ボットネットによるスパムメール送信防止方法の検討

間宮　領一*，　鈴木　秀和，　渡邊　晃(名城大学)

Researches on the Prevention Method of Spam Mails in Botonet

Ryoiti Mamiya, Hidekazu Suzuki, Akira Watanabe (Meijo University)

1．はじめに

インターネットの発展に伴い，ウィルスの被害が大きな問題となっている．近年ではボットと呼ばれる新しいタイプのウィルスが蔓延している．ボットはクラッカーの命令を受けた時のみ活動するため，感染しても発見しにくいという課題がある．

本稿では，ボットが組織化したボットネットがスパムメールの温床となっていることを防止するため，クライアント側でのスパムメール対策を検討した．

2．ボットネットとは

ボットとは，ウィルスの一種であり感染者のコンピュータを遠隔操作できるようにするプログラムである(1)．また，ボットに感染したPCが集まって構成されているネットワークをボットネットという．

攻撃者はIRC（Internet Relay Chat）サーバを通してボットに一斉に命令を送り，ボットをコントロールする．これらの命令により，ユーザの意思に関係なくクライアントから大量のスパムメールが送信される（Fig1.）．インターネットによるスパムメールの70%が，ボットネットによるもという報告がある(2)．

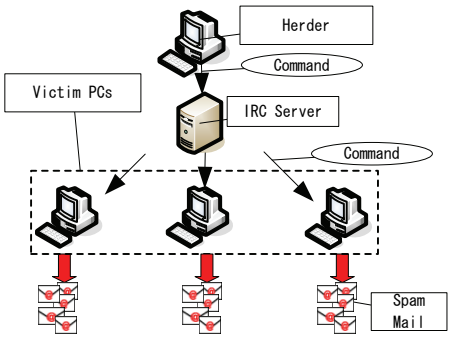


Fig1. Spam Mail Botnet

ボットネットによる被害を防止するにはIRCサーバを停止する方法がある．しかしIRCサーバが冗長化されていたり，IRCサーバを使わない分散型ボットネットもあるため，ボットネット対策をIRCサーバや攻撃者（Herder）に対して施すことは難しいと言われている．

3．クライアント側での対策

ボットは，攻撃者の命令を受けて始めて行動を起こすことに着目し，クライアント側でポート制御を行うことによりボットによるスパムメールを遮断する手法を検討した．

ボットがスパムメールを送信する際，SMTP ポート 25 を使用してメールを送信する．既存のパーソナルファイアウォール（FW）のポート制御機能では，登録したメーラによるメール通信のみ許可し，それ以外のメール通信をすべて遮断することができる．しかし，この機能だけではウィルスが登録したメーラを用いてスパムメールを送信する場合には対処できない．また，ウィルスが通信ログを削除してしまえば，自分がスパムメールを送信したことに気づかない．

そこで，SMTP ポート 25 を常に遮断しておき，ユーザがマウスによりメール送信ボタンをクリックしたことをトリガーにして SMTP ポートを開放する．メール送信が完了したら再度ポートを遮断する（Fig2.）．

この方法により，ユーザにより送信されるメールは正しく処理され，攻撃者の命令によるスパムメールの送信を防止することができる．

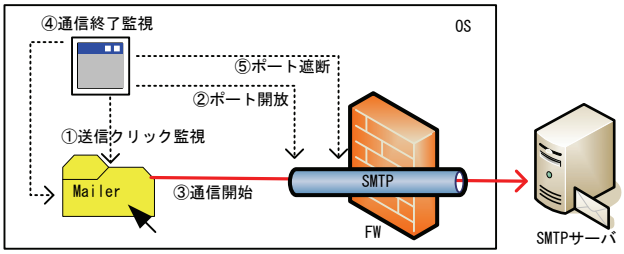


Fig2. Control of Port

4．むすび

ボットによりPCがスパムメールを送信することを防止するための対策として，ユーザがメーラの送信ボタンをクリックしたことをトリガーにして，パーソナルファイアウォールのSMTPポートを開放する手法を検討した．今後はこの手法の有効性を確認するための実装を行う．

文　献

(1) Felix C. Freiling, Thorsten Holz, and Georg Wicherski: Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks

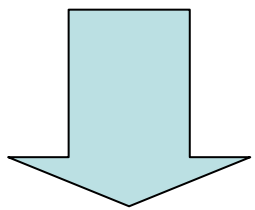
(2) McAfee : ボットネットの撲滅 最前線からの視点, White Paper 2006

