論　　文

# ITセキュリティ投資とリアルオプション

加　藤　　敦
現代社会学部・社会システム学科

## Abstract

How much should a company invest money into IT security investments? IT Security investments are among those where proper evaluations are difficult. Today some scholars and consulting firms suggest Security ROI, modification of ROI which involves insurance theory. However IT security insurance has not yet spread so much and it is not easy to adapt such process for general companies.

We introduce real options, which is an effective means to evaluate uncertainty and compatible with insurance theories. Basically a purchase of insurance is buying of put options. Firstly we consider the critical point to apply real options to IT securities. Secondly we practically recognize and evaluate options value through a case study on network security. We use risk analysis and Balanced Scorecard to evaluate the values precisely.

## 序　論

IT社会の進展の一方、ウイルスや不正アクセスなどセキュリティ問題が数多く発生している。こうした脅威から身を守るために多くの企業がセキュリティ対策を実施している。しかし企業はセキュリティ投資にどこまで金銭を投入すべきであろうか。IT投資の中でもセキュリティ投資は投資評価が難しいとされる分野である。今日、セキュリティ投資の数値化を掲げ、研究者や実務家の間でSecurity ROIの概念が提唱されている。しかしSecurity ROIについては、保険理論の適用等の基本的合意はあるものの、その内容については明確・標準化されているとは言いがたい状況である。加えてセキュリティ対策保険が実社会でまだそれほど普及していないこともあり、保険料率の推定などが難しく一般の企業にとり取り組みにくいものとなっている。

そこで本論では、不確実性を吟味する上で有効な手段であるリアルオプションにもとづき実務的に利用可能な評価法を提案することを目的としている。リアルオプションは、正味現在価値（＝Net Present Value、以下NPV）を中心とする伝統的財務評価を補う不確実性を加味した投資評価法である。リアルオプションは金融分野におけるオプションを、現実の資本投資等に適用したもので、柔軟性の価値を評価できるという利点がある。

本論の構成は次の通りである。最初にセキュリティ投資の実情並びに投資評価の課題を概観する。次にリアルオプションを適用する意義とその際のポイントを指摘する。さらに不正アクセス対策についての事例を通じ、実際にリアルオプション・アプローチにもとづく評価法を進めてゆこう。

## 1．IT セキュリティ投資

### 1.1　IT セキュリティ投資の概要

『平成15年版情報通信白書』は、平成14年における企業の情報セキュリティ被害額を約3,500億円と推計している。内訳は、「ウイルス等の感染」約3,000億円であり、「システム破壊・サーバダウン」は約400億円、「ホームページ等の改ざん」は約20億円、「ウェブ上での誹謗中傷」は約7億円、「顧客情報の盗難・流出」は約5億円である。

『平成15年版情報通信白書』によると、ほとんどの企業が何らかの情報セキュリティ対策を講じている。「ウイルス等の感染」約3,000億円であり、「システム破壊・サーバダウン」は約400億円、「ホームページ等の改ざん」は約20億円、「ウェブ上での誹謗中傷」は約7億円、「顧客情報の盗難・流出」は約5億円である。

### 1.2　IT セキュリティ投資評価の課題

コスト削減や売上拡大を狙ったIT投資はキャッシュフローを推定しNPVやROI（Return On Investment＝投資収益率）によって投資評価を行うことができる。セキュリティ投資の多くは実施によって直接、キャッシュフローの改善が生じる訳ではない。またネットワーク効率性の向上など

IT Security Investment and Real Options

**図表1 企業のITセキュリティ対策（単位%）**

| 情報セキュリティ対策（複数回答） | 設備投資 | 教育等 |
|---|---|---|
| パソコン等の端末にウイルスチェックプログラムを導入 | 83.8 | |
| ID、パスワードによるアクセス制御 | 64.9 | |
| サーバにウイルスチェックプログラムを導入 | 55.9 | |
| ファイアウォールの設置 | 52.0 | |
| 外部接続の際にウイルスウォールを構築 | 18.2 | |
| 代理サーバ等の利用 | 14.5 | |
| 回線監視 | 12.5 | |
| データやネットワークの暗号化 | 8.2 | |
| 認証技術の導入による利用者確認 | 7.7 | |
| 不正侵入検知システム（IDS）の導入 | 4.0 | |
| 社員教育 | | 20.9 |
| セキュリティポリシーの策定 | | 19.1 |
| セキュリティ管理の外部へのアウトソーシング | | 8.6 |
| ウイルスチェック対応マニュアルを策定し、社内教育を充実 | | 8.5 |
| セキュリティ監査 | | 6.5 |
| その他 | 0.6 | |
| 分からない | 1.0 | |
| 特に対応していない | 2.2 | |

出所 『平成15年度情報通信白書』

を主目的として、その一部としてセキュリティ投資が行われる場合が多い。

こうした中でセキュリティ投資効果を計数モデルにより明確化する試みがIT企業やコンサルティング会社等によって提案されている。こうした概念はSecurityROIまたはROSI（Return On Security Investment）と呼ばれている。スコット・ベリナート（2004）は、年間損害予測（Annual Loss Estimate）という概念を示し、障害によって発生する経費の単純な総額に、発生可能性を乗じたものと定式化し、これを投資積算の基礎としている。[1] またアクセンチュア㈱は、SecurityROIに「コンプライアンス」、「ベンチマーキング」、「戦略的セキュリティ投資」、「セキュリティ対策コスト削減」、「損害保険コスト削減」という5つの要素を織り込んでいる。うち「損害保険コスト削減」はセキュリティ向上により、損害保険額にかかるコストを削減することである。[2]

Security ROIの具体的算出プロセスは提唱者によって異なるが、基本的には伝統的ROIにより評価される部分に損失回避による収益寄与分を何らかの合理的手法により加味すべきということである。そのため最も一般的な方法が、確率的に発生するリスクに対処するための損害保険をSecurity ROIに織り込むことである。

最近、ITベンダーと損害保険会社が連携してセキュリティ対策システムとセキュリティ保険を一体で販売する動きが進んでいる。[3] しかしセキュリティ保険では多くの場合、保険会社がケースごとに個別に料率を積算していることもあり、現在までのところ一般的とは言えない状況である。火災保険や自動車保険など一般の損害保険は、同質のリスクを多数集めることで「大数の法則」によりリスクを算出する。これに対しITセキュリティのリスクは企業の業務、ネットワーク利用内容、セキュリティ教育などによって異なり、同質リスクとみるには無理がある。従って一般企業が投資評価にあたり企業が市場的な保険料率を入手することは容易でない。[4]

