ボットの二次被害を防止する方法の提案

070428433　阿南宏教
渡邊研究室

1.ボットの二次被害を防止する方法の提案

近年ボットネットによる SPAM メールの送信や DDoS 攻撃，情報の奪取など様々な問題が蔓延している．ボットはオープンソースとなっているため亜種が多く存在する．また感染前との差異を感じることなくコンピュータを使用できるので，感染したことに気づきにくいといった問題もある．

本稿では，ボットによる感染は完全に防止できないという前提にたち，二次災害を防止するため，クライアント側でのスパムメール対策を検討した．

2. ボットネットについて

ボットに感染した PC が集まって構成されたネットワークのことをボットネットという．ボットネットは悪意のある攻撃者(Herder)によって構築され，IRC(Internet Relay Chat)サーバを通して感染 PC に一斉に命令を送ることによって遠隔操作されてしまう．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(図 1).

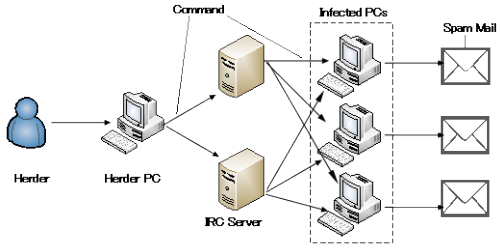


図 1. ボットネットによるスパムメール送信

Herder は複数の IRC サーバと接続しているため，仮に一つのサーバを停止できたとしても他のサーバを介して命令を送り続けることができる．このため，ボットネット対策を IRC サーバや Herder に対して施すことは難しいとされている．

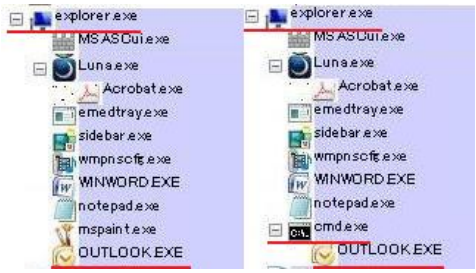
3. 提案方式

ボットは，攻撃者が命令を受けて初めて行動を起こすことに着目し，メールが送信される時，正常なメール送信か否かを判断し，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方法を検討した．

本提案では，通常時は SMTP ポート 25，587 番を遮断しておく．このためにパーソナルファイアウォールのポート制御機能を利用する．この状態で MAPI(Messaging API)と呼ばれる，Windows 上で電子メールを扱うための関数群をフックし，PC の動作を監視する．

メーラを呼び出したのが正常なユーザであると確認できた場合にのみ，ポートを開放し通信終了後にポートを再度遮断する．提案方式では，メーラを呼び出したのが正常なユーザかどうか判断するために，プロセスツリーと送信時のマウス操作を監視する．

図 2 で示すように MAPI が実行されたとき，正常時は explorer.exe が上位プロセスとなる．メーラの上位プロセスが explorer.exe と確認できた場合，さらに直前のマウスクリックが行われたかどうかを確認する．正常でないと判断した場合はボットなどの不正なプログラムがメール送信を実行したとみなし，ユーザにアラームをあげる．この方法により不正なメール送信を防止することができる．



(1)正常時　　(2)異常時

図 2. プロセスツリーによる上位プロセスの確認

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対策として，プロセスツリーと直前のマウスクリックを監視し，メーラを呼び出したのが正しいユーザと判断できた場合にのみ，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提案した．今後は有効性を確認するために実装の検討を行う．

