通信源ホストの分類を利用したダークネット通信解析

早稲田大学 基幹理工学部
笹生　憲, 森　達哉, 後藤　滋樹

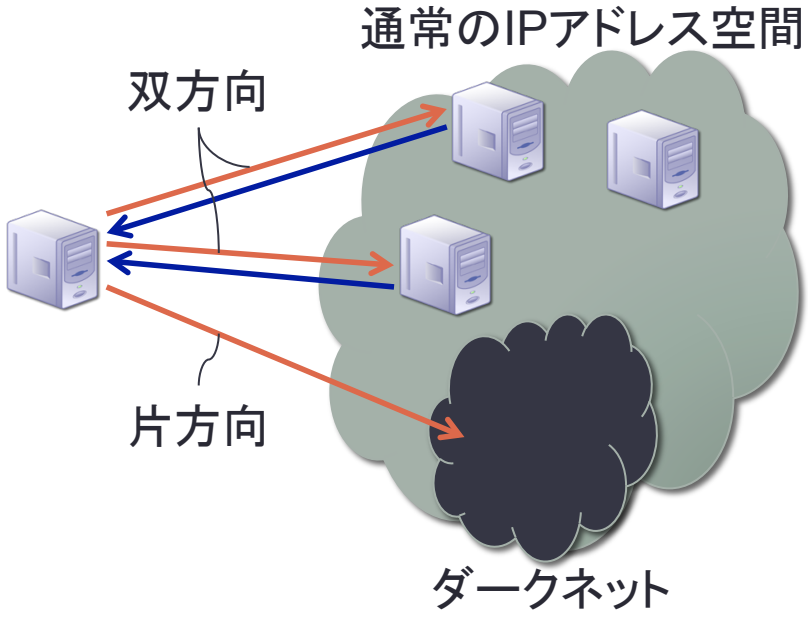
2013年10月23日
MWS2013

目次

- 研究の背景
- 研究の目的
- データセット
- 提案する分析手法
- ケーススタディ
- まとめ

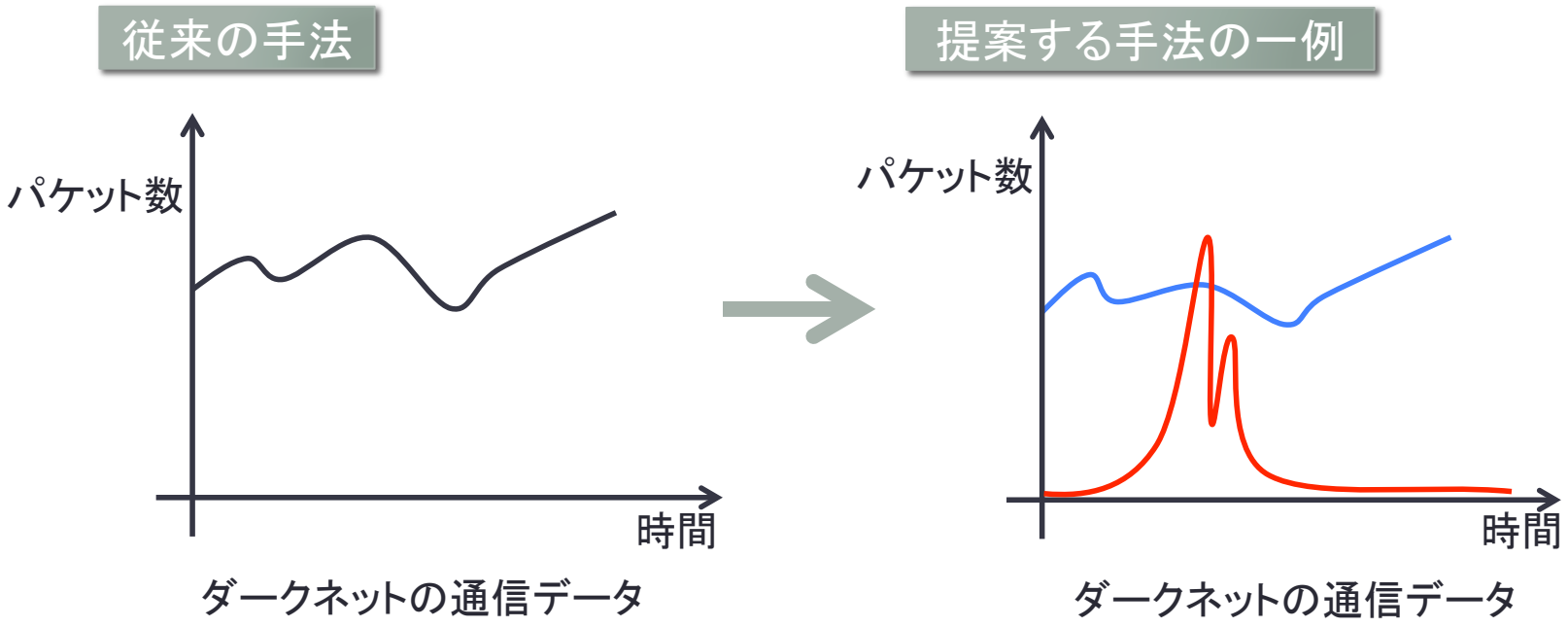
研究の背景

- ダークネットとは、未使用かつ到達可能なIPアドレス空間を観測するシステム
- ダークネットで得られる情報は限定されている
- 脅威の予兆となるパケットが大量のパケットにうもれてしまっている



