『金融研究』（第21巻別冊第１号）所収論文の紹介

日本銀行金融研究所では、その研究成果を広く外部に公表することを狙いとして、『金融研究』[注1]を発行している。以下は、第21巻別冊第１号（平成14年６月発行）所収論文[注2]の要約を紹介したものである。

ＬＩＢＯＲマーケット・モデルのインプリメンテーションについて

―本邦の金利派生商品データを用いた具体例を基に―

石山幸太郎

本稿では、近年研究が進められているイールド・カーブ・モデルであるＬＩＢＯＲマーケット・モデルのインプリメンテーション方法について、本邦金利派生商品データを用いた具体例を使って検討を行うと共に、パラメータの推定事例を示す。また、最近の研究事例として、実際の市場で観測されるインプラド・ボラティリティのスマイルを、ジャンプ過程等を含むＬＩＢＯＲマーケット・モデルで説明する先行研究も適宜紹介する。

モンテカルロ法によるプライシングとリスク量の算出について

―正規乱数を用いる場合の適切な実装方法の考察―

石川達也／内田善彦

金融派生商品（以下、派生商品）のプライシングやVaRなどのリスク量の算出において、モンテカルロ法によるシミュレーションは、有効な計算手法の１つである。複雑なペイオフを持つ派生商品のプライシングや、複雑な損益曲線を持つポートフォリオのリスク量計算では、モンテカルロ法以外の選択肢がない場合も少なくない。このため、多くの金融機関では、何らかの形でモンテカルロ法を実務で利用している。しかし、モンテカルロ法の具体的な実装方法について詳細に検討し妥当な方法を示しているような文献は少ない。実務上でも十分な検討がなされているケースは多くないのが実態であると思われる。こうした観点から、本稿では、正規乱数を用いたモンテカルロ法による派生商品のプライシングやリスク量計算の結果を基に、適切な実装方法の考察を行う。

商品流動性リスクの計量化に関する一考察（その２）

―内生的流動性リスクを考慮したストレス・テスト―

吉藤　茂／大嶽文伸

1997年10月のアジア通貨危機や1998年８月

（注１）『金融研究』所収論文の内容や意見は執筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。なお、『金融研究』第21巻別冊第１号（定価1,050円）は、ときわ総合サービス（株）より販売（詳しくは、巻末の「刊行物一覧」をご覧下さい）。

（注２）所収論文は、日本銀行金融研究所ホームページ（http: //www.imes.boj.or.jp/）「発表論文等」コーナーにも掲載されています。

のロシア危機以来、商品流動性リスクがクローズ・アップされ、その計量化に向けさまざまな取り組みがなされている。本稿では、アジア通貨危機およびロシア危機発生時における実証分析から、リスク管理上のポイントを整理したうえで、ストレス・テストに焦点を絞った商品流動性リスク計量化手法を提案する。

本稿での成果は、以下の２点である。（１）実証分析から、リスク管理上の留意すべきポイントとして、（ⅰ）ファット・テールな状況の顕現化、（ⅱ）相関関係の崩壊（流動性危機の伝播および流動性への逃避現象）、（ⅲ）保有期間長期化に伴い相場の変動性や相関関係の変化が大きくなることの３点を定量的に示した。（２）外生的流動性リスクに焦点を絞り、（ⅰ）ファット・テール調整、（ⅱ）相関崩壊を組み込んだストレス・テスト手法を内生的流動性リスクにも対応可能なモデルへと拡張した。具体的には、各国株価指数先物市場の取引高データから市場ごとのマーケット・インパクト関数を導出し、同関数をファット・テール調整係数に組み込むことで内生的流動性リスクに対応した。

わが国における労働分配率についての一考察

須合智広／西崎健司

本稿では、1960年代以降における民間法人企業部門の労働分配率の動向について分析した。わが国の労働分配率は40年間にわたって上昇トレンドを持ち、景気循環の過程でこの周りを変動しているようにみえる。本稿では、分配率の趨勢的変動が定常状態への移行動学過程を、短期的な変動が移行動学からの短期的な乖離の調整過程をそれぞれ反映していると想定し、実質賃金と労働の平均生産性の誤差修正モデルを用いた実証分析を行った。得られた結論は、次のとおりである。（１）わが国の労働分配率は、資本深化を反映した労働の平均生産性の上昇とともに上昇する特徴を持つ。これは、労働と資本の代替の弾力性が１より小さいことを反映している。（２）短期的には、分配率は景気循環と逆方向に動く。これは、資本と労働の調整費用の存在等により、労働の平均生産性の順循環的な変動が実質賃金の順循環的変動と比べて大きいという特徴を反映している。（３）第１次石油ショック後の労働分配率の急激な上昇は、中期的な均衡労働分配率の上方シフトを伴うものであったが、1990年代の労働分配率の上昇は、均衡労働分配率の上方シフトを伴うものではなかったことが統計的に確認された。

名目ＧＤＰ推計における金融仲介サービスの計測法について

長野哲平

金融機関は金融仲介サービスの提供を通じて、大きな役割をはたしているにもかかわらず、国民経済計算体系（以下ＳＮＡ）では金融仲介サービスが捕捉されておらず、ＧＤＰが過小評価されているとの批判が長らく存在してきた。ＳＮＡの新しい国際基準である93ＳＮＡ（System of National Accounts 1993）では、このような批判を踏まえ、ＦＩＳＩＭ（financial intermediation services indirectly measured）という方法で金融仲介サービスを捕捉しＧＤＰに加算することを提唱しているが、同手法はさまざまな問題点を内在している。本稿では、（１）ＦＩＳＩＭの理論的な問題点を指摘し、（２）こうした問題点を回避する手法としてユーザー・コスト・アプローチを提示したうえで、両手法に基づき、わが国における金融仲介サービスの計測を行い、

