リスク分析とセキュリティ対策について

宇佐美　博

リスク分析は，犯罪対策，セキュリティ対策の検討や，監査対象の選定等に欧米では広く用いられている．しかしわが国ではその実施例はあまり多くない．そこでリスク分析と関連する課題について問題点を提起し，識者のご批判を仰ぎたい．

1.　リスク分析について

リスク分析には，いろいろな方法が提案されている．本節では，まずそれを概観しよう．

期待値（推定値）法

リスク評価の最も基本的な方法は，年間，平均的に予想される損失額を用いることであろう．つまり，犯罪や事故，エラーが生じた場合の1回当りの損失をV(円)，年間の予想発生頻度をP（回/年)，1年当りの損失予想額をL(円/年)とすれば，

$$L=P\times V \qquad (1)$$

となる．しかし，この方法は，1回当りの損失額あるいは損失発生の確率の推定値にきわめて敏感に反応するという欠点があるといわれている．

コートニーの方法

コートニーの方法［1］は，

$$L(\text{円/年})=10^{(p+v)}/a \qquad (2)$$

という式によって，1年当りの損失予想額を求めるものである．

表1

年間発生頻度P	pの値	1回当りの損失V	vの値
3000年に1回	0		
300年に1回	1	10千円	1
30年に1回	2	100千円	2
3年に1回	3	1,000千円	3
100日に1回	4	10,000千円	4
10日に1回	5	100,000千円	5
1日に1回	6	1,000,000千円	6
1日に10回	7	10,000,000千円	7

（コンピュータの稼働日数が3年間で1000日の場合）

ここに，

p：損失発生の頻度に対応する係数

v：その損害発生時の予想損失に対応する係数

a：定数

であり，これらの値はコートニーによって次のように与えられているものである．すなわち，コンピュータの稼働日数が3年間で1000日の場合は$a=3$，コンピュータの稼働日数が4年間で1000日の場合は$a=4$であり，pおよびvは**表1**の数値をとる．

この方法を推賞する人も多い．ごくまれに生ずるような損失については，感度が低く，頻繁に生ずるような損失については，感度が高くなるような算式であるとされているからであろう．しかし筆者の見解によれば，これは誤解と思われる．Pとpの関係は，

$$p=\log\left(\frac{P}{P_0}\right)$$

うさみ　ひろし　東亜燃料工業㈱　監査室
〒100　千代田区一ツ橋1－1－1
パレスサイドビル

と表現できる．ここで，Pは3000年に1回の割合で損失が発生するという確率である．この式を(2)式に代入すれば，年間予想損失額Lを確率Pの関数として，

$$L=\left(\frac{P}{P_0}\right)10^{v/a}$$

と表わされる．

いま，この確率Pがα倍されたとしよう．このとき損害は，$L(\alpha P)/L(P)$倍となるが，この値は上式により，$L(\alpha P)/L(P)=\alpha$となる．すなわち，感度は確率P，つまり発生の頻度には依存しないのである．

また，頻繁に生ずるような損失については，測定データが多いため精度高く推定できるはずであるが，この算式では考慮されない．したがって，コートニーの式によりリスク分析は，大まかな所でしか意味を持たないものと思われる．

ウイルキンスの方法

ウイルキンスは［2］，［3］，次のようなリスク分析の定量的方法を紹介している．

まず，定量化には，次の要因が関係するとしている．

1）価値．情報が権限のない者に，開示されたときの企業の損失．

2）確率のファクター．情報に対する現行の保護レベルを評価するファクターであり，確率そのものではない．許可されていないにもかかわらず開示されてしまう可能性の高いときは4，中程度のときは，3，低いときは2，ほとんどない場合は1という数値を当てる．

3）リスクファクター．1）の価値と2）の確率のファクターの積．

こうして求められたリスクファクターを保護対策や監査対象の優先度の尺度とするというのがウイルキンスの方法である．

さらに，投下資本当りのリスクファクターを求めて，その低下額の大小によって対策を選定する方法も提案している．

しかし，この方法では問題が生ずる“確率のファクター”は，いわば順序づけしただけであり，いうまでもなく本当の意味の確率ではない．また最適対策の選定方法に問題があるが，それについては後述する．こうして得られたリスクファクターも，したがって具体的な意味を持たない数値であり，保護対策等の優先順位を決めるときくらいにしか使えない．

