テロリズムリスクの予測と評価

大内　正俊，大山　達雄

テロリズムに関する研究動向をテロリズムリスクの予測と評価という観点から概観する．テロリズム研究のアプローチは内的モデルと外的モデルの二つに分けることができ，特に後者はテロリズムリスクの予測と評価に有用である．テロリズムリスクの早期警戒指標としてSprinzak指標に基づくテロ可能性指数を改良形とともに紹介する．さらに情報革命の進行とともに形成されてきたネットワーク型組織によってもたらされる，いわゆるネットウォーリスクについて述べる．テロリズムリスクを評価するモデルの例として，Kollerによるモデル分析例をモデルの構築，適用，結果とともに紹介する．

キーワード：テロリズムリスク，予測，評価，Sprinzak指標，テロ可能性指数，ネットワーク型組織，Kollerモデル

1．はじめに

1995年に起こったわが国の地下鉄サリン事件，あるいは2001年9月11日のニューヨーク・ワシントン同時テロ事件，翌年10月のインドネシアバリ島レストラン爆破事件といったような，いわゆる“テロリズム”に基づく事件がわれわれの社会，日常生活にかなりの衝撃を与えたことは記憶に新しい．テロリズムとは何かを考えるために，テロリズムの定義を与える試みは以前からなされており，犠牲形態に重きをおくもの，犠牲と目標との相異に重きをおくもの，暴力行為を重視するもの，異常性を重視するものなど，これまでにも100個以上の異なる定義が与えられている(Weimann-Winn[1]など参照)．テロリズムに対する厳密な定義を与えることは本稿の目的ではないので，ここでは，「テロリズムとは一般社会に影響を及ぼし，衝撃を与えることを意図して，特定のグループ，秘密の集団によって事前に計画された政治的意図を持って一般市民に対して向けられる暴力的行為である(United States Code[2]，Post *et al.*[3，4]参照)」，という程度に定義しておくことにする．

テロリズム（以下，テロとも記す）研究の歴史を振り返ってみると，テロの根本的原因，動機，歴史的パターンを分析する，いわば内的モデル志向のアプローチと，国が直面する多くのリスクのなかの一つのリスクであるというように，トップダウンの立場から検討する外的モデル志向のアプローチがある（Falkenrath[5]）．内的モデルはアカデミックな研究者に多く好まれ，特定の問題の構成要素に焦点を当てる分析的手法に基づく．テロについては現代テロと呼ばれる国際テロの起きた1968年以来，多くの文献が見られる．当初は政治的暴力の一般理論を応用する理論派の動きがあったが，形式的で柔軟性に欠け，焦点の絞り込みができなかったため，1970年代中頃には放棄されたようである．その後，やや説明的な社会学的，コミュニケーション論的，心理学的，また武力外交論的な解釈を重んじる解釈派が多く現れた．例として，心理学的な解釈派は，テロを政治的手段としてではなく，内的に精神病理学的に動かされてそれ自体が目的であると解釈する．武力外交論的な解釈派は，テロを武力志向の道具主義，つまり「戦略的選択理論」に基づくと解釈する．しかしいずれの考え方もテロの一部分を捉えているに過ぎない．内的モデルは，いわば学問的研究の立場であり，過去に実際に起きた事件を基に実証的に進めるという運命を持つものであるが，多くは専門に走り，政治，経済，社会から規定される構造的（外的）因子とグループダイナミックス的，心理的（内的）因子の両方を包括するモデルを作る試みはほとんど行われなかった．

一方で，外的モデルは歴史が浅く，1990年代より米国で大量破壊兵器によるテロの対策の必要性が高まる中で，他の政策との予算配分の関係で優先順位をつける必要性から生まれたもので，テロ政策立案者や国

おおうち　まさとし
東芝ITソリューション㈱
〒210-0006 川崎市川崎区砂子1-2-4
おおやま　たつお
政策研究大学院大学
〒162-8677 新宿区若松町2-2

家安全保障の実務家にとって考えやすいモデルである．テロ対策を，テロ以外のリスクと比較し，リスクによる損失，リスクの発生頻度等に基づくリスク管理の一つとして扱い，テロ行動に対する政策立案を考察するのが外的モデルアプローチである．