研究の目的

- ダークネットの通信データから、より多くの情報を獲得する手法を提案する



データセット

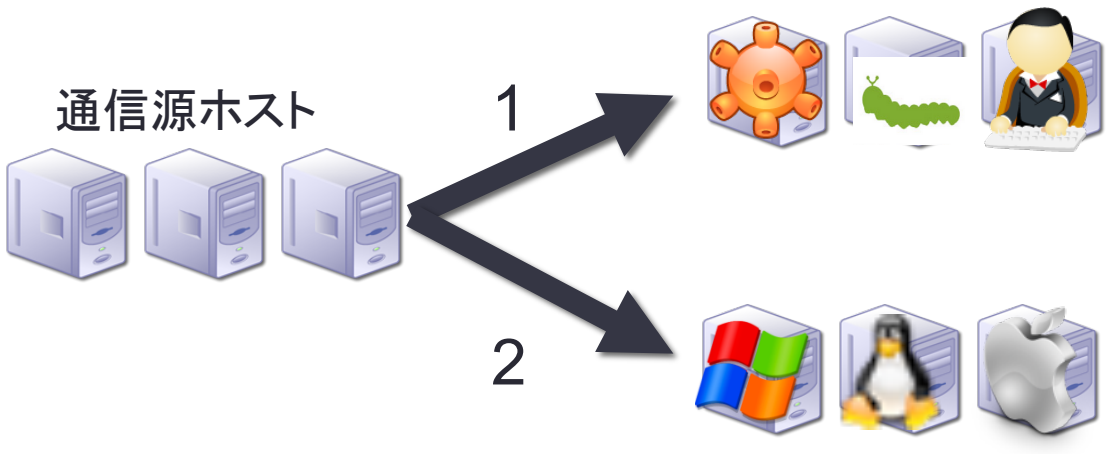
- nicter darknet 2013
  - 情報通信研究機構により提供されたデータ
  - NONSTOP上で分析を行った
  - 4096個のIPアドレス
  - 2011年1月1日から2012年12月31日までの2年間のデータ

