能動的サイバー防御に関する研究

研究分野：サイバーセキュリティ、ネットワークセキュリティ

キーワード：能動的サイバー防御、AIに対する欺瞞とその対策

貢献できるSDGsの区分：

情報システム学部　情報セキュリティ学科 教授 武仲正彦

教員情報URL https://sun.ac.jp/researchinfo/take-masa/

研究概要

サービス妨害やランサムウェア等のサイバー攻撃が激化する一方、保護対象についてもブロックチェーンやAIなど日々新しい技術も増加している。また、世界では「能動的サイバー防御」の必要性が唱えられているが、法的・倫理面での問題も指摘されている。本研究では、最新のサイバー攻撃の分析を行い、様々な技術・サービスに対する対策技術の研究開発に取り組む。また、法的・倫理的にどこまでの能動防御が可能かについての検討も並行して実施する。

また、様々なシステム、サービスへの人工知能（AI）の活用が拡大してきている。AIの活用は、自動化による業務の効率化・生産性向上だけではなく。人間の集中力低下により発生するミスの低減などにも貢献する。一方で、AIは人間とは異なる判断ロジックを用いるため、人間には容易に判断できるものでも、AIは誤った判断を下す場合がある。それを恣意的に実現するのが「AIに対する欺瞞」であり、敵対的生成ネットワークというAI技術を用いれば、容易に「AIに対する欺瞞」が可能になる。本研究では、「AIに対する欺瞞」の分析を行い、それに対する対策技術の研究開発に取り組む。

産学連携の可能性（アピールポイント）

- サイバー攻撃の最新トレンドに基づく防御技術の共同開発
- IoTや産業用制御システム（ICS）に特化したセキュリティソリューションの共同開発
- ランサムウェア攻撃の事前検知・被害最小化システムの開発
- AIシステム向けのセキュリティ評価サービスの提供
- AIに対する敵対的攻撃に強いモデルの共同研究
- サイバー倫理・法制度の共同研究と政策提言
- サイバーセキュリティ人材育成の教育コンテンツ提供

外部との連携実績等

今年度に企業から大学への移籍した直後のため、本学での連携実績はない。

- [現在]英国Queen Mary大学と共同で両国政府の共同公募（AI・情報）に応募中
- [現在]シンガポール本社のセキュリティ企業との共同研究の詳細検討中（サイバーセキュリティ）
- [現在]首都圏企業との共同研究の詳細検討中（量子セキュリティ）
- [今年度]県議会議員向けの研修での講演を予定（10月、生成AI）