本稿の目的は，このようなテロリズム研究の現況をテロリズムリスクの予測と評価という観点から概観し，OR研究者，実務家から見たテロ研究のモデル分析的側面を紹介し，テロリズムリスクのネットワーク構造特性を考察することである．

2. テロリズムリスクの予測と評価

地下鉄サリン事件，あるいはニューヨーク・ワシントン同時テロ事件などに対しては，テロ行動の徴候，危険性に対する警告，注意が不十分であったというよりもむしろ，政治的，民族的，宗教的な特定集団がテロリズムリスクを有している状況に注意を払う総合的，分析的フレームワークを作っておく必要があったということがいわれている（Post *et al.*[3, 4]など参照）．すなわち，テロリズムリスクが増大し，例えば暴力テロといった形に顕在化する過程を総合的に分析するフレームワークを構築する必要があるというわけである．このような必要性に答えるための一つのアプローチとして，テロリズムリスクの予測と評価のためにテロを起こす主要要因は何か，それをどのように整理，評価すればよいかということが分析課題となっている．

Post *et al.*[3, 4]らによるテロリズムに影響を及ぼす要因分析の基礎となったのは，Sprinzak[6]によるテロ集団化の早期警戒指標である．Sprinzak指標は特定のテロ組織がテロを実行するか否かを判定するものではなく，ある組織がテロ組織へと変貌するおそれがあるか否かを判定する指標である．したがって，Sprinzak指標は特定の過激なグループがテロに走る可能性を評価する方法の開発に，その一歩を踏み出したものであるといえる．換言すると，Sprinzak指標は内的モデルの立場から，以下のような課題

(i) テロ発生と相関する政治的，経済的，社会的背景
(ii) 過激化を助長するグループダイナミックス
(iii) グループメンバーの心理

を包括的，系統的に評価し，テロ化の予測に特化した公式的なリスク評価手法にまとめたものである．具体的には，以下に示すような早期警戒指標の評価項目を掲げている．

- 社会構造上，暴力を容認する程度
- グループメンバーが暴力の歴史を持つ程度
- 暴力で立ち向かうことのリスクと機会を合理的に評価する程度
- テロ運動を支える組織的，財政的，並びに政治的リソースを持つ程度
- 相手からの脅威を差し迫ったものと感じる程度
- 他グループとの闘争の程度
- 青年層の活動家の占める割合
- グループに向けられる支援の種類と水準
- 屈辱を受けている程度と復讐の必要性を感じる程度
- 指導者が暴力の歴史を持つ程度

これらの各指標評価項目に評価点数を付けて重み付けし，集計してテロ可能性指数（TPI: Terrorism Potential Index），つまりテロ集団化の早期警戒指標を得るものである．Sprinzakの早期警戒指標に対しては，指標項目数が不十分で，指標間の関係が明瞭でなく，数値化は行ってはいるものの，本質は定性評価であるとの批判があった．

Postらは修正デルファイ法を用いてSprinzakの指標を大幅に改良することを試みた．Post *et al.*[3]では，テロリズムリスクに影響を与える四つの主要な要因として，

(1) 歴史的，文化的な環境特性
(2) 影響力のある重要人物と支持者
(3) グループ・組織
(4) 現在の状況

を掲げ，表1に示すように，それぞれに対する具体的な影響要因を表す変数として，合計32個を提示している．

Postらは具体的に五つのタイプのグループ，国家主義的分離主義者，社会的革命論者，宗教的原理主義者，非伝統的新興宗教家，右翼過激論者の各グループに対して修正デルファイ法を実施し，6人の専門家に約150の質問を5回繰り返した．その結果によると，例えば歴史的，文化的な環境特性は新興宗教家グループ以外のすべてのグループにとって重要な要因であって，それらに関しては公開情報や専門家情報が有効であること，またグループの組織，構成に関する情報はすべてのグループにとって重要であること，あるいは新興宗教家グループのみがそれ以外のグループと常にかなり異なる形態を示していることなどが判明した．今後は，それぞれのタイプへのリスク評価に最も関係

