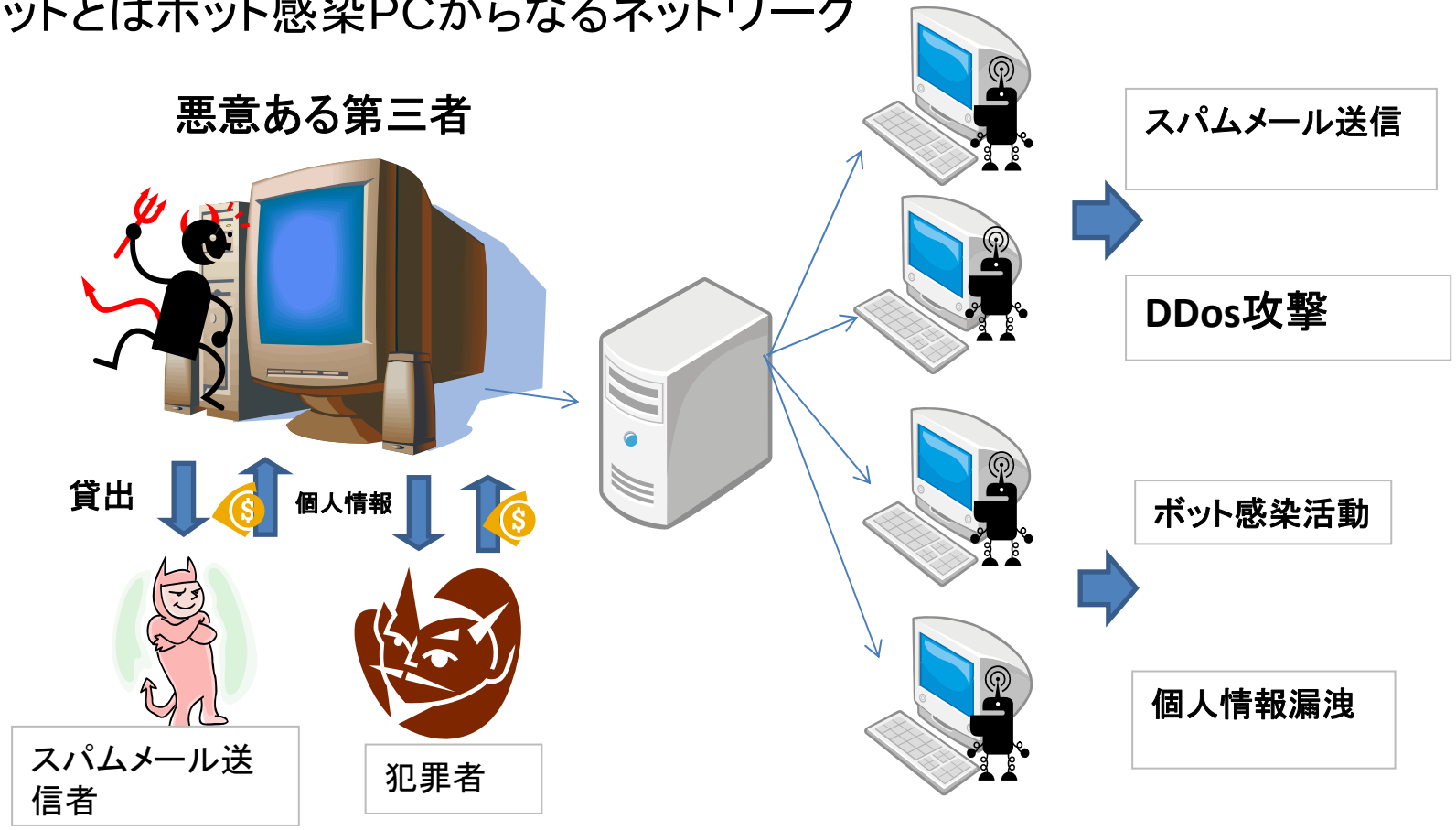
P103　スパース構造学習によるボットネット検出の検討

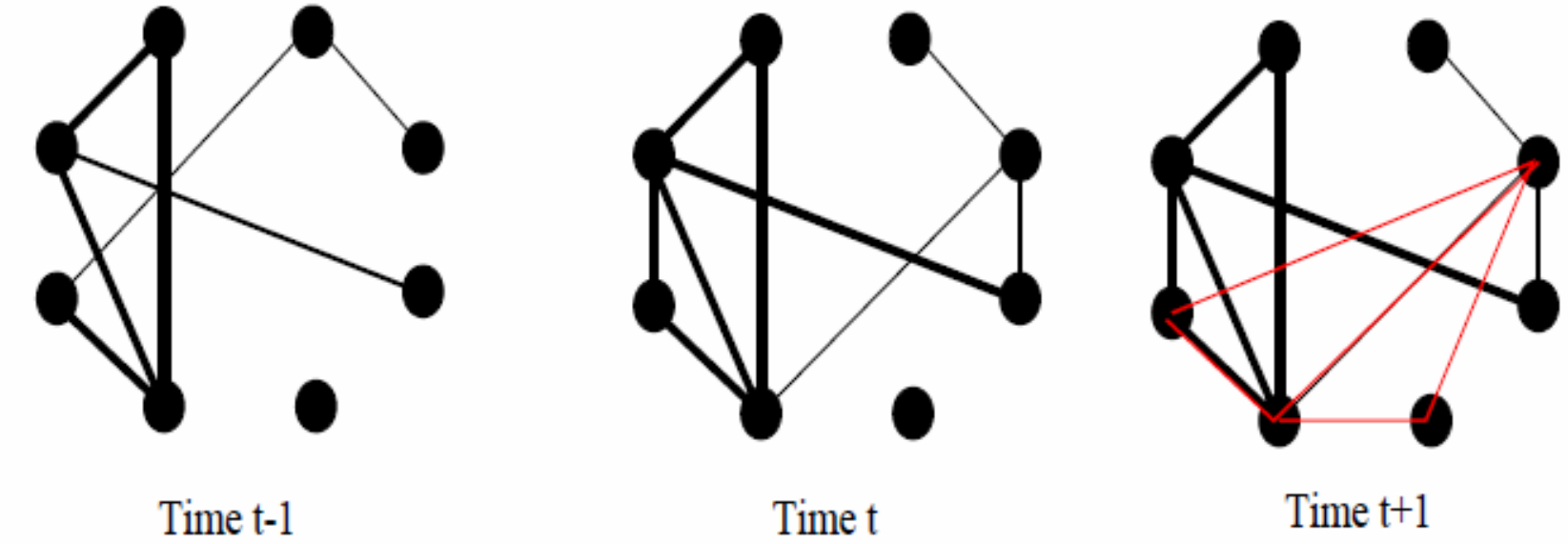
九州大学,九州先端技術研究所　村上慎太郎,濱崎浩輝, 川喜田雅則,竹内純一
横浜国立大学　吉岡克成
情報通信研究機構　井上大介,衛藤将史,中尾康二

ボットネットとはボット感染PCからなるネットワーク



提案手法の概要

グラフの変化を検出



・ノードはソースホストを表す
・各ホストからセンサ(ダークネット)に届くパケット数の時系列を観測
・エッジの太さはノードの時系列間の相関の強さ(エッジがないものは相関なし)

バックグラウンドの通信が定常ならボットによる通信が行われた場合
　　ボットのペアに対応する共分散が一様に増加する
ただしデータが高次元小標本であること、ほとんどの通信が独立であることから
共分散行列の推定をスパース構造学習であるglasso（Friedman,2009）を用いて行う