上記はシステムに関連するリスクの評価の方法であり，いずれによっても，リスクの順序を求めることはできる．ところで，リスクの評価は，その順序づけだけが最終目的ではない．セキュリティ対策の実施や検討の優先度，あるいはセキュリティ対策実施の適否の判定に利用するのが最終的な目的の場合もある．そこで，次のような考え方も併記しておこう．

フィッツジェラルドの方法

フィッツジェラルド［4］，［5］は，システムをとりまくリスクを直接的に算定することが困難な場合に，これにかわる間接的な方法として，業務の重要度の評価法を提案している．

すなわち，業務をめぐる諸要因に対しその状況に応じたスコアを与え（**表2**参照），その値の積をもって，その業務の重要度の尺度とするのである．その諸要因とは次の項目である．

開発のコスト．適用業務開発の時間．処理のタイプ．適用業務の総合度．システムの構成．ファイルのタイプ．年間コンピュータ使用時間．プログラムモジュールの数．システム開発の方法．プロジェクト開発チーム．プログラム言語．データの性格．アクセスされる資産額．報告書提出の要否．

そして，セキュリティ対策の重点をこうして評価した重要度の大きい所におこうというのが，フィッツジェラルドの提案である．

2. セキュリティ対策の選定について

セキュリティ対策の実施や検討の優先度はどの

表 2

要素番号		
1.	概算開発コスト	係数
	・1万ドル未満	1.0
	・1万ドル～5万ドル未満	1.2
	・5万ドル～10万ドル未満	1.4
	・10万ドル～25万ドル未満	1.8
	・25万ドル～100万ドル未満	2.2
	・100万ドル以上	2.5
5.	・集中システム	1.0
	・分散システム	1.5
11.	・COBOLで書くプログラム（それ自身が文書になっている）	1.0
	・COBOLでないプログラム（それ自身は文書になっていない）	1.5
最終得点	（1～14の各係数をすべて掛け合せる）	

ように決めるべきであろうか．リスクの大小や関連する業務の重要度は大きな要素ではあるが，資金や人員には限りがあるので，実施に要する費用や職員の作業量も無視できない．セキュリティ対策の検討自身に要する労力当りのリスクという見方も必要である．この観点から見るとフィッツジェラルドの方法は適当ではない．

セキュリティ対策の実施の可否を検討する場合には，対策の経済性が問題になる．これには，資金回収期間法，投資利益率法，利益額比較法が採用されるが，いずれの場合でも，資金，利益，費用などの絶対額がわかれば投資の可否が判定できる．（したがって，この意味からしてもフィッツジェラルドやウイルキンスの方法は適当でない．）なお，利益や費用は年々変化するので，割引減価法を用いる必要があることも注意しておこう．

ところで，セキュリティ対策実施による効果とその費用には，一時的なものと継続的に毎年発生するものとがある．すなわち費用には，一時的に資金を必要とするいわゆる資本的支出と，毎年継続的に発生する経費があり，一方，効果についても，省力化やエラーの防止によって毎年取得できる効果のほか，セキュリティ対策によって関連する設備投資が減少できるという一時的な利益もある．このように，一時的な支出と収益，毎年発生する支出と収益がある場合，そのままでは比較できない．したがって，経費・収益を割引減価法により初年度の支出・収益に換算するか，一時的な支出，収益を対象（機器の寿命）期間に配分し，支出・収益に置き換えて，費用と効果の大小を判定する必要がある．ここでは，単純化して，初年度の支出・収益に換算したものとして，以下の論を進める．

