

## AIのセキュリティの現状：研究動向と金融分野での活用にかかる考察

宇根 正志<sup>1</sup>

### 要 旨

近年、AI (artificial intelligence) のなかで、とりわけ、機械学習を活用したAIが注目を集めている。金融分野においても、さまざまな業務やサービスでの活用を展望した検討が進められている。機械学習を実装したシステム（機械学習システム）を実運用するうえで、その業務やサービスにおいて要求されるセキュリティを充足することが求められる。本講演では、機械学習システムを対象に、システムセキュリティの観点からリスクと対策にかかる研究動向を説明する。また、金融分野での活用が想定されるいくつかの機械学習システムに焦点を当てて、セキュリティ対策を検討する際の留意点を考察する。なお、本講演で示される意見は、講演者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて講演者個人に属する。

---

<sup>1</sup> 日本銀行金融研究所情報技術研究センター