参考文献

[1]平田祐二，渡邊晃：端末からの不正メール送信を防止するための検討

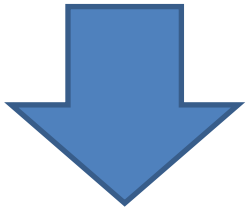
ボットの二次被害を防止する方法の提案

渡邊研究室
070428433
阿南　宏教

研究背景

- インターネットの普及に伴いメールは日々の生活で切っても切れない存在である
- ウイルスの被害が大きな問題となっている

ボットの存在



DDos攻撃、スパムメール、フィッシング詐欺

ボットとは

- ボット

  ーウイルスの一種

  ー増加する亜種

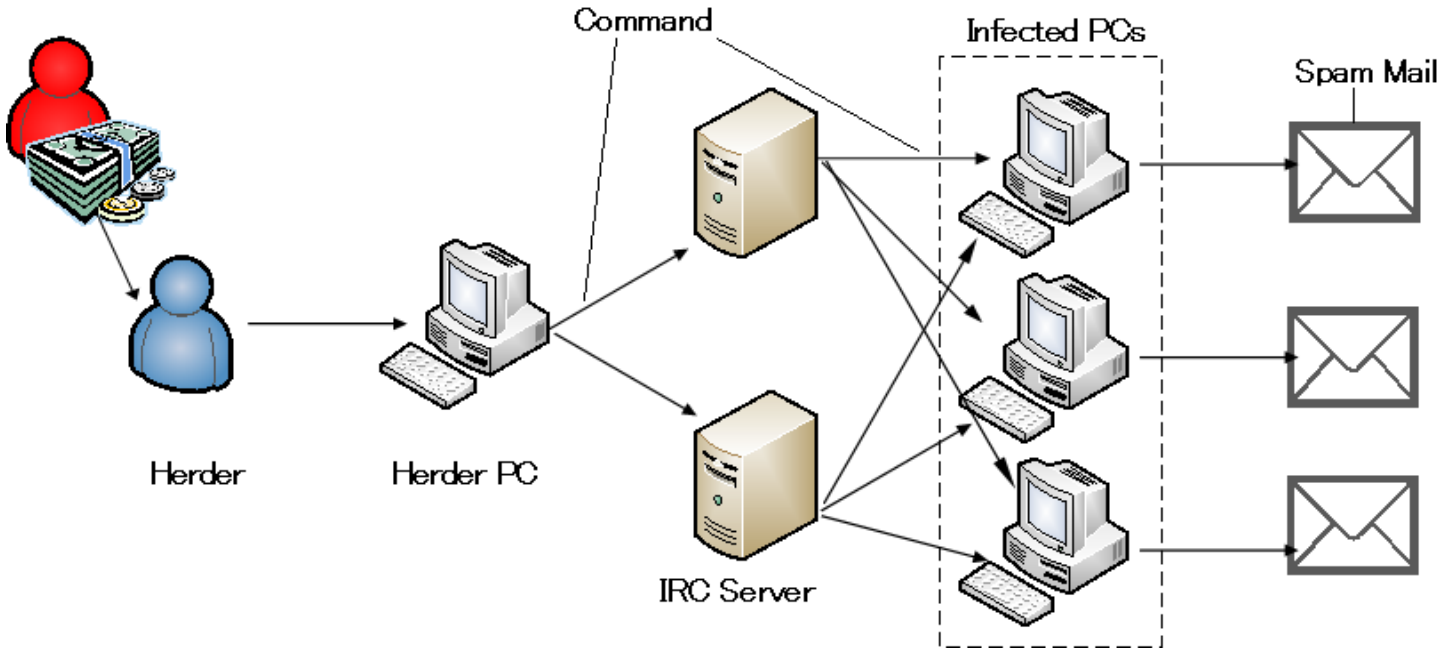
  ー犯罪目的で使用されている

- ボットネット

  ーインターネット経由の命令によって遠隔操作されている
  　コンピュータ群

  ー数千～数万台でネットワークを構成

スパムメール送信



- IRC Serverの冗長化
- IRC Serverを経由してスパムメールを送信する

IRC; Internet Relay Chat

攻撃者;Herder

既存技術によるボット対策と課題

- ヒューリスティック検知

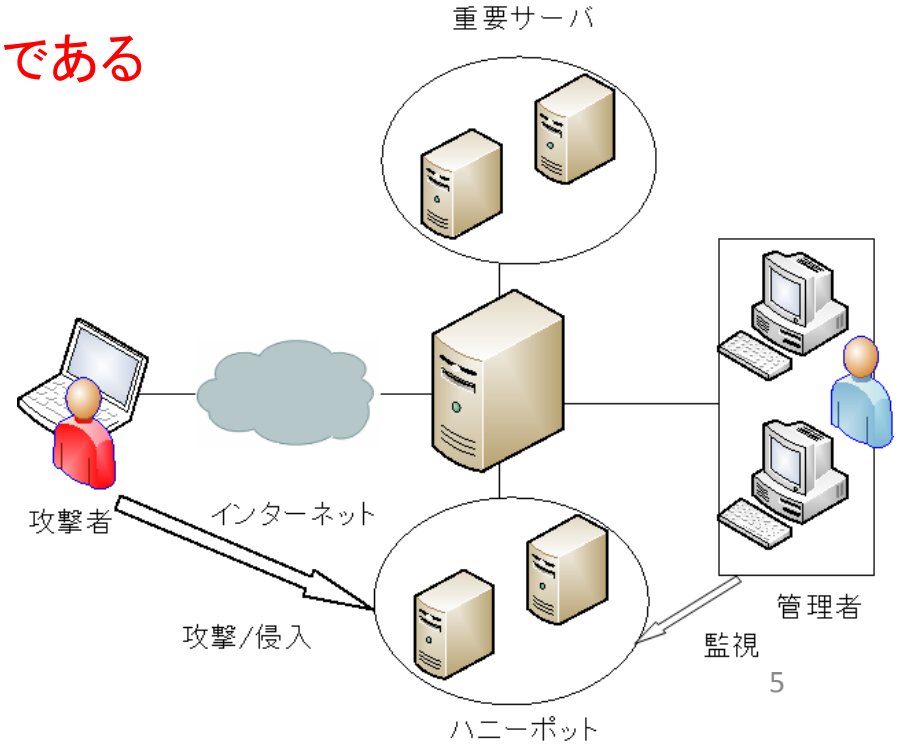
