

『金融研究』（第22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22巻別冊第1号（平成15年6月発行）所収論文^{（注2）}の要約を紹介したものである。

デジタル署名の長期的な利用とその安全性について

松本 勉／岩下直行

インターネットの急速な発達と高性能なパーソナル・コンピュータの普及に伴い、さまざまな産業分野、行政手続の分野において、紙の文書をデジタル化された文書（電子文書）に置き換える動きが加速している。紙の文書から電子文書への移行により、効率性や利便性が向上する一方、電子文書は、何も工夫をしなければ、痕跡を残すことなく内容を変更したり、全く同じものを複製したりすることが極めて容易にできるため、偽造や改ざんといったセキュリティ侵害のリスクが高まることも懸念されている。その対策として、本人認証、完全性確保、否認防止の効力を持つデジタル署名を利用することが有効と考えられている。

ところが、通常のデジタル署名が付与された電子文書を長期保管した場合、デジタル署名の効力が維持できないという問題が発生してしまう。この問題に対処するためには、ヒステリシス署名など、署名生成機能の危殆化対策の施さ

れたデジタル署名方式を利用したり、デジタル署名に加えてデジタル・タイムスタンプを併用したり、原本性保証装置を利用したりするなどの対策を検討する必要がある。

本稿では、デジタル署名を付与した電子文書を、署名・捺印のある紙の文書の代替物として実務に利用するために解決されなければならない課題として、デジタル署名の長期的な利用の問題を取り上げ、問題の所在を明らかにするとともに、今後の改善の方向性について検討する。

デジタル署名生成用秘密鍵の漏洩を巡る問題とその対策

宇根正志

デジタル署名方式は、公開鍵暗号技術に基づいてデータ生成者やデータの一貫性を確認する技術である。インターネット上における電子商取引等を安全に行うためには通信相手や受信データの認証が不可欠であり、デジタル署名方式はそうした機能を果たす技術として活用されている。

デジタル署名方式を利用する際には、署名生

（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22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」をご覧ください）。

（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る。

成用秘密鍵を秘密に管理することが前提となっている。したがって、秘密鍵は内部のデータを物理的・論理的に保護する機構をもつICカード等のハードウェアに格納されることが望ましい。しかし、そうした場合においても、鍵管理方法の欠陥に加え、ハードウェア自体の欠陥や署名方式の欠陥によって秘密鍵が漏洩する可能性は否定できない。

通常のデジタル署名方式を利用している限り、漏洩した秘密鍵によって署名が偽造されるとその検知は不可能であり、なりすまし等の不正が行われるおそれがある。こうした不正が発生すると、署名を再度生成しなおす必要が出てくるほか、当該電子認証サービスの信頼が大きく損なわれると考えられる。電子認証サービスを提供していく際には、秘密鍵漏洩の影響を十分考慮し、必要な対策を検討していくことが望まれる。

本稿では、まず、デジタル署名生成用の秘密鍵管理に関するPKIの役割と問題点、秘密鍵漏洩の可能性とその影響について整理する。そのうえで、秘密鍵の漏洩を前提とした署名偽造への対策技術について説明し、それらの効果、実現方法、想定環境、セキュリティ要件の比較を行う。

ジャンプ拡散過程を用いたオプション価格付けモデルについて

久田祥史

本稿では、ジャンプ拡散過程を用いたオプション価格付けモデル（ジャンプ拡散モデル）の解説を行う。ジャンプ拡散モデルは、ブラック＝ショールズ・モデルに代表されるオプション価格付けモデルと異なり、原資産価格の不連続な変動を取り入れることができるうえ、

市場で観察されるオプション価格をよりうまく表現することができるため、近年再び注目されている。

本稿では、代表的なジャンプ拡散モデルであるマートン・モデルを中心に、マートン・モデル以外のジャンプ拡散モデルを含めてサーベイを行い、ジャンプ拡散モデルの整理を行う。また、日経平均株価指数オプションの市場データに基づき、マートン・モデルのキャリブレーションを行い、ジャンプ拡散モデルの特徴を検証する。

