日本銀行金融研究所
Institute for Monetary and Economic Studies, Bank of Japan

金研ニュースレター

2018年3月

金融研究所（Institute for Monetary and Economic Studies, IMES）は、1982年10月に日本銀行創立100周年を記念して、日本銀行の内部組織の1つとして設立されました。金融研究所は、金融経済の理論、制度、歴史に関する研究を行っているほか、金融経済に関する歴史的資料の収集・保存・公開を行っています。

ハイライト

第19回情報セキュリティ・シンポジウム

「金研ニュースレター」は、日本銀行金融研究所が主催するイベントなどを、幅広い読者を対象に、タイムリーにお知らせすることを通じて、金融研究所の活動を紹介することを目的としています。

第19回情報セキュリティ・シンポジウム

日本銀行金融研究所情報技術研究センター（CITECS）は、3月1日、日本銀行本店において、「量子コンピュータが金融サービスのセキュリティに与える影響」と題する第19回情報セキュリティ・シンポジウムを開催しました。

【量子コンピュータとは】
量子力学の性質を演算処理に応用したコンピュータ。従来のコンピュータよりも高速な演算処理が可能とみられている。

開会挨拶を行う鎌田康一郎 情報技術研究センター長（日本銀行） 写真：野瀬勝一
※各参加者の所属は、本シンポジウム開催時点のものです（以下同じ）。

当日の会場の様子 写真：野瀬勝一

キーノート・スピーチを行う松本勉教授（横浜国立大学大学院）　写真：野瀬勝一

今回のシンポジウムには、情報セキュリティ技術に関わる金融機関、官公庁関係者のほか、大学教員・研究者、システム開発・運用に携わる技術者等、約 120 名が参加しました。

キーノート・スピーチにおいて、松本教授（横浜国立大学大学院）は、金融分野における環境変化を踏まえつつ、シンポジウムで量子コンピュータを取り上げた理由や問題意識について講演しました。

講演1として、東京大学先端科学技術研究センターの中村教授は、量子コンピュータの動作原理や実装について解説したほか、各国の研究機関における開発動向等について発表しました。

「超伝導量子コンピュータ」と題して発表する中村泰信教授（東京大学、左）と、「量子コンピュータの商用化動向」と題して発表する小野寺民也氏（日本アイ・ビー・エム、右）　写真：野瀬勝一

「量子ゲート型コンピュータが暗号に与える影響と対策」と題して発表する清藤武暢（日本銀行、左）と「耐量子計算機暗号の標準化動向」と題して発表する高木剛教授（東京大学大学院、右）　写真：野瀬勝一

講演 2 として、日本アイ・ビー・エム東京基礎研究所の小野寺氏は、量子コンピュータの商用化動向について発表しました。IBMにおける量子コンピュータの開発状況に加え、それらが金融機関や製造業において活用されている事例に言及し、実際に商用化が進んでいる現実について説明しました。

講演 3 として、金融研究所の清藤が、量子コンピュータの中でも任意の問題を高速に解くことが可能な量子ゲート型コンピュータによる暗号解読の方法について説明しました。そのうえで、金融サービスで利用されている各種の国際標準等への影響と対応のあり方について発表しました。

講演4として、東京大学大学院の高木教授は、量子コンピュータを用いた暗号解読に対抗する手段としての耐量子計算機暗号について発表しました。また、米国政府が耐量子計算機暗号の標準化を進めていることや、わが国や欧州における耐量子計算機暗号の利用に向けた調査等について説明しました。

モデレータとパネリスト(左から順に):松本勉教授(横浜国立大学大学院)、四方順司教授(横浜国立大学大学院)、鎌田敬介氏(金融 ISAC)、中山広樹氏(三井住友銀行)、山本英生氏(NTT データ) 写真:野瀬勝一

パネルディスカッションでは、「量子コンピュータの脅威に対して金融機関が検討すべき対策とは」と題して、耐量子計算機暗号への移行の方法や金融機関が移行すべき時期等について、4 名のパネリストによる討議が行われました。会場の参加者も討論に加わり、活発な議論が展開されました。

シンポジウム当日の資料等については、金融研究所ホームページの以下のサイトに掲載しておりますのでご参照ください。

https://www.imes.boj.or.jp/citecs/symp/19/

金研ニュースレター 2018 年 3 月

日本銀行金融研究所(IMES)
〒103-8660 東京都中央区日本橋本石町 2-1-1
TEL:03-3279-1111(大代表)
FAX:03-3510-1265
E-mail:imes.journals-info@boj.or.jp
ホームページ:https://www.imes.boj.or.jp/index.html

※日本銀行金融研究所による最近の研究成果物については、以下をご覧ください。

日本銀行金融研究所による最近の研究成果物

金融研究所ディスカッション・ペーパー・シリーズ

No. 2018-J-4 杉浦志織、「新たな事業形態の登場と法制度の対応について:ライドシェア・サービスに関する労働法上の論点を中心に」、2018 年 3 月

No. 2018-J-3 大橋和彦、「マイナス金利環境におけるファイナンス:課題と研究の潮流」、2018 年 2 月

No. 2018-J-2 清藤武暢、四方順司、「量子コンピュータが共通鍵暗号の安全性に与える影響」、2018 年 1 月

No. 2018-J-1 「ワークショップ『債務契約における会計情報の役割』の模様」、2018 年 1 月

No. 2017-E-12 "The Effect of Bank Monitoring on the Demand for Earnings Quality in Bond Contracts" by Akinobu Shuto, Norio Kitagawa, Naoki Futaesaku, December 2017

No. 2017-E-11 "Market Concentration and Sectoral Inflation under Imperfect Common Knowledge" by Ryo Kato, Tatsushi Okuda, December 2017

No. 2017-J-18 菅沼健司、山田哲也、「マイナス金利を考慮したフォワードレート・モデルと市場の金利見通し」、2017 年 12 月

No. 2017-J-17 首藤昭信、伊藤広大、二重作直毅、本馬朝子、「債務契約における会計情報の役割:先行研究のサーベイとわが国の研究課題」、2017 年 12 月

No. 2017-E-10 "Trend Inflation and Evolving Inflation Dynamics: A Bayesian GMM Analysis of the Generalized New Keynesian Phillips Curve" by Yasufumi Gemma, Takushi Kurozumi, Mototsugu Shintani, November 2017

No. 2017-J-16 中村啓佑、「OAuth2.0 に対する脅威と対策:金融オープン API の一段の有効活用に向けて」、2017 年 11 月

No. 2017-J-15 宇根正志、廣川勝久、「モバイル端末による金融サービスの安全性を高めるために:セキュア・エレメント等の活用」、2017 年 10 月

No. 2017-J-14 「『金融政策:教訓と課題』2017 年国際コンファランスの模様」、2017 年 10 月

金融研究 第 37 巻第 1 号（2018 年 1 月発行）

- 「第 18 回情報セキュリティ・シンポジウム『新たな金融サービスを支える高機能暗号』の模様」
- 芦原聡介、清藤武暢、「共通鍵暗号型の検索可能暗号の処理性能について」
- 太田和夫、「共通鍵暗号による秘匿検索暗号のセキュリティ」
- 沖野健一、「分散台帳技術のセキュリティ要件:銀行口座振替処理への適用」
- 左光　敦、「P2P レンディングの仕組みと法規制:英国の P2P レンディング規制を中心に」