- データ概要
  - 総パケット数　・・・　113,010,088
  - 総ホスト数　　・・・　　7,564,109

分析手法

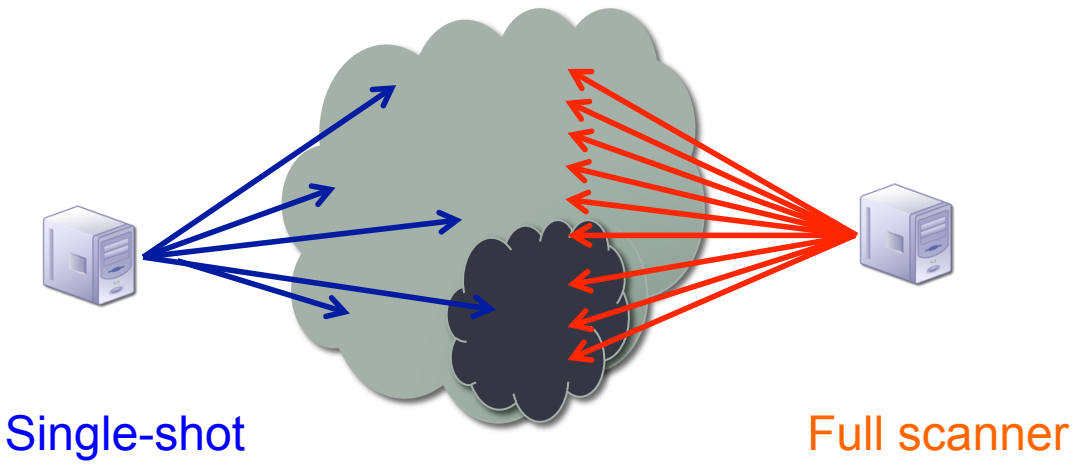
1. 通信源ホストが、どのような通信パターンをとったかで分類する

2. 通信源ホストのOSにより分類する



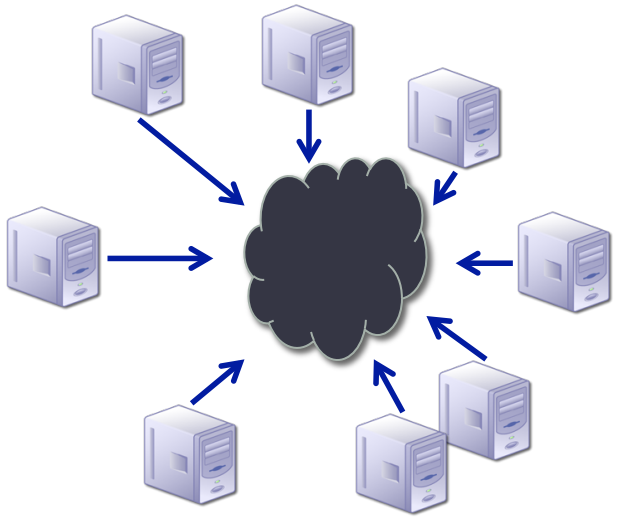
1. 通信パターンによる分類

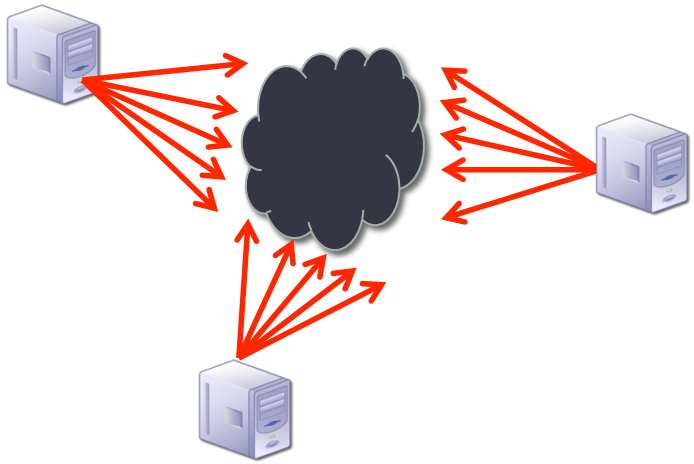
