『金融研究』(第18巻別冊第1号)所収論文の紹介(注1)

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2)を発行している。以下は、第18巻別冊第1号(平成11年9月発行)所収論文の要約を紹介したものである。

一般化状態空間モデルによる分散変動時系列の解析

北川源四郎／佐藤整尚

確率的ボラティリティ・モデルを非線形状態空間モデルで表現する方法を拡張するとトレンド、定常変動と分散変動(ボラティリティ)を同時に考慮し、これらの成分に分解することができる。このようなボラティリティの変動を考慮したモデルのAICは通常のトレンドモデル等よりも著しく小さく、変動するボラティリティを明示的に表現することによってよいモデルが得られることを示している。このモデルに基づく日経225データの解析結果では、トレンドの階差と局所的な分散との間に明らかな関連がみられる。そこで、本稿ではさらにトレンドと分散の関係を仮定したモデル化を行った。日経225データに関しては、このモデル化によってさらにAICが減少し、両成分間の関係が確認できた。一方、為替データに関しては、トレンドとボラティリティ間の明らかな関係は検出できなかった。

Triple DESを巡る最近の標準化動向について

谷口文一／太田和夫／大久保美也子

金融業界では、通信ネットワークを利用した金融取引の安全性を確保するために、暗号技術を広範に使用している。特に、DES(Data Encryption Standard)は、金融業界におけるニーズを背景として米国で開発された共通鍵暗号方式であり、米国政府標準に選定されたこと等を背景に、世界中で使用されてきた。しかし、近年、コンピュータの計算能力向上とコスト低廉化に伴い、DESの安全性低下が明らかとなってきている。このため、DESの後継として、DESを3回繰り返すことにより強度を高めた暗号であるTriple DESへの移行の動きが見られ始めている。

1998年に、米国の金融業界ではTriple DESに関する国内標準を作成した。これに伴い、Triple DESを米国政府標準や金融業務向けの国際標準に認定しようとする動きもある。こうした標準化作業の過程において、Triple DESの安全性に関する様々な検討が加えられている。本

(注1)本稿の内容は、日本銀行ホームページ(http://www.boj.or.jp/)「論文」コーナーにも掲載されています。

(注2)『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18巻別冊第1号(定価1,050円)は、ときわ総合サービス(株)(本『日本銀行調査月報』刊行物一覧を参照)より販売。

稿では、こうしたTriple DES標準化の動きを概観しつつ、その安全性を巡る議論を紹介する。

ＲＳＡ署名に対する新しい攻撃法の提案について

— Coron-Naccache-Sternの攻撃法 —

宇根正志

ＲＳＡ方式は、素因数分解問題の困難性に依拠した公開鍵暗号方式であり、データ守秘（ＲＳＡ暗号）とデジタル署名（ＲＳＡ署名）の両方の機能を有している。ＲＳＡ方式のアルゴリズム自体に対しては、これまで現実的な脅威となる攻撃法が提案されていないことから、安全性の高い公開鍵暗号方式として、金融分野をはじめとする幅広い分野で利用されている。

Gemplus社（フランス）のCoron、Naccache、ルーバン・カトリック大学（ベルギー）のSternは、1999年４月、ＲＳＡ署名に対する新しい攻撃法を発表した。本攻撃法は、一定条件を満足するメッセージの署名を利用して別のメッセージの署名を偽造するというものであり、公開鍵を直接素因数分解するよりも少ない計算量で署名偽造が可能となる。

Coron-Naccache-Sternの攻撃法で注目されるのは、本攻撃法がＲＳＡ署名を利用したデジタル署名方式の国際標準ISO/IEC 9796-2に適用できるという点である。本国際標準は、主にＩＣカード上での実装を想定して策定されており、署名からメッセージを復元できる仕組みとなっている。本攻撃法は、こうしたデジタル署名方式の特徴点を巧みに利用したものであり、ＲＳＡ署名のアルゴリズムを直接攻撃するものではない。Coronらの研究成果は、暗号アルゴリズム自体の安全性だけでなく、その利用方法を含めた総合的な評価の必要性を強く示唆するものである。