もう一つの課題として、セキュリティ投資を含め、組織・教育並びに運用体制などセキュリティ対策全体をどうマネジメントすべきか、という点がある。例えばウイルス対策ソフトを導入するだけでなく、日常のウィルスチェック対応体制を確立しなければ、十分な効果をあげることができないだろう。換言すれば事前評価のみでなく、事後的評価も含めPlan（計画）・Do（実行）・Check（検証）・Action（修正）の体制をどう確立してゆくかが重要である。

## 2．リアルオプション適用のポイント

伝統的ROIに保険要素を加味するというSecurityROIの基本的考え方に異議を唱える者は少ないだろう。しかし一般の企業がこの投資評価法を実際に進めるのは容易ではない。というのはITセキュリティを付保する損害保険が社会ではまだ一般的でなく「保険料金表」が入手できないし、損害保険会社に逐一見積もりをとることは手間がかかり過ぎるからである。こうした中で既に計算手法が確立しているリアルオプションを適用することは現実的な解決策と言えよう。

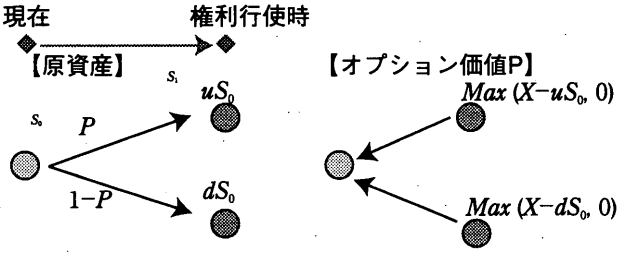
そもそも保険は約定された条件の下で金銭を請求できる条件付請求権の1つであり、オプションのサブセットとして捉えることができる。従って基本的には保険購入とプットオプションの買いは同じである。ただしオプション料（保険プレミアムに相当）が成立するプロセスは異なる。損害保険の場合、我々は複数の投資機会の間で裁定取引の機会を求めている訳ではない。例えば自動車損害保険は発生確率が低く壊滅的な損害が生じる「まさかの場合」の備えであり、期待リターンを求め不動産投資や国債購入と比較することはしない。この場合、損害保険会社がコスト・プラスによって算出した保険料率を購入者が受け入れるか否かであり、裁定機会があるとすれば他の保険会社が提案する保険との間のみである。これに対しセキュリティ投資に目を転じると、社会的に最小限度と認識される水準までは

企業の社会的責任として認識すべきであるが、それを超える部分は他の投資機会との間で裁定取引機会を考慮することが多い。平たく言えば同等の企業規模や同一業界と比較して最低限の額のセキュリティ投資までは義務として実行するが、既に実行済の企業は、資金をセキュリティ投資に投じるか、CRMや合理化投資など他の投資機会に資金を振り向けるべきか、比較検討するだろう。SecurityROIという概念が生まれた背景も、既に多額のセキュリティ投資を実施しているにもかかわらず、不正サクセスなどの急増から次々と新たなセキュリティ投資の必要性が指摘される中で、果たしてどこまで投資を行うべきかといった切実な問い掛けがある。リアルオプションはNPVを拡張したものであり、セキュリティ投資を他の投資機会と比較する場合、有益である。[5]

次に実際の運用にあたって留意すべき点について順次考察しよう。

第1にセキュリティ投資をいかにオプション・モデルとして定式化するかである。セキュリティ投資の価値について、対策前と対策後の2つのプットオプションの価値すなわちオプション料の差としてモデル化することができる。このセキュリティオプション（プットオプション）はITシステムというリスキーな資産が大きく価値を減じた場合に約定価格（例えば現時点でのITシステムの価値）で買い取ってもらう権利である。

**図表　2　セキュリティオプション**




保険料＝オプション価値
　権利確保の対価　損害保険料
　原資産S　プロジェクト価値
　権利行使価格X　売却価格（保険支払額）

この場合は2つの損害保険と考えても同じである。セキュリティ対策前・後のIT資産について何らかのセキュリティ事故の損害を補償する架空の損害保険を考える。この損害保険は危険資産を約定価格で買い取ることを求めるプットオプションとして、保険の価値はオプション価値に等しくなるとする。ここで権利行使価格＝約定されたITプロジェクト価値、原資産＝セキュリティ対策前ITプロジェクト価値、権利確保の対価＝保険料である。

次にオプション価値評価法について考察しよう。オプションの評価は解析法や二項ツリー並びにシミュレーションを利用して求めることが可能である。

金融オプションの場合、完備市場を前提としている。複数の代替金融資産を勘案した投資機会において、裁定取引が生じないように市場が機能するとみて、オプション価値（オプション・プレミアム）を求める。投資評価などリアルオプションの場合は、完備市場の前提は満たされないことが多い。この場合、経営者が主体的に複数の投資機会の中で裁定取引が生じないように、オプション価値（柔軟性の評価）を求めることになる。セキュリティ投資の場合も、これによって得られる保険と他の複数の投資機会と比較し、より有利な投資機会との間で裁定取引が生じないように、価値が求められる。[6]

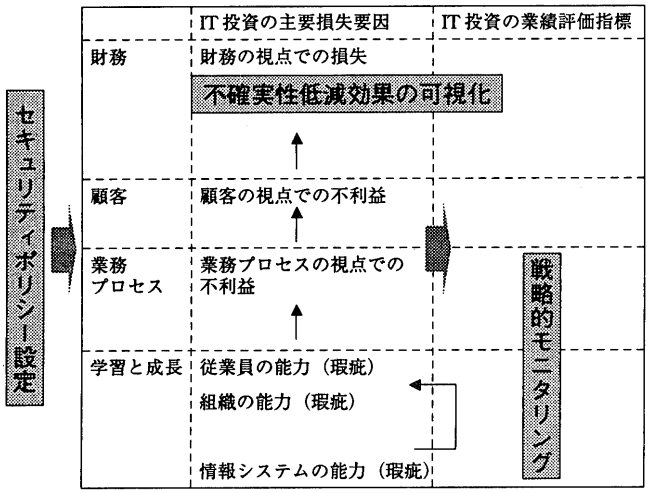
解析法では原資産価値の成長率を無危険利子率と同一として裁定取引が生じない条件下での、オプション契約による境界条件を織り込んでいる。数式から機械的に算出され便利である反面、実務家にとり計算過程がブラックボックス的に見えるため、社内的コンセンサスが得にくい面がある。セキュリティ投資の場合、資産及び交換資産が市場で取引されていないこと、原資産の成長経路並びにボラティリティを推定することから、計算過程が見えにくい解析法は不向きである。換言するとセキュリティ投資においては、交換オプションとして定式化し解析法によりオプション価値を機械的に計算するのでなく、2つの保険とのアナロジーを用いて原資産並びに交換対象資産のリスクを可視化することを重視し、貨幣的価値は経営者の判断に委ねるべきであろう。リスク可視化にはシミュレーション法が有効である。

