# AI技術を利用したサイバー攻撃対策の開発

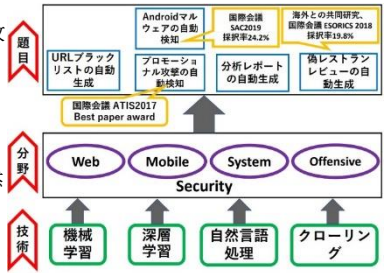
情報科学研究科　森川 智博

## キーワード

サイバー攻撃、攻撃者の視点、人工知能技術

## 研究概要

サイバー攻撃は検知を回避することを意図して巧妙に作成されてきたため、既存の対策に関しては攻撃者の手口の進化に追いついていないのが現状です。本研究室では、実世界でのセキュリティ対策の遅れを目の当たりにし、自然言語処理や深層学習などの技術を利用することにより、未知の攻撃を早期かつ自動的に発見することを狙いとするだけでなく、攻撃者の視点に立ち、最新の人工知能技術を悪用する攻撃手法の実現とその対策の確立を行うことも目指しています。例としては、アプリマーケットにユーザが投稿する大規模かつ不均一なレビュー・コメント情報に深層学習をベースとした自然言語の生成手法を適用し、より人間の言葉に近い不正レビューを自動的かつ大量に捏造することや、それらの不正レビューに対して既存の手法が対応できない高精度かつ高効率な検知アルゴリズムを開発することなどが挙げられます。




## アピールポイント

攻撃者は常に新しい攻撃手法を作り出し、既存の検知システムを回避しています。そのような戦略に対して、攻撃者の思考を先回りするセキュリティ対策が有効であり、従来方法でカバーできなかった検知手法の開発が期待できます。本研究では、国立研究所や国内外の大学等と連携しながら進めています。

## 応用分野

モバイルセキュリティ、ネットワークセキュリティ、IoTセキュリティ、システムセキュリティ、ユーザブルセキュリティ