所属：豊田工業高等専門学校　情報工学科

研究タイトル：

高度サイバー攻撃の振る舞い型検知技術

氏名：	平野　学　／ HIRANO Manabu	E-mail：	hirano @toyota-ct.ac.jp
職名：	教授	学位：	博士（工学）
所属学会・協会：	IEEE，情報処理学会，電子情報通信学会		

キーワード：	サイバーセキュリティ
技術相談 提供可能技術：	・仮想化技術と深層学習を用いた振る舞い型の高度サイバー攻撃の検知技術 ・ランサムウェアなど高度サイバー攻撃の再現と解析をする隔離環境 ・サイバーセキュリティ教育教材

研究内容：

高度サイバー攻撃のための振る舞い型検知技術

ランサムウェアや高度標的型攻撃（Advanced Persistent Threat, APT）などの脅威が増しており，早期に攻撃の兆候を検知して食い止めることの重要性が高まっています。我々の研究室では従来のオペレーティングシステム層で提供されるセキュリティ機能が攻撃された場合でも継続的な保護を提供するため，国産の仮想化技術[1]を用いて「多層防御（Defense in depth）」をおこなう手法を研究しています。仮想化層で得たサイバー攻撃の振る舞いの兆候を深層学習によって学習させて攻撃を早期に検知します。最新の研究成果はセキュリティ分野のトップジャーナルに採録されています[2][3]。

[1] Shinagawa, T. et al. “BitVisor: a Thin Hypervisor for Enforcing I/O Device Security,” In Proceedings of the 2009 ACM SIGPLAN/SIGOPS VEE09, pp.121-130, 2009.
[2] Hirano, M., et al. “RanSAP: An open dataset of ransomware storage access patterns for training machine learning models.” Forensic Science International: Digital Investigation, 40, 301314, 2022.
[3] Hirano, M., et al. “RanSMAP: Open dataset of Ransomware Storage and Memory Access Patterns for creating deep-learning-based ransomware detectors.” Computers & Security 150, 104202, 2025.

高度サイバー攻撃の再現と解析環境

ランサムウェアのような高度なサイバー攻撃に使われる検体を実行し、挙動を解明するためには隔離環境を用います。我々の研究室では右の写真に示すような解析環境を用いることでサイバー攻撃の再現と検知をする研究をおこなっています。

サイバーセキュリティ教育教材

高専機構のセキュリティ人材育成事業の一環としてノートパソコン上で DNS キャッシュポイズニング攻撃と防御を体験する教材を開発しました。高価な市販のサイバーレンジを使わずに学生のノートパソコンだけでサイバー攻撃の防御演習（サイバーレンジ）をおこなうノウハウを提供します。

提供可能な設備・機器：

名称・型番（メーカー）	
ランサムウェア検体を隔離環境で安全に実行できる解析環境	
MITRE ATT&CK に基づき高度サイバー攻撃を隔離環境で安全に実行できる解析環境	
コンテナによるサイバー攻撃の防御演習教材	