



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

2021 年 10 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

本人確認、認証、PBI

スマホ・マルウェア

マイナンバーカード

デジタル署名

アジャイル開発でのセキュリティ確保

「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 22 回情報セキュリティ・シンポジウム

スマートフォンは日々の暮らしを支えるコミュニケーション手段だけでなく、様々なデジタルサービスを楽しむための必須デバイスとなっています。金融サービスもその 1 つであり、預金や証券などの金融資産の取引・管理サービスが提供されているだけでなく、本人確認や認証、デジタル署名などで個人情報を扱う重要な役割も担っています。

金融研究所の情報技術研究センター (CITECS) では、「スマートフォンの利用にかかるセキュリティ」をテーマとしたシンポジウムを 2021 年 9 月 10 日に開催しました。

シンポジウムでは、スマートフォン上で提供される金融サービスの拡大に伴って増加している様々な脅威や、スマートフォンを巡るセキュリティの研究動向、今後のセキュリティ対応のあり方に関して、4 件の講演とパネル・ディスカッションを行いました。

金融機関関係者、スマートフォンを活用した金融サービスを提供する事業者等の実務者、研究者、システム開発・運用に携わる技術者等、約 200 名に参加いただきました。ニュースレターではその概要を紹介し、詳細な報告は下記リンク先で後日公表致します。報告資料は掲載済みです。

https://www.imes.boj.or.jp/jp/conference/citecs/22sec_sympo.html

講演 1 では、高橋健太主管研究員(株式会社日立製作所)が、スマートフォン上で金融サービスを提供する際に用いられている本人確認や認証の現状や、安全性・利便性の向上に役立つ生体認証の最新の研究動向を紹介しました。例えば、認証の都度、デバイス内部で生体情報から鍵を生成して使用する PBI (Public Biometric Infrastructure) が解説されました。PBI は、利便性を確保しつつ生体情報の漏洩を防ぐ技術として注目されています。

講演 2 では、本間輝彰エキスパート(KDDI 株式会社)が、スマートフォンを対象としたマルウェア、いわゆるスマホ・マルウェアに関する最新の攻撃手法や対策技術の動向を紹介しました。近年では、フィッシングやサービス仕様の脆弱性を狙う攻撃が主流となっています。こうした攻撃に対しては、技術面の対策や利用者へのセキュリティ啓発だけでは十分ではありません。利用者からのパスワード漏洩はあり得るものだという前提のもとで、いかに対策技術を整備するかが重要と指摘されました。

講演 3 では、大塚玲教授(情報セキュリティ大学院大学、金融研究所国内客員研究員)が、マイナンバーカードの機能をスマートフォンに搭載する事例を取り上げ、そこで用いられている主なセキュリティ対策機能の仕組みを紹介しました。近年のスマートフォンには高度なセキュリティ対策機能が備わっています。スマホ・マルウェアによる攻撃に対抗しつつ、安全な金融サービスを提供していくうえで、こうした機能を活用していくことの必要性が指摘されました。

講演 4 では、磯部光平研究員(セコム株式会社)が、スマートフォン上で金融サービスを提供する際のリスク管理に関する留意点を説明しました。スマートフォンに標準搭載されているセキュリティ対策機能は、必ずしも期待通りに動作しない可能性があります。スマートフォンのセキュリティ対策機能は自社での検証が難しいため、金融サービス提供の前に第三者によって検証されることができるような体制を整え、十分な検証を踏まえたうえでサービス提供を開始するような枠組み作りが紹介されました。

パネル・ディスカッションでは、金融サービスにおける利便性とセキュリティのバランス、他社とのサービス連携に伴うリスク、アジャイル開発*でのセキュリティ確保に関する留意点などについて議論が交わされました。

利便性とセキュリティをバランスさせるうえでは、ビジネス設計部門とセキュリティ部門が密接なコミュニケーションをとる必要が訴えられました。サービス連携に関しては、事業者間でリスクの認識に差異が生じ、セキュリティ対策が適切に実施されない可能性があるとの指摘がなされました。

アジャイル開発については、看過されがちなセキュリティへの意識付けだけでなく、セキュリティ技術者を開発過程に加えることの重要性が述べられました。また、金融サービス運用開始後にセキュリティの問題が発覚する場合もあることや、サービス内容だけでなくセキュリティ対策も常に見直しを行い続ける運用体制の構築が必要と指摘されました。

* アジャイル開発とは、迅速にソフトウェアを開発するための技法の1つ。従来から行われてきたウォーターフォール開発が、予めソフトウェアなどの全機能に関する要件定義や設計を綿密に行ってから開発に入るのに対し、アジャイル開発では、機能単位の小さなサイクルで、計画から設計・開発・テストまでの工程を繰り返すことにより開発が進められます。



(所属はシンポジウム開催時点)

金研ニュースレター 2021 年 10 月

※本誌に関する照会は、日本銀行金融研究所までお寄せください。

無断での転載・複製はご遠慮ください。

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. 2021-J-8** 田村裕子、「チャージ型決済の実現方法とそのセキュリティについて」、2021 年 9 月
- No. 2021-J-7** 豊蔵力、「暗号資産の保有に係る会計上の取扱いに関する考察—会計マナー・ツリーを用いたアプローチから—」、2021 年 9 月
- No. 2021-E-10** “The Power of Central Bank Balance Sheets” by Athanasios Orphanides, August 2021
- No. 2021-E-9** “Monetary Policy over the Lifecycle” by R. Anton Braun and Daisuke Ikeda, August 2021
- No. 2021-J-6** 神尾英克、森田泰子、「1960 年代末における国際収支に対する認識と金融政策：金融政策の転換前後における日本銀行の視点を中心に」、2021 年 8 月
- No. 2021-E-8** “Adapting to the New Normal: Perspectives and Policy Challenges after the COVID-19 Pandemic Summary of the 2021 BOJ-IMES Conference” by Takuji Fueki, Ken Matsushita, Ichiro Muto, Fumitaka Nakamura, and Shunichi Yoneyama, July 2021
- No. 2021-E-7** “Inflation Expectations and Central Bank Communication with Unknown Prior” by Tatsushi Okuda and Tomohiro Tsuruga, July 2021
- No. 2021-J-5** 『『ニューノーマルへの適応：COVID-19 後の展望と政策課題』2021 年国際コンファレンスの模様』、2021 年 7 月
- No. 2021-E-6** “Monetary Policy Shocks and the Employment of Young, Middle-Aged, and Old Workers” by Fumitaka Nakamura, Nao Sudo, and Yu Sugisaki, June 2021
- No. 2021-E-5** “Recent Trends on Research and Development of Quantum Computers and Standardization of Post-Quantum Cryptography” by Kazutoshi Kan and Masashi Une, June 2021
- No. 2021-J-4** 大塚玲、「ブロックチェーンを利用した暗号資産の安全性と匿名性：原理と限界」、2021 年 6 月

金融研究 第40巻第3号 (2021 年 7 月発行)

- 飯田高、「市場におけるルールと私的組織：市場ガバナンスに関する試論」
- 加藤大輔、五島圭一、「有価証券報告書のテキスト分析：経営者による将来見通しの開示と将来業績」
- 磯部光平、宇根正志、「スマートフォン等のスマート・デバイスにおけるセキュリティ：プラットフォーム化によるリスクの現状と展望」
- 菅和聖、「機械学習システムの脆弱性とセキュリティ・リスク：『障害モード』による分類と今後へのインプリケーション」
- 松本英彦、「新興国における外貨準備の蓄積の費用・便益について」