ボットネットによるスパムメール送信防止方法の検討

名城大学理工学部
間宮 領一　鈴木 秀和　渡邊 晃

研究背景

- ウィルスやボットによる被害の深刻化
- 様々なソフトウェアの脆弱性
- 自分は安全と対策を怠るユーザ
- ボットネットによる大規模な攻撃

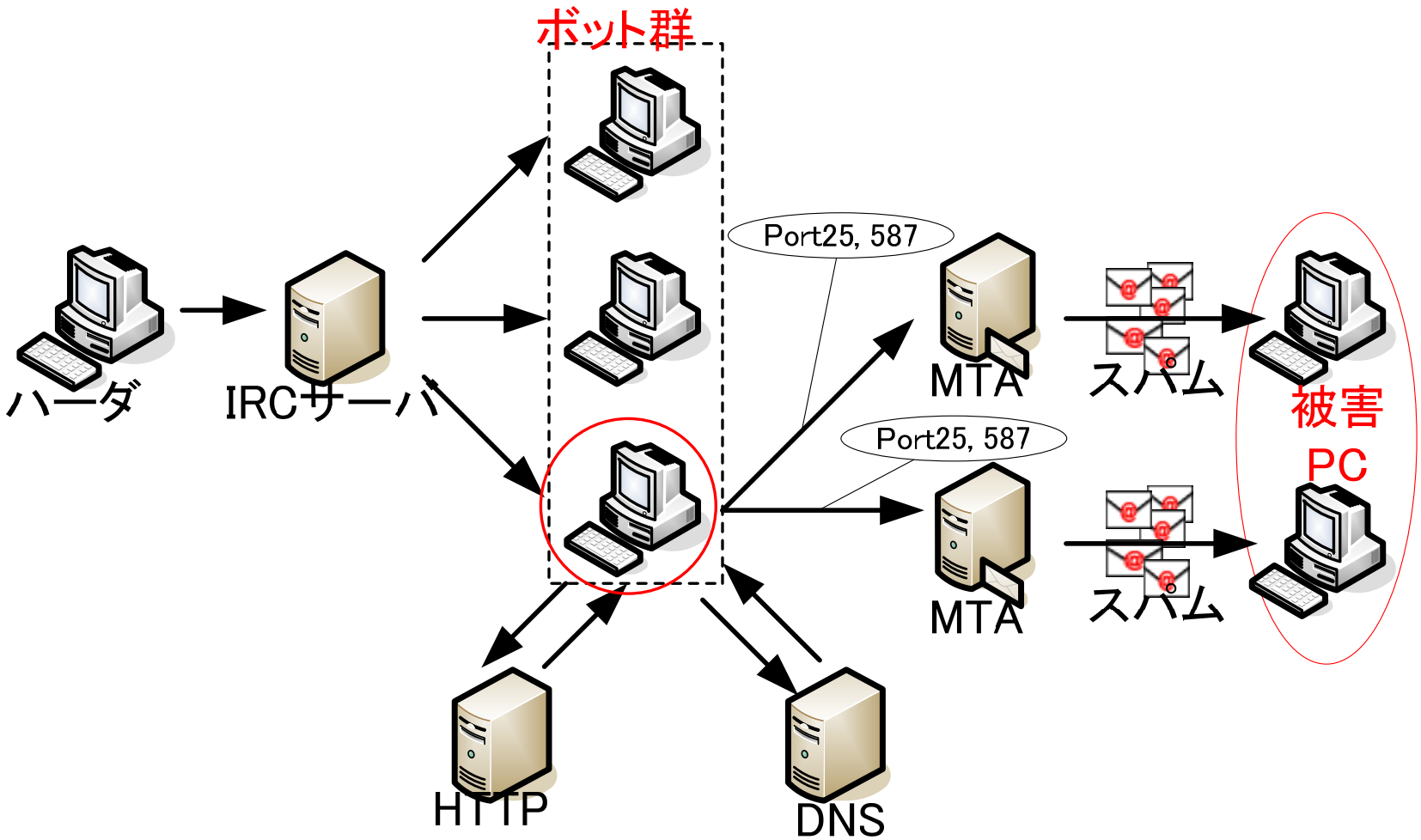


DoS攻撃、スパムの大量発生、個人情報流出