第2にオプション計算の前提となる損害額算定のため適切な手法の選択である。損失額の算定には、障害発生に関係するすべての設備的・人的要因を明らかにした上で、発生が見込まれる損害額、並びに発生確率を求めなければならない。大規模プラント・ネットワーク・セキュリティ対策委員会は対象リスクを分析する代表的手法として、定性的分析手法であるPRA（Preliminary Risk Analysis）、HAZOP（Hazard and Operability studies）、FMEA（Failure Mode and Effect analysis）、ツリーベース分析手法であるFTA（Fault Tree Analysis）、ETA（Event Tree Analysis）を挙げ、それぞれの手法から1つを選択することでスク概要の把握が可能であるとしている。これらはITのみならず環境リスク、設備リスクの分析などにも幅広く用いられている手法である。このうちどの手法を組み合わせて選択する

かは、事例の性格によって判断すべきであろう。[7]

第3がバランストスコアカード（Balanced Scorecard＝以下BSC）の併用である。リアルオプションはNPVとの整合的評価、不確実性を勘案した評価、シナリオ性ある計画の立案が可能であるという長所がある。しかし一方、パラメータの信頼性、市場評価が難しい技術リスクの扱い、モニタリングの困難さ等の課題がある。これらに対処するにBSCを組み合わせることが有効である。すなわちIT投資の総合的評価、IT戦略のブレイクダウンを通じて不確実性パラメータの推定過程を明確化することができる。

**図表3　セキュリティポリシーのBSCへの展開**




また市場評価が難しい技術リスクは、無理にオプション算出プロセスに置かず、BSCによるモニタリングに委ねればよい。またリアルオプションによりIT投資実行後、ともすればおざなりになりやすい日常管理はBSCを通じたモニタリングで克服できる。一方で、BSCの立場からみると、短所であるNPVとの不整合、不確実性の扱い、シナリオの扱い等はリアルオプションの適用により克服される。

## 3．事例研究

セキュリティ投資をリアルオプションにより評価する有用性を確かめるため、不正アクセス対策について事例研究を行う。当事例は複数の実事例を参考に、作成したものである+。

### 3.1　事例の概要

今日、不正アクセス対策は最も重要なセキュリティ投資の1つである。企業組織内LANがインターネットと接続され、外部（インターネット）側からの悪意あるアクセスの危機に晒されている。不正アクセス対策技術にはファイアウォール、プロキシサーバ、DMZ（非武装地帯）の構築、RADIUS（認証）サーバ、VPN等がある。

ファイアウォールは外部からのパケットを選択透過するものである。またプロキシサーバは代理サーバとも呼ばれ、内部クライアントに代わり外部とのアクセスを集中的に担当することにより、内部ネットワーク構成を隠蔽化する。DMZはWEBサーバ、DNSサーバ、メールサーバなどの外部向けサービスを担当するサーバ群を、インターネットとLANの中間地帯に置き、LANを防御するものである。最近注目されている対策としてRADIUS（認証）サーバによる、LANへのアクセス要求者に対する認証の強化がある。さらにVPNはIPSECという暗号化技術によりインターネットをLANのようにセキュア化する技術である。また不正アクセスを試みたり、サーバに障害を与えたりするウイルスも蔓延しており、ウイルス対策も重要である。

ここで従業員約300人の卸売会社A社を想定し、セキュリティ投資事例を考えよう。A社ではLAN内に各種サーバを設け、従業員間で情報共有化を進めている。さらにA社はインターネットを通じて広報のためホームページを公開する一方、従業員全員にインターネットによるメール交換機能を提供している。A社は外部アクセス制御対策として、既にファイアウォール、ルータ、DMZ、プロキシサーバを導入済である。またWEBサーバ、DNSサーバ、メールサーバについては内部LANと隔離したDMZを設けて配置している。さらに外部からのメールに対してはプロバイダのウイルス防御サービスを契約した。

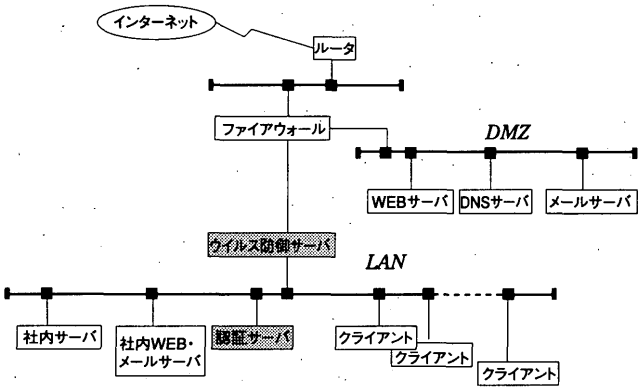
ところが最近、同業のX社が、不正アクセスにより社内サーバに蓄積していた顧客情報が漏洩し、インターネット上でやりとりされるという事件が起き、X社の信用が大きく傷ついてしまった。X社に話を聞いたところ、A社とほぼ同様のネットワーク構成であった。

危機感を抱いたA社では、コンサルタントに依頼してセキュリティ対策投資を実行することになった。コンサルタントはセキュリティポリシーを明確化した上で、システム部門及び一般従業員のセキュリティ意識を向上させることを第一とした上で、RADIUS（認証）サーバ及びウイルス防御サーバの設置が不可欠であると訴えた。

RADIUS（Remote Authentication Dial-In User Service）サーバは様々なサーバにおける利用者の認証情報を一元管理するしくみである。例えば従業員がインターネット経由で営業系サーバにリモート・アクセスしてきた場合、RADIUSサーバがアクセス可能か判断する。