JASDAQ市場のスプレッド比較 — オーダー・ドリブン対マーケット・メイキング —

宇野 淳／柴田 舞／嶋谷 毅／
清水季子／万年佐知子

本稿は、JASDAQ市場で取引されているマーケット・メイク銘柄とオーダー・ドリブン銘柄を対象に、取引システムが価格形成に与える影響を分析する。マーケット・メイク銘柄は、マーケット・メイカーの介在によりいつでも取引が可能であるという特徴を有する反面、投資家が負担する取引コストはオーダー・ドリブン銘柄に比較して高いことがわかった。また、マーケット・メイク銘柄では、市場に提示された最良気配よりもよい価格での約定が、注文3件に1件の割合で生じていたことも確認された。これは、米国のNASDAQやニューヨーク証券取引所（NYSE）でも観察された現象で、顧客からの注文をマーケット・メイカーの気配に反映させる義務がないことなどから生じるパターンと同様のものと考えられる。マーケット・メイカーの行動は、従来のマーケット・メイカー・モデルが想定するような気配提示による競争ではなく、特定顧客との関係を重視する戦略をとっている可能性を示唆するものである。JASDAQ

AQは現在、市場制度の見直しを進めているが、参加者に公平な約定機会を与えるという面での改善が図られるかについて、継続的に評価していく必要がある。

わが国株式投資信託の需要構造について

— 動学的資産選択に基づく設定・解約行動分析 —

田中寛厚／馬場直彦

本稿では、わが国株式投資信託に関する投資家の設定・解約行動について理論・実証両面から分析を試みた。理論モデルとしては、取引コスト存在下での投資家の異時点間を通じた動学的意思決定モデルを採用した。これにより、投信売買時に発生する設定・解約コストや収益率に関する不確実性が、各期ごとの独立した意思決定を前提とした通常のCAPMでは想定されない「投資決定を先送りするオプション」価値を変動させることを通じ、投資行動に影響を与えることが明らかになる。比較静学によれば、不確実性の増大は、設定率のみならず解約率をも引き下げる方向に作用し、数%の販売手数料や信託財産留保金は、投資家の最適な投信保有量を数～10%のオーダーで変化させ得る。

さらに、個別株式投信の日次の設定・解約額についてのパネル・データ分析を通じ、わが国株式投信の需要行動に上述した動学的最適化の特徴が確認できるか実証的に検討した。その結果、サンプル期間中(2000年8月～2001年7月)は、概ねモデルが想定する合理的な投資行動が実践されている可能性を確認した。この結果によれば、近年の株式投信の低迷は、収益率の悪化、不確実性の増大、手数料の高止まりといっ

た環境下で、投資家が設定を合理的に先送りしていることにより生じていると解釈することが可能である。

株式保有構成と企業価値

— コーポレート・ガバナンスに関する一考察 —

西崎健司／倉澤資成

本稿では、株式保有構成と企業価値の関係について分析することにより、株主によるコーポレート・ガバナンス(企業統治)について経済学的視点から考察を行った。

具体的には、わが国における株式保有構成の特徴点と中・長期的動向を概観し、理論的には外部の大口株主による株式保有比率上昇は企業価値に対して正負いずれの影響も与え得ることを示したうえで、わが国において外部の大口株主による株式保有比率の上昇や株式保有構成の変化が企業価値に与えた影響について実証分析を行った。

実証分析の結果、わが国において、(1)外部の大口株主はモニタリング活動等を通じて企業価値に対して正の影響を与えていること、(2)個人の保有比率は企業価値に対して負の影響を与えており、モニタリング活動に関するフリー・ライダー問題の存在が示唆されること、(3)1990年代以降、非金融法人企業による株式持合いが企業価値に負の影響を与えている可能性が高いこと、(4)1990年代にわが国株式市場におけるプレゼンスが著しく拡大した海外部門(外国人投資家)については、投資家・株主として国内投資家に勝るパフォーマンスであったことなどが示された。