IMES DISCUSSION PAPER SERIES

情報セキュリティ・シンポジウム（第25回）の模様：
金融分野におけるセキュリティの潮流
CITECS設立20周年記念

Discussion Paper No. 2025-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

1. はじめに

日本銀行金融研究所・情報技術研究センター（Center for Information Technology Studies：CITECS）は、設立 20 周年を記念して、2025 年 3 月 6 日、「金融分野におけるセキュリティの潮流」をテーマとした第 25 回情報セキュリティ・シンポジウムを開催した。

近年、インターネットやスマートフォンなど情報通信技術の急速な普及を背景に、フィンテックと言われる金融サービスと情報通信技術を結びつけたさまざまな革新的な動きがみられている。さらには、人工知能（artificial intelligence：AI）技術の急速な進展が金融サービスに新たな可能性をもたらそうとしている。

一方、こうした変化に伴い、新たなセキュリティ面での課題も顕在化している。CITECS では、金融分野におけるセキュリティ面での課題への対応を研究面から支援すべく、これまでさまざまな調査研究を行ってきた。そこで、本シンポジウムでは、CITECS における情報セキュリティ研究の 20 年を振り返るとともに、近年関心が高まっている、量子耐性を有するシステム、AI、デジタル決済といったテーマについて講演と対談を行い、今後のセキュリティ対策について考察を行った。

当日は、金融機関やフィンテック企業などの実務家、システム開発・運用に携わる技術者、研究者など約 200 名がオンラインで参加した。本稿では、以下に示したプログラムに沿って、講演と対談の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

【第 25 回情報セキュリティ・シンポジウムのプログラム】

- 基調講演「情報技術研究センター（CITECS）20 年のあゆみ」
  金融研究所情報技術研究センター長　鈴木淳人
- 講演「金融高度化センターの活動 ―高度化センター20 周年 WS の内容を中心に―」
  金融機構局金融高度化センター長　須藤 直
- 講演「量子耐性を有するシステムの実現に向けた金融分野での取組み」
  金融研究所参事役　宇根正志

[1] 文中の講演者やパネリストの所属および肩書きは、シンポジウム開催時点のものである。また、本稿において示された意見はすべて発言者個人に属し、その所属する組織の公式見解を示すものではない。また、本シンポジウムでの講演の資料等については、日本銀行金融研究所のサイト（https://www.imes.boj.or.jp/jp/conference/citecs/25sympo/25sec_sympo.html）を参照されたい。

- 講演×対談「AIがもたらすリスクに対するセキュリティ」
  金融研究所情報技術研究センター企画役　菅 和聖
  情報セキュリティ大学院大学教授　大塚 玲
- 講演×対談「さまざまな決済スキームとそのセキュリティ」
  金融研究所情報技術研究センター企画役　田村裕子
  筑波大学システム情報系教授　面 和成
- 講演「金融分野における今後のセキュリティ対策～シンポジウム総括を兼ねて～」
  京都大学公共政策大学院教授　岩下直行

2. 基調講演「情報技術研究センター（CITECS）20 年のあゆみ」

鈴木は、この 20 年を振り返り、CITECS の設立経緯やこれまでの研究活動等について、次のとおり講演した。

（1）CITECS の設立経緯

日本銀行は、1980 年代から暗号技術・情報セキュリティについて研究を行ってきた。1988 年に稼働した日銀ネットに共通鍵暗号 DES（Data Encryption Standard）を搭載したこともあり、当初はユーザの視点から暗号アルゴリズムの安全性について研究を行っていた。その後、インターネットの普及を背景に、調査研究の対象を理論研究から応用に広げ、金融サービスのセキュリティ対策全般について検討を行うこととなった。例えば、1999 年に開催した第 2 回情報セキュリティ・シンポジウムでは、キャッシュカード取引のセキュリティが低下していることを指摘し、より安全性の高い方式への移行を推奨していた。

しかしながら、金融業界における対応は進まず、2000 年代中盤には、偽造キャッシュカードを用いた預金の不正引出しが社会問題となった。そのため、日本銀行は、情報セキュリティに関する研究体制の強化とより積極的な情報発信を企図して、2005 年 4 月に CITECS を設立することとした。CITECS は、金融界・学界・IT 実務家間の架け橋となり、ひいては金融業界における情報システムの技術革新に貢献していくことを目標に活動を開始した。

（2）CITECS の活動

CITECS では、金融業界が情報化社会において直面する新たな課題について調査研究を行っており、その内容を論文等として公表してきた。また、情報セキュリティ・セミナーや情報セキュリティ・シンポジウムの開催を通して、最新の研究動向などについて情報発信を行ってきた。

情報処理推進機構が 20 年前に公表した「情報セキュリティ 10 大脅威」には

Web アプリケーションの脆弱性による情報漏洩、マルウェアによる情報漏洩、フィッシング詐欺が挙げられており、いまもなお脅威として認識されているものが少なくない。このように情報セキュリティにかかる課題には、変わらないものと新しいものが混在しており、その調査研究には知見の蓄積と知識の吸収が必要となる。実際、1998 年に開催した第 1 回情報セキュリティ・シンポジウムでは、電子マネー、暗号アルゴリズムの移行、公開鍵暗号の安全性などを取り上げており、これらはいまも CITECS における主テーマとなっている。

CITECS における研究テーマは幅広く、暗号理論、決済・電子現金、認証・生体認証、人工物メトリクス、暗号アルゴリズム移行、ハードウェア、ブロックチェーン、AI セキュリティ・セーフティなどがある。本日は、このうち、暗号アルゴリズムの移行、AI セキュリティ・セーフティ、決済・電子現金を取り上げ、それぞれに関する最新の研究内容について研究スタッフから紹介する。

