金型企業のためのサイバーセキュリティ実践講座　【第４回】

インシデント発生時の初動対応と，情報（データ）のバックアップの考え方

―危機管理の視点から対策の実効性を高めていくために―

一般社団法人日本金型工業会　認証運営委員会委員（主席審査員）　川名　正幸

今年に入ってからも，引き続きワナクライ（WannaCry）ウイルス[1]感染などの情報セキュリティに絡んだ事件（以下インシデントと記述）が頻発し，さまざまな犯罪グループが，脅迫による金銭搾取を一つのビジネスと捉え，組織的な活動を活発に行っている。

中でもトヨタ自動車の主要仕入先で発生したインシデントでは，トヨタの14工場にて28ラインが稼働停止に至った。３月末に公表された仕入先社の調査報告書[2]を読むと「子会社が独自に特定外部企業との専用通信に利用していたリモート接続機器」という記述がある。実際に狙われたのは仕入先社の子会社であり，改めてサプライチェーンの情報管理が問われている。

自動車産業と関わりが深い金型業界では，この事件報道にドキッとされた企業も多かったと推察するが，日本金型工業会の技術情報管理認証制度への取り組みについて，改めてその重要性が認識されたことと思う。

今号ではこうした状況を踏まえて，特にインシデント発生時の初動対応と，情報（データ）のバックアップの考え方について解説したい。

情報セキュリティ対策の実効性は大丈夫か

筆者が認証取得の支援や審査を行った企業でも，インシデントが発生した場合の連絡体制や，従業員への意識醸成のための研修計画の作成は当然行われているのだが，自社で本当にインシデントが発生した場合，どのような事態に陥るのかを想定しての，踏み込んだ検討を行っている企業は少ないように感じる。

その大きな理由として，そもそも「当社では情報セキュリティに関する事件・事故は発生していない」の認識が強いように思える。「情報セキュリティ白書2021」におけるサイバー被害状況を見ても，中小企業のうち（回答数1,015），一度でも被害を受けた企業は11.4%となっている[3]。

一方で，興味深いアンケート調査の回答結果がある。IPA（情報処理推進機構）が2021年12月に公表した調査結果[4]だが，見出しに「サイバーセキュリティに関するトラブル，中小企業従業員の10.5%が経験」とあり，情報セキュリティ白書の数値と似たものだが，サブ見出しは「従業員の５人に１人は情報管理のルール違反経験あり，経験した事故やトラブルの半分程度は，会社や上司に報

1）ワナクライ（WannaCry）ウイルス
ランサムウェアと呼ばれる身代金要求型のコンピュータウイルス。コンピュータに侵入し，そこからアクセス可能な他のコンピュータに対して，自動的に再感染しながら被害を拡大させる。初期のころは，パソコン内のプログラムやデータを暗号化した上で，暗号解除の見返りとして身代金を要求するものだったが，最近は暗号化したデータ（情報）を奪って，他社に売りつける旨の脅迫を行い，身代金を要求するなど，時代と共に脅迫のパターンも変化している。
※ランサムウェアとは，「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。

2）有力仕入れ先の調査報告書
https://www.kojima-tns.co.jp/news/news0003235/ を参照。

3）「情報セキュリティ白書2021」P134「図2-4-14 サイバー被害状況」より
※一般社団法人日本損害保険協会「国内企業のサイバーリスク意識・対策実態調査2020 集計報告書」を基にIPAが編集。

4）IPA調査結果の詳細（PDFファイル）
https://www.ipa.go.jp/security/otasuketai-pr/assets/pdf/enq20211208.pdf を参照。

告していないことが判明！」というショッキングな記載となっている。詳細は注釈４）のURLリンクをご覧いただくとして，その一部を**図１**，**図２**に掲載する。

「報告することは，怒られた上に余計な仕事を作るだけ」ということかもしれないが，組織としての連絡体制は定められていたとしても，「即報告」が習慣付けられていなければ，対策の実効性は大きく落ちることになる。ぜひその視点から，インシデントが発生していないこと自体を一度疑って