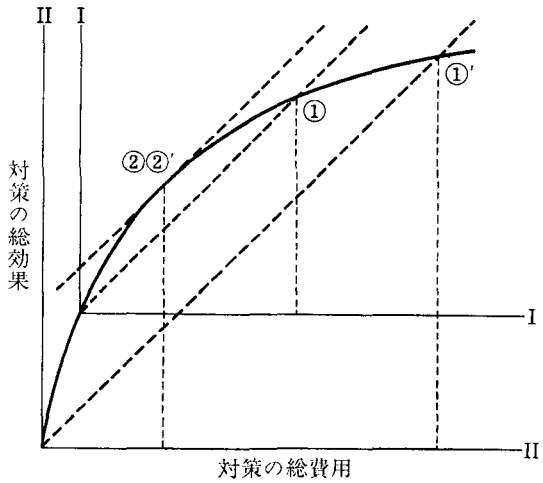


図 1　セキュリティ対策の費用と効果

さて，この費用効果を検討するさい，2つの考え方がある．

第1の方法は，セキュリティ対策費の合計が，その対策の効果の合計を上回らない点（総費用＝総効果）まで，費用対効果の良い対策から個々のセキュリティ対策を積み上げる．第2の方法は，費用対効果の良い対策から個々の対策を実施し，個々の限界対策費がその効果を上回らない点（限界費用＝限界効果）まで，対策を実施するという方法である．この両者について検討を進める．

図 1 に，セキュリティ対策の費用対効果の関係をモデル化して示した．さて，セキュリティ対策費の範囲を決めるのは実はむずかしい問題である．セキュリティ対策といっても，セキュリティだけを目的とするとは限らない．関係者の教育・訓練はセキュリティ対策の大きな柱であるが，エ

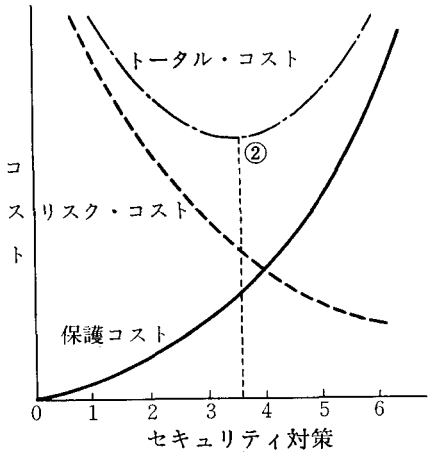


図2　セキュリティ対策の最適点

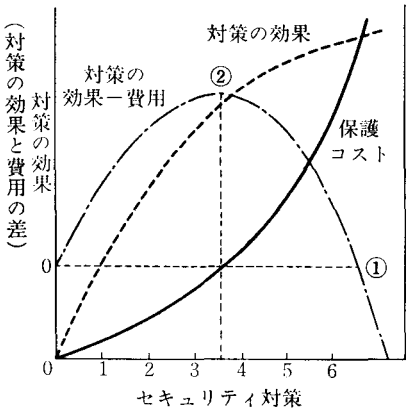


図3　セキュリティ対策のネット利益

ラーの防止，作業効率の向上にも役立つ．耐火構造の事務所は現在では常識であるが，セキュリティ対策の一環でもある．常識的には，安全確保を第一義的目的とする施策，つまり，安全を考慮しなければ，採用しない対策の費用だけをセキュリティ対策の費用と見なすのが妥当であろう．

セキュリティ対策の範囲の採りかたによって，実施の可否が変わることがある．図1に示すように，総費用と総効果の比較からの判断では，範囲を狭くとれば①，広くとれば①′が総費用＝総効果の点だから，ここまでが実施すべき対策になる．しかし，個々の限界費用と限界効果からの判定では，対策に算入すべき対策の範囲が変わっても結論に変わりはない．②，②′，までが採用すべき対策である．

さて，第1の方法，すなわち総費用と総効果から判断する場合には，過去に実施した対策を含めて，すべての対策を考慮するので事務作業が大変であるほか，資本効率の良い対策で得た利益を食いつぶすまで資本効率の悪い対策を実施することになり，一般常識に反する．

