「リスクマッピング」による
リスクマネジメントシステムの実践

吉田　薫

社団法人 中部産業連盟

要　旨

テーマ：　「リスクマッピング」によるリスクマネジメントシステムの実践

企業にとって、リスク管理は優先順位の高い経営課題ととらえなければならない。しかし、旧来のリスク対策の延長ではその効果が十分でないことは、様々な事件・事故が頻発していることからも明らかである。

本論分ではリスク対策としてマネジメントシステムの導入をとりあげる。リスク管理には一貫した流れが必要で、PDCA（Plan-Do-Check-Act）サイクルによる継続的なシステムの改善活動により、その管理レベルを向上させていくことが有効である。システム構築にあたっては、「リスクマッピング」を用いた手法を取り入れ、システム構築の鍵となるリスクの洗い出しをおこなうとともに、業務の標準化を実現することを薦めている。

「リスクマッピング」によるリスクマネジメント構築事例としては、医療分野と情報セキュリティ分野について実践した。両分野ともリスク対策に関心が高いのであるが、この手法によるリスクマネジメントシステムの構築を実現することができた。様々な分野に応用しやすい手法といえる。

－ 目 次 －

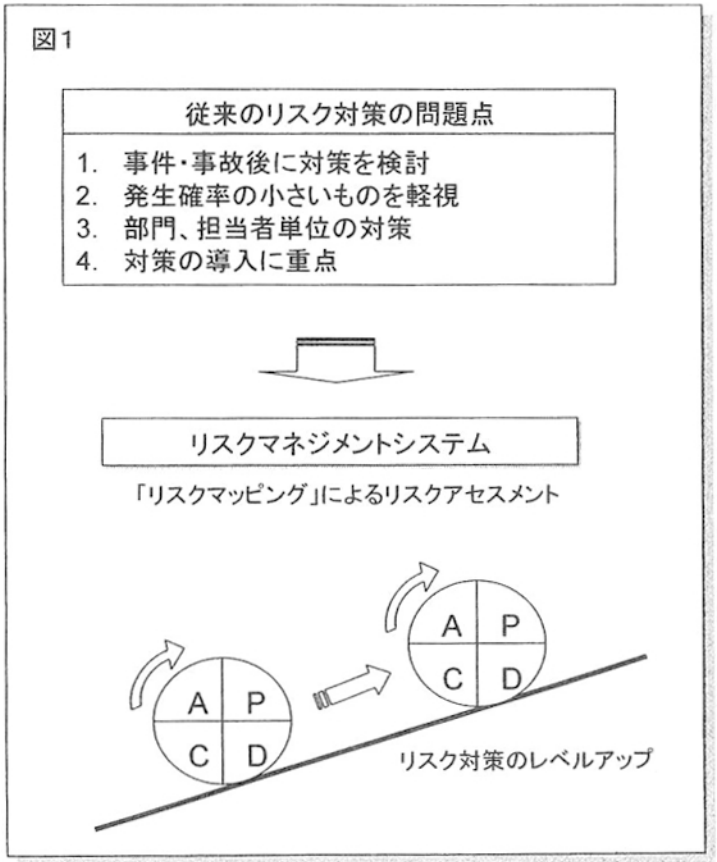
Ⅰ　はじめに

環境が変化し、様々な技術が大きく進歩し複雑化するにともなって、組織におけるリスク管理のしくみも変革が要求されている。企業ではこれまでにもリスク対策を実施してきたのであるが、昨今頻発する事件・事故の状況から次の問題点が指摘できる。第一に、これまでのリスク対策は、事件・事故を実際に経験してからその原因を追究し、対応する事後対応の傾向があった。第二に、発生確率が小さいものについては、それが組織に甚大な被害をもたらすと想定されるものでも対応が後回しになる傾向があった。第三に、リスク対策については、部門や担当者単位で実施されてきており、全社的な対応があまりおこなわれてこなかった。第四として、リスク対策について、その導入への検証は熱心であるが、導入後の運用状況や、その効果や問題点の検証はおろそかになりがちであった。