イ．暗号アルゴリズムの移行

暗号アルゴリズムの移行にかかる課題整理は、古くて新しい研究領域であり、過去の知見のもとに常に新しい課題への対応が必要とされている。約 30 年前には、共通鍵暗号である DES の安全性低下を受け、AES（Advanced Encryption Standard）への移行に向けた検討が行われた。また、2005 年頃には、当時広く利用されていた鍵長を 1,024 ビットとする RSA 暗号などが十分な安全性をもたなくなることが指摘され、2010 年に向けて暗号アルゴリズムの移行が進められた。移行対象は共通鍵暗号、公開鍵暗号、ハッシュ関数であり影響範囲が広かったことから、移行にかかる問題は暗号アルゴリズムの 2010 年問題とも呼ばれた。さらに、現在は量子コンピュータによるリスク対応について検討が必要となってきており、本日は、従来の暗号から耐量子計算機暗号（post-quantum cryptography：PQC）への移行に向けた課題等について整理した内容を紹介する。

ロ．AI セキュリティ

AI セキュリティは、まったく新しい研究領域である。近年の急激な AI 技術の急速な発展を受け、そのセキュリティについての研究の重要性も高まっている。一般的に AI 技術の進化が知られるようになったのは、おそらく、囲碁 AI である AlphaGo[2]がプロ棋士に勝利した 2015 年頃であるように思う。CITECS ではその頃から AI がもたらすリスクに対するセキュリティについて研究を開始してきた。近年は生成 AI の台頭により、セキュリティ研究の重要性が増していることから、今後も高い関心をもって研究活動を行っていく予定である。

[2] AlphaGo は、Google Inc.の登録商標である。

ハ. 決済・電子現金

決済・電子現金は、古くて新しい研究領域とまったく新しい研究領域の組み合わせである。CITECS 設立前より、金融研究所では電子現金に関する研究を行っており、金融研究所から公表した情報技術分野の第 1 号論文も電子現金に関するものであった。当時は世界各国でデジタル決済に関する実証実験が盛んに行われた時期であり、金融研究所も民間企業とともに研究開発を行っていた。本日は、古くて新しい研究内容として、電子現金について再検討した内容を報告する。

また、2008 年以降は、スマートフォンの普及によりデジタル決済の形態が大きく変化したほか、ビットコインの登場によりブロックチェーン技術が注目を集めた。こうした分野は比較的新しい研究領域であり、最新の研究動向をフォローしながらそのセキュリティについて検討していくことが重要であろう。

3. 講演「金融高度化センターの活動について―高度化センター20 周年 WS の内容を中心に―」

須藤は、本年 1 月に開催された金融高度化センター20 周年ワークショップの内容、および、金融機関におけるデジタル技術の実装に向けた課題について、次のとおり講演した。

(1) 金融高度化センターについて

金融高度化センターは、金融機関における先進的な金融技術や金融仲介機能の向上のための取組状況等に関する調査・研究・公表、セミナーやワークショップの開催を通じた金融機関との対話を行っている部署である。こうした活動を通じて、金融機関が金融仲介機能をより有効に発揮していく取組みを支援している。2005 年に、日本銀行におけるプルーデンス政策を、それまでの危機管理重視から、金融システムの安定を確保しつつ、公正な競争を通じて金融の高度化を支援する方向へ切り替えるという方針のもとで設立され、CITECS と同じく本年 20 周年を迎える。

(2) わが国におけるデジタル技術の進展

この 20 年で、デジタル技術は大きく発展し、金融分野においてもデジタル技術の活用が広がってきている。こうしたなか、金融高度化センターでは、2025 年 1 月、デジタル化とわが国の金融の未来と題したワークショップを開催した。デジタル技術を活用しながらどのように金融サービスを効率化・高度化できるのか、また、デジタル技術を活用しながらどのように金融サービスをこれまで

通り安定的に提供できるのかという論点について、講演とパネル・ディスカッションを行った。当日の講演資料は、日本銀行のホームページに掲載している[3]。

イ．デジタル技術活用に伴うメリットとリスクの認識

デジタル化にかかる便益については、大規模データと高い計算能力の組み合わせによる便益と、大規模言語モデルの活用のもとで人とコンピュータ、あるいは人と人との対話が変化することによる便益の 2 つがあるように思われる。この結果、個々の顧客ニーズに即した付加価値の高い金融サービスを、より幅広くかつタイムリーに提供できるようになる可能性がある。もっとも、デジタル化の進展に伴い、リスクも拡大している可能性があることには留意が必要である。例えば、2010 年のフラッシュ・クラッシュは、高速・高頻度取引などのアルゴリズム取引が市場の振幅を大きくした可能性がある事例として知られている。

便益に関するデジタル化の最適なペースは、自社の態勢をみながら自分で選べる一方、リスクに関するデジタル化の最適なペースは、自社の外側でどのようなペースでデジタル化が進むかという点にも影響を受ける。そのため、外のペースが思っていたよりも速く、例えば、不正行為が急に高度化してしまうような場合には、これまで提供できていた付加価値の提供が難しくなる可能性もある。

ロ．デジタル技術と生産性

生成 AI が生産性に与える経路については、人が従事している業務を AI に委ねるという労働力の代替である「自動化」と、労働者の生産性を高める「支援」という 2 つがあると指摘されることがある。金融については、自動化されうる業務と支援されうる業務の双方の割合が高いとする調査報告もあり、生成 AI の影響が大きい業種であるとみられる。