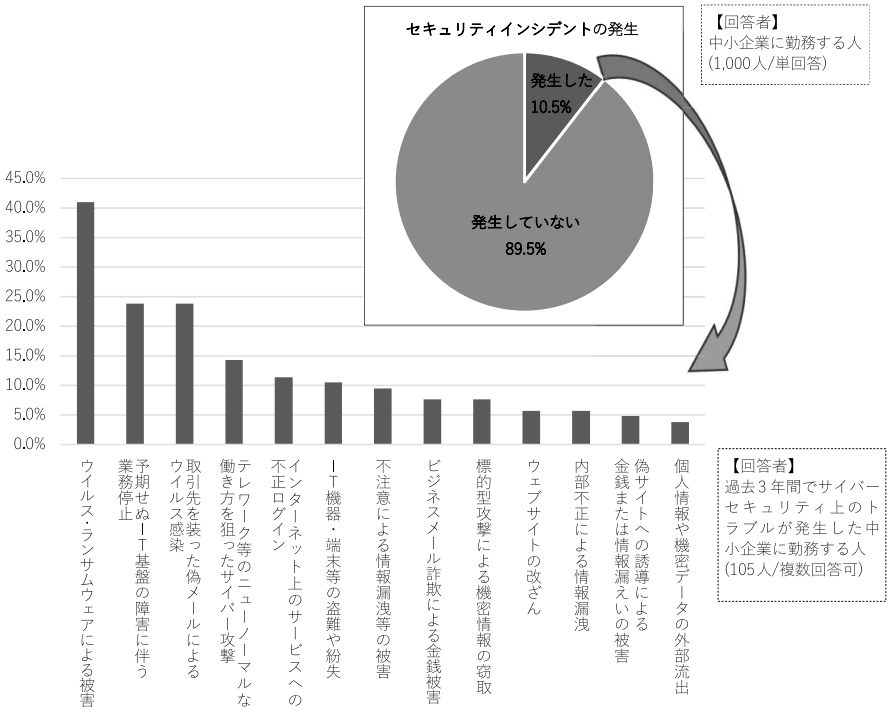

図１　過去３年間に発生したセキュリティインシデントの内容

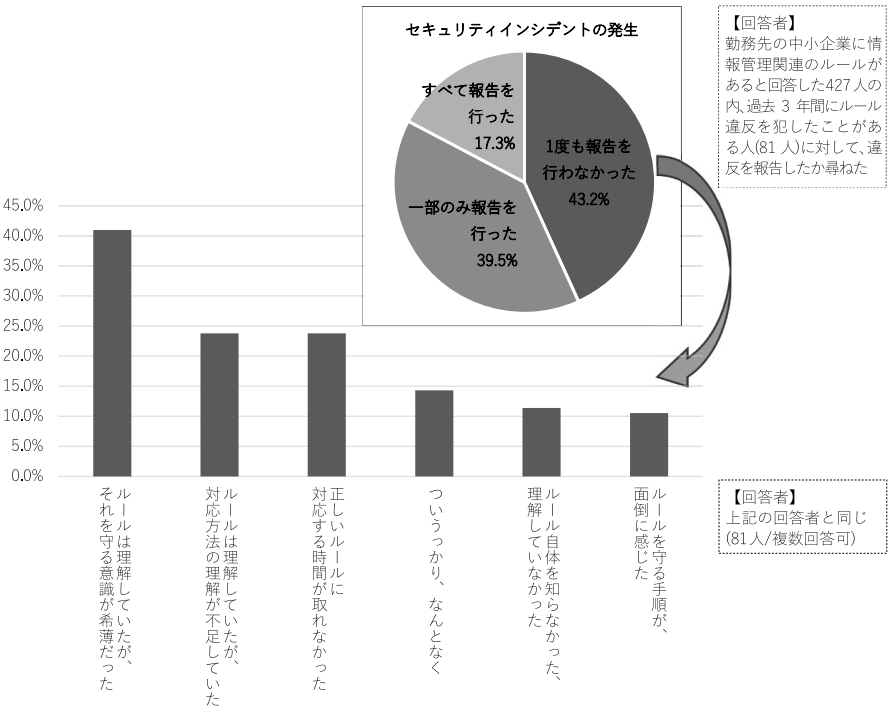

図２　報告を行わなかった理由

みていただきたい。

インシデント発生時の最初の行動は…

企業がインシデントの発生を最初に知る状況としては，社内の情報システムが不審な挙動を検知したり，従業員が自分のパソコンの動きがおかしいことに気付くといった，社内からの第一報だけでなく，警察や顧客などから「おたくの情報が洩れているのでは」という通報がきっかけとなることも多い。

ワナクライのように画面に脅迫メッセージが出るようなケースであれば，容易に感染に気付くが，システムの誤検知やユーザーの誤操作，通報者の勘違いであることも考えられ，特に外部からの通報であれば，情報の裏付けと共に，該当の部門などへのヒアリングを内々に行うことも必要となる。