本論文では、リスク対策の手順や、組織的なしくみづくりとしての、リスクマネジメントシステムをとりあげる。マネジメントシステムとは、ISO9001（品質マネジメントシステム）や ISO14001（環境マネジメントシステム）でもひろく知られたしくみで、PDCA（Plan-Do-Check-Act）サイクルによる継続的改善活動により、仕事のすすめ方、管理や機能レベルを向上させていくことが特徴である。リスク対策には一貫した手順が必要である。限られた経営資源（ヒト・モノ・カネ）を有効に活かすには、リスクの重要度に応じた効率的なリスク対策を実施したい。ここに「リスクマッピング」を活用したリスクアセスメントと業務の標準化を薦めている。

リスクマネジメントシステムはその対応策をつくることが目的ではない。組織に合ったリスク対応策を策定し、組織全体に浸透し、運用しなければならない。リスク対策を基盤とした品質やサービスの向上は、顧客の信頼獲得や競争力の向上に寄与し、また従業者の満足度も高い組織となることができる。これこそマネジメントシステムの目指す姿である。

図1

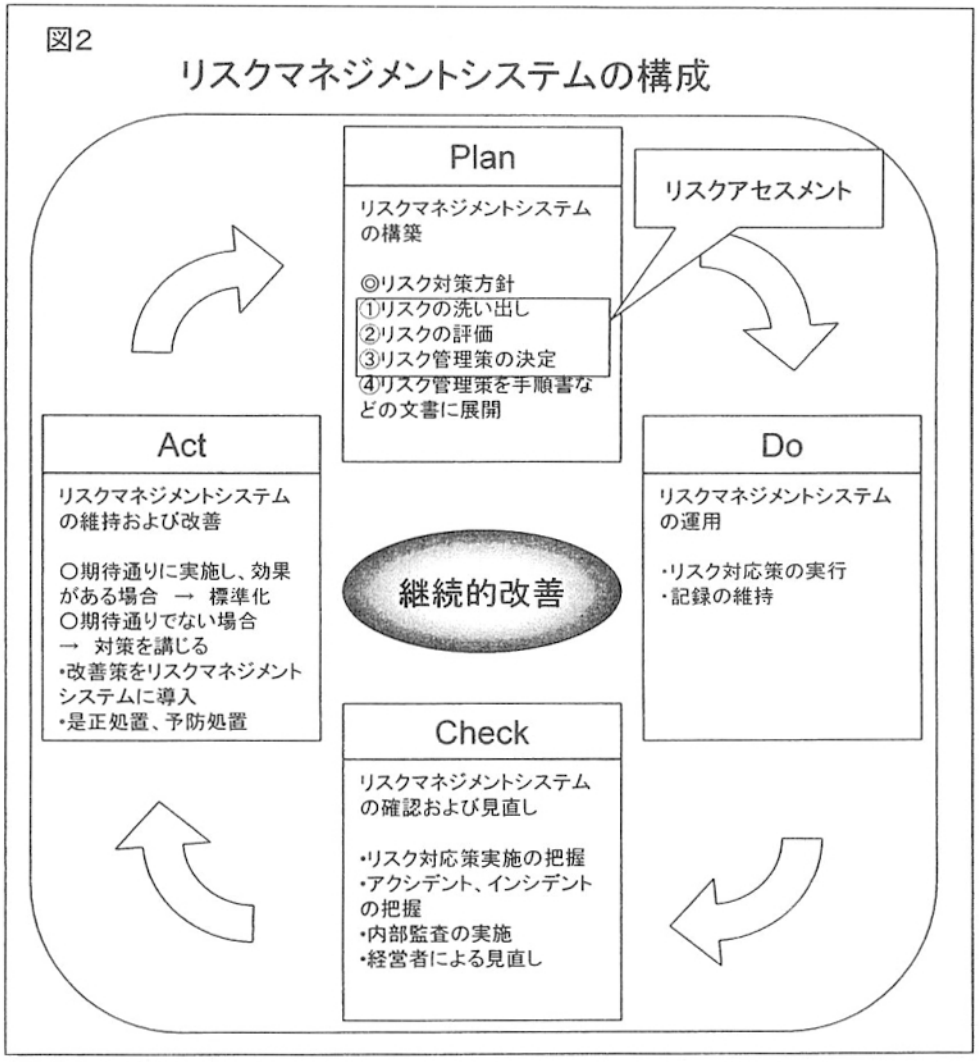


Ⅱ　リスクマネジメントシステムの構築と運用手順

1.「リスクマッピング」によるリスクマネジメントシステムの構築

リスクマネジメントシステムは図２の通り構成される。マネジメントシステムのPDCAサイクルをまわすことによってリスク対策のレベルを継続的に改善しながら、安心して事業展開できるしくみづくりや、サービスの向上につなげていくことを実現する。