表1　主要要因と影響要因を表す変数

主要要因	影響要因を表す変数
歴史的、文化的な環境特性	暴力文化の歴史、社会紛争、政治的経済的社会的不安定性
影響力のある重要人物と支持者	組織体制、反対勢力、構成員と支持者、グループ内競争
グループ・組織	イデオロギーと目標、グループの暴力体験、リーダーの自己陶酔的性格、偏執病的性格、反社会的性格、悪性自己陶酔性、カリスマ性、独裁的全体主義的リーダーシップと意思決定、集団的信念のリスク、党派性と少数グループ、開放性と閉鎖性、新規メンバー調達、社会性、訓練、任務分担と昇進、持久性、集団思考と分極化、屈辱と報復、恐怖性、敵対性、支持形態、テロの利得性、闘争組織、目標グループへの行動、暴力とテロへの最終準備
現在の状況	テロ開始への契機

するカテゴリや変数を見分け，今後の改良に結びつける計画であるとのことである．

3．ネットワーク型組織と階層型組織

情報革命の進行とともに組織のネットワーク化が進み，小規模で以前は地理的に分離されていたグループが相互に意思疎通を図り，連合し，協同歩調を取ることが可能となった．このことによって，紛争はこれまでとは異なる新たな様相を呈することになったといえる．すなわち，グループの指導者がネットワーク型組織の形態，教義，戦略，技術を活用することによって政府等の既存組織あるいは他の組織に影響を及ぼすという，いわゆるネットウォー（netwar）を引き起こす原因となったといわれている（Ronfeldt[7]，Arquilia-Ronfeldt[8]，Whine[9]など参照）．ネットワーク型組織が広範囲に及び，さらに数多くの組織がネットワーク化され，権力がそのような組織内にいる非政府の指導者に移行するようになると，紛争はネットワーク型組織によって行われ，そのようなネットワーク型組織に習熟したものが戦いの中では有利になる．一方，政府の組織構造は従来の階層型のままである．紛争はますます情報通信に依存し，紛争はいわゆるソフトパワー（soft power）をめぐる知識と情報に関する争いになる．このようにして紛争はメディア志向になり，情報操作と認識管理によって実施されることになる．一般に階層型組織がネットワーク型組織を苦手とすることは，多くの国が麻薬密輸の国際犯罪組織に手を焼いていることなどからも分かる．ネットワーク型組織に対しては，ネットワーク型組織で戦うべきであろう．ネットウォーに臨む政府側も組織，戦略を革新し，政府機関間，国際間の協調を構築しなければならない．先にネットワーク型組織の形態に習熟した方が有利になるといわれている．犯罪者にせよテロリストにせよ平和的な社会活動家にせよ，ネットワーク化に長じた者が国の機関よりも力を得ていることはハマス（Hamas）の歴史を見ても分かる．結論として，政府機関間の連絡を密にするなどネットワーク型組織と階層型組織のそれぞれの利点をうまく混合した上で，この新しい脅威に立ち向かうべきである．ネットウォーは情報革命の結果としてもたらされた概念であり，その形跡は組織のネットワークの形態が現れた当初から具現化し，また情報戦略と情報操作の中にも見られ，テロリスト，ゲリラから社会活動家まですべての階層が含まれる．組織のネットワーク形態や教義，戦略を横断的に見て，そのメタパターンに注意を払うことがテロリズムの研究者には要求される．社会的ネットウォーはセグメント化され，多中心的である．そして，イデオロギー的に統合されたネットワークとして活動する形態は軍事活動型と問題解決型の2種類が存在するといってよいであろう．

情報通信技術（ICT）の進歩によって，過激派やテロリストたちの活動の舞台はますます広がりつつある．極度に活動的な集団がイスラム教団（Islamists）と極右団体（the Far Right）であり，ますますネットワーク化が進められている．彼らはこのような技術から，相互意思疎通，匿名性，廉価，力の増進，新たな