結果を比較する。その結果、名目金利がゼロ近傍まで低下した1998年度以降については、ＦＩＳＩＭによる計測結果とユーザー・コスト・アプローチによる計測結果には大きな乖離が認められ、名目ＧＤＰ成長率にも無視できない差が生じることが示された。

インターネットを利用した金融サービスの安全性について

松本　勉／岩下直行

インターネットの急速な拡大を背景に、インターネットを利用して金融サービスを提供する金融機関が増えている。インターネットは世界中の利用者に開かれたネットワークであるため、利便性と効率性が高い反面、セキュリティ上のさまざまな脅威が存在することが指摘されている。インターネットを経由して金融サービスを提供する際には、金融機関もこうした脅威に対する適切な対策を講じておく必要がある。

インターネット・バンキングを提供する金融機関が最も重視しなければならないセキュリティ対策は、無権限者による成りすましなどの攻撃によって、正規の利用者や金融機関自身の財産が被害を受けないようにすることにある。そのような効果を実現するうえで鍵となるのは、インターネット上での利用者の認証方式である。そこで、本稿では、現在のインターネット・バンキングの多くで利用されている、ＳＳＬ、パスワード、乱数表を組み合わせた認証方式にスポットを当てて、考えられる攻撃法について分析した。

その結果、現在の認証方式は、システムの設定次第では、情報の一部が漏洩した場合に成りすましの攻撃を受けるとか、乱数表の情報の一部を推定されるといったセキュリティ侵害のリスクが存在することがわかった。こうしたリスクは、現時点では深刻な問題とはいえないものの、将来、インターネット・バンキングがより広範に利用されるようになると、実際の被害につながりかねないものと思われる。わが国の金融機関が、今後、インターネットによる金融サービスを拡大していくためには、こうしたセキュリティ上の問題点について、適切に対処していくことが望ましいといえよう。

金融分野におけるＰＫＩ：技術的課題と研究・標準化動向

宇根正志

ＰＫＩ（public key infrastructure）は、認証機関が発行する公開鍵証明書を用いて、公開鍵暗号の鍵ペアとその持ち主を結び付けるとともに、鍵ペアの適切な管理を保証する仕組みである。金融分野におけるＰＫＩの利用は、認証サービスの専業会社が発行した公開鍵証明書を、インターネット・バンキングにおける本人確認手段として活用することから始まった。

最近では、金融機関自身が認証機関となると同時に、業界内にルート認証機関を設ける高度な形態のＰＫＩを構築し、企業間電子商取引等における電子認証のインフラとして活用しようとする動きが拡大している。また、証明書ポリシー（ＣＰ）・認証実施規程（ＣＰＳ）の作成指針として、米国国内標準ＡＮＳ　X9.79-1が策定されるなど、金融機関が認証機関として情報セキュリティ対策を検討する際に活用できる制度的枠組みや各種標準等が整備されつつある。

しかし、現時点では、金融機関が参画して構築を進めているＰＫＩにおいては、情報セキュリティ対策に関する情報が必ずしも十分には公表されておらず、認証機関の信頼性等を外部か

ら評価することが困難な状況にあるように思われる。金融機関が認証機関としてＰＫＩの運営に参画していくに当たっては、適切な情報セキュリティ対策を講じたうえで、利用者の信頼を向上させるために情報セキュリティ対策の開示等を行っていくことが重要であると考えられる。

本稿では、まずＰＫＩ関連技術の研究・標準化動向を紹介したうえで、金融機関が参画する主なＰＫＩの構造や情報セキュリティ対策の概要について紹介する。次に、今後、金融機関が認証機関としてＰＫＩの運営に参画していくうえでの課題を説明し、考えられる対応策について説明する。

ＲＳＡ署名方式の安全性を巡る研究動向について

齊藤真弓

インターネット等オープンなネットワーク上において安全なデータ交信を行う手段の１つとして、デジタル署名方式が活用されつつある。デジタル署名方式は、公開鍵暗号技術を利用してデータ通信者の本人確認や交信データの一貫性確認を可能とするものであり、現在、事実上の標準として幅広く利用されている署名方式はＲＳＡ署名方式である。

ＲＳＡ署名方式は、1978年に提案されて以来、その安全な利用方法に関する研究が続けられてきた。ＲＳＡ署名方式に対する主な攻撃としては、（１）公開鍵の素因数分解によって秘密鍵を導出するタイプと、（２）秘密鍵を導出することなく署名偽造を行うタイプの２つが挙げられる。特に、上記（２）の攻撃を想定した場合、メッセージをそのまま秘密鍵によって変換し署名を生成するという方法は安全ではなく、メッセージをハッシュ関数等で変換したうえで、秘密鍵によって署名を生成する必要があることが知られている。

こうした研究成果を踏まえ、ＲＳＡ署名方式を安全に利用するためにはメッセージにどのような変換を施せばよいかに関する研究が行われている。近年では、一定の数学的仮定のもとで安全性が証明可能であり、かつ、高い実用性を有するＲＳＡ署名方式の利用方法が提案されている。それらの中で、現在最も注目を集めているのがＲＳＡ-ＰＳＳ署名方式である。ＲＳＡ-ＰＳＳ署名方式は、国際標準や業界標準等への採用が検討されており、今後幅広い分野で利用されるようになることも考えられる。

本稿では、ＲＳＡ署名方式からＲＳＡ-ＰＳＳ署名方式に至る研究動向について、署名変換データの生成方法を中心に安全性の観点から説明したうえで、ＲＳＡ-ＰＳＳ署名方式を巡る国際標準化動向等について紹介する。