図2



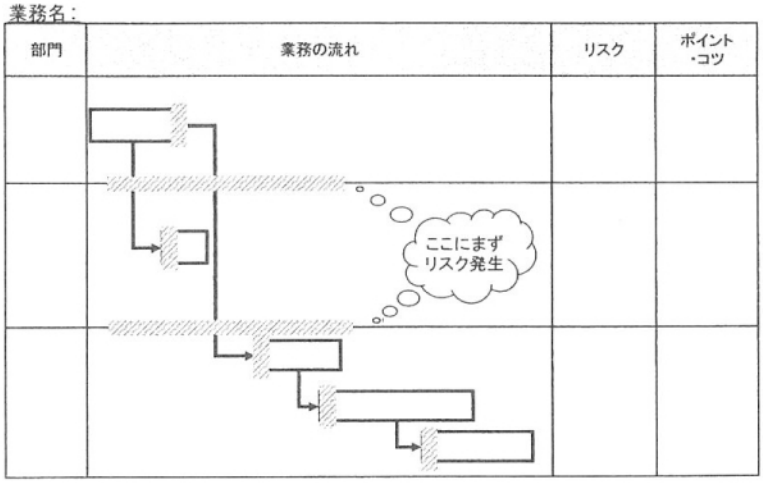
リスクマネジメントシステムの構築段階（Plan）について、①リスクの洗い出しから③リスク管理策の決定までのプロセスをリスクアセスメントと呼び、その手順を紹介する。

(1)　リスクの洗い出し

リスクマネジメントシステム構築にあたってまず実施することは、組織に存在するリスクをもれなくすべて洗い出すことである。これには業務を体系化し、業務ごとに図３に示す「リスクマッピング」の作成が効果的である。これは業務の流れをとらえながらそこに潜むリスクを全て洗い出す方法である。「リスクマッピング」は実際の業務の流れを現場で

確認しながら作成する。机上で想定するとリスクの洗い出しに漏れが生じることをこれまでに何度も経験した。必ず現場で実際の業務をとらえながら実施することが重要である。

図3「リスクマッピング」



リスクはあらゆる場面に想定されるのであるが、とくに人と人の間、業務と業務の間、すなわち図3の矢印にあたる部分に大きなミスがおこりがちである。ここでは次の担当者への情報伝達がうまくできなかったり、時間的に切れ間ができることなどが影響するためである。業務そのものにあるリスク（図3の枠で囲んだ業務）についても確認する。

リスクマッピング作成にあたっては、それぞれの業務についてのポイント・コツを書きとめておく。業務ごと、あるいは担当者レベルでのポイント・コツを標準化し、関係者で共有化すれば、あらたな投資や対策をすることなくリスク対策に活かすことができる。

