

2020 年度 マイクロソフト情報学研究賞紹介



選定にあたって 萩谷昌己

マイクロソフト情報学研究賞選定委員会委員長／
東京大学

2021年3月18日に、2020年度の「マイクロソフト情報学研究賞」が、松原靖子さん（大阪大学産業科学研究所）と松田隆宏さん（産業技術総合研究所）に授与されました。本賞は国内の若手研究者を表彰の対象として2016年度に創設されました。今回で第5回目の贈呈となります。本賞は、企業（大学および公的研究機関以外）所属の若手研究者を対象とする「情報処理技術研究開発賞」とともに、本会第20代会長の故長尾真先生からご寄贈いただいた資金により2005年度に創設され、2015年度までの11年間、若手研究者を顕彰してきた「長尾真記念特別賞」の主旨を引き継いでいます。「長尾真記念特別賞」が毎年3名以内の選考であったのに対して、本賞が2名以内、「情報処理技術研究開発賞」が1名以内であわせて3名以内となっております。なお、本賞の贈呈は2021年3月の全国大会で行われる予定でしたが、昨年に引き続き全国大会がオンライン開催となったため、表彰式は行わず表彰報告をさせていただきました。

本賞は、情報学の主要な分野の研究・開発で国際的に顕著な貢献が認められ、今後もその発展が期待される若手研究者（共同研究・開発の場合はその代表者）を毎年2名以内で顕彰するものです。受賞対象者は、博士号取得後10年以内の若手研究者で、公募推薦の時期に本会正会員として3年以上経過した国内の大学または公的研究機関に所属する者としています。2020年度は2020年11月30日を推薦締切として公募を行ったところ3名の推薦があり、表彰規程ならびに選定手続きに基づき慎重に審議を行った結果、以下の研究業績に関して上記2名の受賞が決定しました。

松原靖子さん：「大規模時系列データのリアルタイム解析と将来予測に関する研究」

深層学習を中心に機械学習の技術が普及し、IoTなどからのビッグデータの解析が進んでいます。しかしな

がら、一般に機械学習ではモデルの構築に多大な時間を要するため、IoTのように時々刻々と変化する環境からのデータを用いてリアルタイムに学習することができません。松原さんはこの課題に対処するために、リアルタイム要因分析・予測技術を開発されました。これは、時系列ビッグデータストリームに基づく動的モデル学習と将来予測技術を融合したもので、深層学習と比較して数十万倍の高速化を達成しています。さらに松原さんはこの技術をソーシャルネットワークの解析などにも応用されています。

松田隆宏さん：「高い安全性と機能を有する公開鍵暗号技術のモジュラーかつ汎用的な設計法に関する研究」

松田さんは、暗号要素技術を組み合わせ、より高機能な暗号技術や通信プロトコルなどの目的技術を一般的・汎用的に構成する方法を研究されました。一般に要素技術を組み合わせる目的技術を実現する方法はモジュラー構成と呼ばれています。暗号の分野でモジュラー構成を与えることは容易ではありません。攻撃者の存在により目的技術が利用される環境が過酷であるため、要素技術の安全性だけでは目的技術の安全性が満たされないことが一般的だからです。松田さんは、長年の研究の末に、受賞テーマである公開鍵暗号技術のモジュラー構成に成功されました。この成果は、この分野における長年の課題を解決するものでありブレークスルーと呼ぶことができるでしょう。

両名ともにマイクロソフト情報学研究賞の受賞者に相応しい優れた研究業績があり、また本会を含む国内外の学会において活躍されています。両名の今後のさらなる活躍を期待しております。また、これからも国際的に活躍する優秀な若手研究者を顕彰していきたいと考えていますので、積極的な応募をお願い申し上げます。

(2021年5月28日)



