リスクマネジメント実践のための着眼点

JNSA 組織で働く人間が引き起こす不正・事故対応WG
大日本印刷株式会社
野津　秀穂

1. はじめに

情報セキュリティマネジメントシステムや個人情報保護マネジメントシステムにおいて安全管理を実施するためには、リスク認識、分析及び対策により、リスクに応じた適切な措置を講じる必要があり、リスクアセスメント技法としてISO31010でも提起されている。実施のための要求事項を各種規格として文書化すると、その記述は、どうしても一般化・汎用化した記述になる。一方、対象とするビジネスは多様性に富む。規格とビジネス局面での解釈を結びつけるためテキストや雛形も公開されているものの、すべての業種の例を網羅することはできない。このような条件下で実務者は、規格を解釈しリスクマネジメントを進めていくことになるが、その結果、どこから着手するか悩み始め、初めの一歩で挫折したり、前例に頼り、対象ビジネス固有の真のリスクを見落としたり、効率的・効果的な対策にたどり着かず、過剰な方法を選択し、ムリを生じかねない。誤解の排除、もしくは、解釈の不足を補うために、別の視点を加えた考察が要求され、関連するマネジメントシステム技術を横断的に検討することにより、規格が何を意図しているかを知ることができる。

本稿では、筆者が所属する印刷産業を例にとり、一般財団法人日本印刷産業連合会「印刷産業のための個人情報保護の手引き」に掲載しているリスク分析の手法をベースに、マネジメントシステムと一般システム理論の考え方と照合し、リスクマネジメント実践のための着眼点を整理する。

2. リスクマネジメントー用語の整理ー

リスクマネジメント[1]は、「リスクについて、組織を指揮統制するための調整された活動」であり、「リスクマネジメントの枠組み」の中で「リスクマネジメントプロセス」で実施する。

2.1　リスクマネジメントの枠組み

リスクマネジメントの枠組みは組織全体にわたって、リスクマネジメントの設計（Plan）、実践（Do）、モニタリング（Check）、レビュー、継続的改善(Act)の基盤及び組織内の取り決めを提供する構成要素の集合体と定義され、PDCAサイクルを含んでいる。

2.2　リスクマネジメントプロセス

マネジメントプロセス（経営過程）は、経営管理論の始祖といわれるH.ファイヨール（経営過程学派）によって提唱された考え方である。

リスクマネジメントプロセスは、コミュニケーション、協議及び組織状況の確定の活動、並びにリスクアセセメント（リスクの特定、分析、評価）、リスク対応、モニタリング及びレビューの活動に対する、運用管理方針、手順及び実務の体系的な適用と定義される。

リスクアセスメントは、特定のリスクにどのように対応し、どのようにして対応の選択肢の中から選択することに関して、情報を得た上での意思決定を下すために、証拠に基づいた情報及び分析を提供することを目的としている。ここは、「意思決定とは代替案の選択である。」「経営は意思決定過程」といった、H.A. サイモンの意思決定論に基づいている。

2.3　マネジメントシステム[2]

マネジメントシステムは、方針、目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素と定義される。この定義は示唆に富むので、改めて整理しておきたい。「互に関連する又は相互に作用する」は、「システム」の定義である。「システム」はギリシャ語のシン（共に）とエステム（立てる）の複合語で「多要素の結合（関連）」を意味する。

ここでの「プロセス」は、「インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動」と定義される。「インプットのアウトプットへ変換」は、狭義のシステム定義であり、一つの作業工程を

●本稿の内容は、筆者の個人的見解であり、必ずしも筆者が所属する組織の見解ではない。

[1]「リスクマネジメントー用語　JIS Q 0073:2010(ISO Guide 73:2009)」日本工業標準調査会　審議

[2]「情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー用語　JIS Q27000：2014」日本工業標準調査会　審議

指し、複数の作業工程がインプットとアウトプットにより相互に関連する構造を表している。「目的を達成するため」とは、目的と実績の乖離を是正するPDCAサイクルを指す。