- 通信パターン
  - Single-shot：
    ダークネットで、一つしかパケットを観測されなかったホスト
  - Full scanner：
    ダークネットのIP空間すべてに対してパケットを送信したホスト



通信パターンによる分析

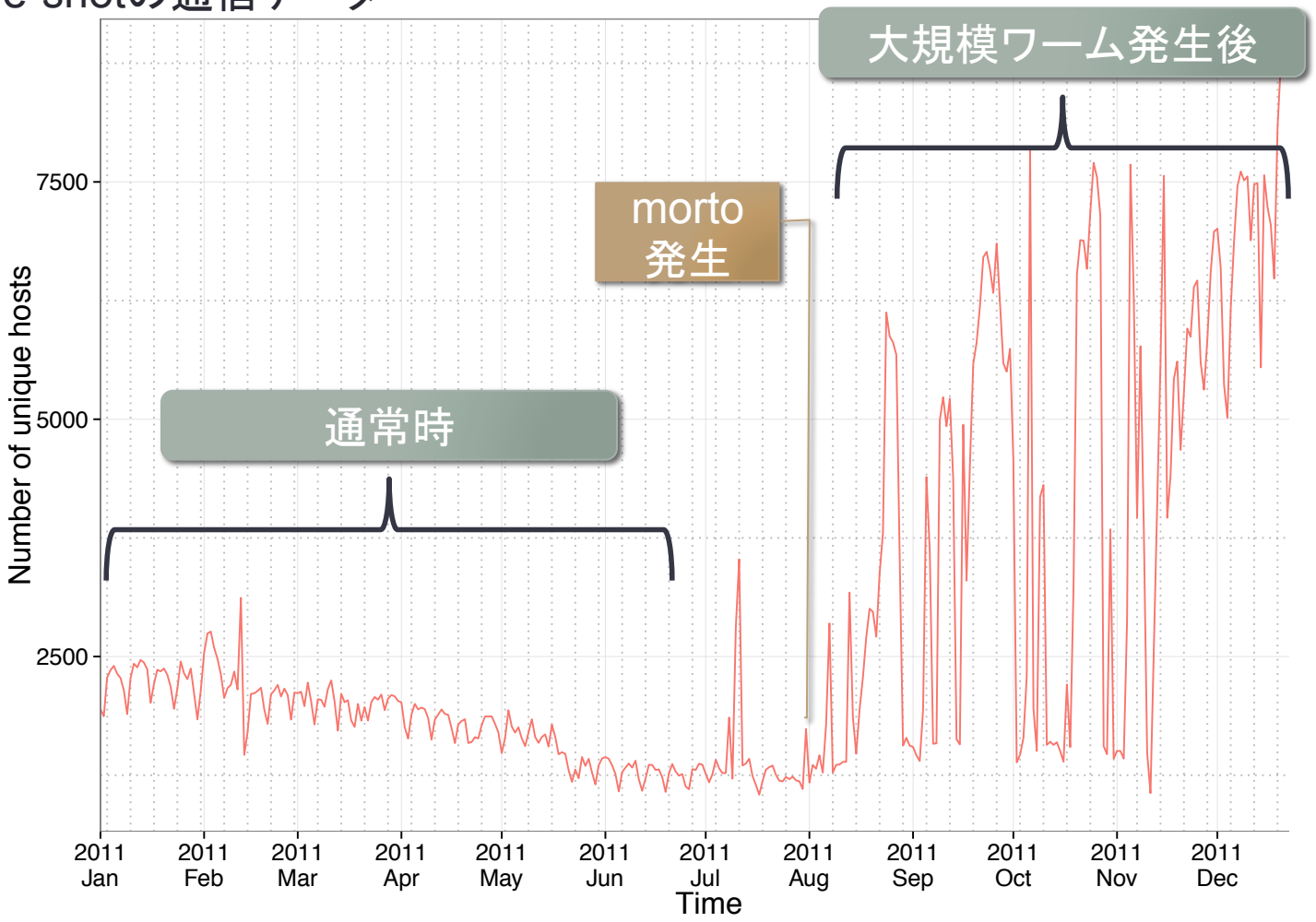
- Single-Shot
  - パケット数は全体の3%
  - ホスト数は全体の42%
- Full Scanner
  - パケット数は全体の55%
  - ホスト数は全体の0.1%