一連のセキュリティ対策には約300万円が必要であるが、

**図表 4　事例 A 社のネットワーク構成**



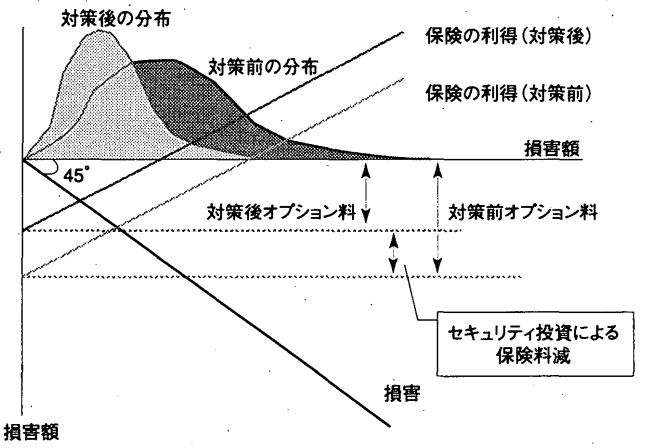

A 社のような中堅企業がそこまでセキュリティ対策投資を実施すべきか、様々な意見が出た。

このセキュリティ対策投資は果たして実施されるべきか、考察しよう。

まず概念として損害保険とオプションが基本的には同じものであるとの立場からはじめるべきだろう。理論的には損害保険は、危険資産に不確実な事象が生じたときに買い取りを求める権利であるので、「プットオプションの買い」に相当する。

ここで不正アクセスの損害を完全に補償する『セキュリティ保険』があったとしよう。実際には完全に補填する保険はないだろうが、議論を単純にするため、そう仮定しよう。我々は保険を得るためには保険料を支払う。保険料は補償額が大きくなりそうな場合は多額になる。

**図表 5　セキュリティ対策と「保険」**




保険会社の立場に立つと、セキュリティ対策前は予想される損害発生分布が幅広く損害額の期待値も高いが、セキュリティ対策を行なうと分布が狭くかつ期待値も小さくなる。したがって保険会社が A 社に対し求める保険料は、セキュリティ対策前よりセキュリティ対策後の方が安くなるだろう。この保険料の差がセキュリティ投資の価値に相当すると考えればよい。

では保険料はどうやって算定したらよいだろうか。ここでは厳密な料金計算ではなく、大まかな料金を求めることで十分である。リスクの特定と発生確率の見通しを FTA というツールで計算し、次に損害計算を行い、最後にシミュレーションによって、発生する可能性がある損害額の分布を求めてみよう。

## 3.2　リスク特定及び損害発生確率推計

まず HAZOP（Hazard and Operability studies）など定性的手法によってリスクを特定し、FTA（Fault Tree analysis）などツリー手法で確率を明らかにする。ここでは HAZOP は実施済として FTA を作成する段階から検討しよう。

### 3.2.1　FTA の作成

FTA（Fault Tree Analysis）を作成し、不正アクセスやウイルス発生といったトリガー行為が生じた場合、実際のシステム障害に至る確率を求める。FTA は最終的なリスク事象に対し、それが発生するための事象を経路だてて整理するものである。事象間の関係には「AND」（論理積）、「OR」（論理和）、「XOR」（排他的論理積）などが連結子として用いられ、確率関係を示すことができる。できれば FTA 作成前に、HAZOP 等によりリスク要因を明確化すると良い。

ここでは不正アクセスを、社内サーバに対する不正パケット侵入及び社内 WEB・メールサーバに対するウイルス侵入が生じた場合であると定義し、セキュリティ対策前及びセキュリティ対策後、実際のシステム障害に至る確率を検討しよう。（本稿末の参考図 1 参照）

### 3.2.2　セキュリティ対策前のリスク発生確率推計

はじめに対策前のリスク発生確率を求めよう。第 1 に不正パケット侵入意図行為が発生した場合のツリーを辿る。このときフィルタリングエラーが重なると、不正パケットは LAN 内に侵入する。1 回の侵入意図行為が試みられたとき、フィルタリングエラーが生じる確率 $P_3=0.370$ である。これは一般パスワード漏洩（確率 $P_1=0.3$）または管理ミス（確率 $P_2=0.1$）のいずれか（OR）が発生した場合の確率であり、$P_3=1-(1-P_2)(1-p_2)$ によって求められる。不正パケット侵入のとき、LAN 構成の漏洩（確率 $P_4=0.5$）が重なると、不正パケットは社内サーバに到達する（確率 $P_5=P_3\times P_4=0.185$）。不正パケットがサーバに到達したとき、認証エラー（確率 $P_6=0.5$）が重なると、社内サーバに不正パケットが侵入する（確率 $P_7=P_5\times P_6=0.093$）。第 2 にウイルス侵入のツリーについてみる。最初に個人パソコンにおいてネットワーク感染型ウィルス汚染が発生する。ウイルス

対策がなされない（確率 $P_8=0.5$）と、ウイルスは社内WEB・メールサーバに達する（確率 $P_9=0.5$）。

### 3.2.3　セキュリティ対策後のリスク発生確率推計

次に対策後のFTAをたどり確率を求める。第1にセキュリティ対策として認証サーバ及びウイルス防御サーバを設置し、適切な維持管理を行うとしよう。認証サーバ導入により、認証エラーの確率が $P_6=0.5$ から $P_6=0.2$ に改善されることから、社内サーバに不正パケットが侵入する確率 $P_7=P_5\times P_6=0.037$ に改善される。第2にウイルス防御サーバの設置された場合を考えよう。個人パソコンがネットワーク感染型ウィルスに汚染された場合、ウィルス対策がなされない確率 $P_8=0.01$ となり、ウィルスが社内WEB・メールサーバに達する確率は $P_9=0.01$ となる。

## 3.3　損害見積額の算定

最初に不正アクセス1件が生じた場合の損害計算をしよう。不正アクセスに伴い、漏洩、改ざん、破壊、サービス低下及び復旧費用が生じる。

**図表6　1件あたり損害額**

| | | 営業情報サーバ | WEB･メールサーバ | 合計 |
|---|---|---|---|---|
| 漏　洩 | 機会損失 | 信用喪失による失注<br>10,000,000円 | | 10,000,000円 |
| | 外部費用 | 得意先クレーム対応<br>200,000円 | | 200,000円 |
| 改ざん | 機会損失 | 誤情報によるロス<br>500,000円 | | 500,000円 |
| 破　壊 | 機会損失 | 情報喪失によるロス<br>200,000円 | | 200,000円 |
| サービス低下 | 機会損失 | | 情報活用力低下のロス<br>200,000円 | 200,000円 |
| 復旧費用 | | 復旧処理<br>300,000円 | 復旧処理<br>100,000円 | 400,000円 |

| | 可能損害額 | 想起確率 | 損害額 |
|---|---|---|---|
| サーバ不正アクセス | 11,500,000円 | 0.3 | 3,450,000円 |
| | 可能損害額 | 想起確率 | 損害額 |
| ウィルス侵入 | 300,000円 | 1 | 300,000円 |

