悪性活動の紐づけ・可視化方式に関する研究
Research on a method for linking and visualizing malignant activity

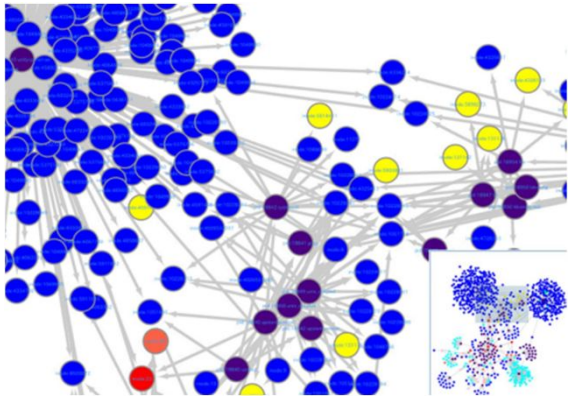
齋藤太新・マネジメント分科会・情報セキュリティ大学院大学

背景：システムに残されたログから攻撃源や悪性活動の全体像を特定する作業の簡易化・効率化のため、ファイルやプロセスの依存関係グラフを活用

課題：依存関係の爆発（グラフのエッジ数が大量になる）問題

先行研究での対処法
- エッジに重みづけ
  （イベント発生頻度、データフロー量等が指標）
- 攻撃の分析に重要ではないイベントの削除
  （一時ファイルの削除等）

より攻撃に関係のある依存関係だけ残す必要がある



依存関係の爆発

今後の研究計画
手法の立案（依存関係をさらに削減できる手法）→ 実装 → 評価実験