2.4　PDCAサイクル[3]

目標を設定してその実行計画（Plan）を立案し実行（Do）し、実行結果と計画（目標値）との乖離（誤差）を測定して評価（Check）する。計画（目標値）と実行結果に乖離（誤差）があった場合には、是正措置・対策（Act）を講じる一連のプロセスをＰＤＣＡサイクルという。

実行結果をチェックして次の改善活動に結びつける仕組みをフィードバック・システムと呼び、「マネジメント（管理）」の基本的な考え方である。

1950年代、品質管理の父といわれるW・エドワード・デミング博士が、生産プロセス（業務プロセス）の中で継続的に行うために改善プロセスが連続的なフィードバックループとなるように提案した。

ＰＤＣＡサイクルは、第二次世界大戦中にドイツのフォン・ブラウン博士が、ロンドン攻撃のために開発したＶ２ロケット兵器の技術として発明した自動姿勢制御機構（フィードバック制御＝ＰＤＣＡ）がＰＤＣＡの起源となる。図1.

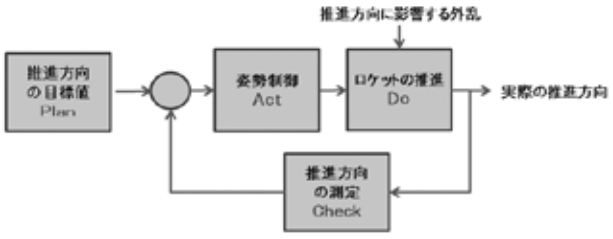

図1. Ｖ2ロケットの自動姿勢制御機構

1916年、H.ファイヨールは、著書「産業並びに一般の管理　都筑栄訳」の中で「管理とは、予測し、組織し、命令し、調整し、統制すること」と定義した。この「統制」が、後に「ＰＤＣＡ」と融合しマネジメントシステムとして確立した。図2.

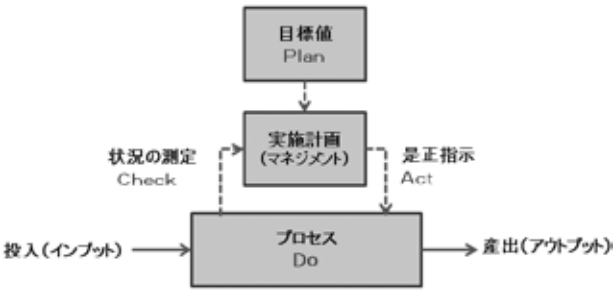

図2. ＰＤＣＡサイクルの経営学への応用[4]

ＰＤＣＡサイクルの考え方は、製造プロセス品質の向上や業務改善などに広く用いられており、情報セキュリティマネジメントシステム（ISO27001）や個人情報保護マネジメントシステム（JISQ15001）の基礎となるマネジメントの仕組みである。

この意味で、リスクマネジメントもマネジメントシステムの範疇と考えて良く、ＰＤＣＡサイクルの考え方を取り入れている。

3. リスクの特定に先立ち現状把握を行う

情報を適切に管理するためには、まず管理すべき対象となる情報資産を明確にするところから始める。

K.E.ボールディングは、一般システム理論[5]でシステムの複雑さに応じて階層（レベル）を整理したが、その中でシステムの第一レベルが、静的構造としての管理対象の全体像の把握である。これを枠組みのレベルと呼ぶ。「リスクマネジメントの枠組み」と同様に全体像を規定することを指し、具体的には、対象要素を一覧表にまとめたり、図に書いたりして検討範囲を限定することを目的としたアプローチである。

3.1　情報資産の棚卸

具体的な進め方としては、各部署で通常業務の基点から終点までを点検し、情報資産が「どこに」「どのような管理状態で」取り扱われているか、情報のライフサ

[3] JNSA　PRESS　VOL.41　職場の５Ｓで考える情報セキュリティ　野津秀穂 2016 年
[4] 企業活動のモデル「企業戦略論」 H.I. アンゾフ 著、広田寿亮 訳、産業能率大学出版部 1985 年
[5] “General System Theory: The Skelton of Science”, Management Science, Vol.2,No3. K.E Boulding 1956 年