先行き 10 年における労働生産性の伸び率の見通しについては、年率 0.05%程度から 1%を超えるものまで、さまざまな見方が示されている。こうした見通しの違いの要因の 1 つは、生成 AI によって被支援業務がどう変化するかといった評価の違いによるものであり、業務への実装の巧拙によって労働生産性への影響が異なるものになる可能性も示唆している。

---

[3] https://www.boj.or.jp/finsys/c_aft/aft250213a.htm

（3）わが国におけるデジタル技術の進展

金融機関が、メリットとリスクのバランスを取り、かつ、デジタル技術の実装を着実に生産性の上昇につなげるには、①業務の見直し、②リスク統制、③人材育成、④関係者の協調などがある。これらは社内リソースの配分にかかる課題となるため、経営トップによるコミットメントが必要になる。

主要国の労働生産性を比較すると、日本の生産性はやや伸び悩んでいる。特に、1990 年代以降の成長率の鈍化が顕著である。こうした生産性の違いを生む背景としては、資本ストックの量などに加え、技術を使いこなせているかという点も重要であると考えられる。デジタル技術の進歩と、今後の実装がこうした状況を大きく打開するかどうかは非常に重要な論点であり、金融高度化センターとして高い関心をもっている。今後も、金融技術やリスク管理手法の高度化という観点から有益な情報を発信していきたい。

4. 講演「量子耐性を有するシステムの実現に向けた金融分野での取組み」

宇根は、PQC への移行に向けた金融分野での取り組みについて、次のように講演した。

（1）PQC 移行対応の特徴

これまでの 20 年間において、金融分野では、サービス提供環境が大きく変化した。ネットワークで結ばれる対象システムが拡大したほか、ステークホルダーも大きく多様化が進んだ。こうした環境のもとで、安全で信頼される金融サービスを提供するには、暗号技術が必要不可欠である。RSA や楕円曲線暗号などの現在主流となっている公開鍵暗号技術は、暗号解読が可能な性能を有する量子コンピュータ（cryptographically relevant quantum computer：CRQC）によって効率的に解読できることが知られており、金融分野では CRQC によるリスクへの対応について検討が進められている。

CRQC の実現時期については、専門家の間でも意見が分かれており、不確実性が極めて大きい。外部機関によるアンケート調査によれば、現在広く使用されている RSA 暗号（鍵サイズ 2,048 ビット）を 1 時間で解読できる CRQC について、その実現の可能性が 5 割以上となる時期が 2039 年までと回答した有識者は約 6 割であったほか、2044 年までと回答した有識者は約 9 割であった。これまでは、コンピュータの計算処理能力の向上スピードを予測して、暗号鍵のサイズを伸長するという対応を行うことが可能であったが、CRQC によるリスクが顕現化する時期の見通しは非常に難しいというのが実情となっている。

PQC への暗号移行がこれまでより難しいとの見方が多いが、その理由の 1 つに、対応すべき範囲が不透明であることが挙げられる。対応方針や責任分担などの調整を要するステークホルダーが多く、対応に時間がかかることが懸念されている。また、脅威が顕現化する時期が不透明であることにより、いつまでに対応すべきかといったタイムラインが未確定であることも課題の 1 つとなっている。さらに、実装技術が十分に成熟していないことから、移行対応後に脆弱性が見つかるリスクも懸念されている。これらの課題を考慮すれば、PQC 移行にかかる検討には早期に着手することが必要であるといえる。

（2）PQC 対応をめぐるこれまでの動き

イ．海外のセキュリティ当局の動き

米国は、2035 年までに CRQC にかかるリスクを最小化させる方針を掲げている。現在、2035 年末までに、既存の連邦政府標準暗号（公開鍵暗号）の使用を禁止する方針についてパブリックコメントが公表されている。また、国立標準技術研究所は数年前から PQC の標準化作業を進めており、昨夏、複数のアルゴリズムが標準化された。

EU では、欧州委員会が加盟国のセキュリティ当局に対して、PQC 移行のロードマップを 2026 年 4 月までに策定するよう勧告している。また、加盟 18 カ国のセキュリティ当局は連名で、PQC 移行に向けた検討の早期着手を推奨するステートメントを公表した。

ロ．実装に向けた動き

実サービスへの実装も始まっている。一部のウェブ・ブラウザの鍵共有プロトコルに PQC が実装されているほか、メッセージング・アプリやテレビ会議システムにおける鍵共有プロトコルにも PQC が導入されている。また、PQC を搭載した IC チップが開発され、第三者によるセキュリティ評価の結果が公表されている。そのほか、IC カードに搭載する IC チップなどのセキュリティ・エレメントに関して、PQC を組み込んだ技術仕様の標準化の検討も開始されている。

ハ．金融分野における主な動き

金融分野においては、欧米の金融当局や金融コミュニティより、さまざまな調査報告やステートメントが発表されている。わが国を含む主な金融分野の動きは以下のとおりである。