聴衆など，新たな利便を享受している．イスラム教団や聖戦運動家たち（Jihadists）はインターネットを活用して新人を獲得し，宗教的指令を全世界のイスラム教徒に発信している．合衆国民兵軍（the US Militias）はインターネットのお陰で密やかに勢力を伸ばし，米国，ヨーロッパなどの白人至高主義者やネオナチらはインターネットを最後に残された干渉されない通信メディアと見なし，最大限に使いこなしている．それを使うのは一般には通信のためであるが，彼らはそれを特に指令と管理に用いるべく努力しているようである（Whine[9]参照）．1990年代に入ると，国家を背景とするテロ（terrorism）は終わり，新しいタイプのテロが出現し，テロの範囲が広がることになった．新しいテロはほとんどの場合宗教的熱狂さを伴い，民族間にわたり，極端な暴力的行為を容認する．新テロは軍隊や国家をターゲットとする場合もあるが，犠牲者はたいてい罪のない市民である．このような新テロの勃興と新ICTの発展とは軌を一にしているといえる．将来の戦争は国家間でなく，国家・団体間で起きるといわれている．テロが多国籍化するにつれてネットワーク化された組織形態は拡大し，テロはもはや国家組織にはよらなくなり，相互に半ば独立国家的になり，同盟者を確保し，他を動かし，また指令と管理を有効にすることになる．ネットワーク組織的なハマスが階層組織的なPLO（パレスチナ解放機構）に取って代わりつつあるのは良い例である．将来にわたって重要インフラへのサイバーテロは不安材料ではあるが，現在のところでは，彼らはICTを通して宣伝を行い，通信，情報収集，それに資金管理を活用するに止まっている．

4. テロリズムリスクモデル例

テロリズムリスクの予測と評価に各種のテロリズムリスクモデルを用いる方法もかなり行われている．例えば，企業が外国に投資をして進出する場合，あるいはまた政府が他国との外交を考える場合にも，対象国におけるテロリズムリスクについて何らかの予測あるいは評価が必要とされる．本節では，Kollerによるテロリズムリスクモデル（Koller[10]）を例としてモデル分析の概要を紹介する．

今日の企業および政治はグローバルな環境下にあり，ビジネスをするには工業的にも経済社会的にもいろいろな発展形態にある国と一緒になり，またそれぞれの国の中で行わなくてはならなくなっている．その際，世界の各地域でのテロ活動の程度に注意を払い，知っておくことが必要である．テロリズムなどの関心事については相対的手法および絶対的手法により計量化，定量化が可能である．いかなる国においてもテロリズムの危険性のない国は存在しないことから，テロリズムについてのリスクを評価することが必要とされる．テロリズムリスクの相対リスクモデルが適用され，最終的にいくつかの適切な対策が確定されると，テロリズムの深刻な影響を緩和させることが可能となる．それらの対策にはいずれも費用がかかる．これらの費用を計算するリスクモデルが作成される．絶対コストを積み上げたリスクモデルを絶対リスクモデルという．絶対リスクモデル向け入力データの作成は困難なので，実際には真剣に考慮する国々に対してのみ行うことになろう．

仮想的な例として，ある国のテロリストを評価するために企業が実施するシナリオ作成について考えてみよう．ここで用いられるアプローチ，あるいはここで構築されるモデルは国の政府機関にとっても適用可能なものである．企業が海外へ投資することによって進出を考えるとき，どのようなリスクを考慮すべきか，どのような国々あるいは地域を避けるべきか，テロ活動からの脅威が一番低いのはどの国々か，どのようなタイプのテロ活動への対抗策をとるべきかといった問題である．大国に進出する場合を除き，大抵の場合は市場，政治，経済等を考慮して，一定地域の複数の国々に投資するものである．もしもそれらの国々の政府が不安定であったり，非友好的宗教団体が活動したりなどネガティブな事柄があるとすれば，そのような地域を明確にし，それらの地域への投資は避けるべきであろう．またビジネスは確かに地域ベースで考えられるべきであるが，各国は個別に評価されるべきである．そうすることによって地域全体を不適合としてしまう過ちを避けることができ，緊迫していない国々の中でビジネスの可能なところを明確にできる．本節で紹介するリスクモデル例は，このような問題に対処することのできるものである．

(1) カテゴリと寄与因子

Kollerによるテロリズムリスクモデルでは，企業のリスク評価担当チームが採用した前提として，テロ活動に対する企業の関心は組織，資金，経験と技術力という三つのカテゴリによって表現できるということが示されている．したがって，それぞれのカテゴリに対して，大きな影響を及ぼすとみなされる寄与因子

