JNSA

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

ハニーポットの使い方

ハニーポットWG
園田道夫

ハニーポットとは

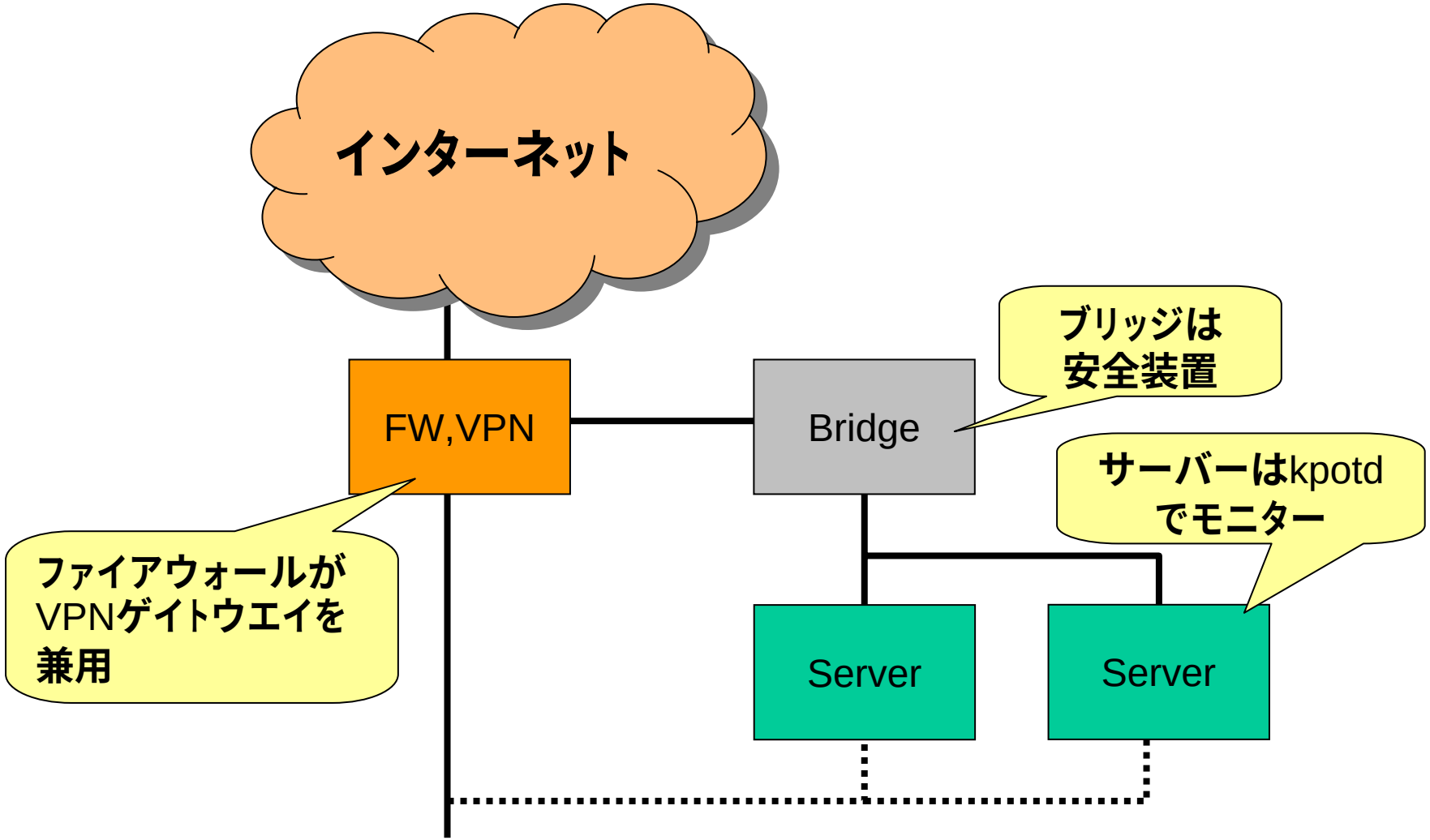
- Unauthorized Accessを記録する仕組み
- 脆弱であるフリをして、誘い込むサーバー

- 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
- その他いろいろ

ハニーポット事例とか(主に日本)

- honeynet project
  - http://www.honeynet.org/
  - http://www.vogue.is.uec.ac.jp/secteam/honeynetpapers/ (有志による日本語訳)
- Windowsセキュリティ ハニーポット顛末記
  - https://www.port139.co.jp/ppt/SThoneypot.pdf
- 濱本さんのVMwareハニーポット
  - http://internet.watch.impress.co.jp/cda/event/2003/10/24/886.html
- LAC社のSombria Project
  - http://www.lac.co.jp/security/intelligence/sombria/
  - http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20040220/140204/
- 田原さんの記事
  - http://www.atmarkit.co.jp/fsecurity/special/13honey/honey01.html

ハニーポットWGの ハニーネット



活動報告っぽいことも書いておかないと

JNSA

- 構成、実装の検討
  - 踏まれないようにする
  - とはいえ、お客さんが少しはいろいろできるようにする
- お客さんへのプロモーション
  - ポートが開いているというのが最大のプロモーション
- 現在使用しているブツ（予定も含む）
  - NetScreen、Snort（1CD）、FW-Bridge、VMware、kpotd、dumnet
- インシデントレスポンスは複数で24時間以内の対応
  - もちろん土日はお休み（笑）？

唐突ですが、定点観測について

- 現在の定点観測の問題点
  - 詳しいことがわからない（次にどんなものが、どこからどうやって出てくるのかわからない）
  - 地震予知のようなもの？（振動や火山活動が活発になっている、程度？）
- ハニーポットが解決策になり得るのか？
  - ハニーポットは手間がかかるわりに大したデータが取れないと思われているが、ほんとうにそうなのか？
  - さらに詳細な情報を得て、定点観測を補完できないか？
  - ワームなどの大規模災害の予測、延焼遅延に使えないか？

観測装置としてのハニポ

- IP、TCP、UDP、ICMPなど、プロトコルレベルでのデータ収集装置
  - 量的変化を分析（トラフィック解析）することでさまざまな傾向を洗い出す
  - 観測装置dumnet
  - 分析支援ツール
    - RRDTOOL（http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/）
    - CACTI（ http://www.raxnet.net/products/cacti/）
- ペイロードデータの収集装置
  - この側面はいろいろ微妙
  - しかし、検体は取りたい
- キーログ取得装置
  - 攻撃的アクセスの情報はやっぱキーログに限る（by Sombria）
- Honeynet Security Console
  - http://www.activeworx.org/programs/hsc/index.htm

進化形観測網への応用

- ハニーポット、ハニーネットなどの仕組みを基軸に、現在と異なる側面からの観測を行う調査研究が必要
  - 仕組みの基軸がハニーポット、ハニーネットで良いのかどうか、検証する
  - ハニーポット、ハニーネットを大規模化して運用できる仕組みを構想、構築する
- トラフィック解析、パケット解析、定量化などの研究開発も行いながら、総合的に災害判断を助ける観測網を構築する
- 同時に、観測分析できるスペシャリストも育成していく
  - そのためのノウハウ蓄積
- 観測行為の法的側面についても研究していく

- ・・・中期的には「人材育成」と「仕組みの構築」による実効性ある観測網の構築を、長期的には「災害に強いネットワークインフラを支える仕組み」を目指す

ハニポの応用

- トラップ（誘導技術含む）
- ワーム拡散遅延装置
- 異常検知型IDS（侵入検知システム）

- いずれにしても新しい考え方による分析が必要になりそう
  - 観測装置の仕様もそれによって決まってくる