2022 年 11 月	米国金融分野におけるセキュリティ技術の標準化を担う ASC X9 が、量子コンピュータによるリスクに関する調査報告を公表。
2023 年 3 月	セキュリティ・インシデントの情報共有などの共助の取組みを行う FS-ISAC がリスク対策に関する調査報告を公表。
2023 年 6 月	中央銀行のコミュニティ（国際決済銀行・仏中銀・独連銀）が、共同プロジェクト「Leap」の報告書を公表。Leap は、仏中銀と独連銀間で VPN（Virtual Private Network）ネットワークを構築し、既存暗号と PQC のハイブリッドで通信するもの。
2023 年 11 月	イギリスの銀行協会（UK Finance）が、リスク・シナリオや対応方針に関する報告書を公表。
2024 年 1 月	世界経済フォーラムが、リスク対応における連携（民間部門と当局、国家間）の重要性に関する提言を公表。
2024 年 2 月	シンガポール金融管理局が、量子コンピュータによるリスクへの対応を金融機関に勧告。
2024 年 9 月	クレジットカード取引の国際的な決済技術の標準を策定する EMVCo が、リスク対応のポジション・ステートメントを公表。
2024 年 9 月	G7 のサイバー・エキスパート・グループが、リスク対応に関する提言を公表。
2024 年 10 月	FS-ISAC が、暗号アジリティ[4]の重要性と方法論のガイダンスを発表。
2024 年 11 月	預金取扱金融機関の耐量子計算機暗号への対応に関する検討会（PQC 検討会。事務局：金融庁）が報告書を公表。
2024 年 11 月	仏中銀・シンガポール金融管理局が、共同プロジェクト（メールへの PQC 実装）の報告書を公表。
2025 年 2 月	欧州域内の金融業界における PQC 移行の課題を検討するフォーラム Quantum Safe Financial Forum がリスク対応の推奨事項を公表。

わが国では、2024 年 11 月に、金融庁が事務局となって同年 7 月から 3 回にわたって開催された PQC 検討会による報告書が公表された[5]。同報告書では、PQC 移行対応において経営層が認識・対処すべき事項として、リーダーシップの発揮、および、全社的な施策としての対応方針の策定を挙げている。また、PQC を使用可能にするタイミングに関して、優先度の高いシステムについては 2030 年代半ばとしているほか、海外の規制動向にも留意してタイミングを設定すべきであるとしている。移行に向けた事前準備として、暗号利用箇所やアルゴリズムの棚卸し、リスク評価、優先順位付けを挙げたうえで、これらへの早期着手を推奨している。また、IT ベンダーや金融インフラ提供事業者、フィンテック企業、政府当局、他の重要インフラ事業者といった多様なステークホルダーと連携が重要であるとしている。

4 暗号アジリティとは、別のアルゴリズムに入れ替えやすい特性を指す。

5 https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf

（3）PQC 対応にかかる今後の課題

CRQC によるリスクを取り巻く環境は今後も変化しうる。量子コンピュータの開発進捗状況、暗号の解読アルゴリズムに関する研究の進展、海外における規制動向をフォローしながら対応を進めていくことが求められる。また、PQC を搭載したソフトウェアやハードウェアを実装した後で、それらにおいて脆弱性が発見されるリスクもある。PQC 実装における脆弱性に備えた体制整備も必要となろう。

金融機関においては、まず、PQC 移行に向けた体制を整備することが必要である。具体的には、量子コンピュータや PQC に関する情報の収集、社内での PQC 対応の必要性に関する啓発活動、ステークホルダーとの調整、暗号使用箇所の調査と使用状況に関する情報の収集・管理体制（暗号インベントリ）の整備、リスク評価、他の金融機関や重要インフラ事業者との連携などが挙げられる。

次に、PQC 移行のロードマップの策定が求められる。わが国では、金融 ISAC において、金融業界としてのロードマップのひな形が検討されている。各金融機関は、このひな形を参照するかたちで、自社の事情に合致したロードマップをそれぞれ作成するという流れとなろう。また、こうした作業を通じて PQC 移行における課題を洗い出すとともに、それらを必要に応じてステークホルダーと共有し連携して対応することが重要である。長期的には、今回と同様に、暗号アルゴリズムの移行が将来必要となりうる点を踏まえ、暗号移行に柔軟かつ効率的に対応できるシステム・アーキテクチャを検討することが望ましい。

欧米では、業界団体やコミュニティによる検討や提言が活発化している。わが国でも、PQC 検討会の報告書を参照するなどして、各金融機関において検討が活発化することを期待したい。

4. 講演「AI がもたらすリスクに対するセキュリティ」

菅は、AI の研究開発動向を概観したうえで、AI がもたらす脅威とセキュリティ・リスク、対策の動向について、次のとおり講演した。

（1）AI の研究開発動向

AI のリスクを論じる際には、これをもたらす技術との対応関係を把握しておく必要がある。AI に対応する最も広い技術のクラスは機械学習であり、機械学習には多層のニューラル・ネットワーク・モデルを用いる深層学習が含まれる。そのうち、動画像や音声、テキストなどのコンテンツを出力するものが生成 AI

である[6]。さらに、生成 AI の中に、汎用人工知能（artificial general intelligence：AGI）が含まれる。AGI は、人間のように広範な知識をもち、多様なタスクを処理し、思考する AI を指す概念である。10 年前には、AGI の到来は近未来に予見されないとの見方が大勢であったが、今日の最先端の生成 AI は、すでに AGI の領域に到達している。

これまで AI は、①諸分野の知を統合する方向、②情報処理とエネルギー消費の効率を高める方向に発展してきた。とくに、②の方向性は、単なるエネルギー節約を超えて、推論能力や汎化能力といった知性の獲得に本質的な役割を果たしたとみている。今後は、言語や動画などを統合処理するマルチ・モーダル化、推論能力の深化、自律的に行動するエージェント化によって、AI は現実世界の広範なタスクを処理できるようになり、用途が拡大していくと見込まれる。これに伴い、AI が社会にもたらす脅威も変化していくため、AI セキュリティの研究の重要性は高まっていくだろう。