(2)　リスク値の評価

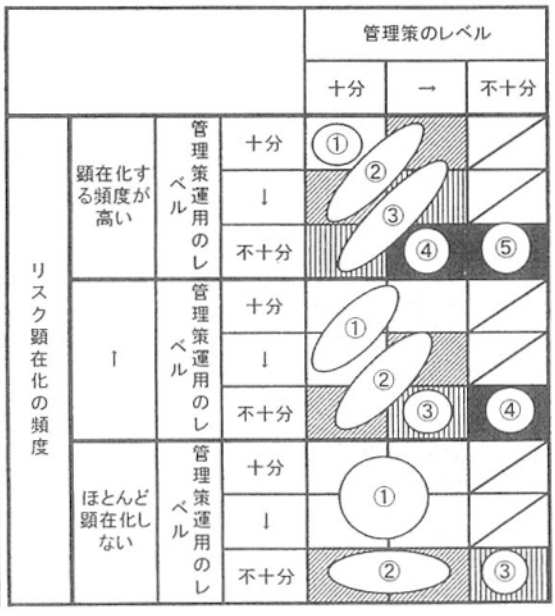
図4

リスク値　＝　リスク管理レベル　×　脅威・脆弱性レベル

リスク管理レベル評価の例

リスク管理レベル	判定基準
4	組織として最大の管理の必要なリスク。 リスクの発生により、人の生命にかかわる、あるいは社会問題となるほどの信頼問題、遵法性に関わる問題となったり、廃業に匹敵するほどの影響を与える可能性のあるもの
3	十分な管理の必要なリスク。 リスクの発生により、サービスの質、顧客の信頼・遵法性（処罰の対象外）に関わる問題となったり、一定期間事業停止となるほどの事業活動に影響を与える可能性のあるもの
2	適切な管理の必要なリスク。 リスクの発生により、事業停止などの事業活動、顧客の信頼や遵法性の問題は無いが、ある程度事業活動に影響を与える可能性のあるもの
1	一般的な管理レベルで問題のないリスク。 リスクの発生により、サービスの質、事業活動、遵法性に問題のないもの。

脅威・脆弱性レベル評価の例



リスクを洗い出した後は、リスクの重点化をおこなう。本当に対策すべきリスクは何かを認識し、優先順位をつける。リスク対策を考えるにあたって注意しなければならないのは、組織のリスクの重要度に応じて対策案を決定するのであり、決して採用するリスク対策からそのリスクの意味づけをしてはならないことだ。原則的にはすべてのリスクについて何らかの対策をおこないたいところだが、限られた経営資源で対策を実施するには、どのリスクをどのレベルまで管理するかの判断基準が必要となる。対策の可否判断の基準を設定し、適切に経営資源を配分することにより、組織としてバランスのとれたリスク対策をおこなうことができる。

リスクの評価方法の例として、組織のもつリスクの重要性をリスク値として算出する方法を紹介する。これはリスク管理レベルと脅威・脆弱性レベルの積で算出する。リスク管理レベルについて、図4では4段階で評価している。脅威・脆弱性レベルはそのリスクの発生の可能性とリスク対策の管理レベルの要素からなる。つまりリスク値としては、リスクの管理レベル、リスク顕在化の頻度、リスク管理策のレベル、管理策運用レベルの4要素を考慮したものである。組織の規模やリスク対策の重要度などに応じて配点や評価要素を変更しながら組織の実情にあったリスク値を求める。

(3)　リスク対策の策定

リスクの評価により、対策すべきリスクの重点化について整理したら、そのリスク対策を策定する。図5はリスク対策を実施するときに活用しているリスクアセスメントシートの例である。各業務について洗い出されたリスクについて、前述の評価基準によってリス

図5

リスク値　　6未満 ⇒ リスクを許容
6以上 ⇒ リスク管理策が必要

リスクアセスメントシート

業務	リスク	リスク評価	現状		管理策	管理策適用後		関連文書
			脅威・脆弱性レベル	リスク値		脅威・脆弱性レベル	リスク値	

管理策適用後もリスク値が6以上の場合
⇒ 即、改善計画を作成
⇒ リスク回避（該当業務を止める）
⇒ リスク移転（アウトソーシング、保険をかける）

ク値を算出する。現状のリスク値が高いものに対しては、そのリスク値を下げるおおまかな管理策を検討する。管理策を実施した場合のリスク値がどの程度になるかを算出し、そのリスク対策を効果的かどうかの妥当性を判断するのである。関連文書欄にはその管理策を展開する規定や手順書などのタイトルを記述する。

評価したリスク値については、低ければ低いほどよいのであるが、組織の事情によりある程度までしか対策は実施できないものもある。そこで組織の事業内容や規模などを考慮しリスク許容のレベルを決める。図5ではリスク値が6未満であればリスクを許容するとしている。つまりリスク値6未満について、組織としてそれ以上対策のパフォーマンスを求めないとしている。組織のリスク対応レベルの高まりとともにこの値を下げていく。

リスク値6以上についての対応は次の3つである。まずはここであげた管理策とは別に何らかのリスク改善計画を策定することである。次にリスクを回避（もしリスクが発生した場合に事業継続そのものが困難となることが想定できるのであればあえてその事業を行う必要がないと考える）すること、最後にリスクを移転（リスクが発生した場合にその責任の所在を他に移転する）することである。