(contributing-factor) を提示し，それらの因果関係を明らかにするための寄与因子図をもとにどのようなモデルを作成するかを決める必要がある．モデルを決定するに際しては，決定ツリー (decision-tree) モデル，線形計画 (LP, linear programming) モデル，あるいはモンテカルロ (Monte Carlo) モデルなどが考えられる．決定論的ツリーあるいは確率論的ツリーの場合には，モデルの中の変数間の関連付けを行うのに必要な柔軟性がなく，決定論的ツリーの場合には，現在リスク評価担当チームの手元にあるソフトウエアを使用すると，解が単一の期待値のみであるので，企業の経営陣にとって一連の意思決定ができるような区間情報と関連確率とが得られず，本課題には適切ではないとされた．またLPモデルは，変数間の関連付けについては柔軟性があるが，決定論的結果しかもたらさない．さらには，グループでは依存関係，失敗確率，リスクで重み付けした価値などが分析を行う上での重要な要素であるとしたが，これらをLPモデルに組み込むことが困難となったことによって，結局，モンテカルロモデルがメンバー達の合意点となった．モンテカルロモデルを用いると，確率概念の導入や変数のとりうる範囲の設定，変数間の相互依存関係や失敗の確率の設定も可能となるので，諸戦略の比較分析に必要とされるリスクの重み付けが自動的にできるようになった．

(2) 相対リスクモデル

第1のカテゴリである“組織”には，任意の国のテロリストグループがどの程度組織化されているか，その組織の規模はどれくらいか，当該政府から提供されている兵站的支援はどうかなどに関する評価を表す変数が含まれている．第2のカテゴリである“資金”には，資金源がどの程度多様性をもっているか，資金力の水準はどれくらいかといった変数が含まれている．第3のカテゴリである“経験と技術力”には，組織メンバーの経験レベル，テロ活動の実行力の有効性，それに技術力水準を評価する変数が含まれている．寄与因子図 (contributing-factor diagram) を作成する担当グループは相対尺度を1から10の尺度で表現することを決定した．

第1のカテゴリである“組織”を構成する変数は組織化の水準，組織の規模，当該政府から提供される兵站的支援の三つとなる．第2のカテゴリである“資金”を構成する変数は資金源の多様性と資金力の水準の二つとなる．また第3のカテゴリである“経験と技術力”を構成する変数は組織メンバーの経験水準，テロ活動の実行の有効性，技術力の水準の三つとなる．それぞれの変数に対して，その水準を表す値1から10の数値を割り当てることになる．