（2）深層学習モデルによる自然言語処理を可能にした技術進歩

第 3 次人工知能ブームのきっかけは、画像認識のコンペティションにおいて、畳み込みニューラル・ネットワークが従来の機械学習手法を大きく上回る性能を達成したことである。もっとも、この時点では、複雑な構造をもたない画像データであれば深層学習モデルで処理できるが、意味や文法などの複雑な構造をもつ自然言語はうまく処理できないだろうとの見方が一般的であった。

現在では、さまざまな工夫の積み重ねにより、自然言語処理が可能となっている。代表的なものには、注意機構と呼ばれるモデル・アーキテクチャの工夫がある。注意機構とは、文の中で重要性の高い部分に自動的に大きな重みを割り当てる仕組みを指す。注意機構以外にも幾つかの重要な工夫があり、その多くは 2013 年に開発された Word2Vec と呼ばれるモデルの登場時点で既に提唱されていた。 1 つ目の工夫は、データ構造である。Word2Vec は、単語を高次元のベクトル空間に埋め込む。このとき、ベクトル空間において「queen」－「woman」＋「man」＝「king)」といった意味の演算が概ね成立することから、ベクトル空間への埋め込みの有用性が注目を集めた。2 つ目は、文章生成のアルゴリズムである。コンピュータによる文章生成メカニズムを、意味や文法を捨象して、確率的なプロセスによる単語列の生成と単純化してとらえた。3 つ目は、訓練データである。Word2Vec は、ある単語の出現確率を、周辺にある単語群から推定する CBOW（continuous bag of words）という手法で推定した。これは、現代

[6] 生成 AI は、必ずしも深層学習モデルである必要はないが、事実上、深層学習モデルに包含されると言ってよい。

的には、自己教師あり学習と位置付けられる。大規模言語モデルでは、コーパスの一部を削り、その部分を周辺の文章から予測する「穴埋め問題」を大量に解くことで自己教師あり学習を行う。

（3）AI セキュリティ

AI セキュリティの研究分野は、①AI システムを守る、②AI を攻撃に悪用する、③AI を防御に活用する、という 3 つの目的に分かれる。ここでは、①に焦点を当てて説明を行う。

イ．AI のセキュリティ・リスクの特徴

一般的な情報システムの脆弱性対応では、脆弱性のある部位を特定して修正し、脆弱性の解消を行う。ここでの脆弱性のある部位とは、プログラム・ソースコードや設定ファイルなどの不具合（バグ）である。これに対し、深層学習モデルは、何億個ものモデル・パラメータの組み合わせで機能が発現している。そのため、機能の一部に不具合があっても、その原因となるパラメータを特定することは困難である。また、パラメータが特定できても、その数値を変更することで不具合を解消できるとは限らない。一般的な情報システムのように、局所的な対応によって機能の不具合が解消できない点が、深層学習モデルのセキュリティ・リスクの特徴である。

また、大規模言語モデルは、自己教師あり学習によって確率予測の精度を高めるという原理に基づいているため、リスクをゼロにすることも不可能である。セキュリティ・リスクに対処するには、モデルの頑健性向上などの技術的対応に加えて、サプライチェーン管理や利用者教育といった非技術的対応も合わせて必要になる。

ロ．失敗によるリスクの分類

深層学習モデルのセキュリティ・リスクを包括的に捉えるには、脆弱性という原因ではなく、モデルによって生じる不都合な事態、すなわち失敗を分類することが合理的と考えられる。その大まかな分類としては、セキュリティ、セーフティ、サプライチェーン・リスクがある。

（イ）セキュリティ

セキュリティは、悪意のある攻撃者がいるもとでの安全性を指す。例えば、敵対的サンプル攻撃は、入力データに微小なノイズを付加することにより、誤った出力データを誘発するものである。また、大規模言語モデルには、有害情報

やプライバシー情報を出力しないように制限がかけられているが、プロンプト（入力文）の工夫により、この安全装置を巧みに回避するジェイル・ブレイク攻撃がある。ジェイル・ブレイク攻撃では、システム・プロンプトを無視するよう指示するプロンプトや、善良な目的を装うプロンプトが悪用される。バックドア攻撃は、条件付きで発動する不正な機能を機械学習モデルに埋め込む攻撃である。不正な機能は、攻撃者が定めた特徴（トリガー）を入力データが有している場合にのみ発動するため、通常は気が付きにくい。この攻撃は、機械学習モデルや訓練データを外部から調達する場合に脅威となるため、サプライチェーン・リスクとの関係が深い。

（ロ）セーフティ

セーフティは攻撃者がいないもとで安全を確保するものであり、モデル性能の不足のほか、倫理への適合性の問題がある。後者は、出力データがプライバシー保護や差別などの倫理規範に抵触するリスクを指す。倫理規範は地域や文化によって異なるうえ、時代や利用目的によって異なりうる。したがって、利用状況に応じて適切な対応がとれていることを、AI サービスを提供する事業者は、継続的に確認していくことが望ましい。

（ハ）サプライチェーン・リスク

サプライチェーン・リスクは、訓練データやモデルの社外からの調達、業務委託によって生じるリスクである。対応策を考慮する際には、セキュリティやセーフティにかかるリスクとあわせて評価する必要がある。

ハ．セキュリティ・リスクへの対策とまとめ

AI を安全に利用する対策アプローチとして、AI 自体の安全性の向上、AI に対する攻撃への対処、外部から調達した AI の検査、外部装置によるフェール・セーフな仕組みの導入、サプライチェーンまたは業務委託先の管理、利用者教育やリスク・コミュニケーションに分類できる。