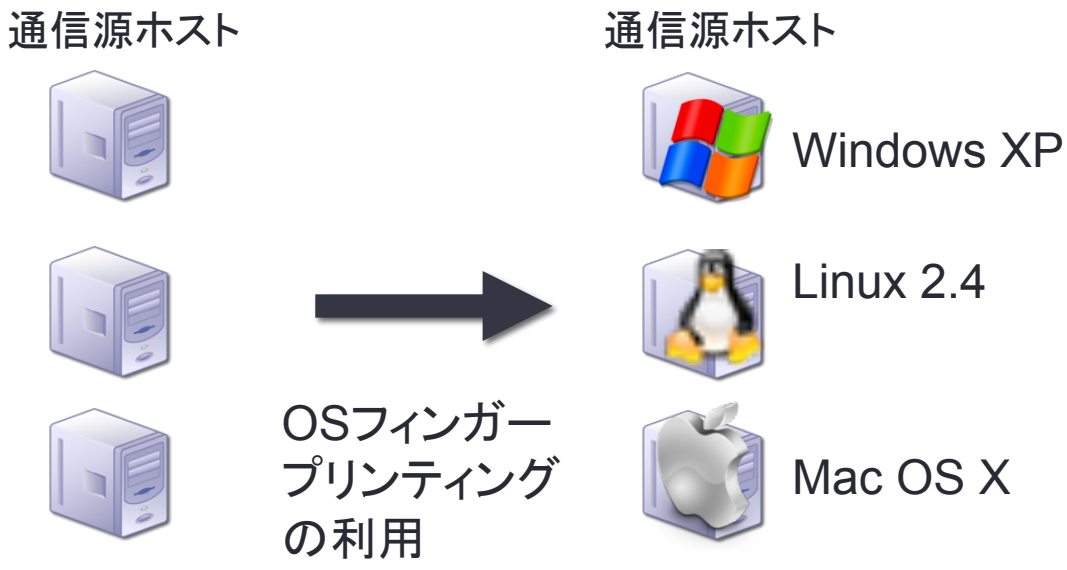
通信パターンの変化

Single-shotの通信データ



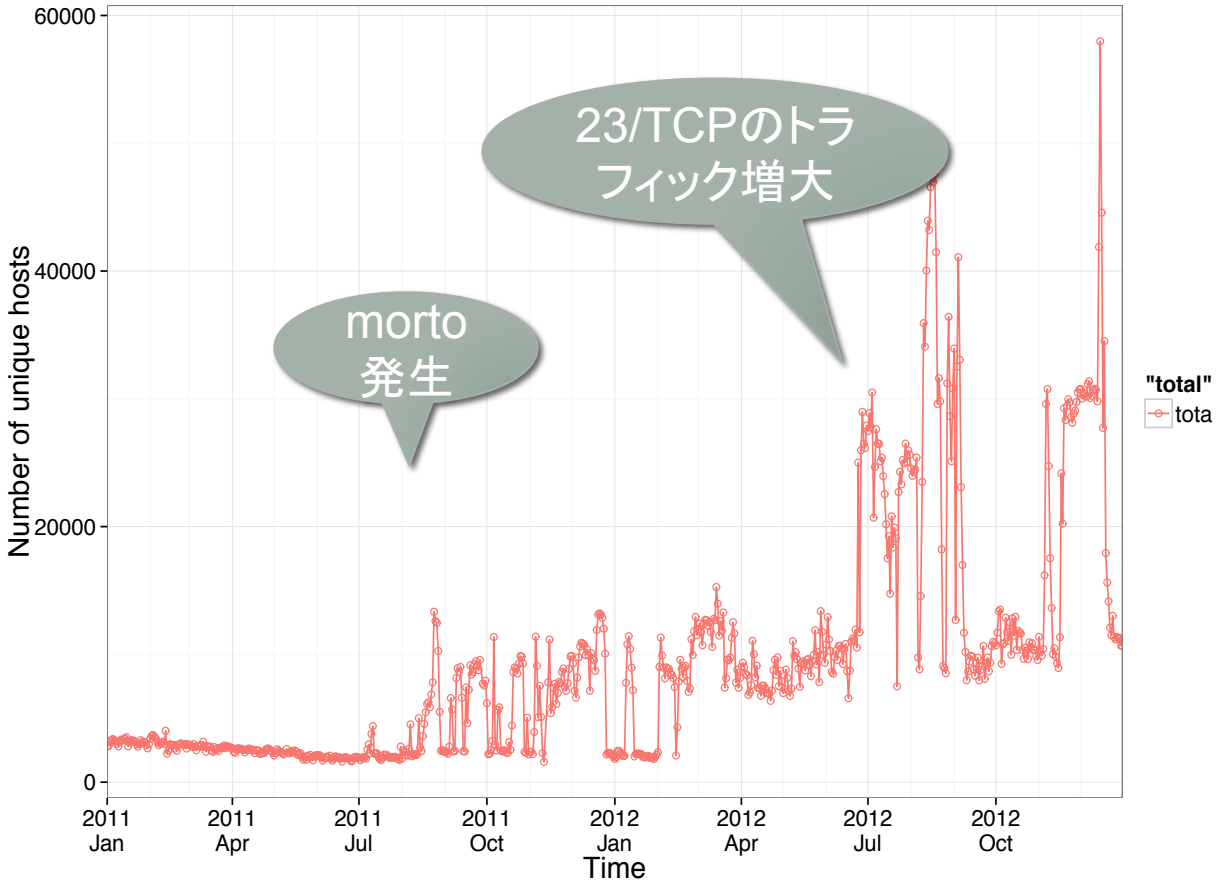
2. ホスト種別による分類

- OSフィンガープリンティングの利用
  - TCP/IPスタックの実装がOS毎に異なる事を利用して、TCPパケットのヘッダ情報から通信源のOSを推定する技術である
  - p0fというツールを利用して、通信源ホストのOSにより分類をおこなった