イクルに沿って明確にする。ここでの注意点としては、通常業務の中の重要情報を優先して洗い出すことである。情報は日々生まれるため、洗い出し作業に没頭すると、いつまで経っても終わることなく、次のリスク分析やリスク対策のフェーズに進むことができなくなり、初めの一歩で挫折する典型的なパターンに陥る。

どのような情報をどのような単位で抽出すればよいか、例えば、「電子ファイルはファイル単位ごとに洗い出さなければならないのか」などの統一基準を予め定めてから調査を開始する。個人ごとに担当する業務を洗い出したら、各部署ごとに集約し重複した業務を整理し、一覧表にまとめる。

3.2　不要な情報資産の整理

「過去は利用していたが、現在では特に利用していない」（廃棄忘れ情報）や「原本が他の部門にあり複写を持っているだけ」（不適切な配布・コピー情報）、また「マスターとなるデータベースから業務の利便性向上のために個人的に加工し保管している情報」（不用意な再利用情報）などは、情報管理の方法や責任ならびに保管・廃棄のルールが不定な場合がある。このような情報については、情報漏えいのリスクを多く抱えていることから、「本当に当該情報は保有すべきなのか」を綿密に議論したうえで、適切な処置（廃棄・回収等）を講じる必要がある。

3.3　業務の全体像の把握（フロー図の作成）

管理対象の情報資産を洗い出したら、次に、個々の情報資産の関係を明確にする。

情報資産を取得してから、返却・廃棄するまでの流れ「情報のライフサイクル」をフロー図にして確認する。K.E.ボールディングの一般システム理論では、第二のレベルとして「予定通りに動く単純なシステム」いわゆる「時計仕掛けのレベル」としての「プロセス」を図式化する作業に相当する。「時計仕掛けの仕組み」とは、投入（インプット）が予め定めた手順によってプロセス（作業工程）から産出（アウトプット）される仕組みをいう。

情報のライフサイクルとは、特定した情報が社内に入ってから出て行くまで、「取得・作成」→「処理・加工」→「保管・バックアップ」→「移送・送信」→「返却」→「消去・廃棄」という、情報の取扱の流れを指す。続くリスク認識は、情報のライフサイクルの全ての局面ごとに検討する必要がある。

> フロー図（フロー・ダイアグラム）
> フロー図は、情報を取り扱う各局面（プロセス）に対して、情報がどこから来るか（インプット）と、どこへ行くか（アウトプット）を図式化する技法。情報のライフサイクルをフロー図にするためには、一つ一つのプロセスをインプットとアウトプットでつなげて全体像を記述する。
>
> **インプット** ⟶ **プロセス** ⟶ **アウトプット**
>
> ［参考］類似の手法に流れ図（フロー・チャート）がある。フロー・チャートは、プロセス内の処理内容の順序や判断分岐を記述することに特徴を持つ、主にプログラム構造を記述するために使う手法である。

この作業により、得意先と自社の各部門、委託先の間で、情報の流れを具体的に把握でき、業務の内容と責任範囲を明確にすることができる。

「情報のライフサイクル」によっては、委託や提供など情報が社外に渡る場合、倉庫やデータセンターなどロケーションが異なる場合や、委託先とのやりとりや支店間の輸送において外部に依頼する場合もある。

作業工程を経るごとに、管理責任部門が変わることがあるので、工程間の情報の授受については、特に責任を明確にすることが重要なポイントとなる。例えば、情報を移送する場合、前工程が送信（届ける）のか、後工程が受信（取りに行く）のかなど責任の所在を確認する必要がある。