最先端の AI は、すでに AGI の領域に到達しているが、その登場から間もない。今後は社会において AGI の活用が進み、その副作用も顕在化していくとみられる。その対処を考えるうえで、AI セキュリティの研究の重要性も高まっていくと思われる。

（4）対談

人工知能学会傘下に設立された「安全性とセキュリティ研究会（SIG-SEC）」について、**菅**は、まず、設立発起人である大塚教授に立ち上げの経緯について

尋ねた。**大塚**は、これまで、AI 研究者が研究する安全性は主に AI セーフティであり、サイバーセキュリティ研究者が研究する安全性は AI セキュリティであるという大まかな棲み分けがなされていた経緯を説明したうえで、AI 研究者とセキュリティ研究者の両者の知見を融合させていく必要があるという問題意識から SIG-SEC を設立したと説明した。そのうえで、両者の専門的知見から AI セーフティと AI セキュリティに関する研究を深めていきたいと説明した。

続いて、菅は、AGI の出現でサイバー攻撃と防御がどのように変化するかを問うた。**大塚**は、オープンソース・ソフトウェアにおいて、セキュリティ・パッチからエクスプロイト・コード[7]を生成する際に AI を悪用する研究事例を紹介し、マルウェアの作成が高度化、効率化する可能性を示唆した。サイバー防御に関しては、DEF CON[8]において、AI のみでシステムの脆弱性を自動的に発見および修復するコンテストが 2 年がかりで開催されていることを紹介したうえで、こうしたコンテストで活用される手法から有益な示唆が得られると指摘した。

さらに、菅は、AGI を超えた超知能（Artificial Super Intelligence：ASI）のリスクをどのように考慮すべきかを尋ねた。**大塚**は、AI がメイン・タスクを達成するために、人間にとって有害なサブ・タスクを設定するリスクがあることを指摘した。例えば、コーヒーを淹れるタスクを課された AI が、コーヒー・メーカーの電源を抜こうとする人物がいたときに、目的達成のために当該人物を排除するという下位の目標を立ててしまうことがありうる。ASI のような人知を超えた AI であれば、人間の予測がつかない解決策を思いつき、思わぬリスクをもたらしうると述べた。

2. 講演「さまざまな決済スキームとそのセキュリティ」

田村は、デジタル決済に関する研究開発の経緯について紹介するとともに、決済スキームのセキュリティについて、次のとおり講演した。

（1）デジタル決済に関する研究の勃興

デジタル決済に関する研究は 1980 年代に遡る。インターネットや家庭用パソコンの普及、IC カードの実用化を背景に、デジタル決済に関する研究開発が盛んに行われた。こうした研究開発は、クレジットカードなどのアナログ処理で

---

[7] ソフトウェアの脆弱性を悪用した不正な動作を再現するために作成されたスクリプトやプログラム。

[8] DEF CON は、毎年ラスベガスで開催されている大規模なセキュリティ・カンファレンス。企業や政府機関のセキュリティ研究者やハッカーが集まり、ハッキングの講演やハンズオン、Capture The Flag コンテストなどが開催される。

行われていた決済手段をデジタル化するものと、現金を代替する手段をデジタル技術で実現することを企図したものがあった。

金融研究所では、1990 年代より、現金を代替する手段である「電子現金」について研究を行っていた。電子現金は、現金の電子化を目指したものであり、現金に見立てた電子データのやり取りによって決済を完了させる方式をいう。具体的には、銀行から引き出した電子現金を IC カードに格納し、それをショッピングや個人間送金に利用するという運用が想定されていた。電子現金に関する実証実験も複数行われており、非対面決済を想定した「インターネットキャッシュ」と、主に対面決済を主とした「スーパーキャッシュ」と呼ばれる実証実験はその代表例である。スーパーキャッシュの実証実験は、24 の金融機関、約 1000 の店舗、約 2.2 万人のユーザの協力を得て、大規模に実施されたと記録が残っている。実証実験の結果を踏まえて、普及に向けての課題などが整理されたが、その後は非接触 IC カードを利用した決済サービスが登場したことなどもあり、電子現金に関する検討は一旦収束した。

（2）台帳を使用しない決済方式

現在、われわれが使っているキャッシュレス決済の多くは、サービス事業者が決済を仲介するものである。つまり、サービス事業者が台帳に決済内容を書き込むことにより決済が完了する。政府はキャッシュレス比率の最終目標を 8 割としており、今後のキャッシュレス決済のさらなる普及を見据えれば、サーバやネットワークの障害といった決済に及ぼしる影響についてより一層の考慮が必要になってくると思われる。

電子現金における送金処理は、サーバを介さずユーザ 2 者間でのデータ通信に閉じるものであることから、サーバやネットワーク障害、あるいは、サーバの処理性能への依存度の面からは、優位な可能性があるといえる。そのほか、電子データそのものに価値を持たせたものであることから、例えば、電子現金にプログラム機能を持たせるといった応用も考えられる。この点、電子現金スキームは、決済に閉じない発展の可能性を秘めた技術であるとみている。

（3）電子現金の基本構成

電子現金の基本スキームでは、電子現金を発行するサービス事業者のほか、サービス事業者とは独立した組織として認証機関を想定する。ユーザは認証機関に対してユーザ登録を行い、電子現金の送受信に使う鍵ペアに対する証明書の発行を受ける。ユーザはサービス事業者から発行された電子現金をインターネット、あるいは、近距離無線通信を通して別のユーザに送ることができる。