ボットとは

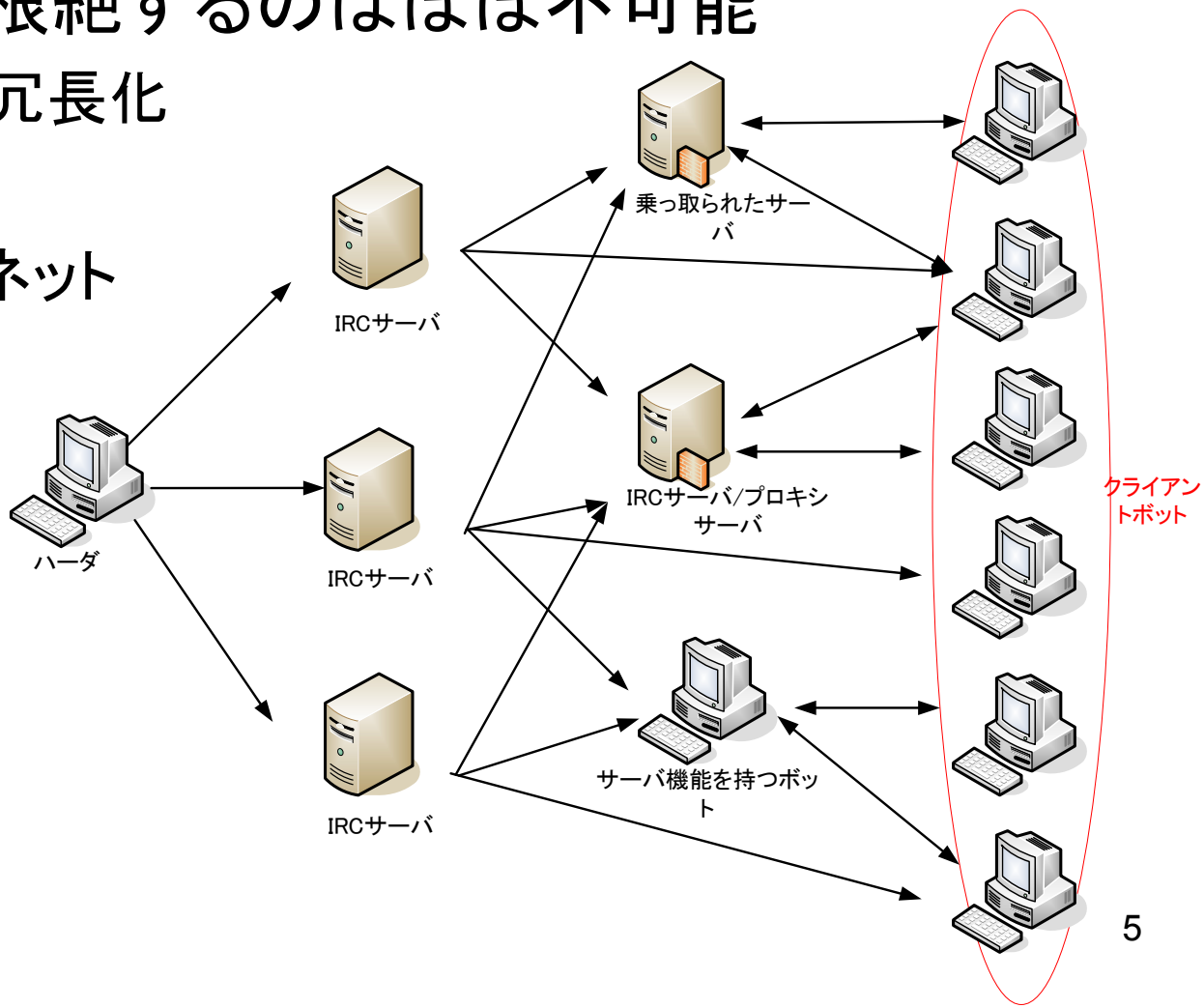
- ボット
  - 外部からコントロール可能な感染PC
  - 用途に合わせ様々な機能に拡張
- ボットネット
  - ボットに感染したPCが集まって構成されているネットワーク
- スパムボット
  - スパムメールを送信するためのボット

ボットネットの動作(スパムボット)