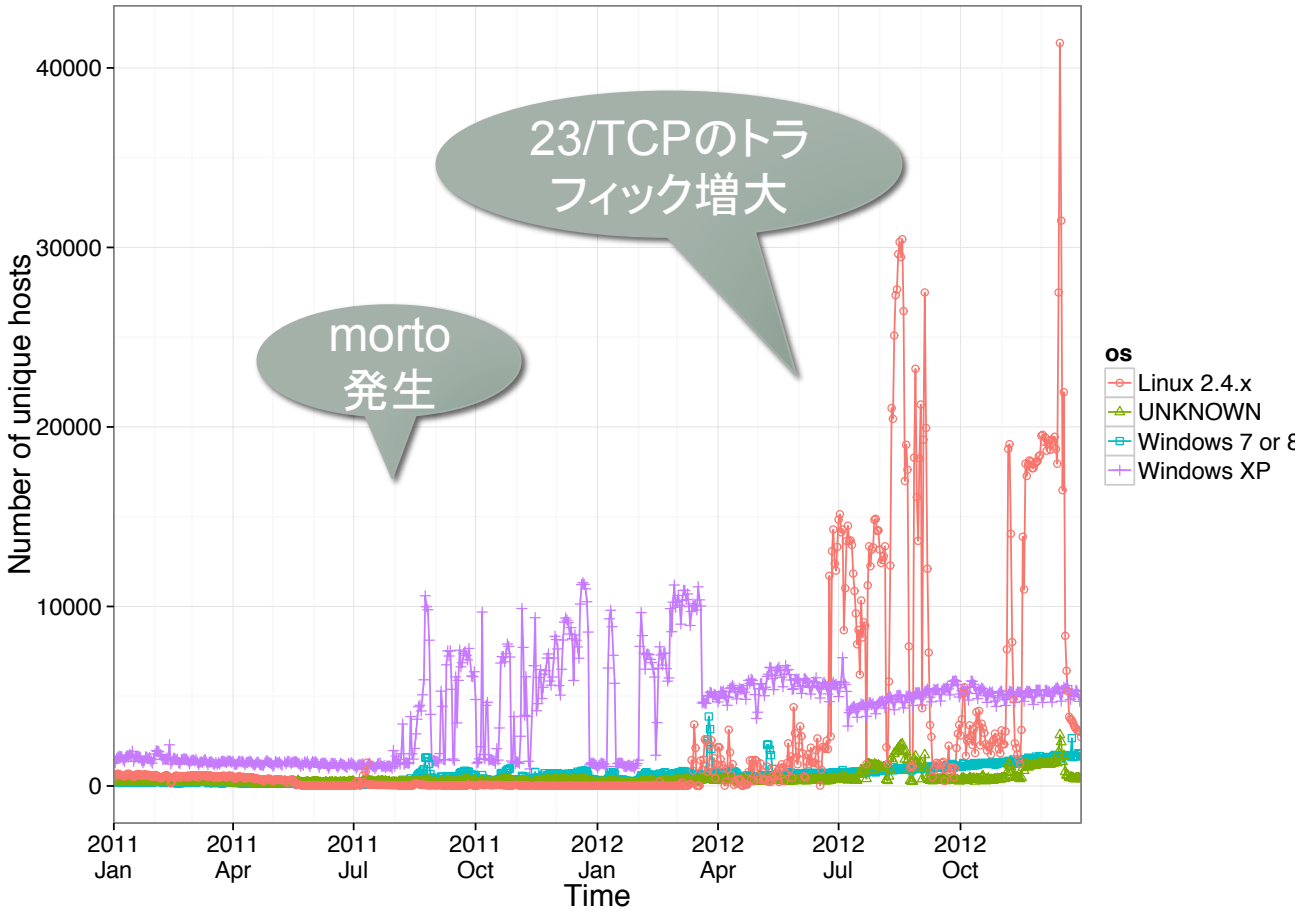
ホスト種別による分析

- ユニークホスト数（従来の手法）



ホスト種別による分析

- ホスト種別によるユニークホスト数



ケーススタディ

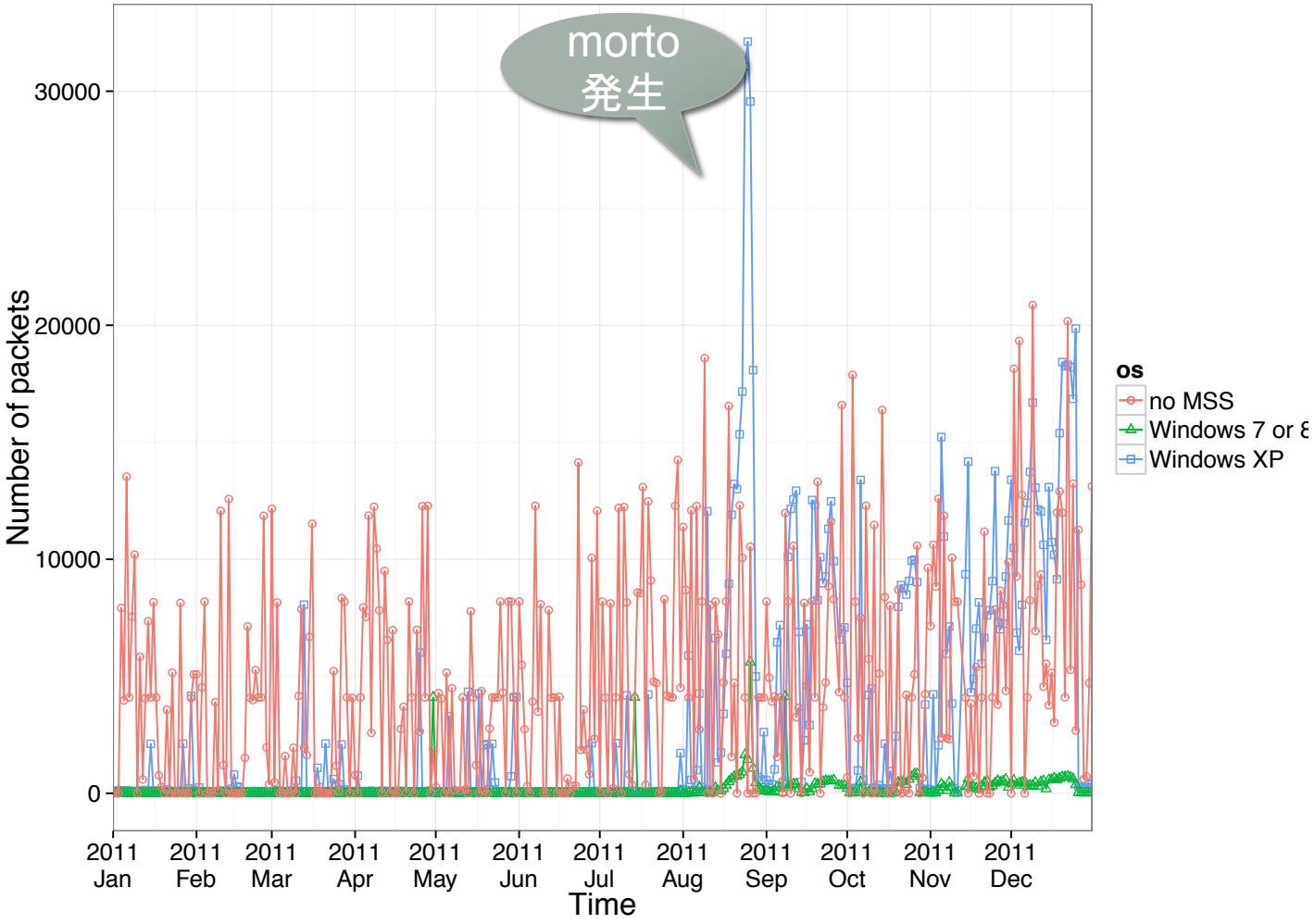
1. 大規模感染マルウェア Morto
2. 23/TCPのトラフィックの増大
3. Apple端末の通信解析