時系列ビッグデータのリアルタイム将来予測と社会実装への取り組み

【受賞タイトル】大規模時系列データのリアルタイム解析と将来予測に関する研究

松原靖子 大阪大学 産業科学研究所

このたびは、大変名誉ある賞をたまり大変光栄に存じます。本会の皆様、日本マイクロソフト（株）様、ならびに本賞選定委員会の先生方に心よりお礼申し上げます。

私はこれまで、IoT/センサデバイス、Web上のアクティビティ等、大規模かつ多様な時系列ビッグデータを対象とし、重要な情報を非線形モデルに基づき自動的かつリアルタイムに解析し、動的要因分析や将来予測をするための基盤技術を開発してきました。

実社会においてIoTやWebを巡る環境が急速に変化し、特に製造業におけるDXやカーボンニュートラルに関する取り組み、Webと連携した災害時の情報提供や予測等、リアルタイム性が求められる大規模データ解析技術が幅広い分野で強く求められています。世界におけるビッグデータ・AIに関しては主に深層学習が用いられ、急速に応用範囲が拡大していますが、その一方で、これらの手法はブラックボックスモデルを使用していること、大量の教師データと多大な計算時間を必要とするためリアルタイムに学習ができない、刻々と変化する環境の中で柔軟に適応することができない等の課題も残されています。

我々の研究では、既存の深層学習等に基づく技術では実現できなかった、高速、省メモリ、高精度のモデル学習、特徴自動抽出、要因分析、将来予測を

可能とする新たなリアルタイムデータ解析手法を開発しました。これまでの研究における一連の要素技術は、データマイニング、データベース、Web分野のトップ国際会議において数多くの成果として発表しており、国際的にも高く評価されています（KDD 2012 にて2本、KDD 2014, ICDM 2014, SIGMOD 2014, WWW 2015, KDD 2016, WWW 2016, KDD 2019, CIKM 2019, ICDM 2019, KDD 2020 等）。さらに、我々の開発した最新のリアルタイム要因分析・予測技術は、世界最高精度、最小計算コストの時系列予測を可能とし、その有用性と独自性により、産業界からも高い評価をいただいています。さまざまな有力企業と連携しながら技術の実用化に向けた活動を継続的に実施しており、特に製造業においては、大規模設備の故障予測、組み込み機器や小型デバイス等のエッジ端末向けリアルタイムAI技術について、事業導入に向けたソフトウェア開発を行っています。

今後も引き続き、本研究成果を発展させ、学術面で世界最高レベルの研究成果を発信しつつ、技術の実用化と社会実装に向けた積極的な産学連携を行って参ります。時系列ビッグデータ解析に関する世界のデファクトスタンダードとも呼ぶべき技術を開発することを念頭に、数多くの企業の方々と協調しながら、先駆的な技術開発に取り組んでいきたいと考えております。今回の受賞を励みとし、日本における情報処理分野の発展に貢献すべく、一層の努力を尽くして参りたいと存じます。

(2020年5月17日受付)

松原靖子（正会員） yasuko@sanken.osaka-u.ac.jp

2012年京都大学大学院情報学研究科社会情報学専攻博士後期課程修了。博士（情報学）。2019年より大阪大学産業科学研究所准教授。2016年度日本データベース学会上林奨励賞、2018年度IPSJ/ACM Award for Early Career Contributions to Global Research等受賞。

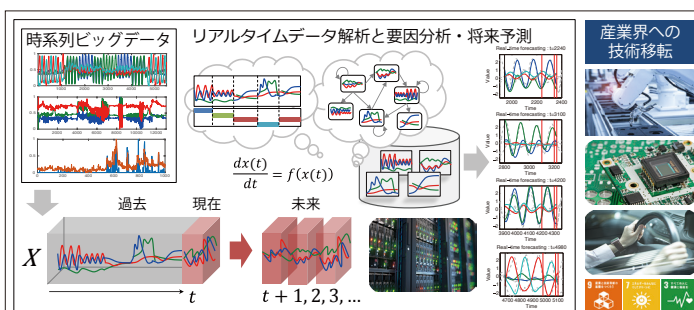


図-1 時系列ビッグデータのリアルタイム解析と産業界への技術移転



暗号技術のモジュラーな設計

【受賞タイトル】高い安全性と機能を有する公開鍵暗号技術のモジュラーかつ汎用的な設計法に関する研究

松田隆宏 国立研究開発法人 産業技術総合研究所

このたび、マイクロソフト情報学研究賞という栄誉ある賞をいただき大変うれしく思います。これまでお世話になった恩師、共同研究者を始め関係者の方々に深く感謝いたします。