すべての変数およびカテゴリの間の相互関連を表す寄与因子図を図1に示す．モデルのいろいろな構成要素の強調の度合を表すために重みを用いる．例えば，

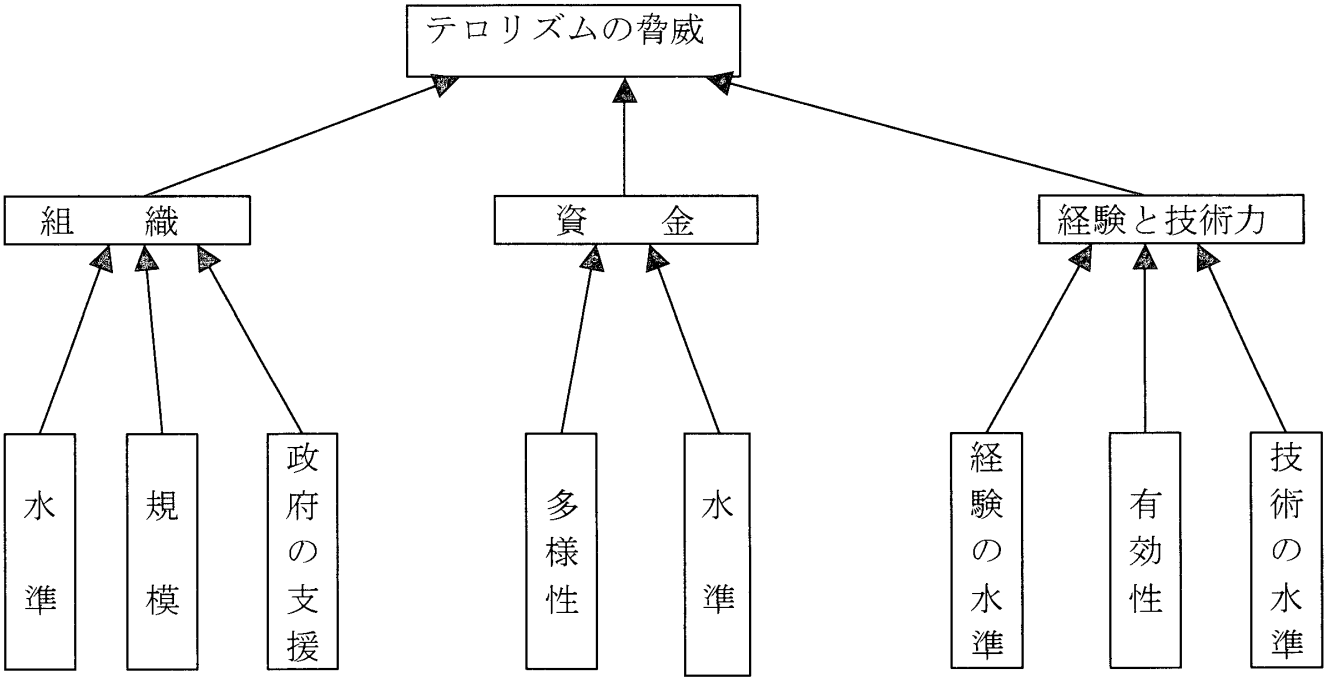

図1　寄与因子図

対象とするテロリストグループが長期にわたって存在し，しかも政府機関や企業に名称が浸透している組織であるとすると，資金面を重視することが考えられるであろうが，テロリスト組織が活動している国に最高機密の軍事施設が存在する場合には，我々はハイテク兵器を使用する能力に関心を寄せるであろう．そのような兵器を用いると，軍用通信を妨害あるいは盗聴でき，また軍事施設の敏感で重要な電子機器に損傷を与えるような電磁的パルス（EMP）を発生させることができてしまうからである．したがって，このようなテロリストグループを評価する場合には，資金のカテゴリには小さい重みを与え，技術的能力には大きな重みを与える．カテゴリの重みは0と1の間の数値で与え，しかも三つの重みの合計が1となるようにする．カテゴリの重みについて，カテゴリが比較的小さい重み値を得るのは，企業がそのリスクを軽減するのにほとんどあるいは全く何もできないパラメータを有する場合である．逆に，カテゴリが比較的大きい重み値を得るのは，十分な資金があるときに，企業がリスクを軽減できる機会があると考えられる場合である．ただし，重みはそのカテゴリを構成している個々のパラメータの値の大小にはよらない．

ここで紹介するリスクモデルは世界中のあらゆる企業で使用可能である．リスクチームのメンバー達は彼らのモデルが総括的でしかも単純でなければならないという点では一致している．彼らのリスクモデルでは，すべての分布や重みを決定した上で，以下に示すようなモデル構造式体系に基づいた計算が行われる．

(全リスク)
＝(組織面のリスク)＋(資金面のリスク)
＋(経験技術面のリスク)
(組織面のリスク)
＝(組織面の重み)×((組織化の水準)
＋(組織の規模)
＋(当該政府から提供される兵站的支援))/3
(資金面のリスク)
＝(資金面の重み)×((資金源の多様性)
＋(資金力の水準))/2
(経験技術面のリスク)
＝(経験技術面の重み)×((組織メンバーの経験水準)
＋(テロ活動の実行の有効性)＋(技術力の水準))/3

以上の前提のもとに組織，資金力，経験と技術力という三つのカテゴリに対してそれぞれの寄与因子のリスク値の分布を最小値，最尤値，最大値をもとにして計算する．これらのデータを相対リスクモデルに入力すると，モンテカルロ法に基づいた計算結果として，各々のカテゴリに対する重み付きリスク値と重み付けされた総リスク値の分布が得られる．このアプローチをいくつかのテロリスト組織に対して適用すると，各々に対するカテゴリ別リスク値あるいは総リスク値の分布が得られるので，それらが比較可能となる．

(3) 絶対リスクモデル

リスクや不確実性の専門家でない意思決定者とモデルの結果について論じるのは容易ではない．このために絶対リスクモデルとしての絶対コストモデルを構築する．コストモデルには本来，有形無形の多くのコストを取り入れるべきであるが，企業経営層に説明するために簡単で首尾一貫した説明を行うこととし，相対リスクモデルと同様のものを作成する．このモデルには分布を定義する入力データの単位としてコスト金額の絶対額が必要である．企業には毎年出費が必要であるが，工場建設費などは初年度に大きな金額となり，交際費等の水準のようにコストが毎年上昇するものもある．例えば10年モデルを計算するために，各パラメータを時系列的に決めてモデルに入れるというのでは，分析は現実的な手間では終了せず，説明が難しく，議論もやりにくいので，ここではより簡単に年平均コストを推測する方法を用いる．