社内サーバ不正アクセスの場合には、漏洩に伴い機会損失として信用喪失による失注10,000千円、得意先クレーム対応による外部費用200千円、改ざんに伴い誤った情報による営業ロス500千円、破壊に伴い情報喪失による営業ロス200千円、復旧費用300千円がかかると見られる。その合計は11,500千円であるが、不正アクセス者が悪意である可能性が0.3として、損害見通しは3,450千円である。

内部WEB・メールサーバへのウイルス侵入の場合は、情報活用力低下に伴うロス200千円、復旧費用　100千円の合計300千円の損害が見込まれる。

次に不正アクセスが年間何回発生し、毎年の損害額がどのように予想されるか計算しよう。FTAによってひとたび侵入意図行為やウイルス汚染パソコン持込が起きた場合、最終的な不正アクセスに結びつく確率は既に示している。ここで侵入意図行為やウイルス汚染パソコン持込が年間何回発生するのか、推定しなければならない。ここでは経営者及びシステム担当者が平均値と上限値をそれぞれ推定するものとする。上限値はいわゆる「2シグマ」すなわち正規分布を前提とするとき、全体の95%がその範囲内に入る数値を示すものとする。

ここでは、社内サーバ不正パケット侵入の試行頻度は年間で平均3回と考え、上限値を5回とみた。また社内LANへのウイルス汚染パソコン持ち込みは年間で平均5回として、上限値は10回とみた。

これら数字にもとづき、それぞれの年間損害額をセキュリティ対策前とセキュリティ対策後の見通しを計算し、さらに両者を合計する。その結果、対策前損害見通しの期待値は1,707千円（上限値3,096千円）、対策後損害見通しの期待値は398千円（上限値668千円）となる。なお標準偏差は「上限値＝平均＋2 $\sigma$」とみて計算すると、対策前 $\sigma=694$ 千円、対策後 $\sigma=135$ 千円となる。

**図表7　対策による損害額縮小**

社内サーバ不正パケット侵入

| | 試行頻度 | 対策前頻度 | 対策後頻度 |
|---|---|---|---|
| 期待値 | 3.000 | 0.278 | 0.111 |
| 上限値(95%) | 5.000 | 0.463 | 0.185 |

社内WEB・メールサーバ　ウィルス侵入

| | 試行頻度 | 対策前頻度 | 対策後頻度 |
|---|---|---|---|
| 期待値 | 5.000 | 2.500 | 0.050 |
| 上限値(95%) | 10.000 | 5.000 | 0.100 |

不正パケット損害額　　(千円)

| 損害単価 | 対策前損害見通し | 対策後損害見通し |
|---|---|---|
| 3,450 | 957 | 383 |
| 3,450 | 1,596 | 638 |

ウィルス侵入損害額

| 損害単価 | 対策前損害見通し | 対策後損害見通し |
|---|---|---|
| 300 | 750 | 15 |
| 300 | 1,500 | 30 |

損害額合計

| | 対策前損害見通し | 対策後損害見通し |
|---|---|---|
| 期待値 | 1,707 | 398 |
| 上限値(95%) | 3,096 | 668 |
| 標準偏差 | 694 | 135 |

## 3.4　リスクの可視化

次にリスクを可視化するためモンテカルロシミュレーションを行う。実際の進め方として、エクセル組み込み関数により擬似乱数を発生させることも可能であるが、ここでは専用ソフトの一つである「クリスタル・ボール」(㈱構造

計画研究所）を用いる。

### 3.4.1　シミュレーションの前提

まずセキュリティ投資の償却年数が3年間と考えて、この期間に生じる損失見通し額の現在価値を求めることとしよう。

1年目、2年目、3年目の損害期待値は様々な分布をとる確率変数である。「クリスタル・ボール」では確率分布として正規分布の他、対数正規分布、ポアソン分布などを想定できるが、ここではできるだけシンプルに考えるため、正規分布を想定する。

先に行った年間損害額推計から、セキュリティ対策前の場合、1年目、2年目、3年目共に期待値は1,707千円、標準偏差　694千円である。またセキュリティ対策を実施した場合、それぞれの期待値は398千円、標準偏差135千円に縮小する。ここで割引率＝0.1とし、1年目、2年目、3年目の損害を合計した対策前損害見通し、対策後損害見通しをそれぞれ割引現在価値求める。この割引現在価値もやはりこれは期待値（平均値）である。モンテカルロシミュレーションは期待値を含めた分布を可視化するものである。

この2つの期待値を予測対象として設定し、モンンテカルロシュミレーションを行い、対策前損害見通し、対策後損害見通しの現在価値がそれぞれどのような分布をとるか、検討しよう。

**図表8　対策前後の損害額割引価値**

対策前　（千円）

| | 1年 | 2年 | 3年 | |
|---|---|---|---|---|
| 損害期待値 | 1,707 | 1,707 | 1,707 | 対策前損害予想 |
| 標準偏差 | 694 | 694 | 694 | |
| 割引後損害 | 1,545 | 1,398 | 1,265 | 4,207 |

対策後

| | 1年 | 2年 | 3年 | |
|---|---|---|---|---|
| 損害期待値 | 398 | 398 | 398 | 対策後損害予想 |
| 標準偏差 | 135 | 135 | 135 | |
| 割引後損害 | 398 | 398 | 398 | 1,194 |
| 割引率 | 0.10 | | | |