被害の拡大防止にはスピードが最重要であり，原因究明よりも優先されるが，こうした確認作業の時間が経過する中で，誰がどんな情報をもとにインシデントと判断するか（できるか）という点も，迅速な初動対応を行う上で重要なポイントとなる。

結果としてインシデントだと判断した場合には，「情報管理委員会」のような全社組織が立ち上がり，組織的対応の役割を担うことになる。そこで最初に求められるのは，情報システムやネットワークの停止/遮断の範囲と，業務停止などの事業への影響度の判断であり，その影響度によっては，警察や所轄官庁への届け出に加え，社外のステークホルダーに対してインシデントの発生の事実と対応状況，復旧の目処や暫定対応措置などを，遅滞なく公表していく必要がある。

これらの対応は，サイバーセキュリティのインシデントに限らず，紛失/盗難や社内不正などの人為的なインシデントでも，基本的には同様と言えるが，一連の対応フローについて検討する際の参考にとして，JPCERT/CC[5]が公開している資料のURLを記載しておく[6]。

このように，初動対応は連絡網の整備だけで，あとは「何事も臨機応変に」とはいかないことは理解いただけると思うが，日々情報システムを運用管理している部門（担当者）でも，いつ発生するか分からない危機管理時のオペレーションは「頭では分かっていても，体が付いてこない」になりがちである。事業環境が許される範囲で定期的に訓練を行うことを勧めたい。

訓練の必要性と実施のポイント

訓練には，その目的と企業の置かれた環境を踏まえてさまざまな形態（方法）があるが，ここでは２つの訓練について，実施に際して考慮すべき点を述べたい。

（1）不審メール訓練（標的型攻撃メール訓練）

疑似メールを社員に送付して対応力を養う訓練は以前から行われてきたが，「最近の不審メールは巧妙で，専門家でも見抜くのが難しいと聞くので，訓練しても無駄ではないか」という意見がある。

また訓練に当たっては，「他社では不審メールを開封してしまった率はどの程度ですか」とか，「開封率[7]を何パーセントまで下げる必要がありますか」という質問をよく受ける。

しかし不審メール訓練の目的（目標）は，開封率をゼロにすることではない。

前述のアンケート調査結果にもあったように，開封してしまっても黙ったままの従業員がいる中では，単純に開封率が前回よりも “減った”, “増えた” という「開封率= ０%」を目指すことは，あまり意味がない。

また，単純に報告したかどうかという「報告率=100%」を目指すことだけでもない。

重要なのは，訓練で送付されてきたメールに対して，不審なメールだと見極める力を持つ社員を

5）JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）
日本国内でインターネットを介して発生するインシデントについて，報告の受付から，対応の支援，発生状況の把握や手口の分析，再発防止対策に至るまで，技術的立場から検討や助言を行なっている。特定の政府機関や企業からは独立した中立の組織である。

6）『組織内CSIRT構築の参考資料　インシデント対応マニュアルの作成について』
https://www.jpcert.or.jp/csirt_material/files/13_incident_response_manual_20211130.pdf

7）開封率
訓練対象者の中で，メール本文内にあるURLや添付ファイルを開いた人の割合であり，「訓練用の疑似攻撃メールに引っかかってしまった人」の割合ともいえる。

増やすこと，および添付ファイルを開封したり，URLリンクをクリックするなどして，異常な状況が発生した場合に，「どれだけ迅速に上司や定められた報告先に報告できるか」という点にある。

したがって，従業員に訓練を通じて徹底すべきことは「おかしなメールのファイルは開封するな」だけでなく，それ以上に「開封した／しないに関わらず，すぐに報告しろ」という点である。したがって，日常の管理指標（モニタリング指標）も，たとえば訓練メールを開封してしまった時点から報告が上がるまでの時間が，より重要な指標と言える。

ただし，要員が限られる中小企業において実際に時間を指標として管理するには，記録を取るなどの負荷もあり，現場としての創意工夫が求められる。

(2) ネットワーク遮断（業務停止の可否判断）の訓練

インシデント発生時の初動対応として，もう一つ述べておきたい訓練に，ネットワークの遮断がある。

昔は「パソコンがおかしな挙動をしてウイルス感染が疑われたら，即パソコンにつながっているLANケーブルを引き抜け」と言われていたが，最近のパソコンは無線LAN（Wi-Fi）接続がほとんどであり，どうやったらネットワークから遮断できるのか分からない従業員も多いのではないだろうか。