本モデルは必要コストの絶対金額を計算するが，ある特定の変数あるいはカテゴリについて重要性の尺度は，それぞれに対して支出してもよいとする金額に現れるはずであるので，本モデルではカテゴリ別の重みは用いないことにしている．絶対リスクモデルは各コストの単純な確率的総和として与えられるので，方程式は単純で直接的である．例えば，組織関連総コストは，組織化の水準を下げるコストと組織の規模を下げるコストと当該政府からの兵站的支援を下げるコストの総和として与えられる．同様に，資金関連総コストは，資金源の多様性を下げるコストと組織の総予算を下げるコストの総和として与えられる．また技術関連総コストは，個人メンバーの経験水準を下げるコストと組織の有効性を下げるコストと組織がハイテク兵器を入手し，装備する能力を下げるコストとの総和として与えられる．

(4) まとめ

リスクモデルを作成することの主要な利点は，どのような疑問に答えるべきかについて参加者に合意を促すことにある．これは多くの場合，かなり達成困難で

あるが重要な目標の一つである．リスクチームがモデルのタイプ（モンテカルロか決定ツリーかLPモデルか）を決定できるということがもっとも重要である．その上に，相対リスクモデルと絶対リスクモデルが必要であると合意することと各モデルの変数の定義と値について合意することが有意義であり必要である．参加者全員が“同一の頁”を見るということが，困難ではあるが基本的な過程である．

ここに紹介したリスクモデルは一つの方法に過ぎなく，必ずしも最善の方法とは限らない．モデルの妥当性の検証は時間経過によって判明する．“採用しなかった方法”の結果を知ることは難しい．ここに詳述した企業のケースでは，検証できる唯一の方法は，モデルの結果を用いた意思決定が最終的に企業にとって良い決定であったかどうか，ということである．仮に多くの意思決定によって企業が経済的繁栄を保持することができたとすると，モデルの妥当性が証明されたといってよいであろう．また，仮に企業がリスクモデルの手法すら考えることなく，他の方法で行ったとしても，同等あるいはもっとよい結果を得たのではないかという議論が起こるかもしれない．本作業の副産物は，モデルにデータを割り付ける際に必要な会話であるといえる．相対的ランク付けや実際の金額をあれこれ議論するとき，チームメンバーはそれぞれの国のそれぞれの変数に関し，詳細で意義深い会話に入らざるをえない．こういう会話がモデルを実地に適用したり結果を解釈することよりも重要であることが非常に多い．

相対リスクモデルはコンセンサスを得る手法の一つであり，本質的に総括的である．つまり，リスクチームはモデルを再三繰り返すことによって別の国を新たに評価するのに，あるいは同一の国々を時間の経過後に再評価するのにも使用することができるということである．モデルの解の変数があらかじめ決められたスケール（今の場合，1～10）の予測値をとるので，モデルで評価された国々すべてを比較しランク付けできることになる．

絶対リスクモデルの出力によると，経営者は出費の幅を想定した対応戦略を確率に関係付けて考えることができる．この種のモデルではどのような意思決定を行うべきかについてはあまり明確にはしない．しかし，このようなモデルから得られることは意思決定過程に不可欠な内容である．Kollerモデルについての詳細はKoller[10]を参照されたいが，文献[11]にはその概要紹介と具体的数値分析結果についても記載されている．

5. おわりに

節1に述べたようにテロ研究に関しては内的モデルアプローチと外的モデルアプローチという大きく二つのアプローチがある．テロ研究としては前者が古くから行われ，採用されてきたのに対して，後者のアプローチはテロ対策として組織をどのように構成し，資源，予算をどのように配分すればよいか，といった研究が必要とされるに伴って，最近の10年余に盛んに行われるようになったもので歴史が浅い．今後大きな成果が期待されているのはむしろ後者の分野であるといえよう．Falkenrath[5]には大量破壊兵器（WMD, weapon of mass destruction）とテロとの関連，特に米国におけるテロ対策に関する戦略，政策研究について詳細が記され，テロ研究の将来の方向が示唆されている．