現状

- ボットネットを根絶するのはほぼ不可能
  - IRCサーバの冗長化
  - 踏み台
  - 分散型ボットネット



既存技術による対策

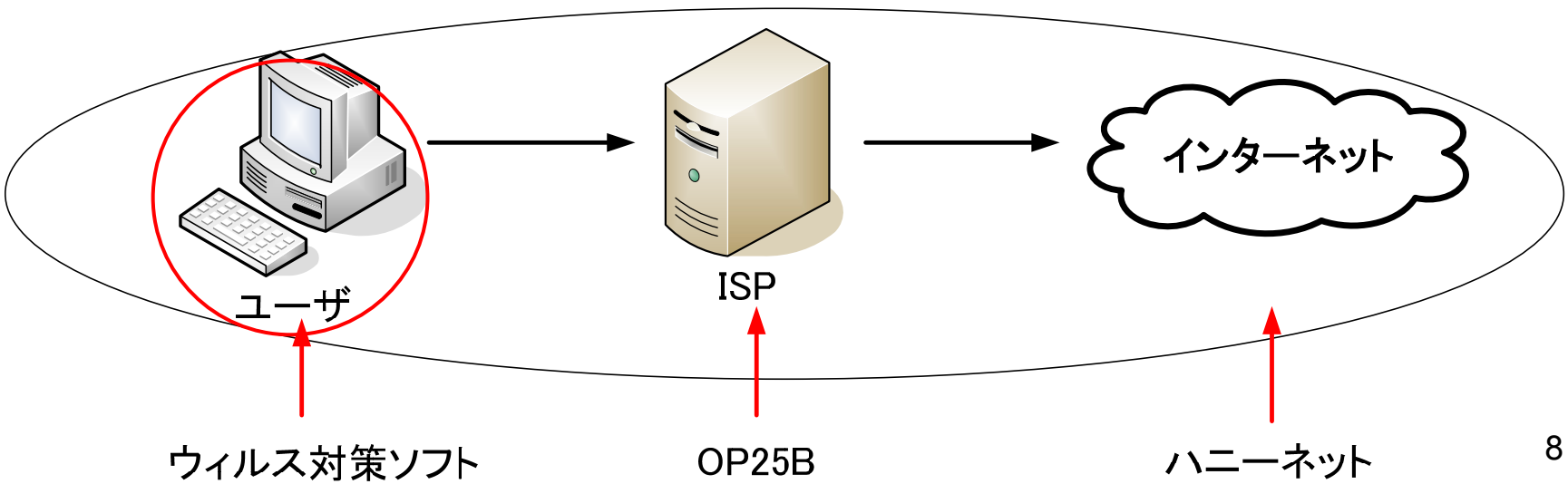
- ハニーネット
  - 不正アクセスを受けるための囮
  - 囮を使い大事なネットワークを守る
- OP25B(Outbound Port25 Blocking)
  - 契約外のメールサーバを使用したSMTP通信を拒否
  - 認証機能付きのSMTP通信サービス
- 既存のウィルス対策ソフト

既存技術の問題

- ハニーネット
  - しっかりとしたボットの管理が必要
  - コストがかかる
- OP25B
  - 正規のユーザを装ってメールを送信
- 既存のウィルス対策ソフト
  - 新規のウィルスには対応できない

