ネットワーク フォレンジック

東京電機大学
八槇　博史

ネットワークフォレンジック

ネットワークフォレンジックとは、「セキュリティ上の攻撃や問題を発生させるインシデントの発生源を発見するために、ネットワーク上のイベントをキャプ チャ、記録、分析すること」である。

ネットワークフォレンジックのタスク

各種の記録から「何が起きているのか」を解析・復元する

- ファイアウォール
- プロキシサーバ
- メールサーバ
- IDS/IPS
- パケットダンプデータ等

多岐にわたるデータを、対象となるネットワークシステムから抽出し、組合わせることが必要

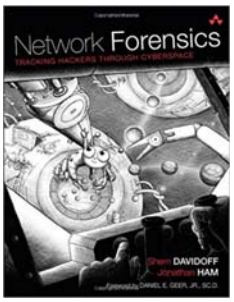
ネットワークフォレンジックの特性

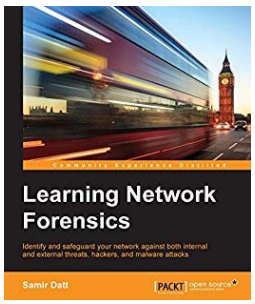
- 分散した情報源
  - 複数のシステムのデータをつなぎ合わせて事象を再現
  - 一つないし少数の筐体に注目することの多い旧来のデジタル・フォレンジックとはやや異質
- 膨大な時系列データ
  - ネットワークシステムの中で様々な事象が時系列で発生進行する事態に対して同時並行的に対処する
- 多くの事象は正常系によるもの
  - 「異常かつ危険な兆候」をどのように識別するかが課題

「デジタル・フォレンジックの基礎と実践」記述に当たっての底本

ネットワークフォレンジックに関する教科書

- Network Forensics: Tracking Hackers through Cyberspace, S. Davidhoff 他, 2012.
- Learning Network Forensics, S.Datt, 2016.
- Incident Response & Computer Forensics, J. Lutgens他, 2014





従来の書籍等の課題

どのテキストも、具体的なツールの説明に行きがち

- 方法論に基づいてどのような計画のもとに何を行う、というよりも、各種のツールを使うとどういう情報が得られるか、に主眼がおかれている
  - ツールが使えるようになるのだが、「わかった」感じがもう一つ足りない

攻撃方法や解析環境の進化とそれへの追従

- IDS、IPS
- ログ監視システム
- SIEM
- AIによる攻撃監視　　etc.

今後に向けて

- 体系化
  - 他のデジタル・フォレンジック各分野と比較して立ち後れ感
  - 「証拠保全ガイドライン」との対応など
- 演習環境
  - 現状ではパケットダンプやすでにあるログの分析など
  - サイバーレンジ的なシステムを使って情報収集を行うなどの高度化が本当は望ましい
- ネットワーク技術に関する前提知識
  - CySecではTCP/IPの各種プロトコルなどは知っている前提だが、他の教育環境に適用するときにはそれでよいか