3．リスクマネジメントシステムの運用・維持・改善

(1)　教育・訓練の重要性

教育・訓練の軽視が禁物なことはいうまでもない。どんな業務でもレベルを上げるのも下げるのも人次第である。「人がエラーをおこすこと」に対しては十分な準備と周到な計画をもってしても偶発的におきてしまうものであるが、日頃の教育によりエラーをおこす可能性や、おきた場合の対応に大きな差がでるものである。

教育は繰り返し実施する。定期的に、あるいは事故発生時やあらたな技術の導入時などには随時実施し、日常各自が行っている業務の重要性や役割、責任などを認識させる。リスク対策としての管理策の実施に対するやらされ感をなくす工夫が必要である。

教育・訓練を実施した後には、受講者、講師ともその教育・訓練についての評価をおこなう。受講者はよく理解できたか、内容は適切か、現場での実用性はどうか、講師から感じた受講者の反応はどうか、質問内容は今後の講義にとりいれるべきかなどを検討し、次の教育・訓練にフィードバックし、教育のレベルを向上させる。

(2)　システムのチェックと経営者の見直し

リスクマネジメントシステムが意図したとおりに運用されているか定期的にチェックすることが必要である。これを ISO9001 などでは内部監査とよんでいる。監査は運用の状態をチェックし、決められたとおりに実施されているかを確認する。時間とともに運用の方法が変化したり、環境変化に対応できていないなど、システムの改善の機会を見出す。

経営者によるシステムの見直しについては、システムの運用により維持される様々な情報（内部監査の結果と是正処置状況、インシデント・アクシデント報告やその再発防止対

応の効果、法規制の変更など）を総合的に判断する。とくに事件・事故があった場合にはその原因を追究し再発防止策の効果の確認が必要である。適切に対応され、効果も期待できるのであれば、組織全体で活用できるようこれを標準化する。環境が変化したり、意図したとおり運用されていなかったり、効果が上がっていない場合、経営者はマネジメントシステムの改善を指示したり、経営資源の投入を決定する。ここでいう「経営者」とは必ずしも組織の経営者である必要はない。リスクマネジメントシステムの運営責任者がシステムの見直しや、経営資源を投入できるよう権限を委譲し、現場に近いところでの迅速な対応がリスクマネジメントには有効である。

Ⅲ　リスクマネジメントシステムの実践事例

昨今、事件・事故が頻発し社会問題となっている代表的な分野として、医療分野と情報セキュリティ分野をとりあげ、「リスクマッピング」による実践事例を紹介する。

1．医療分野での実践事例

医療分野も情報セキュリティ分野同様に事件・事故について報道されることが多く、生命にかかわることもあり、社会的な関心の高い分野である。

医療機関においては、これまでの関心は安全性よりも、診療時間内に診察できる患者の数を増やすこと、患者の待ち時間を少なくすることという効率化に熱心にとりくまれてきた。しかし、医療の安全性に対する意識の高まりとともに、その考え方や対策の整備が必須となった。2002年度の医療制度改革において、医療安全体制の整備として、①安全対策のための指針が整備されていること、②安全管理のための医療事故等の院内報告制度が整備されていること、③安全管理のための委員会が開催されていること、④安全管理の体制確保のための職員研修が開催されていること、の４点が求められるようになり、リスクマネジメントシステムの導入がますます重要となった。

(1)　注射・点滴時のリスクマッピング事例

医療リスクにおいて、薬剤に関する事件・事故の発生がもっとも多く、常に危機意識を持つことが必要な分野である。薬剤を取り扱う分野で代表的な、注射・点滴業務についてリスクマッピングを作成した。

注射・点滴のリスク発生の主原因は、誤薬、患者の誤認、確認忘れなどのポカミスである。図６は、注射・点滴の流れのなかで想定されるリスクを洗い出すとともに、そのポイント・コツをあらわしたものである。各自が日頃実施しているポイント・コツは共有化し、組織として標準化すれば、それ自体十分なリスク対策に取り組むことになる。

