告されることになる。ここで重要なのは、漏洩は問題だが、紛失や所在不明程度ならよいといった間違った解釈をしないことだ。ある事例では、車上あらしを実行するため、朝から反社会的勢力が車3台で対象車両を待ち受け、代わる代わる追尾して、15分程度駐車した間に見事に盗取している。このように計画的に狙われた場合に、逃れられる可能性は極めて少ない。しかも上記のような場合、企業内では、単なる「車上あらし」で報告されており、「個人情報漏洩事件」としての取扱いを受けていないことが一般的である。しかし、彼らは着実に企業に浸食し、情報を入手している。企業が漏洩に気が付く頃にはかなりの詐欺被害者が発生しているのが実情である。こうした詐欺被害者をできる限り少なくするためには、企業側の行う対策として、原因究明後ただちに是正策を講じて2次被害を抑止し、同種の事件を回避するため、詐欺被害の手口の開示、警告、詐欺集団の告発などを積極的に進めていくことである。そのためには情報主体への通知･公表を継続して行い、一方で情報を絶えず収集しながら情報主体と共に、一体となって反社会的勢力と戦うことに他ならない。

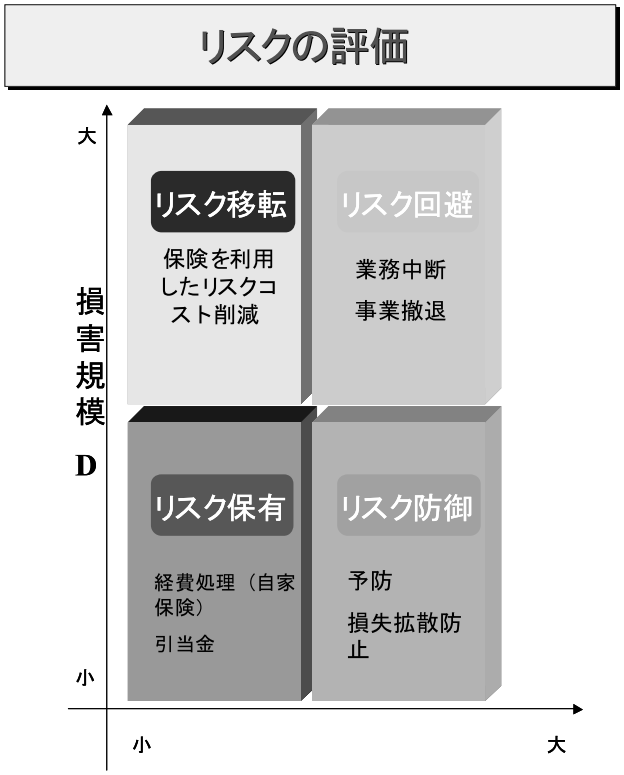
（8）シミュレーション･トレーニング

シミュレーション･トレーニングを行う理由は、予備訓練を行うことで危機的状況が発生した場合に無理なく各自のアクション･プランを遂行し、最終目標として企業の危機に対する損失を極小化することにある。そうした意味では、クリアーすべきバーは低いものでは意味がない。図表6にはシミュレーションのガイドラインを示したので参考とされたい。今後の企業の大きな課題は、人的安全管理措置を軸とした教育･訓練であり、シミュレーション･トレーニングは最も有効な訓練となるはずである。

最後に

企業の危機は、毎年その範囲を広げ、その態様も複雑さを増している。法的環境も変わり、国民の関心も大きく動きつつある。さらに、個人情報に係る問題は、社会不安を招く点からも対応が早急に求められている。企業はいかなる事態が発生しても、冷静に対処できる組織、訓練されたスタッフ、効果的なアクション･プランなどを備えておくことが、これらの危機を回避する唯一の方法であることを最後に申し上げたい。