印刷業におけるダイレクトメール発行業務を例としたフロー図を図3.に記す。

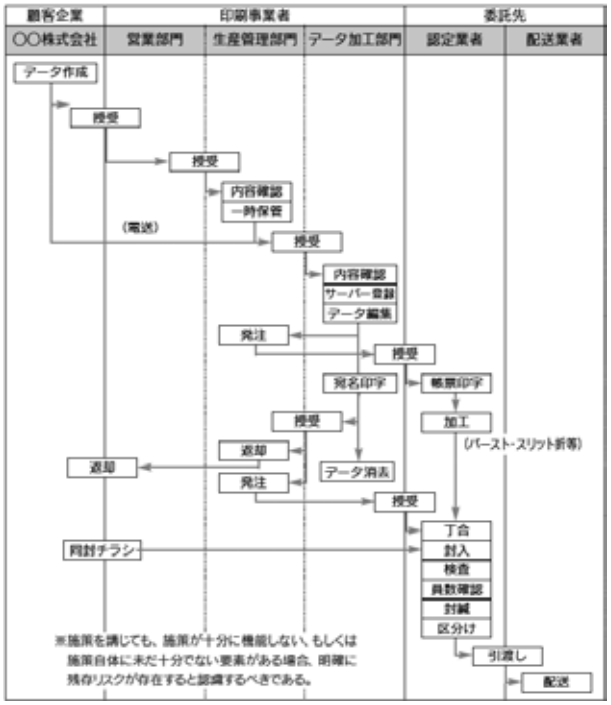

図3. [6]印刷業におけるダイレクトメール発行業務のフロー図

3.4　フロー図のモレのチェック

プロセスとプロセスを→でつなぐ。このとき、アウトプットとインプットで情報のデータ形態が一致しているか確認する。例えば、前のプロセスのアウトプットが「応募ハガキ」で次のプロセスのインプットが「宛名データ」となっている場合、「入力」プロセスの記述が欠落していることがわかる。

3.5　フロー図の先頭と最後

フロー図の先頭は、インプットの→から始まり「取得（授受）」のプロセスにつながる。分かり易くするために、先頭のインプットの前に「どこ／データ形態」を記述する。

フロー図の最後は、情報が無くなる「納品（移送）」、「返却」または「消去・廃棄」となる。例えば、インプット「応募ハガキ」をアウトプット「宛名データ」にする「入力」プロセスでは、入力したパソコンに残る情報（中間生成物）の「消去・廃棄」プロセスまでつなぐ。

4. リスク特定

情報資産を洗い出し、情報のライフサイクルのフロー図を作成したら、各局面（プロセス）においてのリスク因子（脅威と弱点）を発見し、認識し記述する。これを「リスク特定」という。

リスク特定の目的は、システム又は組織の目的の達成に、影響を与えるどのような事態が発生するか又はどのような状況が存在するおそれがあるかを特定することである。

「リスク」とは、目的に対する不確かさの影響であり、具体的には、本人への被害や事業活動の損失、好ましくない結果の可能性をいう。

フロー図の各局面（インプット、プロセス、アウプット）について影響を与える要素を書き出す。

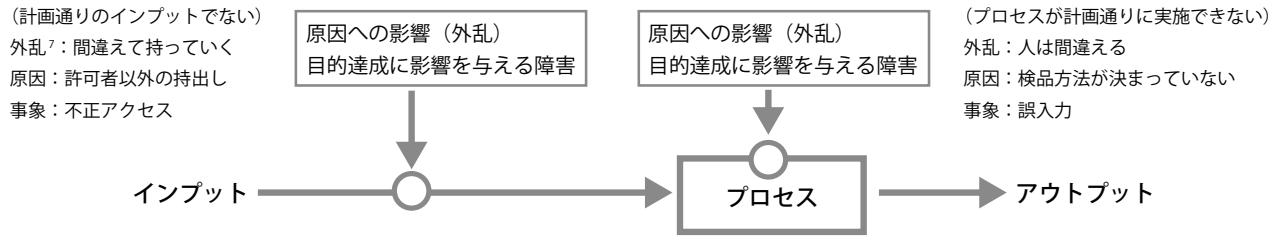

図4．リスク（好ましくない結果の可能性）：事象と原因、外乱の影響で、アウトプット品質が目標値と偏差がある

[6] 印刷産業のための個人情報保護の手引き　p59　一般社団法人　日本印刷産業連合会　2009 年
[7] 多乱（disturbance）とは、アウトプットを目標値からはずれさせようとするリスク源への影響