図6

注射・点滴時のリスク

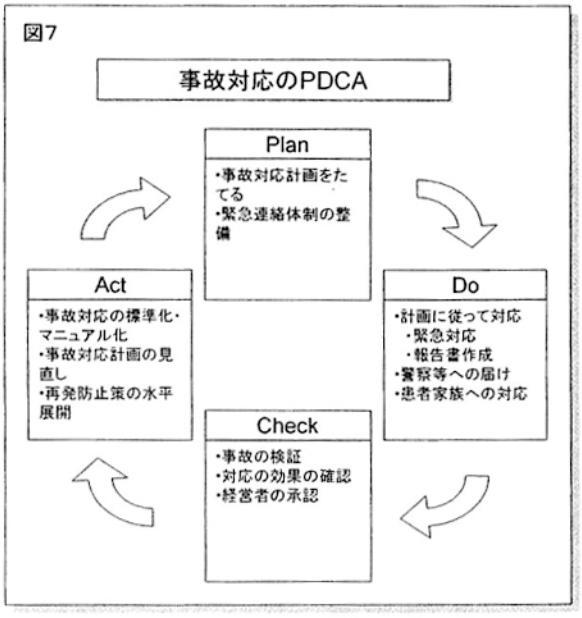
- 誤薬
- 患者の誤認
- ポカミス(確認忘れなど)

手順		ポイント・コツ	レベル	リスク
指示の確認	・指示票を確認する	・文書で受けとる ・薬剤の単位確認 ・時間に余裕を持つ	・氏名確認 ・V(バイアル)、U(単位)等見誤りやすいものに注意する	○薬剤のまちがい ・薬剤そのもののまちが ・薬剤の相互作用 ○処方量のまちがい
	・指示票にサインする			
	・疑義を確認する			
準備	・患者のトレイを準備する	・患者一人ひとりに専用トレイを用いる		○他の患者分との誤記入
	・薬剤をトレイにセットする	・患者一人ひとりに専用トレイを用いる		○薬剤のまちがい ・薬剤そのもののまち ・用量のまちがい ○薬剤の不良
	・薬剤を混合する			○薬剤のまちがい ・薬剤そのもののまちがい ・用量のまちがい ○薬剤の不良 ○処置のミス
	・指示票と照合する			
実施	・患者を確認する	・患者に氏名を言ってもらう		○患者の誤認
	・点滴・注射を実施する		・筋注、静注、皮下注を確認	○処置のミス
	・患者を観察する			
実施後の処理	・患者と指示票を再度見て、同一であると確かめる	患者の様子を確認		○薬剤のまちがい ○調合量のまちがい ○薬剤の不良 ○患者の誤認
	・指示票にサインする			○記入ミス

(2)　事故報告と再発防止

事故を防止し、事故発生を減少させるためにインシデント(ヒヤリハットしたこと)およびアクシデント(実際におこった事故)の実態を正確に把握することは、医療分野では特に重要である。しかし、報告書の様式は存在し、運用されていても、経営者に包み隠さず報告されていることは稀である。報告書を集めることが目的になっている場合もある。集まった報告を分析し、原因を追究(犯人を捜すのではなく)し、分析し、

図7



有効な対策を組織全体にわたって取り組み、再発防止に役立てなければならない。

事故対応についても PDCA サイクルを実践する。まず事故対策の計画（P）をたてる。事故が発生した場合の処置・手順や連絡、報告体制を整備し、この対応計画を従業者に教育し、周知徹底する。報告は犯人探しや個人責任を追及するものでなく、その後の組織にとって重要であることを認識させ、些細なことでも正確に、正直に報告することを求める。

事故が発生した場合（D）には計画にしたがって事故対応を実施する。事故の一次対応をおこない、報告書を作成する。事故対応についてはここで終わってしまうところを多く見かけるが、事故対応についてはむしろこのあとが重要で、その事故についての検証（C）や効果の確認、および経営者らが関与しその事故対応の仕組みが適切であるか、他部門にも展開する必要があるかどうかを検証（A）し、再発防止にとりくむことのである。そして効果的なものを組織全体で標準化していく。

2．情報セキュリティ分野での実践事例

IT の普及により誰もが一度に大量の情報が利用可能となるとともに、情報漏えいや改ざんなどのリスクも急速に増大した。個人情報の漏洩事件や、情報システムのトラブルが頻繁に報道されている。これまでは IT の活用に多くの関心が向いており、情報セキュリティについて軽視されてきた結果である。平成 17 年 4 月からは個人上保護法が施行されることもあり、情報セキュリティへの要求はますます高まるであろう。この分野でのリスクマネジメントは不可欠となった。