対策効果

3,013

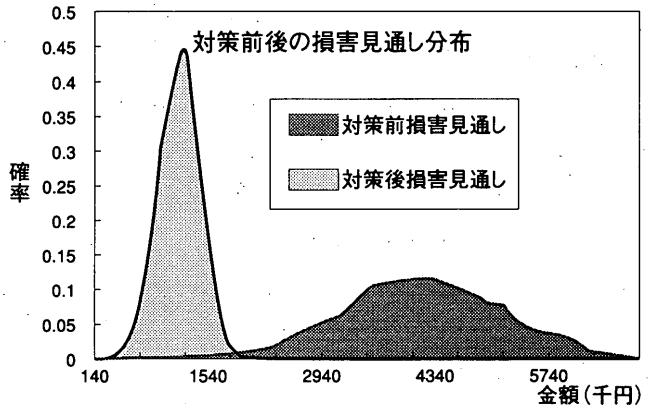
### 3.4.2　シミュレーション結果

10,000回の試行を行ったシミュレーションの結果は次の通りである。セキュリティ対策前の損害額の割引価値はほぼ正規分布に従い分布し、その期待値は4,225千円で標準偏差957千円となる。またセキュリティ対策後の損害額割引価値の分布もやはり正規分布のような形で期待値は1,195千円（標準偏差232千円）である。これ2つの分布を重ね合わせると図表10のような形になる。対策後は期待値が下がるのみでなく、標準偏差も大きく縮小することが確かめられる。

**図表9　モンテカルロシミュレーション結果**

| | 対策前 | 対策後 | 効果 |
|---|---|---|---|
| 試行回数 | 10,000 | 10,000 | |
| 期待値 | 4,245 | 1,195 | 3,050 |
| 標準偏差 | 957 | 232 | |
| 平均値＋1 σ | 5,202 | 1,427 | 3,775 |

**図表10　対策前後の損害見通し**




さてセキュリティ対策前の損害期待値すなわち保険受取額の期待値が4,245千円ということは、これが保険料（オプション料）に相当すると考えてよいだろうか。確かに、保険を購入する者も売る者の双方がリスク中立的な場合はそのとおりである。実際にオプション理論ではこうした仮定を設けるので保険料は4,225千円となる。しかし読者が保険会社だったら、この分布をみて期待値で保険を引き受けるだろうか。おそらくリスク見合い分を割増した保険料を求めるのではないだろうか。

現実の損害保険では保険会社はできるだけ多くの同種リスクを集めてきて、同種リスクのプール化により「大数の法則」から、リスク中立的に振舞うことができる。セキュリティ投資の場合は、1社毎にリスクの内容は異なる訳であり、保険会社といえどもリスク中立的に振舞うことは難しいだろう。リスク中立的な保険会社の場合、セキュリティ対策前の保険料は4,225千円、セキュリティ対策後の保険料は1,195千円で、両者の差額は約3,000千円がセキュリティ投資の効果となる。しかし保険業者がリスク回避的であるならば、保険料は期待値をかなり上回るものとなるだろう。あるリスク回避的な保険業者は損害発生額の分布を考え、保険支払額の分布を正規分布と考え、全体の84%がカバーされる価格（「平均値＋1 σ（標準偏差）」）に保険料を設定するかもしれない。このときセキュリティ対策前の保険料は5,202千円、セキュリティ対策後の保険料は1,427千円とな

り、両者の差額は約3,800千円となる。また別の会社は分布全体の90%を保険料によりカバーしようとするかもしれない。

理論的には不確実性を伴う損失見通しの評価はバリューアッツリスクとして整理されている。一般に損失の分布を考えるとき下側確率がpになる点を信頼水準がpのバリューアットリスク（Value at Risk＝VaR）と呼ぶ。信頼水準84%のバリューアットリスクとなる水準はセキュリティ対策前で5,202千円、対策後に1,427千円に相当する。また信頼水準が90%となる水準はセキュリティ対策前5,470千円、対策後1,492千円に相当する。

いかなる信頼水準を選ぶかにより損害保険の価値が変わってくる訳であるが、事務部門の役割として原資産並びに交換対象資産のリスクを可視化まで進めたならば、こうした貨幣的価値への変換は経営者の判断に委ねても良いだろう。

### 3.5 PDCAとBSC

投資により期待通りの成果を上げるには、それを使いこなすためのマネジメントサイクルすなわちPlan（計画）、Do（実行）、Check（検証）、Action（修正）の体制をしっかり構築しなければならない。セキュリティ対策の場合もサーバ導入などの設備投資のみで完結する訳ではない。パケットフィルタリング設定ミスや不適切なログ管理が放置されたままならリスクを減らすことは困難だろう。

セキュリティ投資効果を発揮させるためには、システム担当者は細心のサーバ管理を行い、一般の営業社員はパスワード管理の徹底、不用意なダウンロード防止、汚染パソコンの持ち込みを避けるなどの行動に努めなければならない。一方、顧客に対してもセキュリティ上、問題になる可能性がある事柄について、サービスレベルや危機対応指針を予め明らかにしておくことは、信用維持のために不可欠である。

PDCAのマネジメントに適したツールがBSCである。企業として明確なセキュリテイポリシーを設定し、これを財務、顧客、業務プロセス、学習と成長の各視点に展開し、従業員及び顧客に対し明確な方針及び目標を示す。またセキュリティオプションにおいては、価値算定の基礎としてFTAを用いたが、これは顧客、業務プロセス、学習と成長の視点が抜けていた。

CSF（Critical Success Factor＝戦略的目標）にもとづき業務プロセス及びシステム資源、人的資源の各分野においてコントロール可能なKGI（Key Goal Index＝業績評価指標）並びにKPI（Key Performance Indicator＝先行指標）を適切に設定し、その遂行状況をモニタリングしてゆくことが重要である。例えばユーザ部門の自己管理をCSFとして、そのための中間指標として例えばセキュリティ意識について質問表により定期的に確認することも必要だろう。（本稿末の参考図2参照）

BSC作成は計画の実行管理に力を発揮するが、そのためにはBSCを作ることで満足してしまわないように定期的に委員会等を通じて中間指標の達成度をフォローすることが重要である。

## 結　論

我々はセキュリティ投資の価値をセキュリティ対策前と後における2つのプットオプション（厳密には交換オプション）の価値の差として定式化した。また現実に近い事例を用い、セキュリティ投資の価値を算出するプロセスを例示した。その結果、再確認したポイントは次の通りである。

