所属：豊田工業高等専門学校　情報工学科

研究タイトル：

仮想化技術、ID 管理、デジタルフォレンシックス

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，ディジタルフォレンジック		
技術相談 提供可能技術：	・仮想計算機モニタ　BitVisor　を用いたディジタルフォレンジックのシステム ・フォレンジックデータから証拠を迅速に発見する分散並列処理システム ・ランサムウェアなどのマルウェア解析と機械学習による自動判別 ・サイバーセキュリティ教育		

研究内容：

仮想計算機モニタ　BitVisor　を用いたディジタルフォレンジックのシステム

研究室では、(1) 監視対象のコンピュータから自動的にディスク入出力などのシステムの挙動を示すデータをクラスタへ転送してロギングする 「監視システム」と、 (2) 得られた監視データを統計処理ならびに機械学習で分析して大量データからインシデントに関連するデータを探し出す「解析システム」を開発している。提案システムは、サイバー犯罪や各種インシデントが発生した際に、過去のタイムラインを再構築し、大量のデータを高速に解析、インシデントの証拠を発見するのに用いる。学術論文 [2] をベースにシステムを開発している。

[1] Takahiro Shinagawa, 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.

フォレンジックデータから証拠を迅速に発見する分散並列処理システム

学術論文 [2] において、確率的なランダムサンプリングに並列分散 処理クラスタの演算を組み合わせることで、提案する「解析システム」を用いて 99%の信頼度で 100 TiB の大量の解析データから 10 MiB の証拠データを 約 3 分 で検索できることを示した。大量のデータから効率的に証拠を発見することが可能である。

[2] Hirano, M., Tsuzuki, N., Ikeda, S., & Kobayashi, R. (2018). LogDrive: a proactive data collection and analysis framework for time-traveling forensic investigation in IaaS cloud environments. Journal of Cloud Computing, 7(1), 18, Springer.

ランサムウェアなどのマルウェア解析と機械学習による自動判別

マルウェアを隔離された環境で安全に実行させ、挙動を上記の「監視システム」で解析するシステムを構築している（写真）。

サイバーセキュリティ教育

高専生向けのサイバーセキュリティ演習を実施している。隔離環境を構築して攻撃ツールを動作させ、いかに安全なシステムを構築するかを授業で実施している。

提供可能な設備・機器：

名称・型番（メーカー）	
ディジタルフォレンジック目的の監視と解析サーバ 分散並列処理クラスタ	
マルウェア解析環境	