(1)　印刷業における個人情報に関するリスクアセスメント事例

印刷業では DM 制作などの業務で大量の個人情報を受託する。この情報が漏洩すれば、企業存続が危ぶまれるほどの損害が発生する。依頼者は安心して業務をまかせることができる印刷業者を選別しなければならない。印刷業での情報セキュリティの取組みは、「信頼でき、選ばれる印刷業者」として競争力を強化することにつながる。

図 8 は DM 業務における個人情報の保護に特化した「リスクマッピング」である。DM 業務では顧客から預った個人情報が状態（媒体）を変えながら管理されていく。従って、ここでは媒体ごと（MO やパソコン、サーバーなど）に異なるリスクを洗い出している。

図 9 は媒体ごとに洗い出された個人情報のリスクについてリスク値の評価を行った結果（リスクアセスメントシート）である。評価方法は前出の評価方法で評価した。顧客から預った個人情報のリスク管理レベルは最高ランク「4」とした。リスク対応策を策定し、実施後のリスク値の評価を実施したが、「悪意を持った社員によるリスク」、「外注先の不適切な管理によるリスク」のリスク値は期待したリスク許容レベル「6」以下になっていない。多発している個人情報漏洩事件の原因は、まさにここであり、さらに厳しい管理策が望まれることとなった。