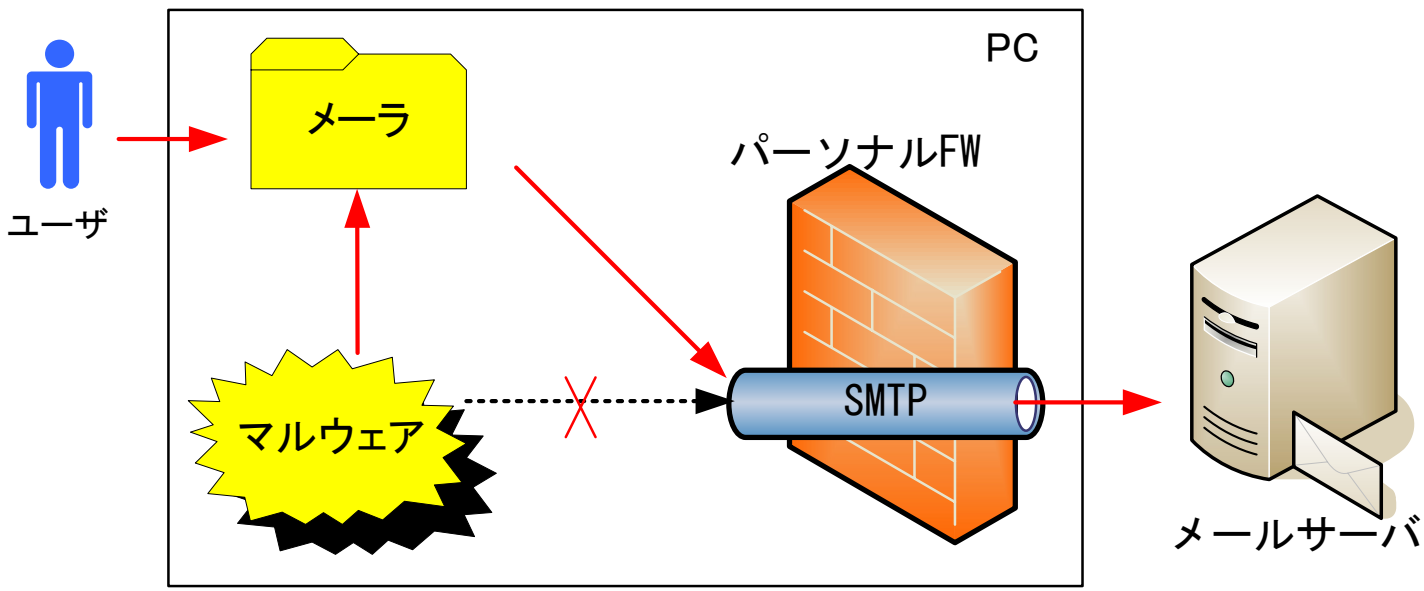
クライアント側での対策

- ボットの感染は避けられない
- スパム送信を防止する方法を検討
  - 既存のウィルス対策ソフトを併用
- メーラのプロセスを監視



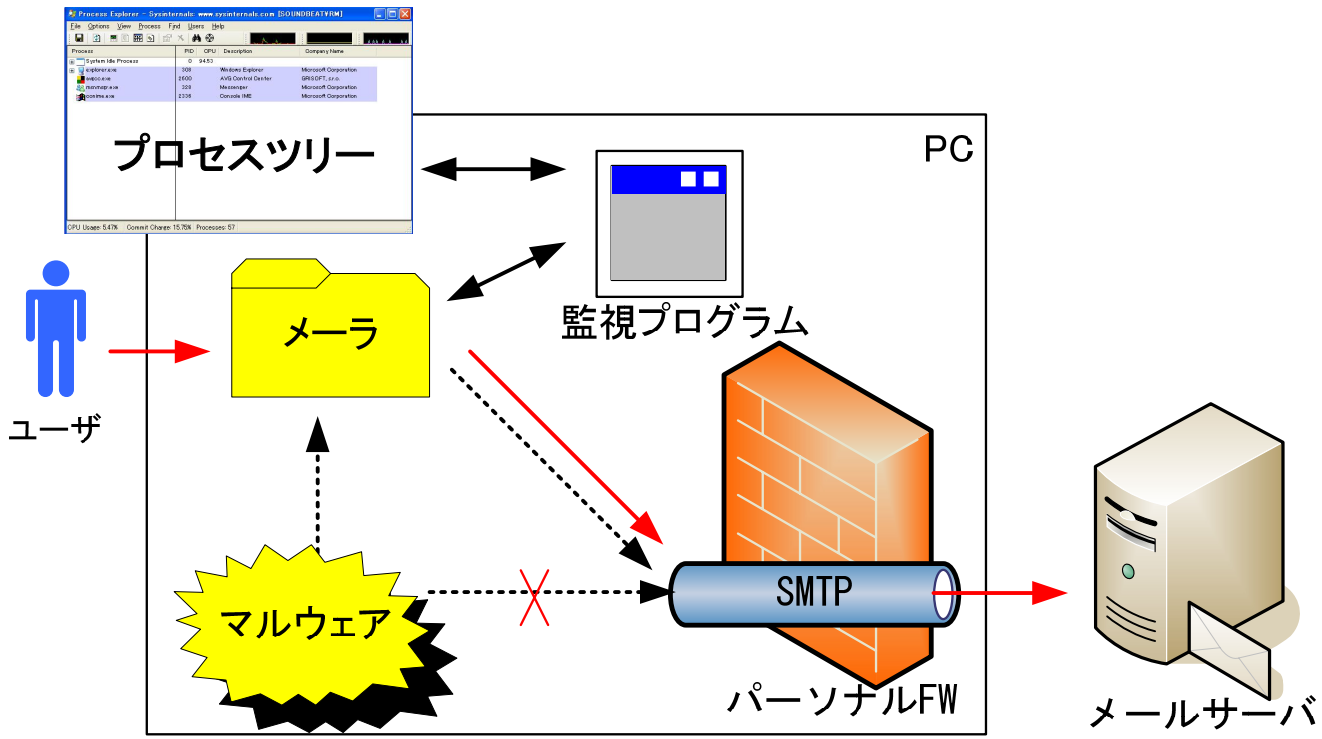