「目的」：組織のオペレーションを守ること[8]。PDCAのPlanを達成すること。
「不確かさ」：起こり得る事象、結果、起こりやすさに関する情報、理解若しくは知識が、たとえ部分的にでも欠落している状態。
「起こり得る事象（event）」：好ましくない結果を生む潜在的な原因。リスク事象（ペリル peril）はリスク源によって引き起こされる。
例）不正アクセス、盗難、流失、改ざん、紛失、毀損・滅失、破壊、誤用・誤操作、追跡不能
「リスク源」：リスク事象の起こり易さを生む要素。セキュリティ・ホール。危害要因（ハザードhazard）。
例）ドア、窓などの物理的保護の欠如、監査証跡（ログ管理）の欠如、アクセス管理の欠如など
「起こりやすさ」：何かが起こる可能性。一般的な用語を用いて示すか、又は数学的に示す。
例）発生確率。所定時間内の頻度

5. リスク分析・リスク評価

特定したリスクを可能な限り定量化する。

「リスク分析」：リスクの特質を理解し、リスクレベルを決定するプロセス。
「リスクレベル」：結果とその起こりやすさの組み合わせで表現されるリスクの大きさ。
「リスク評価」：リスク及び／又はそのおおきさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス。
「リスク基準」：リスクの重大性を評価するための目安となる条件。

5.1 被害の大きさ

リスクの高い個人情報の項目［被害の大きさ］の例として代表的なものは、特定の機微な個人情報とクレジットカード情報がある。（明示的な本人の同意がある場合、法令に基づく場合などを除き）特定の機微な個人情報の取得利用又は提供を行ってはならない。クレジットカード情報（カード番号、有効期限等）の漏えいは不正使用によるなりすまし購入などの二次被害が発生につながる。

表1.（相対的な）被害の大きさの例

分類(例)	(相対的な)被害の大きさ
クレジットカード情報、特定の機微な個人情報	高
一般生活者の個人情報	中
ビジネス・コンタクト情報	低

表1. は相対的な「被害の大きさ」のランクであり、「一般生活者の個人情報」の漏えいより「特定の機微な個人情報」や「クレジットカード情報」の漏えいの方が、「被害は大きい」とういう比較となる。

「特定の機微な個人情報」や「クレジットカード情報」等を扱っている特定の部門以外では、「一般生活者の個人情報」が「高」になる。

5.2 起こりやさ

［被害の発生の可能性（発生確率）］でいう確率は、一般的な「客観確率」では測ることがでない。

「客観確率」は、繰り返し試行（過去の実績）によって発生する頻度として確率を求める。この方法で考えると、例えば「個人情報の保管キャビネットを施錠していない」という「弱点（リスク発生源）」に対して、「盗難」の発生という「脅威（リスク事象）」が、過去に発生したことがないので発生確率は0、即ちリスクは“ない”となるが、これは誤りである。

リスク分析では、過去に発生していない事象について「発生の可能性」を考える。例えば前例の「個人情報の保管キャビネットを施錠していない」は、“常に”「盗難」の可能性があるので発生確率は「高」と考える。この手法を「主観確率」という。

[8]JNSA PRESS VOL.33 セキュリティ実現の原点から見た内部不正要因事故抑制手法 甘利康文、新井真司、内田順一 2012 年

表2. 被害発生の可能性（発生確率）の例

分類(例)	被害発生の可能性(発生確率)
常態化している(いつでも起きる可能性がある)	高
ミス（たまに起きる可能性がある）	中
不正事件(意図的に起こす可能性がある)	低

