JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

ハニーポットWG２００４年度 活動報告

園田　道夫

2005年6月13日

ハニーポットの種類

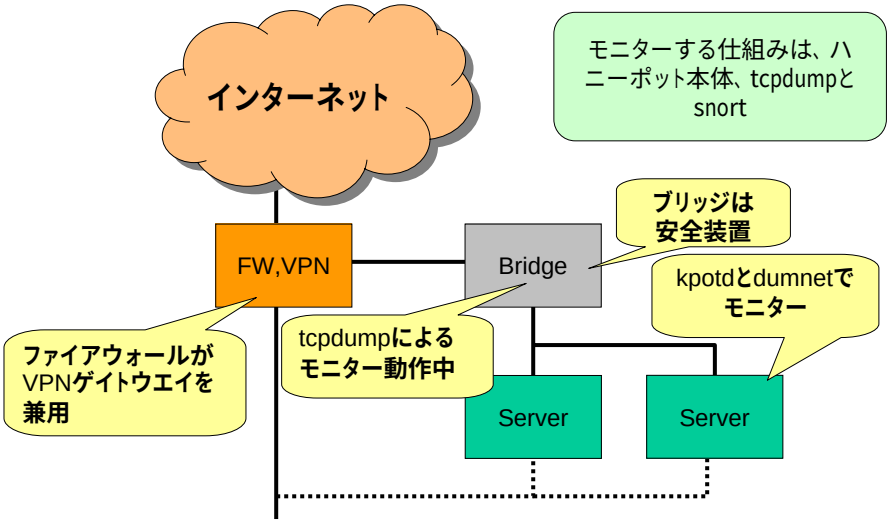
JNSA

- 第一世代ハニーポット（エミュレーションサーバー）
  - Symantec社のDecoyサーバー（旧ManTrap）
    - http://www.symantec.com/region/jp/products/decoy/
  - Network Security社のSpector
    - http://www.specter.com/default50.htm
  - honeyd
  - kpotd
- 第二世代ハニーポット（ハニーネット）

honeynet.orgによる世代定義

第一世代	エミュレーション 擬似的なサーバ
第二世代	本物と変わらないサーバを記録、分析システムが取り囲む
第三世代	第二世代の進化形 CDROM化、シグネチャの自動更新など

現在稼働中のネットワーク



現在の外部仕様

- 外からはとにかく接続できる（ACKを返す）サーバーとして見える＝dumnet
  - 第一世代ハニーポット（エミュレーション型）
  - 取得できる情報には限りがある
- 外からは何種類かのサーバーに見える＝kpotd
  - 第二世代に近い（Sebekプラスアルファ）
  - dumnetよりは多くの情報が取得できる

取得できる情報

- dumnetは単独ではログを取得しないため、tcpdumpのログになる
  - ACKを返し続けるだけ
- kpotdはexeclogとttylogを取得できる
  - ローダブルカーネルモジュール
  - execlogはカーネルコールのログ
  - ttylogはキーストロークのログ

取得結果などの報告書

- とりまとめ中m(_ _)m
- しばらくお待ちください

今後の計画

- 第三世代ハニーネット化
- Windowsハニーポット
- データ集中管理実装

今年度前半？

ハニーポットとなるサーバーを増強し、Security Consoleなどによる監視、解析も行っていく予定