図8

リスクマッピング

業務名 ： DM業務

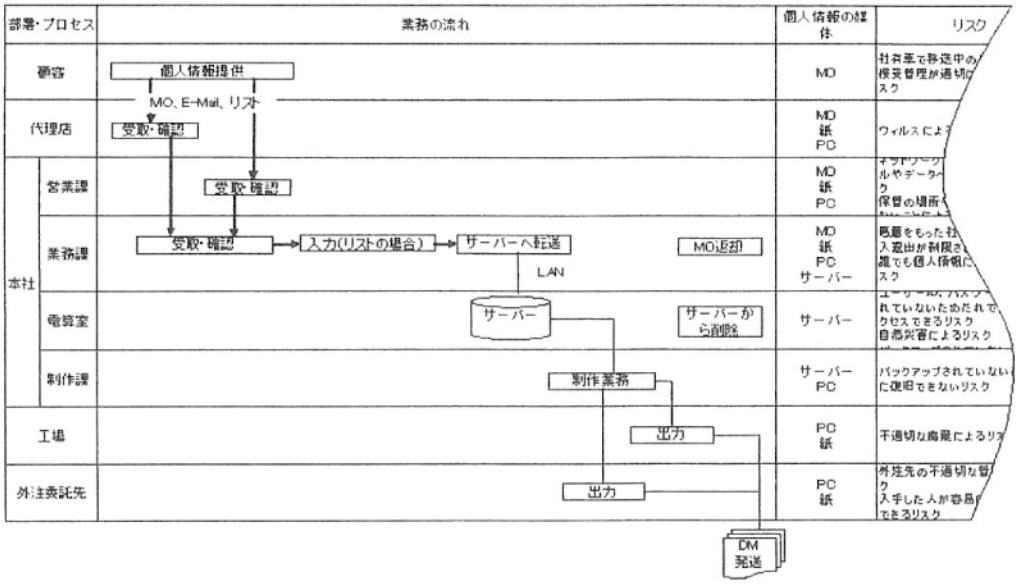


図9

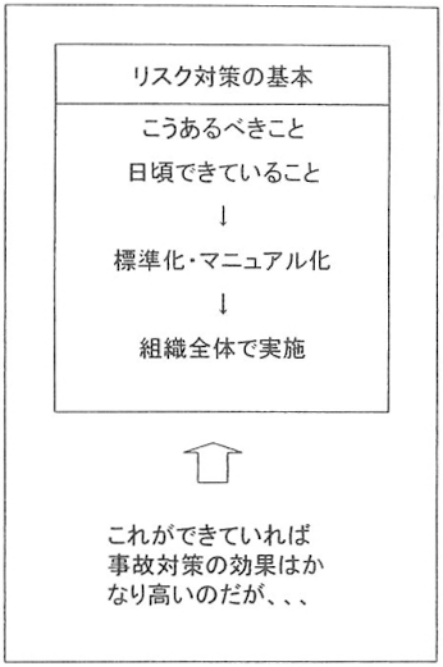
リスクアセスメントシート

業務名 DM業務

個人情報	媒体	移転評価	リスク発生プロセス	リスク	現状		対応策	管理策後	
					脆弱性	リスク値		脆弱性	リスク値
DM用個人情報	移動可能な電子媒体	4	収集	社有車で移送中のリスク	5	20	社有車に放置せず、社有車を離れるときは電子媒体を身につける	1	4
		4	収集	授受管理が適切にできていないリスク	4	16	授受簿や受取帳を運用する	1	4
		4	利用	悪意をもった社員によるリスク	5	20	セキュリティに関する誓約書を提出させる セキュリティ教育を定期的におこなう	2	8
		4	利用	入手した人が容易にデータを利用できるリスク	3	12	暗号化処理、ファイルにパスワードを設定する	1	4
		4	保管	入退出が制限されていないため、誰でも個人情報にアクセスできるリスク	5	20	セキュリティ区画を設定し、セキュリティエリアへの入室を制限する	1	4
		4	保管	保管の場所や方法が徹底されていないことによるリスク	3	12	媒体に応じた保管管理をおこなう カギのかかる保管庫に保管する	1	4
		4	保管	自然災害によるリスク	2	8	保管は耐火、防水対策の十分な場所にする	1	4
		4	保管	バックアップされていないため社屋に復旧できないリスク	3	12	定期的にバックアップをおこない、バックアップメディアは安全な場所に保管する 定期的に復旧の試験をおこなう	1	4
		4	保管	ウィルスによるリスク	5	20	電子媒体はウィルチェックをおこなったあとに参照処理をおこなう	1	4
		4	委託	外注先の不適切な管理によるリスク	5	20	外注先とセキュリティ確定書を締結する 定期的にセキュリティの取組みを監査する	2	8
		4	廃棄	不適切な廃棄によるリスク	4	16	廃棄する場合には媒体を破壊して再生できないようにする	1	4
	サーバー	4	利用	ユーザーID、パスワードが設定されていないためだれでも容易にアクセスできるリスク	3	12	ユーザーID、パスワードは個人に設定し、パスワードは3ヶ月に1回更新する	1	4
				ファイルやデータ	3	12	権限に基づいたファイル クセス制御を		

Ⅳ　まとめ

日常業務おいて、リスク対応を意識するかしないかにかかわらず、それぞれの従業者が日頃できていることを標準化し、適正化する。これを組織全体で実施する。新らたな従業者にも教育する。他部署の良いところをどんどん吸収する。これだけでミスはかなり防ぐことができる。



リスクマネジメントとは本来こういうもので、何か新しく特別なことをすることでもなく、思い切って新たに経営資源を投入することもなく、効果の高いリスク対策が実現するはずなのである。事例で紹介した医療分野での取り組みはこれにあたる。あたりまえのことではあるが、実践することはむずかしい。

しかし、昨今の環境変化に対応し続けるためにはこれだけで対応は十分なものとはならなくなった。世間のリスクに対する関心も以前とは比べものにならないくらい高まった。“何か起きてから対応しても遅い”ということもある。ここにリスクマネジメントシステムの必要性がある。

本論文では、リスク対応について、マネジメントシステム導入のメリット唱えた。リスクマネジメントには一貫した流れが必要である。リスクを重点化すること、ここではリスクの洗い出しと業務の標準化を狙った「リスクマッピング」の効用を強調した。PDCA サイクルをまわし、経営者の関与による継続的な改善活動の方法や、その実施による機能やレベルを向上させていくことがマネジメントシステムの特長である。この流れを適用した事例として医療分野と情報セキュリティ分野をとりあげた。今後は他分野への適用に取り組みながら、さらに効果の高いリスク管理手法へとつなげていきたい。

企業の社会的責任（CSR）が重視されている。組織における最大の社会的責任は、CSR で第一にとらえている法令順守はもちろんであるが、組織特有の使命（情報セキュリティ分野では情報システムが機密性・完全性・可用性を保つこと、医療の場合では患者の命を守ることや患者の健康に貢献すること）には、リスク対策にこそ目を向けるべきである。これを実現することがなにより社会的責任であり、それによって顧客重視の実現でき、従業者にも喜ばれる組織になれるのである。