図表1

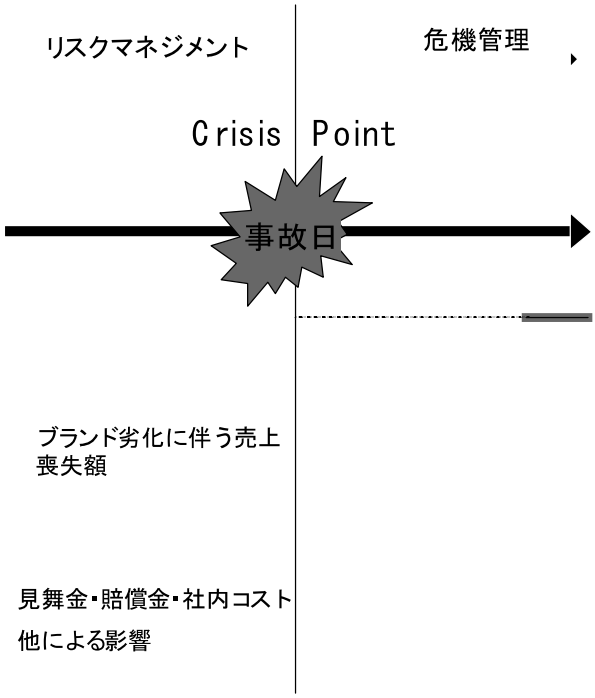


図表2

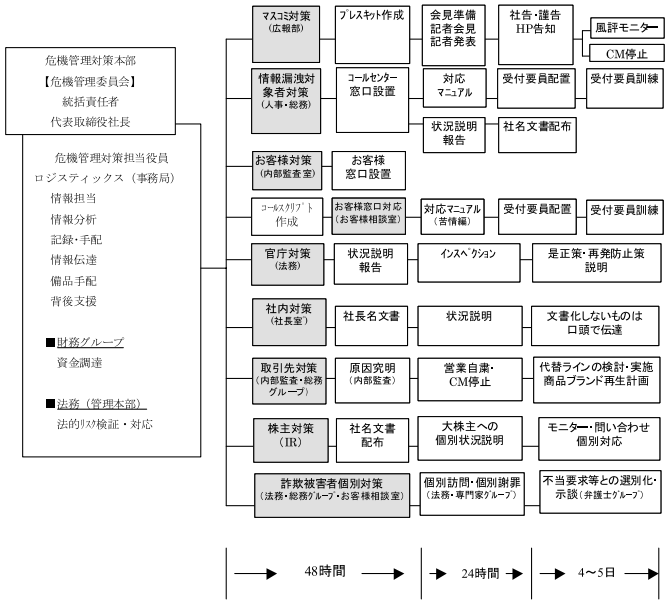
【アンケート結果】2004年7月、ＡＩＵ保険会社調べ

【質１】常設の情報管理責任者がいる
YES：57社（34.55%）　NO：109社（65.45%）
【質２】ﾌﾟﾗｲﾊﾞｼｰｽﾃｰﾄﾒﾝﾄまたはﾌﾟﾗｲﾊﾞｼｰﾎﾟﾘｼｰが存在する
YES：46社（28.40%）　NO：116社（71.60%）
【質３】ﾌﾟﾗｲﾊﾞｼｰﾏｰｸ、TRUST e、ISMSのいずれかの認証を得ている
YES：12社（7.41%）　NO：150社（92.59%）
【質４】個人情報漏洩はガバナンスの重要課題である
YES：155社（95.68%）　NO：7社（4.32%）
【質５】個人情報漏洩発覚後の見舞金は必要ない
YES：98社（64.05%）　NO：55社（35.95%）
【質６】電子媒体における不当なｱｸｾｽ等のﾌｧｲｱｰｳｫｰﾙに不安を感じる
YES：129社（78.66%）　NO：35社（21.34%）
【質７】外部業者に対するリスク管理に不安を感じる
YES：132社（80.98%）　NO：31社（19.02%）
【質８】社内の情報持ち出しリスクに不安を感じる
YES：145社（88.96%）　NO：18社（11.04%）
【質９】既に情報が漏れているかもしれないことに不安を感じる
YES：103社（63.19%）　NO：60社（36.81%）
【質10】個人情報漏洩発覚後の備えに保険加入を検討している、
または加入済みである
YES：26社（16.15%）　NO：135社（83.85%）

図表3

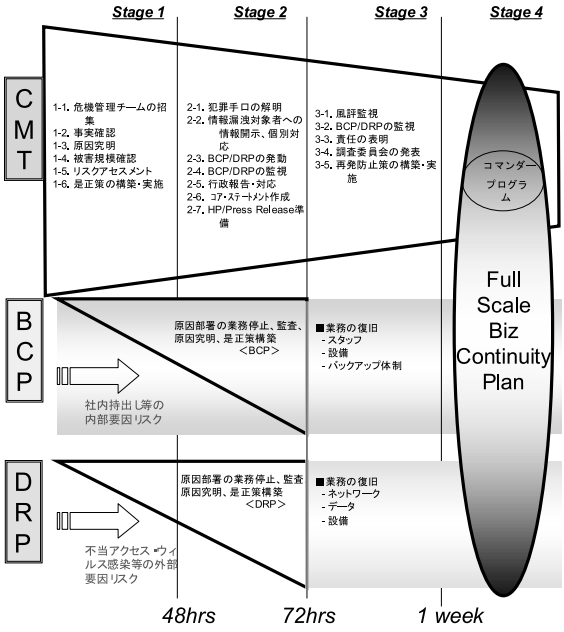


図表4　危機管理対策本部組織図



図表5

個人情報漏洩後の危機管理計画・情報開示計画



Model (Draft)

図表6

訓練は以下の想定シナリオ策定手順に従い実施する。

（1）事前決定事項

以下の内容を事前に決定し、実効的なシナリオを策定する

・漏洩情報の種類（センシティブな情報か否か）
・対象組織の規模（シミュレーションの規模をどこまで広げるか）
・初報と危機レベルの認識のタイミングは（平日・休日・夜・昼）
・クレームシナリオ（悪い条件下でシナリオを想定）
・社外の個人信用情報漏洩の拡大性の有無
・漏洩数
・消費者からの問い合わせ
・メディアからの問い合わせ
・行政関連からの問い合わせ

（2）シミュレーション

以下の事項を訓練の中で実施し、危機管理計画上の問題点を洗い出しする

・危機管理委員の招集（緊急連絡網）
・対策本部の設置宣言（場所はどこに、主要関係者への通知など）
・各チームのアクションプラン
・事実関係の調査・報告
・経営判断（本人への通知、行政届出、公表など）
・公表用コア・ステートメントの作成
・関係当時者への通知文作成
・ホームページ開示文書、社告の作成
・行政届出内容の作成
・苦情対応整備（コールセンターの受付ツール、コールスクリプトの作成）
・メディア対応の整備（Q&A作成やフリーダイヤルの設置など）

（3）チェックポイント

以下の観点から訓練における検証を行い、是正を行う

・タイムマネージメント（各チームが時間とおりに調査・報告がなされたか）
・報告の正確性
・経営判断における工程（各選択肢のメリット・デメリットを見極めたか）
・消費者、行政、メディアへの合理的説明は存在するか
・備品・情報伝達媒体（電話、メール、携帯、ファックスなど）
・設備は使用可能か
・緊急資金の調達は万全か
・各チームの現場での役割は明確かつ行動基準は正しく遂行されたか
・現在の行動基準に齟齬はないか
・是正・代替案の可能性はないか