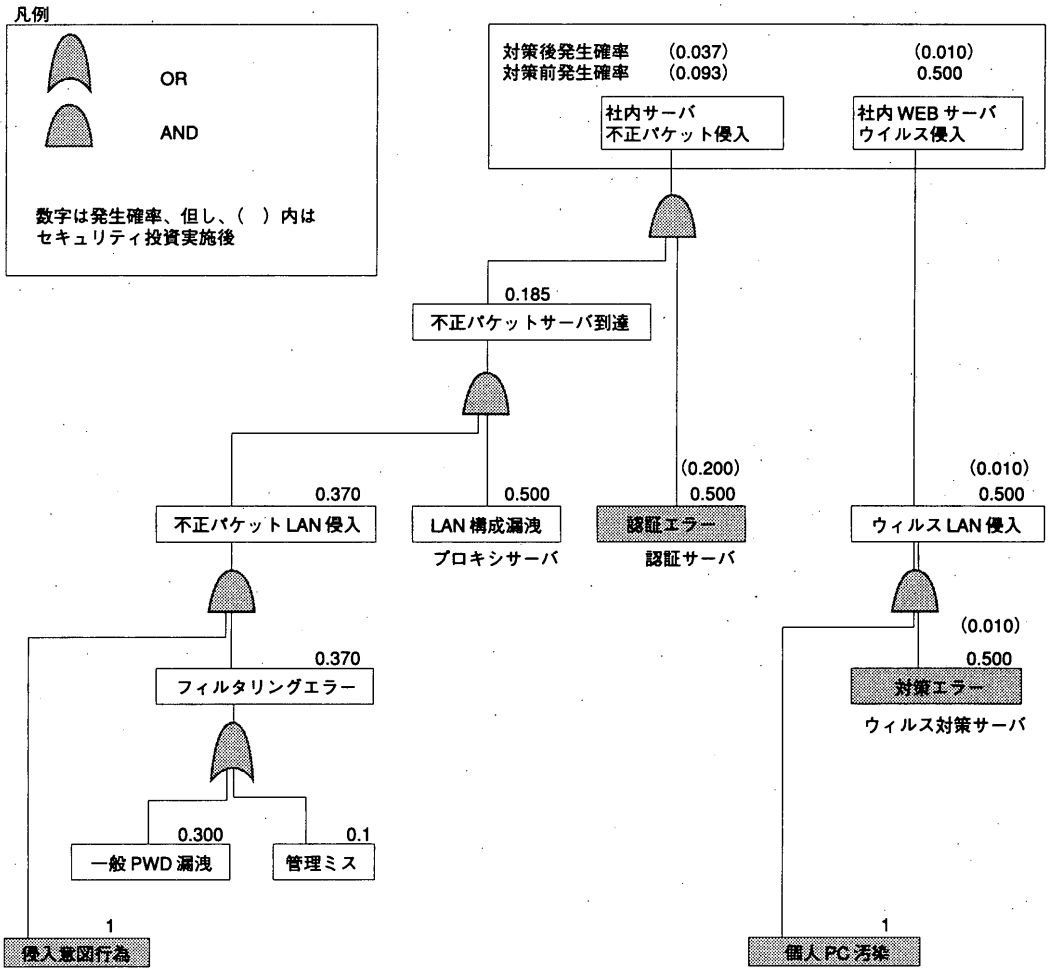
第1にセキュリティ投資の場合、解析法によりオプション価値を機械的に計算するのでなく、シミュレーションを活用し原資産並びに交換対象資産のリスクをできる限り正確に可視化することが肝要で、経営者が貨幣的物差しにしたがって経営判断するための材料を提示することに意味があることを確認した。

第2にオプション計算の前提として損害額算定のため、事例の性格によってHAZOP（Hazard and Operability studies）など定性的分析手法とFTA（Fault Tree analysis）などツリー分析手法を組み合わせて選択すべきである。

第3にバランストスコアカード（Balanced Scorecard＝以下BSC）の併用することで、リアルオプションの長所である、NPVとの整合的評価、不確実性を勘案した評価、シナリオ性ある計画立案などを生かし、パラメータの信頼性、モニタリングの困難さ等の課題を克服することが可能である。

セキュリティ投資評価に保険的要素を織り込むべきと提唱されているものの、セキュリティ対策保険の未普及から契約料率などを入手し字際に計算することは簡単ではない。本論の意義は、こうした中でリアルオプションにもとづき実務的に利用可能な評価法を提案した点にある。このときFTAなど既にSecurityROIの中でも指摘されているツールのみでなく、BSCを積極的に活用するなどの工夫により、実行管理の水準向上、より精度の高いボラティリティ推計等が可能になる。

**参考図1　FTA（Fault Tree Analysis）**




また今回のように具体的事例を提示することが、新たな意思決定手法の可能性を実務家に示すためのテンプレートとして意義があり、我々研究者の使命は多様な事例を提案し、実務家のフィードバックを得て、より実用的な形にすることであると考える。

## 謝　辞

本研究にあたり㈶企業活力研究所並びに㈲研究ネットワークに助成いただいた。

## 注記

[1] スコット・ベリナート（2004）によるとALE＝(R−E)+Tと定式化している。ただしR＝不正アクセスに伴う復旧費用、E＝セキュリティ投資により節減できた費用、T＝セキュリティ対策費用である。

セキュリティ障害が発生する確率は、実施するセキュリティ対策によって変化するため、こうした変化を反映させて「修正ALE」を求め、セキュリティ投資評価に反映すべきである。

