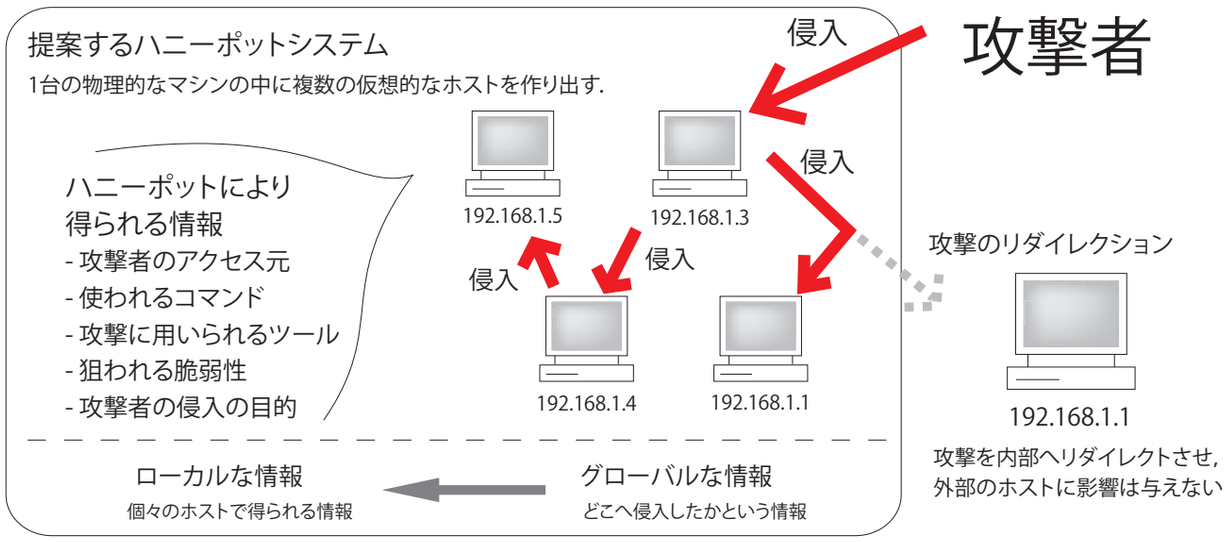
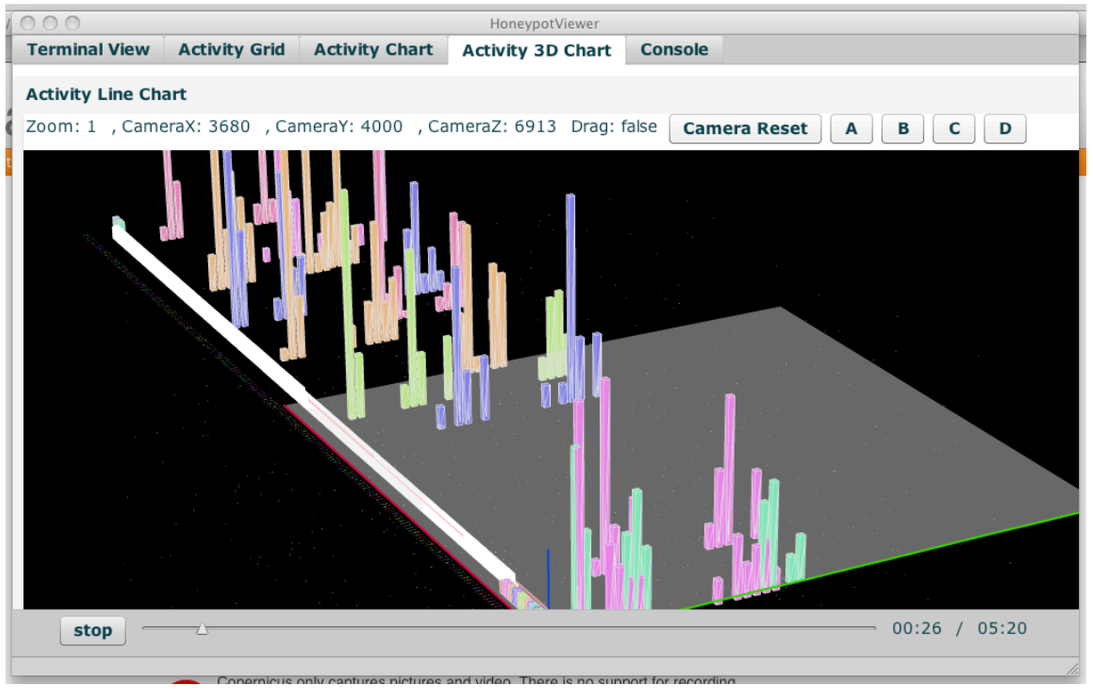
仮想ネットワークを利用した攻撃監視システム

- 安全に攻撃者・マルウェアの攻撃行為を観察する -

複数の仮想的なホストを内部に持つ攻撃監視システム(Honeypot)を実装した.
仮想的なホストを作り出し攻撃をそこへリダイレクトさせることでシステム外部へ危害を与えることなく攻撃者の行動を観察することができるのが特長である(下左図).
また，これらのホスト全体でログを得られるという利点を活かし，ホスト間にまたがった侵入者・マルウェアの情報の提供をグラフィカルに行った (下右図).





「プロセスレベルの仮想化」により1台のホストの中で複数のホストを作り出し，攻撃者をその中に閉じ込め，彼等の情報を安全に収集する.

2009年度上期未踏IT人材発掘・育成事業(未踏ユース)
鈴木友博 (東京大学)