本稿では、まず、これまでのＲＳＡ署名の安全性に関する主な研究成果を整理し、ISO/IEC 9796の概要を説明する。その上で、Coron-Naccache-Sternの攻撃法について説明し、情報セキュリティ技術の標準化を担当するISO/IEC JTC1/SC27の対応状況やＩＣカード等の標準規格への影響について説明する。

インターネット等のネットワークを使った個人間の電子マネー送金方法について

— 電子メールによる電子マネー送付の可能性 —

中山靖司／赤鹿秀樹／森畠秀実

ネットワーク環境における電子マネーの支払いは、通常、支払者と受取者がインターネット等のネットワークによってオンラインで接続され、数回の情報のやり取りをリアルタイムで行うことによって実現されている。受取者が電子商店等の場合には、通常、いつでも顧客からの取引の申し出を受付けられるようにサーバーをインターネットに常時接続しているため、電子マネーの支払いの申し出に対しても、リアルタイムにレスポンスでき、顧客である支払者の都合によっていつでも取引を行うことが可能と考えて差し支えない。しかしながら、個人間で電子マネーの譲渡を行おうとした場合に、電子マネーの受取者となる一般の利用者は、インターネットを利用する度にパソコン等の機器をダイヤルアップで接続していることが多く、いつでも電子マネーの受け取りができるような待機状態にあるとはいえない。したがって、このような取引を行うことは現実的には運用上困難と考えられる。

そこで、支払者と受取者がネットワークでオ

ンライン接続されている必要がなく、リアルタイムで通信を行わなくても、例えば電子メールに情報を添付することなどにより電子マネーを支払う（送金する）ことが可能な方法をいくつか提案する。また、それらの方法のうち、最も実装が容易であると考えられる方法について、ＩＣカードを用いて実際に実装を試みた過程で生じた問題点およびその対策についてまとめる。

社債流通価格にインプライされている期待デフォルト確率の信用リスク・プライシング・モデルによる推定

―改良型ジャロウ・ランド・ターンブル・モデルを用いて―

家田　明

近年、理論的な発展が著しい信用リスクのプライシング・モデルを活用すれば、社債流通市場で観測される価格から期待デフォルト確率という具体的な数字を抽出することができる。本稿では、信用リスク・プライシング・モデルの一つとして、Kijima and Komoribayashi［1998］が示した“改良型ジャロウ・ランド・ターンブル・モデル”を採用して、本邦の社債流通価格にインプライされている格付ごとの期待デフォルト確率の推定を行った。

その結果、Ｂ格、ＣＣＣ格のデフォルト確率が非常に高い水準にあることを確認した。この点に関しては、Ｂ格、ＣＣＣ格のサンプルが少ないため断定的な結論を導くことは難しいが、これらの格付銘柄に対して市場が格付機関よりも一層厳しい評価を下している等の背景があると推測できる。また、株価情報から推定した期待デフォルト確率と比較すると、本稿のサンプルではＢＢＢ格以上では、概ね同様の傾向があることもわかった。

社債流通価格にインプライされている期待デフォルト確率の信用リスク・プライシング・モデルによる推定（２）

―ロングスタッフとシュワルツのモデルを用いて―

家田　明／吉羽要直

本稿では、信用リスク・プライシング・モデルの一つであるロングスタッフとシュワルツのモデルを用いて、本邦の社債流通価格にインプライされている個別企業の期待デフォルト確率を推定する。

推定の結果、期待デフォルト確率は、①個別企業でなく格付ごとの平均的な水準をみると、格付が低いほど大きくなる傾向があり、格付機関の評価と市場の評価が概ね整合的であること、②同一格付内でもかなりばらつきがあり、格付という離散的な指標では捉え切れない連続的な信用度を市場の評価が織込んでいる可能性があることがわかった。

また、別のタイプの信用リスク・プライシング・モデルである改良型ジャロウ・ランド・ターンブル・モデル（家田［1999］）での期待デフォルト確率の推定結果と比較し、各格付の平均的な期待デフォルト確率が両モデルとも同様の傾向があることを示す。さらに、両モデルの長所・短所にも触れ、分析目的に応じてモデルを選択する必要があること等を指摘する。