テロ研究の歴史は長いとはいえないが，特にテロリズムリスクの予測と評価をできるだけ客観的，合理的，科学的に行うことが求められている．Hofman[12]にはテロリズムの本質がどのようなものであるか，そしてアルカイーダ（Al Qaeda）についての分析とともに2001年9月11日以降に得られたテロ対策の教訓についても述べられ，これまでにどのようなことが起こったかということよりも，どのようなことが起こっていないかについて考慮することが必要であると強調されている．またBrannan[13]にはテロ研究者の姿勢について論じられ，テロ研究者はテロを単に過激派集団による行動という見方のみに限定すべきではなく，むしろテロは社会現象であるとして捉えるべきであると述べている．Tsfati-Weimann[14]には，現代のテロ研究に欠かせないインターネットとの関連が情報伝達，利用方法，技術的側面，などの特性といった諸側面から詳細に述べられている．テロリスト関連サイトについても多くがリストアップされており，研究者にとって有用であると思われる．テロ研究はテロリズム自体が有する歴史，文化，宗教といった背景，そしてまた社会的，政治的，あるいは経済的な諸側面など，多種多様多面的な複雑さゆえにその解決，対策は決して容易ではないであろうが，研究分野として，OR研究者，実務家にとって貢献の可能性を秘めた魅力ある分野であるといえよう．今後このような分野に対しても多くの研究者が現れ，成果が得られることを期待したい．

参考文献

[1] Weimann, G. and C. Winn, *The Theater of Terror*, New York : Longman Publication.

[2] United States Code (合衆国現行法律集), http://www.access.gpo.gov/uscode/uscmain.html

[3] Post, J. M., K. G. Ruby and E. D. Shaw, "The Radical Group in Context : 1. An Integrated Framework for the Analysis of Group Risk for Terrorism", *Studies in Conflict & Terrorism*, Vol. 25, No. 2, pp. 73-100, 2002.

[4] Post, J. M., K. G. Ruby and E. D. Shaw, "The Radical Group in Context : 2. Identification of Critical Elements in the Analysis of Risk for Terrorism by Radical Group Type", *Studies in Conflict & Terrorism*, Vol. 25, No. 2, pp. 101-126, 2002.

[5] Falkenrath, R., "Analytic Models and Policy Prescription : Understanding Recent Innovation in U. S. Counterterrorism", *Studies in Conflict & Terrorism*, Vol. 24, No. 3, pp. 159-181, 2001.

[6] Sprinzak, E., "From Theory to Practice : Developing Early Warning Indicators for Terrorism", Washington D. C., USIP, 1998.

[7] Ronfeldt, D., "Netwar Across the Spectrum of Conflict : An Introductory Comment", *Studies in Conflict & Terrorism*, Vol. 22, No. 3, pp. 189-192, 1999.

[8] Arquilia, J. and D. Ronfeldt, "The Advent of Netwar : Analytic Background", *Studies in Conflict & Terrorism*, Vol. 22, No. 3, pp. 193-206, 1999.

[9] Whine, M., "Cyberspace—A New Medium for Communication, Command and Control by Extremists", *Studies in Conflict & Terrorism*, Vol. 22, No. 3, pp. 231-245, 1999.

[10] Koller, G., "Risk Modeling for Determining Value and Decision Making", Chapman & Hall/CRC, 2000.

[11] 日本オペレーションズ・リサーチ学会創立40周年記念事業 研究助成特別研究プロジェクト, "ネットワーク構造を有するライフラインシステムの危機対応管理体制に関する研究報告書", 日本オペレーションズ・リサーチ学会, 2001年3月20日.

[12] Hofman, B., "Rethinking Terrorism and Counterterrorism since 9/11", *Studies in Conflict & Terrorism*, Vol. 25, No. 5, pp. 303-316, 2002.

[13] Brannan, D. W., P. F. Esler and N. T. Anders Strindberg, "Talking to "Terrorists" : Towards an Independent Analytical Framework for the Study of Violent Substate Activism", *Studies in Conflict & Terrorism*, Vol. 24, No. 1, pp. 3-24, 2001.

[14] Tsfati, Y. and G. Weimann, "www.terrorism.com : Terror on the Internet", *Studies in Conflict & Terrorism*, Vol. 25, No. 5, pp. 317-332, 2002.