

『金融研究』（第24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24巻別冊第1号（平成17年7月発行）所収論文^{（注2）}の要約を紹介したものである。

マリアバン解析を用いたオプションのリスク指標の数値計算について

今村 悟／内田善彦／高橋明彦

本稿では、マリアバン解析とモンテカルロ法を用い、原資産価格が拡散過程に従うときのプレーンバニラ、デジタル、アジア型の各オプションのリスク指標（デルタ、ガンマ）に対する効率的計算方法を検討した。特に、Fournié *et al.* [1999] の方法を拡張し、プレーンバニラ・オプションのガンマなどに対してはより効率的な方法を、アジア型オプションのガンマに対しては新しい計算方法をそれぞれ考案した。また、価格の変動を記述する確率微分方程式についても、彼らが用いた例（対数正規過程）と共に、CEV（constant elasticity of variance）過程に対し、われわれの方法の有効性を検証、確認した。さらに、対数正規過程に関する既存の結果に関しても明示されていなかった証明を示した。

与信ポートフォリオの信用リスクの解析的な評価方法：

極限損失分布およびグラニュラリティ調整を軸に

安藤美孝

与信ポートフォリオの信用リスクの計量は、計算負荷の高いモンテカルロ・シミュレーションに頼ることが一般的であるが、近年、その近似的な解析表現を得る方法が幾つか提案されている。特に、極限損失分布およびグラニュラリティ調整を用いる方法は、幅広い水準のパラメータで精度の高い近似を与える有力な方法である。本稿では、多くの信用リスク計量モデルを含む一般的なモデルの枠組みで、同手法を用いた信用リスクの解析的な計算手法を解説する。また、実務での利用を前提に、1ファクターのマートン型モデルの枠組みでの信用リスクの具体的な近似解析表現を導出し、近似精度を数値検証する。さらに、マルチ・ファクター・モデルの枠組みでの信用リスクの評価、証券化商品の経済的資本の解析表現も解説する。

（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24巻別冊第1号（定価1,050円）は、ときわ総合サービス（株）より販売されている（詳しくは、巻末の「刊行物一覧」を参照されたい）。

（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る。

デジタル署名の長期利用について

田村裕子／宇根正志／岩下直行／
松本 勉／松浦幹太／佐々木良一

電子政府の推進や民間での電子文書の利用に関する法整備が進むにつれて、紙文書から電子文書への移行が進んでいる。電子文書は、紙文書とは異なり、痕跡を残さずに内容を改ざんすることが容易であるため、電子文書の一貫性確保、本人認証等を行うために、今後、デジタル署名の利用が拡大していくものと考えられる。ただし、デジタル署名が付与された電子文書の一貫性確認を長期的に実施しようとした場合、署名検証に必要なデータの損失や署名生成鍵の危殆化といった問題が発生し得る。署名の長期利用のためには、そうした問題に対して、予め対策を講じておく必要がある。これらの論点については、日本銀行金融研究所が開催した第5回

情報セキュリティ・シンポジウムにおいて問題提起され、筆者たちが、その後さらに考察を深めるための研究会を開催してきた。本稿は、同研究会における研究成果を取りまとめたものである。

本稿では、署名の長期利用をどのように位置づけるかについて議論し、署名検証を行う際の手続、問題点、既存の主な対策技術を整理する。そのうえで、署名の長期利用に関する具体例として、ETSI TS 101 733の署名トークンについて考察を行う。この署名トークンは、PKIやタイムスタンプ等の既存のインフラによって実装可能であり、IETFやW3Cの技術仕様においても採用されているほか、本署名トークンを利用した商用システムも既に提案されている。本稿では、署名再検証を可能とするための十分条件を導出することにより、署名トークンを今後利用していくうえで留意すべき点や今後の課題を示す。