慌ててパソコンの電源を切っても，パソコンを再起動した時に動き出すウイルスもあるので，ネットワークからの正しい遮断方法は徹底しておく必要がある。また一方で，LANケーブルを引き抜いたり，無線LAN（Wi-Fi）を無効にすると，感染直後のパソコン内部の情報が変わってしまうので，後々パソコン内の情報を解析するに当たって支障があるという意見も聞く。

後々の原因調査と被害拡大防止とのどちらを優先するか？　そのために専門家や業者に相談したくても，その間にも感染リスクが増大する。そのため，あらかじめ初動対応時の判断基準（対応の考え方）を，社内の研修資料や，危機管理に当たる情報管理委員会などの運営ガイドに具体的に記述し，慌てず迅速に対処していただきたい。

ネットワーク遮断に当たってのもう一つの考慮点に，情報システムの運用管理部門（担当者）の日頃からの対応がある。インシデント発生時に，ネットワーク構成図や設定情報から影響範囲を見極めようとしても，構成や手順の情報が古く，的確な対応ができないということがありがちである。重要な業務プログラムやデータが格納されているサーバーを，どこの接続先を遮断して被害から護るのか？　また顧客や仕入れ先などのネットワークの接続相手先に対して，業務の優先度を判断しながら的確なネットワーク遮断の可否判断を行えるか？　こうしたことを短時間に，かつさまざまな判断を行うためには，常に最新情報に更新しておくことが求められる。

訓練では，以上述べてきたことをシナリオに展開して実施していくことになるが，中小企業では，自社の情報システムのテスト環境を専用に構築・保有していることは稀であり，ネットワークの遮断や，ここだけは切断できない相手先に対する接続テストなどの実施も，本番システムの環境下で実施することになり，訓練自体が大きなリスクとなってしまう。したがって現実的な訓練としては，シナリオを基にした机上シミュレーションから始めることが適当と言える。

なおシナリオの作成も，まずは最も発生の可能性が高いインシデントを取り上げて，発生時の関係組織，キーマネジメントの動きとともに，業務への影響度と停止の可否判断を机上でシミュレーションすることから始めてはどうだろう。要は発生時の現場を具体的にイメージし，**表1**のような確認ポイントを評価していくことになるが，ここでも上述のJPCERT/CCのURLリンク先の資料が参考になると思う。

一点，補足となるが，情報管理委員会の事務局を，情報システム部門の関係者が担当しているケースを多く目にする。平常時であれば妥当と言えるが，インシデント対応の非常時には，情報システム部門の関係者は，目の前の対応に忙殺される。したがって社内外との情報連携や各種調整を，迅速かつ円滑に行う役割を担う事務局の構成には，関連組織から適任者がアサインされるよう，十分な配慮が必要である。

表１　ネットワーク遮断訓練における主な確認ポイント

	対象	ネットワーク遮断訓練における主な確認ポイント
1	情報管理委員会	✓ 情報管理委員会の招集判断と、判断指示系統は適切か ✓ 社内外との連絡は機能するか(ネットワーク遮断時の代替手段があるか) ✓ 管理者不在時の報告経路(エスカレーションパス)は妥当か ✓ 経過時間と活動の記録は取れるか(後々の報告や経験として活用) ✓ 事務局機能として対応に当たる管理者や従業員の人数は十分か
2	情報システム 担当部門（者）	✓ ネットワーク構成図、設定情報など、必要な情報に誤りはないか ✓ ネットワークの遮断/復旧の見極めと手順は適切か ✓ 情報システム/ネットワークの代替手段（冗長化/切替え)は有効か ✓ 初動対応や緊急対策にあたる担当者は、適切に配置できるか ✓ 原因の分析に必要な情報(データ)は入手可能か ✓ 技術的対策に必要な相談先はあるか
3	業務部門/ 営業部門	✓ 業務への影響を踏まえた遮断/復旧の優先順位が付けられるか ✓ 顧客や取引先からの問い合わせ対応に必要な情報は入手できるか ✓ 顧客や取引先の対応に当たる担当者は、適切に配置できているか ✓ 情報管理委員会や情報システム担当部門(者)との情報連携はできるか

重要情報の保管と護り方

「火事と喧嘩は江戸の華」と言われるほど，江戸の町は火事が多く，1867年の大政奉還までの267年間で，大火災だけでも49回も発生したと言われている。

商家では近所で火事が発生した場合，大事な顧客や取引の情報が書かれた「大福帳」を井戸の中に投げ入れて，火から護ることが行われていたようだ。文献によると，大福帳は特殊なコンニャクで作った和紙が使われており，墨で書かれた文字が水に浸かっても滲むことがなかったため，さらに今は見かけることが少なくなった油紙で固く包んで，迷うことなく井戸に投げ込んだとある。