大規模感染マルウェア Morto

- Morto
  - 時期　　・・・　2011年8月末ころ
  - 感染経路　　・・・　3389/TCP
  - 感染する環境　・・・　Windows系

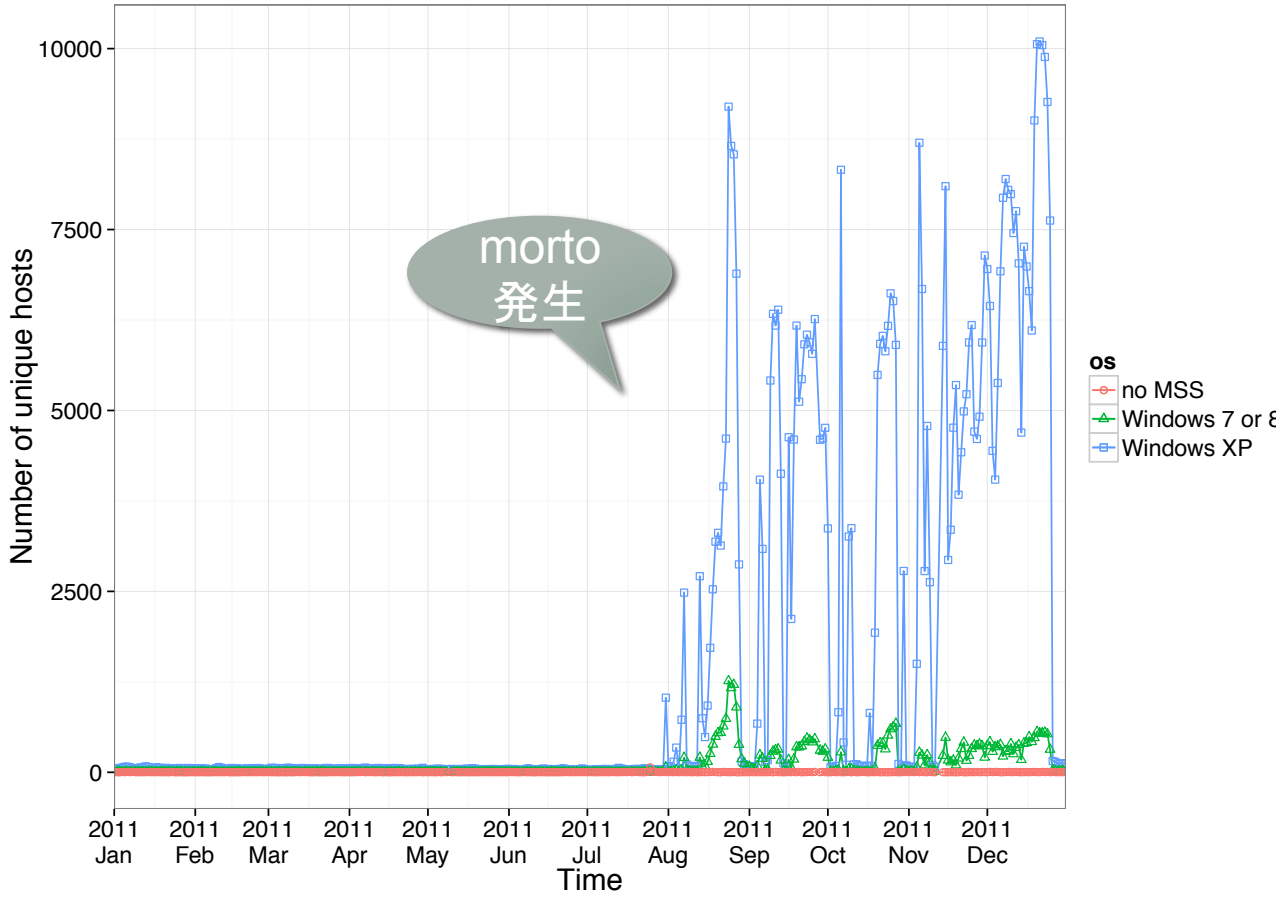
- 発見した事
  - 3389/TCPには、Full scannerの傾向をみせるアクセスが常にあった
  - Full scannerを見せるホストMortoの発生に影響を受けなかった
  - 急激な通信の増加がWindows XPであることが即座に分かった