電子現金は転々流通が可能であり、最終的にサービス事業者にすべて還流させることで二重使用チェックを行うというシンプルな構成となっている。

電子現金の偽造・改ざん対策は、サービス事業者によるデジタル署名によって実現される。電子現金の送受信は、電子現金の移転履歴とセットで行われ、その移転履歴には、電子現金の保有者に関する情報が記載される。これにより、正当な保有者以外のユーザが複製して使用することができないよう対策が講じられている。例えば、ユーザ A からユーザ B に電子現金を送信する際、A は移転履歴に B の公開鍵に関する情報を記載してデジタル署名を付与する。B は、移転履歴を検証することで、A が自分宛てに送信したものであることを確認することができるほか、1 つ前の移転履歴をみることで、同電子現金が過去に A に送金されたものであることを確認できる。移転履歴の更新に使用するデジタル署名用の秘密鍵については、本人であっても不正な使い方ができないようセキュリティ対策を講じておくことが必要であるが、中長期的観点からは、セキュリティ機能の安全性が低下する可能性についても考慮が必要である。電子現金スキームには、事後的な二重使用検知機能が付与されており、還流してきた電子現金のなかに同じシリアルナンバーをもつものが存在した場合、それぞれの移転履歴を比較することで二重使用者を特定できるようになっている。

（4）電子現金の実機検証

今般、現行技術で電子現金を実装した場合、どの程度のユーザビリティを確保しうるか再検討を行った。電子現金の送受信処理についてボトルネックとなるのは、送金ユーザ側で行われる移転履歴更新にかかる時間と、データの通信時間である。そこで、現行のスマートフォンを用いて実機検証を行ったところ、100 枚の電子現金の送受信にかかるトータル時間を 230 ミリ秒（0.23 秒）と概算することができ、既存の非接触 IC カードによる決済手段とほぼ同程度の時間で送受信できることがわかった。もっとも、電子現金の場合には、送金先の選択や送金額の入力といったスマートフォンでのアプリ操作が必要となるが、実用可能性は低くないとの結果が得られたといえる。

そのほか、更なる効率化やプライバシー強化の方法についても検討を行っており、詳しい内容をディスカッション・ペーパーにまとめている[9]。なお、今回の実機検証は技術的な観点からの検証を目的としたものであり、法律や制度、実運用等、社会実装に向けた実現可能性は検討の対象外である。

---

9 田村ほか、「台帳を用いない決済方式に関する技術面からの一考察」、金融研究所ディスカッション・ペーパーNo. 2024-J-19、日本銀行金融研究所、2024 年

（5）決済スキームのセキュリティ

オンラインでのクレジットカード決済、インターネットバンキング、コード決済といった既存の決済サービスは、台帳ですべての取引を管理している。そのため、不正な取引については、サービス事業者が検知できるようになっている。これらのサービスでは、サーバ側でアカウント管理しており、アカウントにログインした者が正しいユーザであるということを前提としていることが多い。こうしたログインにはパスワードを用いるものが多いため、人の脆弱性を突いてパスワードを特定しようとする攻撃への対策が非常に重要となる。フィッシング詐欺はその一例であり、正しくユーザ認証を行うということの難しさが顕著となっていることを表している。

また、暗号資産については、台帳ですべての取引が管理されているという点は既存の決済サービスと同じであるほか、不正な取引もブロックチェーン参加者によって排除される。暗号資産取引は、デジタル署名を付与したトランザクションデータの記録によって行われるものであることから、不正送金を防止するには、正当なユーザだけが秘密鍵を用いた署名を生成できるような仕組みが必要となる。実際、秘密鍵を安全に保管するためのウォレットと呼ばれるデバイスが多く登場している。

これに対し、電子現金には、取引を記録する台帳はないが、他人の電子現金を複製して使用しようとした場合には、電子現金の受信側でこれを検知することができる。しかしながら、送信者が過去に使用した電子現金を再度使用するような二重使用については、受信側で検知することができない。そのため、電子現金スキームでは、サービス事業者が還流した電子現金を事後的にチェックすることとしている。なりすまし対策については、暗号資産と同様、電子現金送信時に生成するデジタル署名用の秘密鍵を安全に保管することが重要となる。そのため、電子現金の実装を考えるにあたっては、暗号資産分野で先行しているセキュリティ対策の事例が参考になろう。

（6）対談

まず、**面**から、デジタル決済等に使用するデジタル・ウォレットの種類とそのセキュリティについて説明が行われた。デジタル・ウォレットとは、一般に、重要なデジタルデータを保管するデバイスを指し、暗号資産取引に使用するウォレット、個人情報などを管理するID管理ウォレットなどがある。このうち、暗号資産ウォレットは、一般に、ホット・ウォレットとコールド・ウォレットに分類され、コールド・ウォレットの方が安全であるといわれている。しかしながら、これらはデバイスが常時インターネットに接続した状態か否かで分類

したものに過ぎず、コールド・ウォレットであっても、暗号資産の取引時にインターネットに接続されれば、ホット・ウォレットと同様のリスクが生じると指摘された。

これに対して、**田村**は、PC 等がマルウェアに感染した場合のリスクについて尋ねた。**面**は、マルウェアによるリスクとして、送金先の改ざんにより暗号資産が意図しない先に送金されてしまう可能性を指摘した。ブロックチェーンに書き込まれた取引は取り消すことができないため、送金内容をモニタで人間が最終確認するなど、マルウェアに感染したとしても安全に取引できるようにするという考えが重要であるとの見方を示した。