当時は「大福帳」のバックアップとして同じものを複数作成することは難しく，まさに原本そのものをどう護るかだったのだと思う。その点，現在のIT環境では，さまざまな方法で重要情報のバックアップを取ることが容易となり，逆にそのことが，情報漏洩につながるリスクにもなっている。

表２に非常時の情報の取扱いについて江戸時代との比較をしてみたが，この中で特に江戸時代ではできなかった複製の点から情報のバックアップについて考えてみたい。

江戸時代の手書きの大福帳ではできなかったのが，「複製と世代管理」の考え方だ。

図３　伊藤忠商事のホームページにある大福帳の写真
（https://www.itochu.co.jp/ja/about/history/tougegoe.html）

情報（データ）のバックアップ自体は，情報セキュリティが重視される以前から，システム障害や停電等の災害対策として，運用管理の基本要件であった。

銀行のオンラインシステムでは，リアルタイムに正副のデータベースに書き込み・更新がされ，万一の障害発生時には，瞬断することなくバックアップシステムに切り替わる。また定期的に複製を取り，何世代もの情報が保管・管理されている。

表２　非常時を意識した情報の取扱い

視点	江戸時代	現在
保管媒体	✓ 滲まない紙と防水対策	✓ デジタル媒体とマルウェア感染対策
保管場所	✓ 自宅内の井戸や土蔵	✓ ネットワーク、運送等により遠隔地に保管
複製	✓ 基本的には不可	✓ デジタルデータとして複製 ✓ 何世代もの情報を保管可能

当然，そのための仕組みにコストが掛かり，さらに自社内で維持管理していく場合は，人材育成を含めた運用保守を担う要員コストに目を向ける必要があるため，情報管理の現場判断に任せるのではなく，状況を理解した上での経営判断が求められる。

特に経営者に誤解が多いのは，「情報（データ）は複製したものがあるから，すぐに障害発生前の状態に戻せる」と思っていることだ。通常の企業では，銀行のようにリアルタイムで更新していることはないので，インシデント発生時の復旧対策として，昨日朝の状況に戻せるのか，１ヶ月前の時点なら戻せるのか，戻った時点から直近までの空白の時間の取引データはどうするのかなど，戻った時点での状況を十分理解して対応に当たる必要がある。

また，世代管理された複製ファイルが保管されていても，それ自体が元のファイルと同様にネットワークに接続された環境下にあれば，ワナクライのウイルスで，複製ファイルまで暗号化されてしまうことになりかねない。

昨年，病院でワナクライに感染して電子カルテが使えなくなった事例が話題になったが[8)]，幸い紙のカルテは法律で５年間の保存義務があり，大変な苦労があったものの，再入力してシステムを復旧できたようだ。ぜひ最重要のデータは，ネットワークから遮断した環境下での保管を併せて行うことなど，運用管理面での考慮をいただきたい。

なお，バックアップが必要なのは情報（データ）だけでなく，業務プログラムについても同様の対応が求められる。特に業務プログラムについては，業務自体の変更に合わせて適宜機能の更新が行われているはずなので，世代管理された業務プログラムを用いてシステムを復元した場合，直近の業務機能との整合性を十分確認する必要があることも念のため付け加えておく。

まとめ（情報管理＝事業継続の視点）

筆者がこの講座を最初に担当した第186号（2022年１月号）記事の冒頭で，事業継続計画に触れ，リスクマネジメントと危機管理の考え方をまとめた表（**表３**）を掲載した。

何度も述べてきたように，初動対応が迅速かつ的確に取られるためには，平時からの備えが欠かせず，そのためにも表３に示すリスクマネジメントの取り組みのアプローチが求められる。

これを技術情報管理認証に当てはめて考えると，リスクの特定・分析・評価は，自社の情報システム環境を俯瞰的に眺める中で，重要技術情報の絞り込み特定することである。

その際に役立つのが，認証審査で使用されるチェックシートであり，組織と経営者，従業員，IT技術，執務室／工場，外部委託などのさまざまな視点で，リスクの有無を影響度と発生可能性から分析・評価し，事前の対策を講じるという流れになる。