ウィルス対策ソフトによるポート制御

- 常にポート25, 587を遮断
- メーラのSMTP通信のみ例外として許可
- マルウェアによるメーラの通信を止められない



プロセスの監視

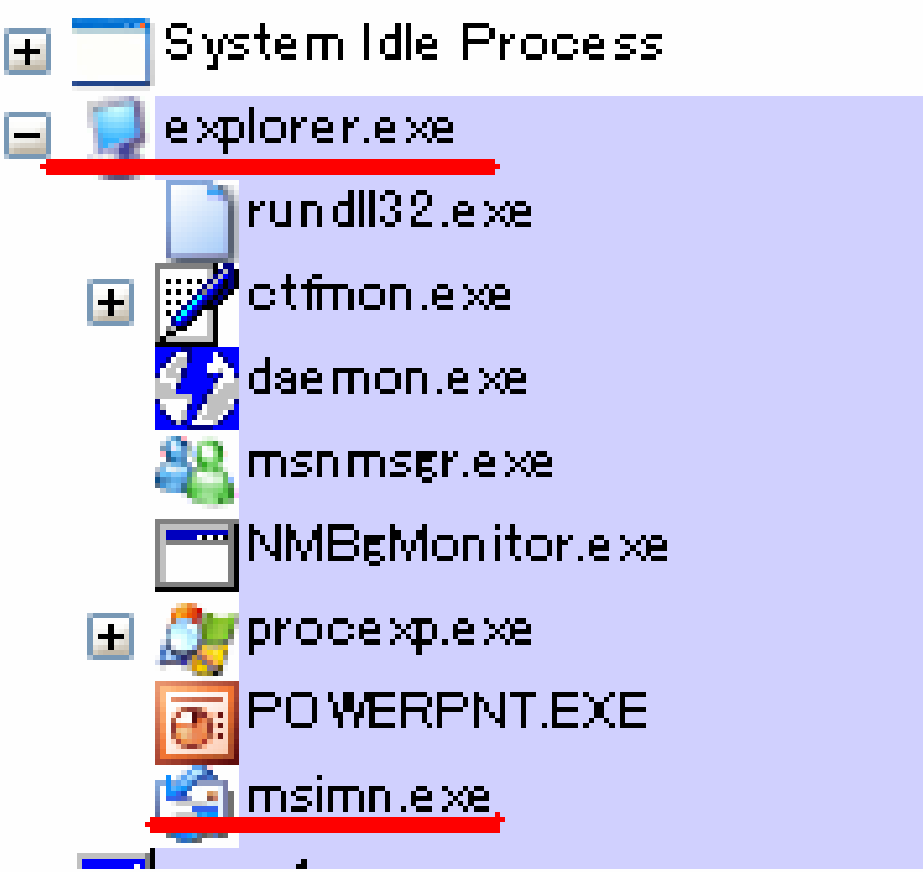
- メーラの通信を監視
- 監視プログラムがプロセスツリーを監視
  - メーラの親プロセス