暗号技術はインターネットでの通信を始めあらゆる場面（多くの場合、利用者の意識しないところで）利用されています。数ある暗号技術の根幹を支えるのは、公開鍵暗号や電子署名などの「暗号要素技術」です。暗号要素技術の構成法は、数論や線形代数などを駆使して目的技術を直接構成する方法と、公開鍵暗号や電子署名といった基礎的な暗号要素技術の組合せにより目的技術を一般的・汎用的に構成する方法（モジュラー構成）とに大別できます。今回賞をいただいた研究は、そうしたさまざまな暗号要素技術のモジュラー構成やその不可能性についてのものです。部品から目的技術をボトムアップに構成する、という手法は多くの分野や場面で当たり前の考え方なのですが、暗号要素技術では「暗号化したデータを復号すれば元に戻る」といった機能的な要件に加え、厳密に数学的に証明された安全性も同時に満たす必要があります。そこに暗号分野特有の難しさ（と面白さ）があります。ひとたびモジュラー構成法が示されれば、以降は部品としての要件を満たす暗号要素技術ならばどれを用いても目的技術を構成できるため、モジュラー構成には構成要素の取り換えが容易になるという重要な実用的意義があります。近年では、耐量子計算機安全性を持つ暗号技術が研究分野において中心的な研究テーマの1つとなっていますが、部品となる暗号技術を量子計算機に対して安全なものに取り換えることで、構成された暗号要素技術もまた量子計算機に対する安全性を保証できますので、耐量子計算機安全性を持つ暗号技術の構成という目的にも有用性を発揮します。

私は修士時代に初めて暗号分野の研究に触れ、その魅力に引き込まれました。（なぜか）特に「受動的攻撃者に対する安全性しか満たさない公開鍵暗号方式を部品として組み合わせ、実利用上必須の能動的攻撃者に対する安全性を満たす公開鍵暗号方式を構成できるか？」という暗号理論では基礎的な問題が未解決であることに魅せられ、解決に貢献したいと思い研究を続けてきました。この問題は、後者を前者からモジュラー構成できるかを問うものです。現在でも完全な解決には至っていませんが、部品に仮定を追加したり、目的技術を少し変えてみるなどの試行錯誤の結果が幸運にも研究成果に繋がりました。またその過程で、目的技術を一気に達成しようとするのではなく、より簡素な部品の組合せへと分解して構成を考えたり安全性解析（安全性証明）を行うというモジュラー構成のアプローチは、さまざまな高度な機能や安全性を有する暗号要素技術の構成においても有用であると分かり、研究対象とする要素技術の範囲を広げていくことでさまざまな研究成果に繋げることができました。

暗号技術や暗号理論の進展速度は目まぐるしく、さらに近年では秘匿計算技術など従来は理論的な技術とされていた暗号技術の社会実装に向けた取り組みがどんどん進んでいます。そのため最近ではこれまでの暗号要素技術の理論研究に加え、そうした社会での応用を見据えた暗号技術の研究にも取り組んでいます。今後も本研究で培った知見や経験を基に研究に励んでいきたいと思っています。

（2021年5月24日受付）

松田隆宏（正会員） t-matsuda@aist.go.jp

2011年 東京大学大学院情報理工学系研究科電子情報学専攻博士課程修了。博士（情報理工学）。2年間の日本学術振興会特別研究員（PD）を経て2013年より産業技術総合研究所研究員。2017年より同主任研究員。