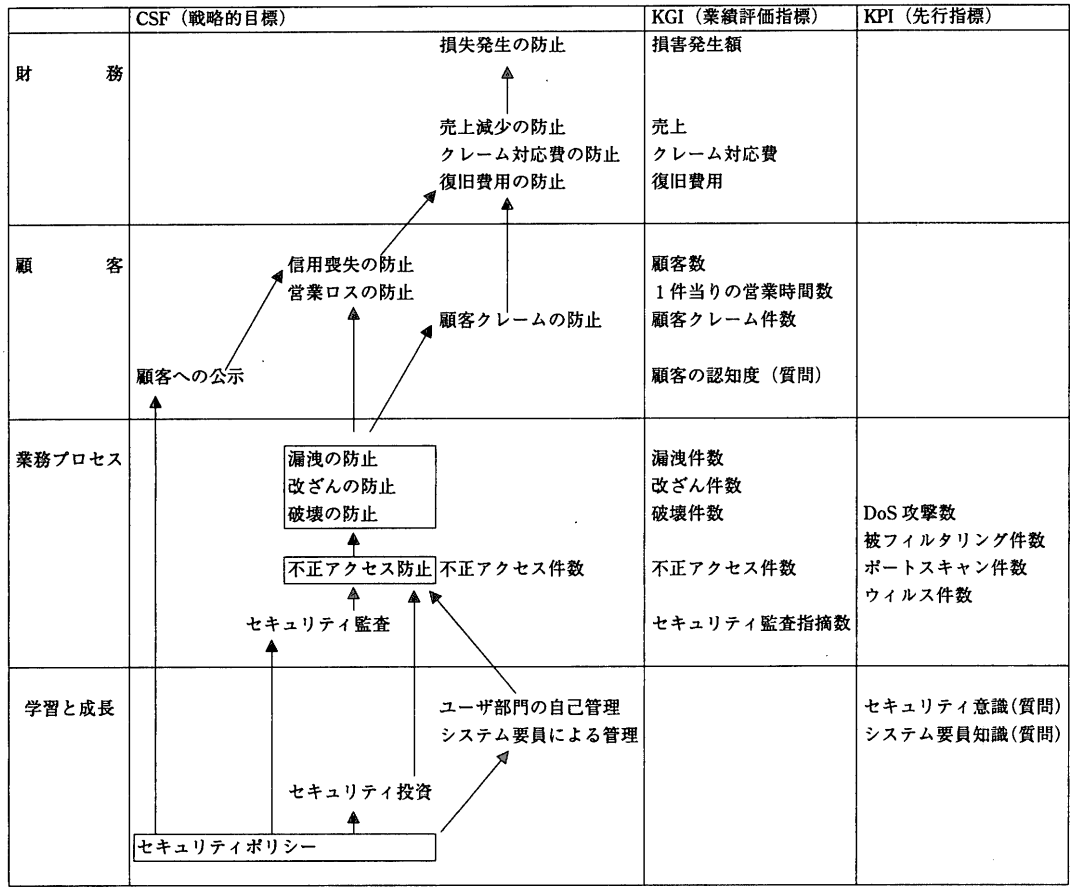
[2] 武田圭史（2003）「個人保護コンプライアンスと情報セキュリティ投資評価」，http://nikkei.hi-ho.ne.jp/accenture3/vol14/program1.html、2004年9月2日閲覧

[3] 日経新聞（2004年9月1日）によると、日本ユニシスと東京海上保険は、情報漏洩や外部からのウイルス攻撃を防ぐセキュリティシステムと事故発生時に備えた保険商品をセットにして売り込む。

また損保ジャパン、大塚商会、トレンドマイクロ、マイクロソフトなど9社は、情報漏洩防止ソリューション提供のための企業連合を結成した。その中で情報セキュリティシステム実装商品ごとに評価ポイントを設定し、ポイント合計を保険料・補償額に反映させる新たなセキュリティ保険の開発・提供に努める予定である。（大塚商会「ニュースリリース」2004年7月22日）

[4] Jaquith, A.（2002）は、とるべきセキュリティ対策手

**参考図2　BSCによるITセキュリティ投資推進**




（注）CSF＝Critical Success Factor、KGI＝Key Goal Index、KPI＝Key Performance Indicator

段が企業毎に多様であることを述べている。

5　オプションを含むデリバティブと伝統的保険との間には厳密には違いがあるとの考えもある。土方薫（2001）は次の違いを指摘している。

・支払条件：伝統的保険では損害の発生原因を特定し、相当因果関係を確認する。

・支払金額：保険は実損てん補の考えに立ち、損害額を上限とする。

6　ただし高度なセキュリティ投資を行っても完全にリスクを除去できる訳ではなく、発生確率が低く壊滅的な損害が生じる「まさかの場合」の可能性が残る。このリスク除去の判断にあたっては、オプションでなく社会における損害保険の加入を考慮するべきである。

7　白石高義はFTAにもとづく情報リスクマネジメント手法を提唱している。〔白石（1992），白石（2001）〕

## 参考文献

大規模プラント・ネットワーク・セキュリティ対策委員会（2000）「大規模プラント・ネットワーク・セキュリティについて」通商産業省

白石高義（1992）「情報セキュリティリスク波及分析の提案」『修道商学』32-2，pp39-64

白石高義（2001）「情報セキュリティの基本原理」http://www.fine.lett.hiroshima-u.ac.jp/011208/shiraishi.html，2004年12月20日閲覧

スコット・ベリナート（2002）「数字がセキュリティ投資を正当化する」『CIO Magazine』，2002年9月号，pp62-71

スコット・ベリナート（2004）「セキュリティ対策のROIを測る」『CSO Magazine』、vol. 3，オンライン版，http://www.cioj.com/contents/、2004年9月2日閲覧

総務省（2003）『平成15年版情報通信白書』ぎょうせい

土方薫（2001）『総解説保険デリバティブ』日本経済新聞社

平石次郎他（1998）『化学物質総合安全管理のためのリスクアセスメントハンドブック』丸善

松島桂樹(1999)『戦略的IT投資マネジメント』白桃書房

山田啓一・原田要之助・抜山勇（1997）『経営革新と情報セキュリティ』日科技連出版社

Amram, M., and N. Kulatilaka (1999), *Real Option: Managing Strategic Investment In Uncertain World*, Boston: Harvard

University Press

Benaroch, M., and R. J. Kauffman (1999) "A Case for Using Option Pricing Analysis to Evaluate Information Technology Project Investments", *Information Systems Research*, Vol 10, No1, pp70-86

Chatwin,R (2000) "Real options Valuation for E-Business : A Case Study", in Trigeogis, L,. (ed.) *Real options and Business Strategy*, London: Risk Books、

Copeland, Thomas, E., and Valadimir Antikarov (2001), *Real Options*, NY:Texere

Dos Santos, B.L., (1991), "Justifying Investment in New Information Technologies", *Journal of Management Information Systems*, Vol7, No4. Spring, p71-79

Evans, James R.,and David Olson (1999), *Introduction to Simulation and Risk Analysis*, NY: Prentice Hall,（邦訳『リスク分析・シミュレーション入門』服部正太監訳、構造計画研究所）

Jaquith,A. (2002), "The Securities of Applications: Not all Are Created Equal", @stake research report

Kaplan,Robert and David Norton (1996), *Balanced Scorecard*, Boston: Harvard Business School Press,（邦訳『バランススコアカード』吉川武夫訳，生産性出版

Moore,William T., (1998), *Real Options and Option Embedded Securities*, NY: Joh·Wiley&Sons, Inc.（邦訳『リアルオプションと金融デリバティブ』加藤敦訳、エコノミスト社）

Panayi,S., and L. Trigeogis (1998), "Multi-stage Real Options: The Case of Information Technologies and International Bank Expansion", *The Quarterly Review of Economics and Finance*, Vol38, pp675-692