また、**面**は、マイナンバーカードに搭載される暗号アルゴリズムが 2026 年を目途に ECDSA（Elliptic Curve Digital Signature Algorithm）に移行することを受け、ECDSA を使用している暗号資産用のウォレットとしてマイナンバーカードを応用できる可能性を指摘した。もっとも、デジタル署名用の鍵ペアはマイナンバーカードごとに固定であるため、これをそのまま暗号資産取引に使用すると、異なる取引が同一ユーザによるものであるという情報が露呈することでプライバシーの問題が生じる可能性があると指摘した。

これに関連して、**田村**は、電子現金においても同様の課題があることを紹介し、取引用の鍵ペアを都度生成することで取引の関連付けを切断するとともに、ゼロ知識証明を使用して、認証機関に登録を行った正しいユーザであることを証明する方法を紹介した。

6. 講演「金融分野における今後のセキュリティ対策～シンポジウム総括を兼ねて～」

岩下[10]は、シンポジウムの総括を兼ねて、CITECS における課題や今後の活動への期待について述べたうえで、金融分野における今後のセキュリティ対策について、次のとおり講演した。

（1）シンポジウムの総括

本日のシンポジウムでは、CITECS における 20 年の活動を振り返るとともに、現在のセキュリティ上の課題が整理され、金融分野のセキュリティ対策を考えるうえで大変有益なものとなった。PQC 移行については、金融機関のセキュリティ関係者の間では話題になっているものの、必ずしも正しい情報が共有され

[10] 岩下教授は、日本銀行において金融分野における情報セキュリティ技術の研究に従事し、CITECS の初代センター長を務めた。

ていないとも感じており、今回のような客観的かつ正確な情報発信は非常に重要である。また、AI セキュリティについては、生成 AI の台頭に伴うセキュリティ・リスク、倫理的課題、金融業界が直面する新たな課題について多くの洞察が得られた。生成 AI の仕組みを理解することは容易ではないものの、その活用にあたっては、仕組みを理解したうえでリスクを認識しておくことが必要との示唆が得られた。また、決済スキームのセキュリティに関する講演では電子現金に関する検討結果が紹介された。近年、ステーブルコインと呼ばれる暗号資産が注目を集めているが、技術への理解が乏しいユーザの参加が増えてきているのも事実であり、電子現金スキームの再検討から得られる知見をもとに理解を深めていってほしいと思う。

（2）金融機関に必要な対応

金融機関が直面する状況はそれぞれに異なり、脅威の確度も一概に断定できるものではない。そのため、金融機関には、常に最新の情報をアップデートして、自らが知る範囲を最大限に拡大しながら、適時適切に最善の決断を下すことが求められる。そのためには、技術研究者と金融機関実務家とをつなぐ結節点のような存在が必要であり、それこそが CITECS なのであろうと思う。

（3）セキュリティとセイフティ

日本において「安全」という言葉は、セキュリティ（Security）とセイフティ（Safety）の両方を含む。インターネットが普及する以前は、外部からの脅威に対する「セキュリティ」はあまり重要ではなかった。実際、金融情報システムセンターによる安全対策基準においては、不慮の事故やバグによるシステム停止への対策を、「セイフティ」の意味で安全対策と呼んでいたが、世界中の端末がインターネットでつながったことにより、セキュリティの重要性は徐々に増していった。

わが国の金融機関は、長きにわたってインターネットから切り離すことで、社内システムのセキュリティを確保するという考え方を採用していたが、最近ではインターネットとフルに接続したうえで、しっかりシステムの安全性を確保する「サイバーハイジーン[11]」という考え方に移行しつつある。

---

11 マルウェア感染などを予防し、IT 環境を健康・健全に維持する衛生（ハイジーン）管理のことをいう。

（4）CITECS に期待する役割

CITECS の活動は、単なる技術研究にとどまらず、社会的インパクトや社会実装、標準化、法規制との関わりを通じて金融分野におけるイノベーションを支えてきた。今後も、未知の技術やリスクへの挑戦を続け、金融分野の情報セキュリティの未来を切り開いていくことを期待したい。

そのためには、まず、①基盤技術の検証が必要である。どの技術が金融分野のセキュリティを支える基盤となるかを評価し、短期的な流行に惑わされることなく長期的な視点で検討することが求められる。そのうえで、②結節点としての機能を持ち合わせてほしい。研究者、技術者、実務家をつなぎ、単なる技術研究ではなく、実際に使われる技術に育てていくといった役割を担うことが求められよう。また、③技術の受容プロセスの支援も必要である。「何の役に立つのか？」という疑問が持たれる段階から研究し、十分な検討を経て、社会に受け入れられる道筋をつくっていくという取組みを期待したい。

（5）CITECS の今後の課題

CITECS における今後の課題は、①既存技術の維持と継承である。安全であることが当たり前になると、安全対策のための技術が適切に維持・継承されないリスクがある。CITECS にとっては、コモディティ化した技術をどう支えていくかが課題となろう。2 つ目の課題は、②新しい技術領域への挑戦である。CITECS には、未来の基盤技術を発掘し、既存の枠組みでは捉えられないリスクを先取りする力を備えてほしい。3 つ目は、③社会実装のギャップを埋めることであり、技術的な正しさだけでなく、実際に使われる技術としての現実的な道筋をつくることである。

安全であることが当然の世界において、CITECS が果たすべき役割は、研究・技術・実務の間に生じるズレを調整し、先を見据えて動くことにあると思う。未来を予測するのではなく、変化に適応し、技術の受容プロセスを支える役割こそを、CITECS の強みとしていってほしい。

以　上