5.3　リスク評価

リスクは、［被害の大きさ］と［被害の発生の可能性（発生確率）］の組み合わせで評価される。

このように［被害の大きさ］と［発生の可能性］二つを考慮したリスクのランク付けを行い、放置することによる事業活動への影響や、現実化したリスクへの対応（必要の有無／優先順位）を決定する。

「ビジネス・コンタクト情報」であっても、直接ビジネスがある得意先担当者の名刺情報（自社案件）と、得意先が保有すると得意先の取引情報（受託案件）とでは、「漏えい」した場合などの「被害の大きさ」には差がある。謝罪の他、事実の公表、所轄官庁への届け出が必要となる場合がある。

表3.（相対的な）リスク評価の例

（相対的な）被害の大きさ	被害発生の可能性（発生確率）	リスク評価（ランク）
高 クレジットカード情報 特定の機微な個人情報	高（いつでも起きる可能性）	高
	中（たまに起きる可能性）	高中
	低（意図的に起こす可能性）	高低
中 一般生活者の個人情報	高（いつでも起きる可能性）	高中
	中（たまに起きる可能性）	中
	低（意図的に起こす可能性）	中低
低 ビジネス・コンタクト情報	高（いつでも起きる可能性）	高低
	中（たまに起きる可能性）	中低
	低（意図的に起こす可能性）	高低

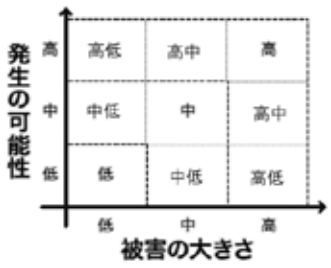

図5. リスクマトリックス

［被害の大きさ］と［発生の可能性］の組み合わせを図5. のようにリスクマトリックスで表す。

実際に発生すると、どれひとつでも、重大な被害に至る可能性を残しているが、だからといって、「高」の判定が多いと、優先して対策すべき対象が判断できない。ここでは、リスクの順位付けを行い、リスク対策の優先順位を検討するためのインプット情報となるよう意識してランク付けをする。

ハインリッヒの法則[9]では、被害の大きさが「低」の軽微なミスや「ヒヤリ・ハット」でも、発生の可能性が大きい異常は、重大な事故の前触れであり、優先対策課題と教えている。このように、実際のリスク評価では、よりきめ細かい考察が必要となる。

6. リスク対策

リスク分析により“対策を施すべき”とした「リスク」について、組織的、人的、物理的、技術的な観点から費用、構築の容易さ、運用の容易さ、効果等の観点から実効性のある対策が必要となる。

K.E.ボールディングの一般システム理論では、第三のレベルとして「サーモスタット」を代表例とする「制御機構またはサイバネティクス・システム」を掲げており、リスク対策の設計に有効な考え方である。

炬燵のサーモスタットのフロー図を図6.に例示す。

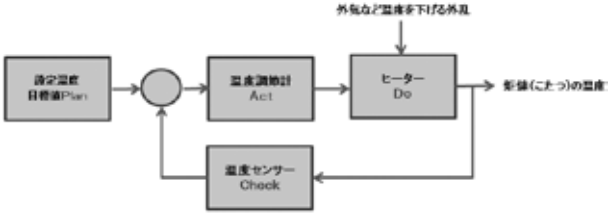

図6. サーモスタットのフロー図

サーモスタットは、測定した温度が、設定温度に等しくなると、ヒーターはOFFになり、そこから温度低下が始まる。温度が低下すると再びヒーターがONになり、設定温度を維持するよう動作する。設定温度（Plan）に