ホスト種別による3389/TCPのパケット数



大規模感染マルウェア Morto

- ホスト種別による3389/TCPのユニークホスト数



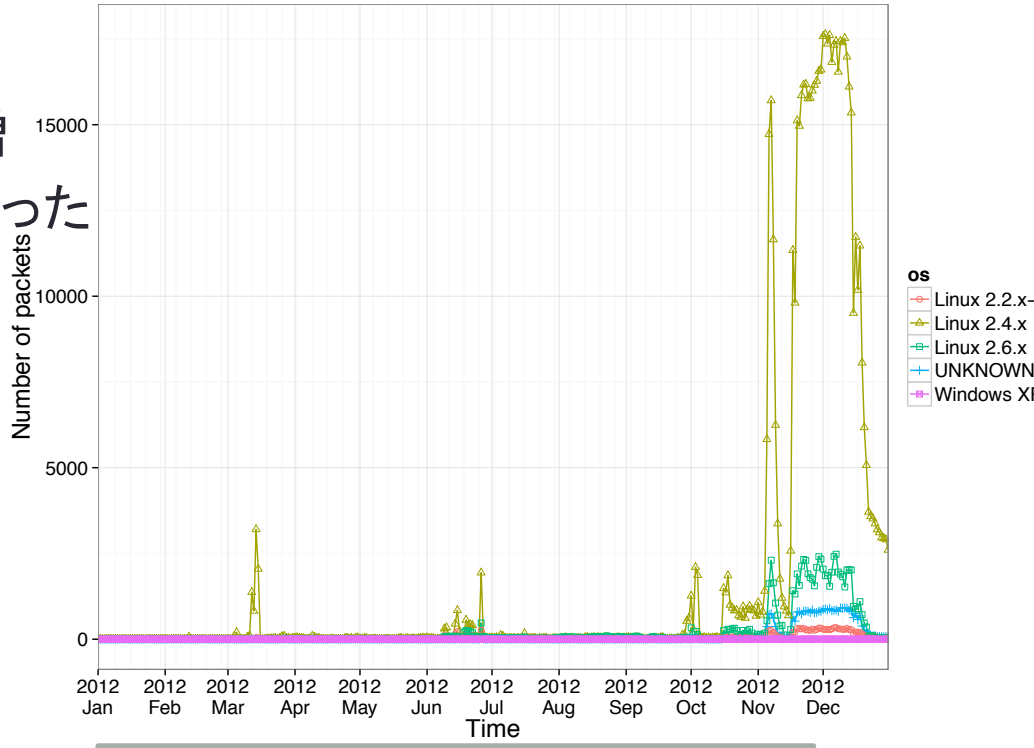
23/TCPのトラフィックの増大

- 2012年の年末にかけてパケット数の急増が観測された

- 発見した事
  - Linux系端末のホスト数が急増
  - Single-Shotが多いことがわかった

↓

Linux系に感染するワームと推測できる

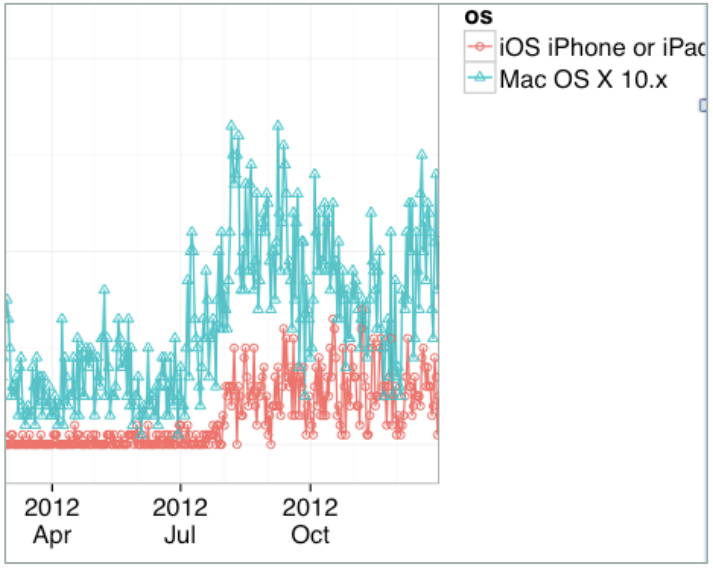


23/TCPホスト種別とSingle-shot

Apple端末の通信解析

- Apple系端末の通信解析
  - セキュリティ上あまりフォーカスされていないApple系端末からダークネットに届く通信の解析をおこなった

- 発見した事
  - iOS iPhone or iPadと判別される通信が増加傾向にあることがわかった



まとめ

- nicter darknet 2013で提供される4096個のIP空間で構成されるダークネットに対して、通信源ホストの分類を行った

- 以下の埋もれていた情報を新たに獲得できた
  - Single-shotの通信パターン変化の検出
  - 3389/TCPの通信の増加はWindows系である
    => OSの特定ができた
  - 23/TCPの通信解析
    => 原因が予想できた
  - Apple系携帯端末のダークネットへの通信が増加傾向にある
    => 総量としては少数の端末の傾向をつかめた

今後の課題

- 通信パターンのより詳細な分類
  - portに関する情報の利用
  - パケットに関する時間情報について利用
- 未知のシグネチャを持つホストの解明
  - OS推定において判別できなかったシグネチャの分析

- ご清聴ありがとうございました