NEWS RELEASE

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

2024 年（令和 6 年）4 月 9 日

「メタな視点に基づく平均時計算量の研究」で NII の平原秀一准教授が若手科学者賞を受賞

～令和 6 年度の文部科学大臣表彰～

文部科学省が 2024 年（令和 6 年）4 月 9 日(火)に発表した「令和 6 年度 科学技術分野の文部科学大臣表彰」において、「メタな視点に基づく平均時計算量の研究」の業績により、国立情報学研究所（NII、所長：黒橋 禎夫、東京都千代田区）情報学プリンシプル研究系の平原 秀一 准教授が、若手科学者賞(*1)を受賞しました。

【研究の背景】

現在、インターネットで広く使われている公開鍵暗号は、情報の暗号化を行う際と復号を行う際に別々の鍵を使う方式で、公開鍵と計算結果であるメッセージの組み合わせから、秘密鍵を計算するのに膨大な時間がかかり困難であることから、安全と言われています。しかし、本当に安全かどうかは未だに証明されていません。その安全性を議論するためには、計算の平均的な難しさを計る「平均時計算量」がどれくらいなのか解析するのが必要不可欠です。平原准教授は、その平均時計算量を新しい視点から解析するため、「計算問題の計算量を問う計算問題（メタ計算問題）」を考えるという、メタな視点に基づき、証明手法を開発してきました。

【評価の対象となった研究成果】

平均時計算の困難性を示す証明手法として「ブラックボックス帰着」と呼ばれる手法がありますが、この手法では暗号の安全性を証明するための未解決問題を完全に解決できない「ブラックボックス帰着の限界」があることがわかっています。平原准教授は、先に述べたメタ計算問題に着目し、ブラックボックス帰着ではない平均時計算困難性を解析するための革新的な証明手法を世界で初めて開発しました。この業績により、長年未解決だった暗号の安全性を証明するための中心的問題の解決への道筋を確立し、2022 年には、理論計算機科学のトップ会議である FOCS に採択されたうえ、その年の最も優れた計算量理論の研究成果に贈られる Complexity result of the year を日本人で初めて受賞するなど、国際的に非常に高く評価されています。

今回、こうした業績が評価され、平原准教授は令和 6 年度 科学技術分野の文部科学大臣表彰の若手科学者賞を受賞しました。

(*1) **「若手科学者賞」**： 萌芽的な研究、独創的視点に立った研究等、高度な研究開発能力を示す顕著な研究業績をあげた 40 歳未満の若手研究者個人（ただし、出産及び育児により研究に専念できない期間があった場合は、42 歳未満の若手研究者個人）

National Institute of Informatics

大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
総務部企画課 広報チーム
〒101-8430 東京都千代田区一ツ橋 2-1-2
直通：03-4212-2164 E-Mail：media@nii.ac.jp

Web: https://www.nii.ac.jp
X(旧 Twitter): @jouhouken
facebook: https://www.facebook.com/jouhouken

受賞に関する情報は以下の通りです（年齢は 2024 年 4 月 1 日現在）。

令和６年度 科学技術分野の文部科学大臣表彰 若手科学者賞

メタな視点に基づく平均時計算量の研究

平原（ひらはら） 秀一（しゅういち） 32 歳 情報・システム研究機構 国立情報学研究所（NII）情報学プリンシプル研究系 准教授

業績要約：計算量理論は、計算問題を解くために必要な計算量（＝計算時間などの計算資源）を解析する理論である。現在広く使用されている暗号は、計算量理論の P 対 NP 予想や、平均時計算量に一般化された P 対 NP 予想に基づいており、真に安全かどうかは未解決である。
氏は、メタ計算問題（＝計算問題の計算量を問う計算問題）に着目することにより、NP の平均時計算困難性を解析するための革新的な証明手法を開発し、世界で初めて「ブラックボックス帰着の限界」を突破することに成功した。さらに、計算量理論の根源的定理である Cook-Levin の定理に遡る約 50 年来の未解決問題を解決した。
本研究成果は、我々の日常生活で通信の秘密を守っている暗号技術が本当に安全かどうかを決定し、真に安全な情報通信社会を確立することに資すると期待される。

主要論文：「NP-Hardness of Learning Programs and Partial MCSP」Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)、p968~979、2022 年発表
「Non-Black-Box Worst-Case to Average-Case Reductions within NP」Proceedings of the IEEE Annual Symposium on Foundations of Computer Science (FOCS)、p247~258、2018 年発表

平原 准教授のコメント：
「このような名誉ある賞を頂き大変光栄に存じます。計算量理論には多くの未解決問題があり、そのほとんどの未解決問題に対して解決への道筋すら確立されていません。これまでの私の研究で、平均時計算量に関する未解決問題に関して進展を与えたことが評価され、嬉しく思います。しかしながら、私の目指す最終的なゴールに到達するまでにはまだまだ道のりは長いと感じています。究極的には、公開鍵暗号方式の安全性を証明することによって、我々の情報通信社会が本当の意味で安心・安全であることを保証することを目指しています。今回の受賞を励みに、今後も計算量理論の未解決問題を解決し、それによって未来の社会に貢献することを目指して日々邁進していきたいと思います。」

〈メディアの皆様からのお問い合わせ先〉

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
総務部企画課 広報チーム
TEL：03-4212-2164 E-mail：media@nii.ac.jp