[9] ハインリッヒ研究会編訳「ハインリッヒの事故防止」1956 年

対しヒーターをON（Do）し、測定温度と設定温度（目標値）との乖離（誤差）を測定して評価（Check）し、設定温度（目標値）と測定温度に乖離（誤差）があった場合には、是正措置・対策（Act）を講じるフィードバック制御を行っており、これはＰＤＣＡサイクルである。ここで一般システム理論とマネジメントの仕組みが一致していることを確認できる。原初的なＰＤＣＡは、結果を見てからの後追いの対策になり、目標値と結果に差異が生じないと是正指示（改善）が生まれない。そこで、目標を達成した際には、更に高い目標を設定して、改善活動を推進する。これが「ＰＤＣＡサイクルをスパイラル的に継続する」意義となる。

＊より高度なPDCAでは、後追いの対策だけではない。
印刷機の制御部などで導入されているPDCA（制御機構）では、
⑴ 目標値と実際の差を是正する機構（比例制御）
⑵ 過去の実績を反映する機構（積分制御）
⑶ 先を予測する機構（微分制御）
の組み合わせで定常的な目標達成を行っている。

リスク低減のためのアプローチとして、［被害の大きさ］を低減させる、または、「被害の発生の可能性（発生確率）］を低減させることを検討する。

6.1　［被害の大きさ］の低減

被害が発生しても、被害が拡大しない対策を「ダメージ・コントロール」と言い、改善活動の一種である。
「人は間違える」と言う発生の可能性を確実に低減することは、できない。間違えても被害を及ぼさない対策としては、例えば

① 誤入力が発生しても、二重入力により間違いを発見して次工程に正しいデータを送る。
② 紛失が発生しても、データを暗号化することにより、拾得者が不正にデータを使えない。

6.2　［被害の発生の可能性（発生確率）］の低減

リスク発生原因を除去することにより、発生させない（または発生しにくくする）方法を検討する。

リスク発生原因の影響を受けない対策としては、例えば

① 保管キャビネットを常時施錠し、鍵管理することにより不正持ち出しを排除する。
② 入退出セキュリティ設備を導入し、不正侵入者による盗難を防止する。

フロー図では、「弱点への影響（外乱）」を除去する「フィルター（雑音除去装置）」を挿入する。

リスク発生原因を除去する対策を「リスク回避」といい、構造改革の一種である。

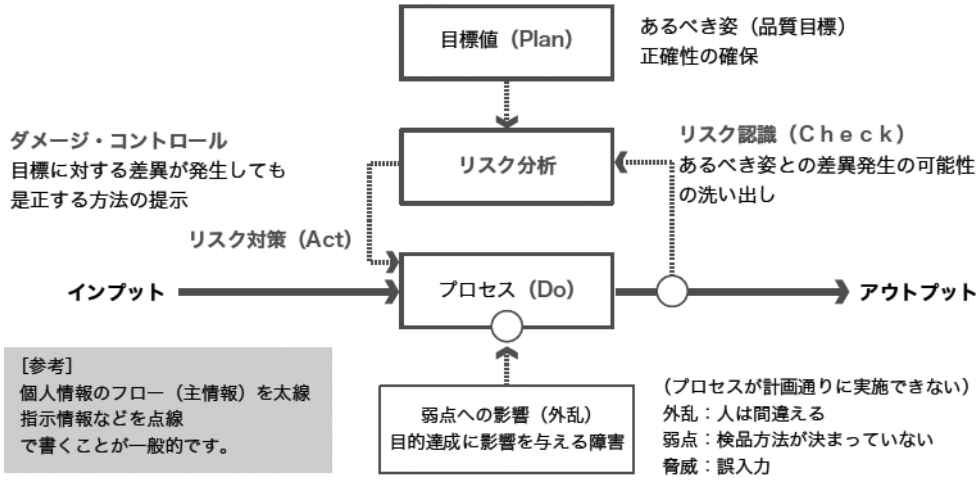

図7.［被害の大きさ］の低減対策を加えたフロー図

6.3「被害」の補てん

被害が発生した場合、経済的な被害について補てんするために、「個人情報漏えい保険」に加入することにより、個人への補償を用意している会社の姿勢（取り組み）も“見える化”できる。この対策を「リスク・ファイナンス」といい「リスク移転」の一種である。リスクは移転しても、なくならない。ビジネス全体から顧客視点（生活者視点）に立ち、真のソリューション（解決策）検討が必要となる。