8）ランサムウェア，徳島県の病院から学ぶこと
https://softwareisac.jp/wp/?p=19936 を参照。

表３　リスクマネジメントと危機管理の視点

視点	リスクマネジメント	危機管理
目的	✓ 損失の最小化と収益の最大化	✓ 不測の事態発生時の適切な対応
取り組みのアプローチ	✓ リスクの特定・分析・評価（影響度と発生可能性） ✓ リスク対応（事前の対策） ✓ モニタリング及びレビュー	✓ 危機発生時の対応と平時の備え ✓ インシデントの見える化（報告の徹底と再発防止） ✓ 事業継続計画（BCP）の作成
対策	✓ リスクの低減 ✓ リスクの移転 ✓ リスクの回避 ✓ リスクの受容	✓ 初動対応 ✓ 緊急対策 ✓ 復旧対策 ✓ 再発防止策

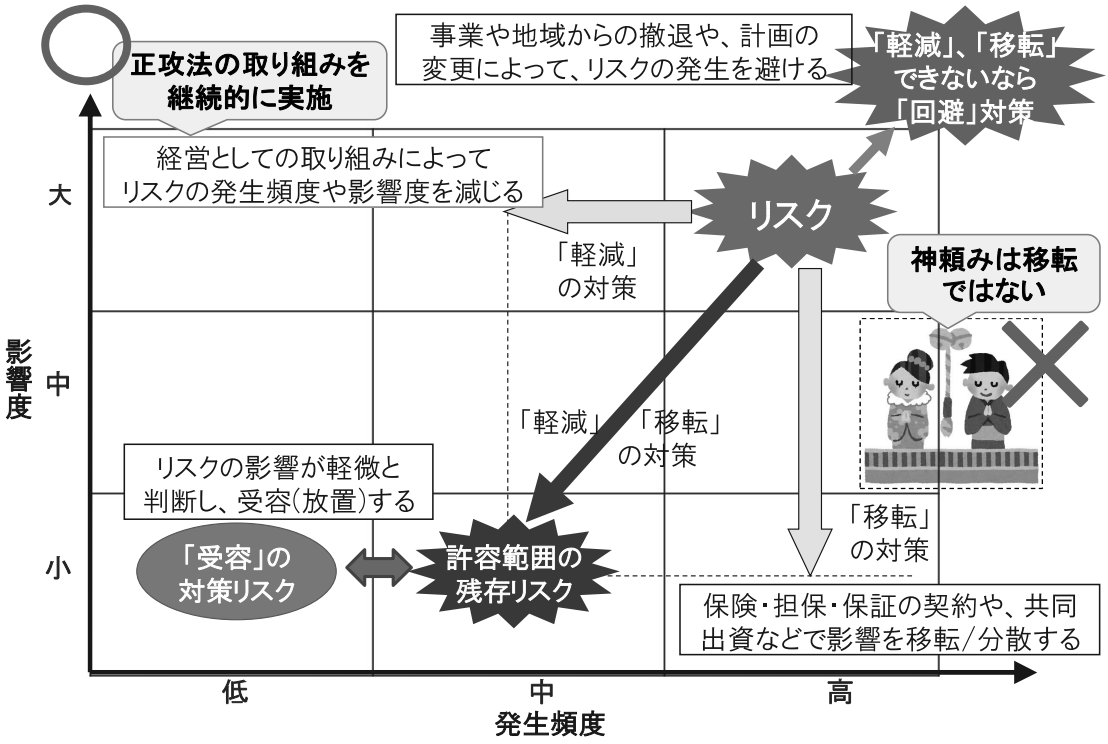

図４　リスク対応の考え方

またリスク対応として検討すべき対策には，**図４**のようにリスクの軽減，移転，回避，受容といったさまざまな視点がある。企業の事業継続に不可欠な技術情報管理の対策が，決して神頼みとならぬように，モニタリングとレビューを通じて，毎年少しずつレベルアップしていくことをお願いしたい。

最後に付け加えることとして，「情報管理の仕組みや日常の運用を，企業全体に根付かせて習慣化させていく」活動は，現場にさまざまな変更や調整を求めることから，推進担当者の負担感が高まるだけでなく，変えることへの拒否感，不安感などから理解を得られず，いつの間にか頓挫することになりがちだ。したがって特定の担当者に任せっきりにせずに，経営者の継続的な関与が必須となる。技術情報管理認証制度では，その継続性を３年ごとの更新と毎年のPDCA活動で担保しているが，認証の取得と日々の運用に当たっては，ムリ，ムダ，ムラのない継続可能な仕組みで定着を図っていただきたい。