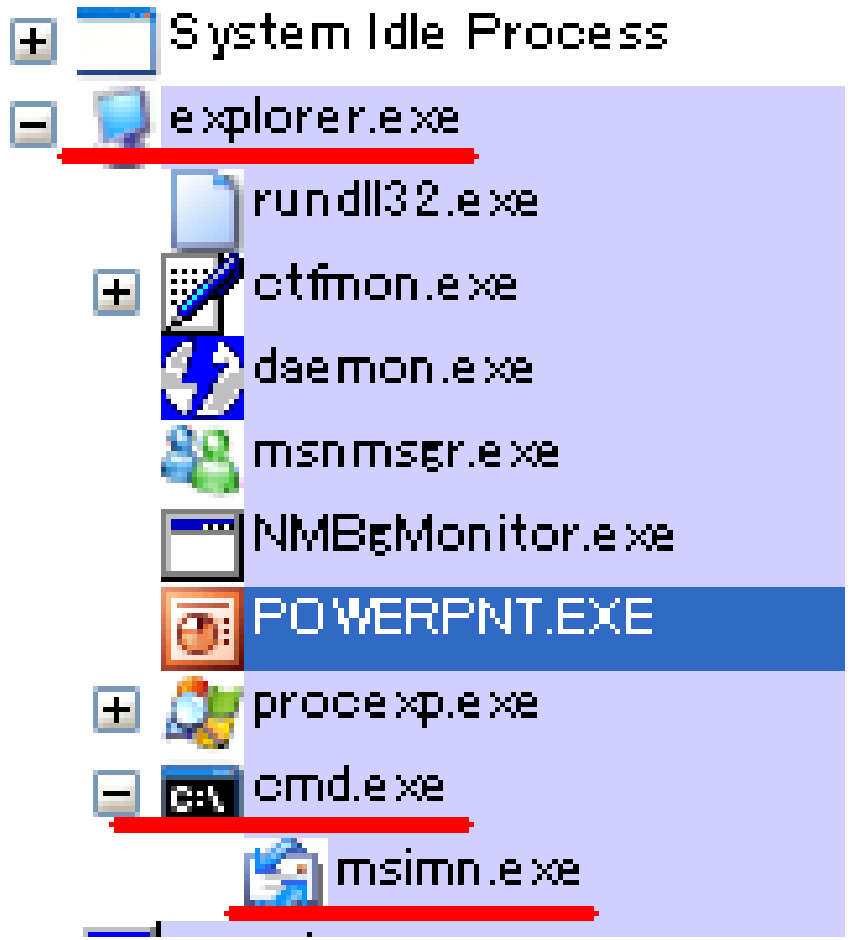


プロセスツリー

- 実行中のプロセスをツリー状に可視化
  - 正常なメーラの親プロセスはexplorer.exe
- メール送信時にメーラの親プロセスを確認
  - メーラの親プロセスがexplorer.exe
    → 正常な実行
  - メーラの親プロセスがexplorer.exe以外のプロセス
    → 不正なプログラムが実行

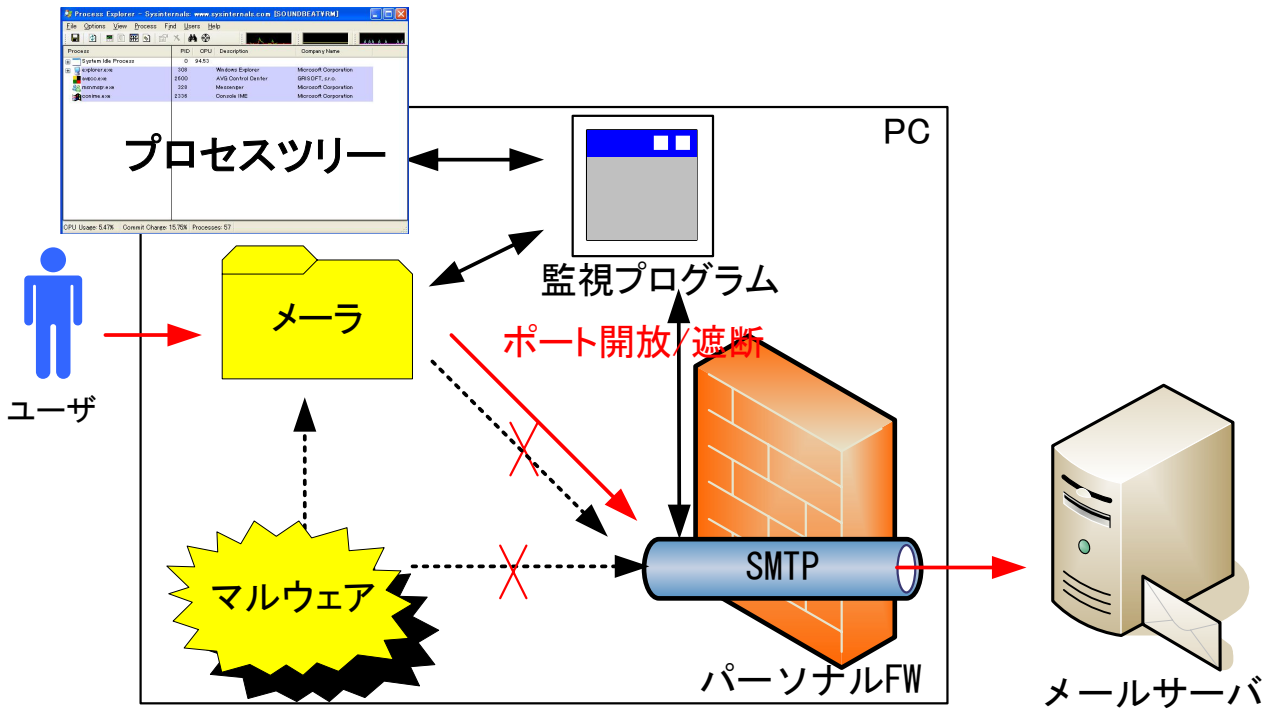
プロセスツリー


System Idle Process
explorer.exe
rundll32.exe
ctfmon.exe
daemon.exe
msnmsgr.exe
NMBgMonitor.exe
procexp.exe
POWERPNT.EXE
msimn.exe