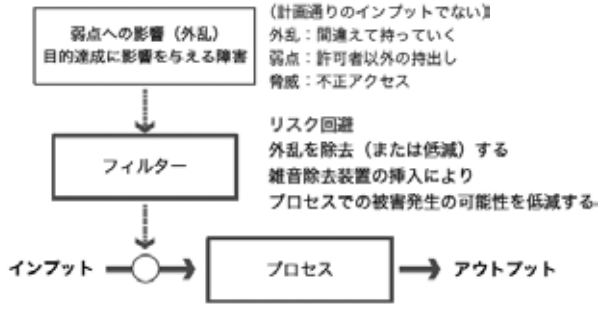

図8.［被害の発生の可能性］の低減対策を加えたフロー図

6.4　残存リスクの認識

現状で可能な限りの対策を講じた上で、未対応部分については残存リスクとして把握し、管理する必要がある。これを「リスク受容」という。

6.5「緊急連絡網」の整備

想定外事象への対応として「緊急連絡網」を整備すしたり、危機管理計画を策定する。この対策を「クライシス・マネジメント」という。

7. セキュリティ・バイ・デザイン

とりあえず実施（Do）して、点検（Check）の結果、目標との間に差異があったら見直し（Act）するという、後追いの活動では、毎日が事故だらけで、不良品検品に終始することになってしまう。

実施に先立ち、セキュリティ対策を組み込んだ計画を検討しルール化しておくことが必須となる。この取組をセキュリティ・バイ・デザインという。

実施計画立案にあたり、目標値どおりに行かない場合を事前に想定する（リスク認識）。このリスクがプロセスに及ぼす影響を想定し（リスク分析）、この結果、対策を定めてルール化（リスク対策）する。これは、事前想定でＰＤＣＡを回すことを意味し、フィードフォワード制御の考え方の導入が求められる。

実作業開始後には、事前計画（リスク対策）通りに進行しているか？について、実際の状況を点検し、もし目標値との間に差があれば、是正するフィードバック制御（ＰＤＣＡ）と事前計画のフィードフォワード制御は、両方を組み合わせて使うことが重要である。図9

8. リスクの定期的見直し

リスクは環境の変化（受注量や生産量の拡大等も含む）や技術の進展等により常に変動する。従って定期的な見直しは必須であり、必要に応じて随時見直しを行うこともルール化する。ある部門で顕在化したリスクやヒヤリ・ハットが他の部門でもあてはまる場合がある。そのような時は、顕在化した部門内での見直しに止まるのではなく、情報を共有化する。定期的な見直しでは、目標値設定のレベルアップにも取り組む。

9. おわりに

本稿では、リスクマネジメントについて、マネジメントシステムの考え方とK.E.ボールディングの一般システム理論の考え方と照合し、共通する考え方を体系的に整理した。リスクマネジメントが何を意図しているかを理解し、実践する上での一助になれば幸いである。

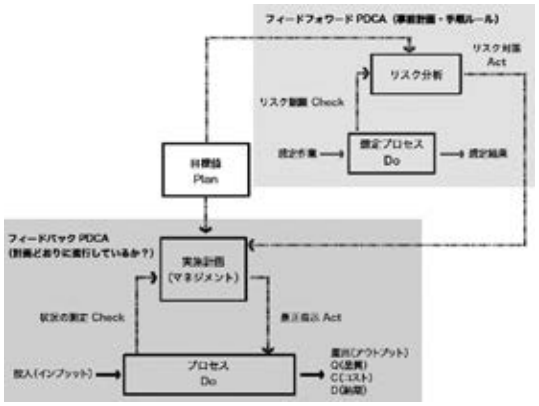

図9. 事前想定のPDCAを加味したフロー図