これに対して第2の方法は，関連する対策の検討は必要であるが，個々の対策と効果のみを考慮すればよいので，事務作業も簡単である．このように，総費用を基準とすべきか，その限界費用を基準とすべきかを比較すれば，限界対策費がその限界効果を上回らないことをその判断基準とすべきである．さらにこの他に，リスクコストと保護（セキュリティ対策のコスト）のコストの和が最小になる対策（の組合せ）を選ぶべきだという説もある．この場合には**図2**，**図3**の②が選択すべき結論である．セキュリティ対策の実施によるリスクコスト（損害額）の減少は換言すれば，セキュリティ対策の効果である．したがって，②は限界効果と限界費用が等しい点である．これは，図1の②，②′の点と同一であり，したがって，このリスクコストと保護のコストの和が最小になる対策を選択すべきだとする考え方は一応妥当である．（ただし，図では，セキュリティ対策1～6を等間隔に配置したが，これは各費用が等しいことに対応している．一般には，費用に比例した間隔とし，さらに費用／効果の良い順に配置すべきものである）

3. セキュリティ対策間の関連について

上記の議論は，セキュリティ対策が相互に独立であることを前提にしている．しかし，対策を個々に実施した場合と，合せて実施した場合の個々の効果は同一とは限らないということがある．たとえば，パンチ・エラーの防止のために，検孔と目検を実施する場合，それぞれを別個に実施すれ

ば1％ずつの効果があるとき，両方を実施しても2％のエラーの減少になるとはかぎらない．

一方，対策を併用すれば相乗効果によって，効果が高まることもある．たとえば，パスワード・システムとＩＣカードを併用すれば，セキュリティが高まる．しかし，パスワード・システムは，それが盗まれたことが認識できない，本人以外の者が使用したことがわからない，などの欠点がある．また，ＩＣカードは，落とした場合には直ちに悪用される可能性がある．しかし，ＩＣカードを落としたことは当人が認識できるので，その時点で悪用される危険性が予測できる．したがって，ＩＣカードとパスワード・システムを併用すれば，ＩＣカードを紛失しても，パスワードさえ盗まれていなければ，セキュリティは侵害されない．また，パスワードが破られても，ＩＣカードが盗まれていなければ安全が確保できる．

上記は例であってすべての状況を示しうるものではないが，イメージをいだくことはできよう．

また，上記の例は，個々のセキュリティ対策の効果を分離することのむずかしさを物語っている．さらに，より完全な対策を実施したために，ある対策が無意味となることもある．たとえば，教育・訓練によってパンチ・ミスを皆無にできれば，目検や検孔は無用になる．

費用についても，前述のように確定するのが困難な場合が多い．関連する費用のすべてを対象にするのではなく，問題とする対象についての費用という考え方をとる必要がある．

以上のことから，セキュリティ対策の費用対効果を検討するときには，個々の対策について検討すべきであるが，これは正しくは，他の対策群との相関のない対策群ごとに評価すべきだということになる．

さてディボルト社（ヨーロッパ）［1］は，「データ保護の20の基本ルール」を発表しているが，その1つは「保護対策は，さらされている脅威の大きさに比例すべきである．重要でない事項を保護の対象とすべきではない」ということであるが，これが本稿で検討した課題に関連するのである．

そのほかに，「保護システムの強さは，その最も弱い部分で決まる」とも述べられている．たとえば，出入口が数箇所ある場合，侵入者は最も警備の弱い出入口から入り込むであろう．この場合，それ以外の場所の警備は過剰ということになる．これは，最も警備の弱い出入口を他の場所なみに強化すれば全体としての警備体制が強化されるので，警備のレベルを上げる場合の費用は1カ所だけですむという価値ぐらいしかない．しかしこのルールを社会一般でとらえたとき，別の観点がある．他の条件が同一であるが，A社の警備体制がB社に比較して非常に弱い場合，よく研究している侵入者は，当然A社を攻撃目標に選ぶであろう．この場合，B社はA社と明らかな有意差がある程度に，警備体制を整備しておけばよいということになる．このように考えれば，警備体制等のセキュリティ対策を他社なみ，あるいは平均よりも多少よい程度とすることも合理性があるといえよう．

