AIセキュリティ・プライバシー（佐久間 淳）
AI Security and Privacy (SAKUMA Jun)

SAKUMA Jun, Ph.D.
Professor
Master's/Doctoral program of Computer Science,
Degree programs in SIE,
Graduate School of Science and Technology,
University of Tsukuba

E-mail address: jun@cs.tsukuba.ac.jp
URL: https://www.mdl.cs.tsukuba.ac.jp/

安全・安心な人工知能/機械学習技術の確立を目指して

機械学習技術の急速な発展に伴い、画像や音声などの認識精度が人間の認識能力を超える程度にまで改善しました。機械学習が優れた予測・認識能力を発揮するためには大量のデータが必要となります。当研究室では、データが個人情報を含む場合に、プライバシ保護と機械学習における活用を両立させるための暗号理論や統計的プライバシ保護技術を研究開発しています。今後は機械学習が人間や社会にとって重要な判断や意思決定の一部を担うようになることが予想されます。研究室レベルでは良好に動作する機械学習も、社会で実際に利用される場面においては、その悪用を企む者の存在のために、安定的に期待した動作をするとは限りません。当研究室では、AIを安定に動作させるためのAIセキュリティ技術を研究しています。

Safety and Security of AI/Machine learning

Large amounts of data are required for machine learning to demonstrate excellent prediction and recognition ability. We study cryptographic theory and statistical privacy protection technology that achieve both privacy protection and machine learning when data contains personal information. Machine learning is expected to support important decision-making performed by experts. Machine learning is expected to support important decision-making for humans performed by experts. Machine learning that works well at the laboratory level while it does not necessarily produce the expected behavior because of the existence of those who are planning to misuse it. Our laboratory is studying AI security technology to make AI operate stably.