System Idle Process
explorer.exe
rundll32.exe
ctfmon.exe
daemon.exe
msnmsgr.exe
NMBgMonitor.exe
POWERPNT.EXE
procexp.exe
cmd.exe
msimn.exe

メール送信制御

- メーラの親プロセスを確認
- メーラの親プロセスがexplorer.exeの場合にSMTPポートを開放（それ以外は遮断）
- 通信終了後にポートを遮断



むすび

- スパム送信防止方法としてクライアントでの対策を検討
  - プロセスを監視することにより通信を制御
- 今後の課題
  - 提案技術の実装と評価
  - DoS攻撃についての対策

補足:ボットが流行する理由

- ボットネットのレンタル
- コストがかからない
- 低負荷なプログラムなため感染しても気がつかない

補足：検体収集総数

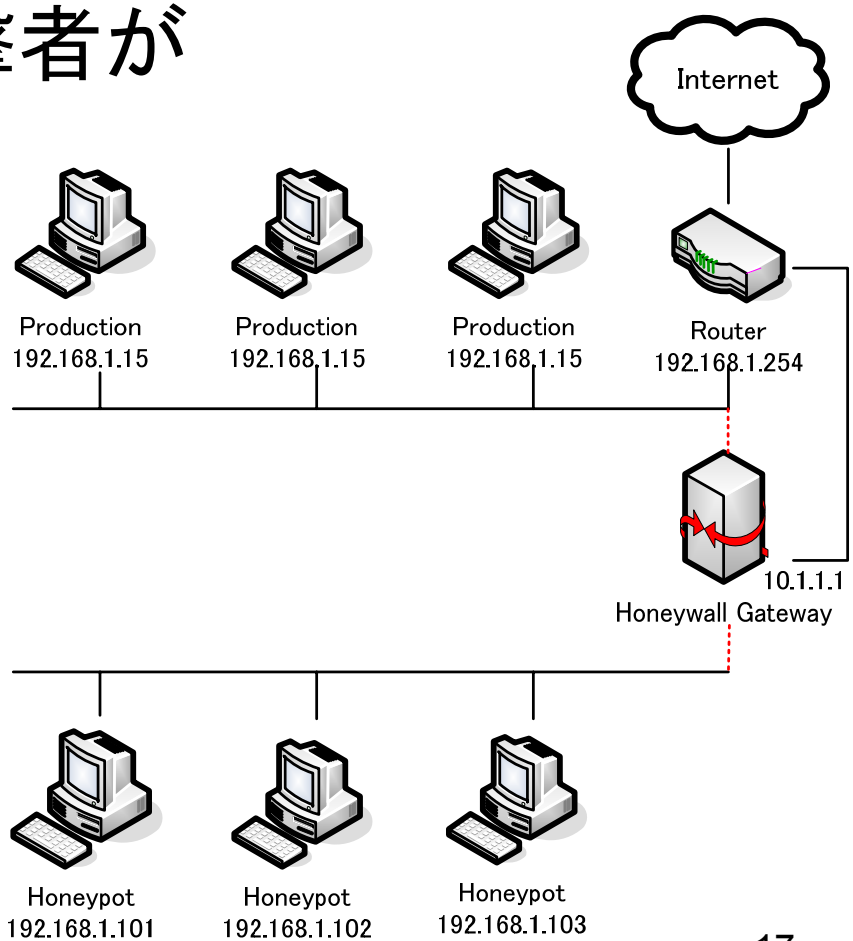
- 検出数　2005年4月1日～5月12日（TELECOM SAC JAPANより）

	トータル		平均/日	
	件数	種類	件数	種類
検出数	31,846	3,705	758.2	88.2
既知	28,309	767	674.0	18.3
未知	3,537	2,938	84.2	70.0

- 1日70種類の未知のウィルスが出てきている

補足：ハニーネット

- ボットネットに侵入し攻撃者がどのような命令をだしているかを観測
- ハニーポット、ルータ間にハニーウォールを置く
  - 外向きの通信を制御
  - ゲートウェイでデータキャプチャ＆コントロール



補足：OP25B(Outbound Port25 Blocking)

例：OCNと契約

① 他社ISPメールサーバ使用した通信(Port25)

② 他社ISPからOCNのメールアドレスを使用した通信(Port25)

③ POP before SMTPを 使用した通信

④ OCNのメールアドレスを使用した通信(Port587)