さらに，意図的な相手の対応を考慮すべき場合も多く，上記の例はこれにも該当するものである．先のルールにも，「保護障壁の効果は，それを破るために費される時間で測ることができる」という項もある．つまり，意図的な侵入者に与える損失が，セキュリティ対策の効果である．したがって，前述のセキュリティ対策の費用対効果はセキュリティを侵害しようとする者の努力・費用と，これを防御する者の努力・費用の比較と見なすことができよう．これは，いわゆるミニ・マックスの問題として論じることができるものと思われる．

4. おわりに

リスク分析とセキュリティ対策に関連する課題について検討した．セキュリティの問題は，それ

に関連して検討すべき事項が多く，複雑であるので，単純化した説明がなされる場合も少なくない．したがって，その説明が実態に即したものであるか否かを十分に考慮する必要がある．

筆者は，システム監査やコンピュータ・セキュリティに関して勉強している者であり，ORの専門家ではない．ここで述べた筆者の見解や提起した問題に関してORの専門家からのご批判，ご提案を期待してやまない．

参考文献

[1] 上園忠弘：コンピュータ・セキュリティ．近代科学社，1981年

[2] Barry J. Wilkins : The Internal Auditor 's Information Security Handbook, The Institute of Internal Auditors, Inc., 1979

[3] バリー，ウイルキンス，渡部一元・宇佐美博・富山茂 訳：システム監査人のための情報セキュリティ入門．日刊工業新聞社，1986年．[2]の翻訳書

[4] Jerry Fitzgerald : Designing Controls into Computerized Systems, Jerry Fitzgerald and Associates. 1981

[5] 鈴木勝彦監訳：情報システムのコントロール設計 日経マグロウヒル社，1986年．[4]の翻訳

[6] 宇佐美博：コンピュータ・セキュリティの費用について，日経コンピュータ，7月23日号(1984) 155～158

●ミニミニ●　　●OR●

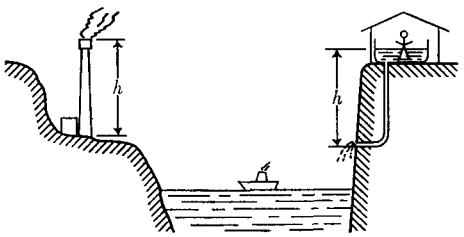
ユーレカ！

伊豆の，海岸に面した崖っぷちにある家で温泉につかった．ちょっと塩分を含んだ透明なお湯をゆっくりと楽しんだ後，湯舟の栓を抜いた．お湯は小さな穴から，猛烈な勢いでキューと音を立てて流れ出し，湯舟はまたたく間に空になってしまった．

おそらく，湯湯の流出孔にはパイプがつながれ，はるかずっと下の方まで導かれていたのであろう．トリチェッリの定理によれば，流出速度は$\sqrt{2gh}$(g：重力加速度 h：水面と噴出口までの落差)である．だから，落差が大きければ，それだけお湯の減り方が早くなるわけだ．いいかえれば，パイプはあたかもポンプのような役割をはたしていることになる．

そこでフト思いついた．煙突が高いのもおなじ理由だ．燃焼室でもえた熱いガスは浮力をもつ．——重力と比べれば向きは正反対だし，大きさも小さいが，その働きはまったく同様である．燃えたガスを引っ張り出し，新鮮な空気を吸いこんで，燃焼をさらに促進する．——そのポンプの役割をはたしているのが煙突だ．

"浮力加速度" fを適当に定義するならば，高さhの



煙突の出口における流速は$\sqrt{2fh}$になるはずだ．お月様にはご迷惑でも，ポンプとしては高いほど強力だ．

蒸気機関車の煙突も昔は高かった．高くては都合が悪いので短くしたいが，それでは十分な燃焼が得られない．蒸気をつかって強制的に煙を追い出すという工夫が生まれてやっと煙突を短くすることが可能になったのである．

風呂の中で裸のままユーレカ！を叫んだものの，残念ながら，煙突は筆者の発明ではない．市川亀久弥氏の「等価変換理論」の一例題を得たことで大いに満足しておかなければなるまい．(からくり堂主人)

＊市川亀久弥『創造性の科学』，日本放送出版協会，1960