ーウィルス定義ファイルの挙動などを解析し、特徴的な動作の有無を調べる手法

ーウィルスを改変した亜種は発見できない，誤認知してしまう問題がある

- ハニーポット

ーウイルスを調査するために設置された、サーバやネットワーク機器のこと

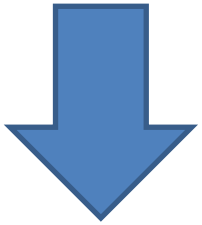
ー安易にハニーポットを設置するのは危険である



提案するボット対策の方向性

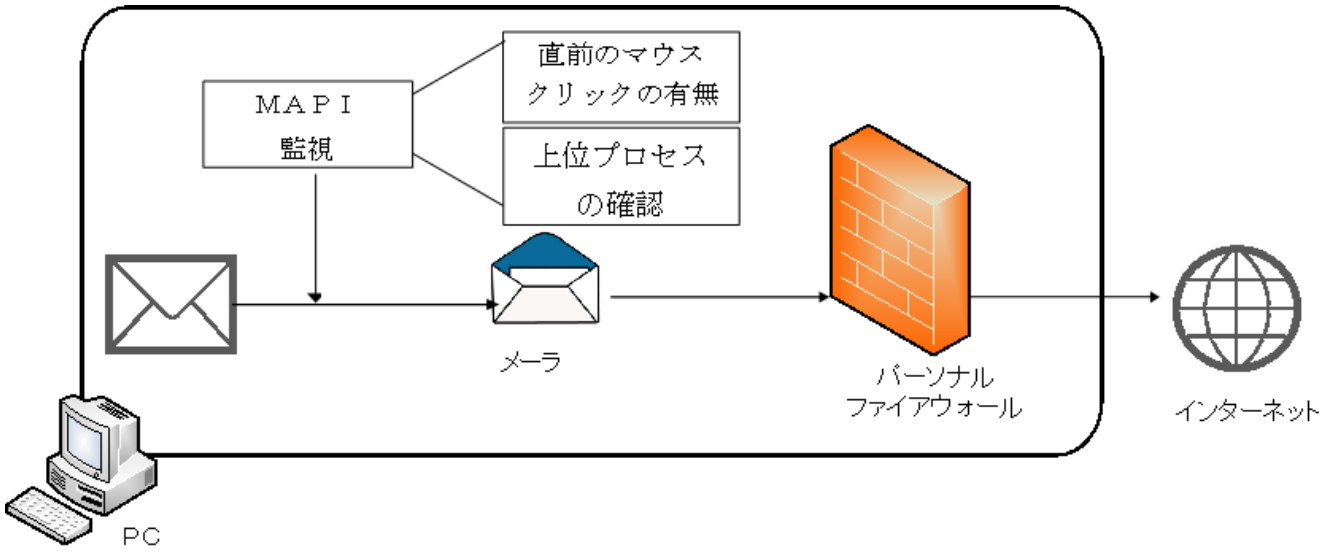
- 日々亜種が作成されるボット

⇒ボットの感染活動を防ぐことは不可能である



二次災害を防止する方法を提案

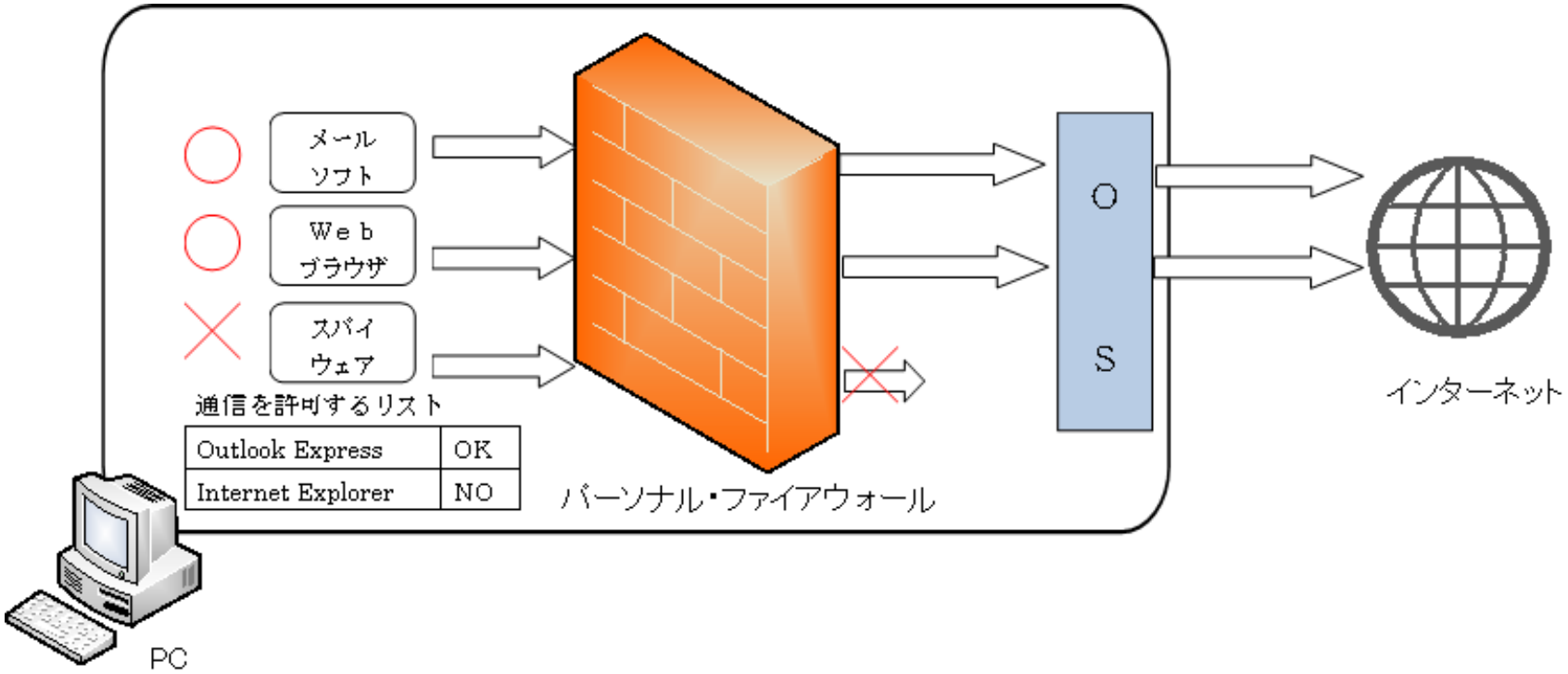
提案方式



- MAPI(Messaging API)を監視
- プロセスツリーを監視
- メール送信直前にマウス操作があったかチェック
- パーソナルファイアウォールの利用

⇒メール送信

パーソナルファイアウォールの利用



- プライベート ネットワークへの、またはプライベート ネットワークからの許可のないアクセスを阻むことを目的とするシステム

ー常にSMTPポート25，587番を遮断しておく

ー送信時のみSMTPポートを解放する

MAPIの監視

- MAPI はWindows 上で電子メールを扱うための標準仕様でメールメッセージを作成，転送するための関数郡である．一般的にWindows上ではMAPI によりメールを送信する

ーMAPI関数のMAPILogon，MAPIsendMailをフックする

セッション名	機能
MAPILogon	メールサーバーへログオン．ユーザ名とパスワードを指定し，成功時にセッションハンドルを返す．
MAPISendMail	MAPIMessage構造体のメールコンテンツを送信する．

プロセスツリー

- 実行中のプロセスをツリー上に表現したもの

―メーラの親プロセスがexplorer.exeの場合（1）

⇒正規ユーザの実行と判断

―メーラの親プロセスがexplorer.exe以外の場合（2）

⇒不正なプログラムがメーラを呼び出したものと判断

1.正常時　　2.異常時

マウスクリックのチェック

- プロセスモニター（Process Monitor）

－ファイルシステム，レジストリ，プロセスおよびスレッドの活動をリアルタイムで表示する，Windows 向けのツール

⇒送信時のマウスクリックがあったか監視する

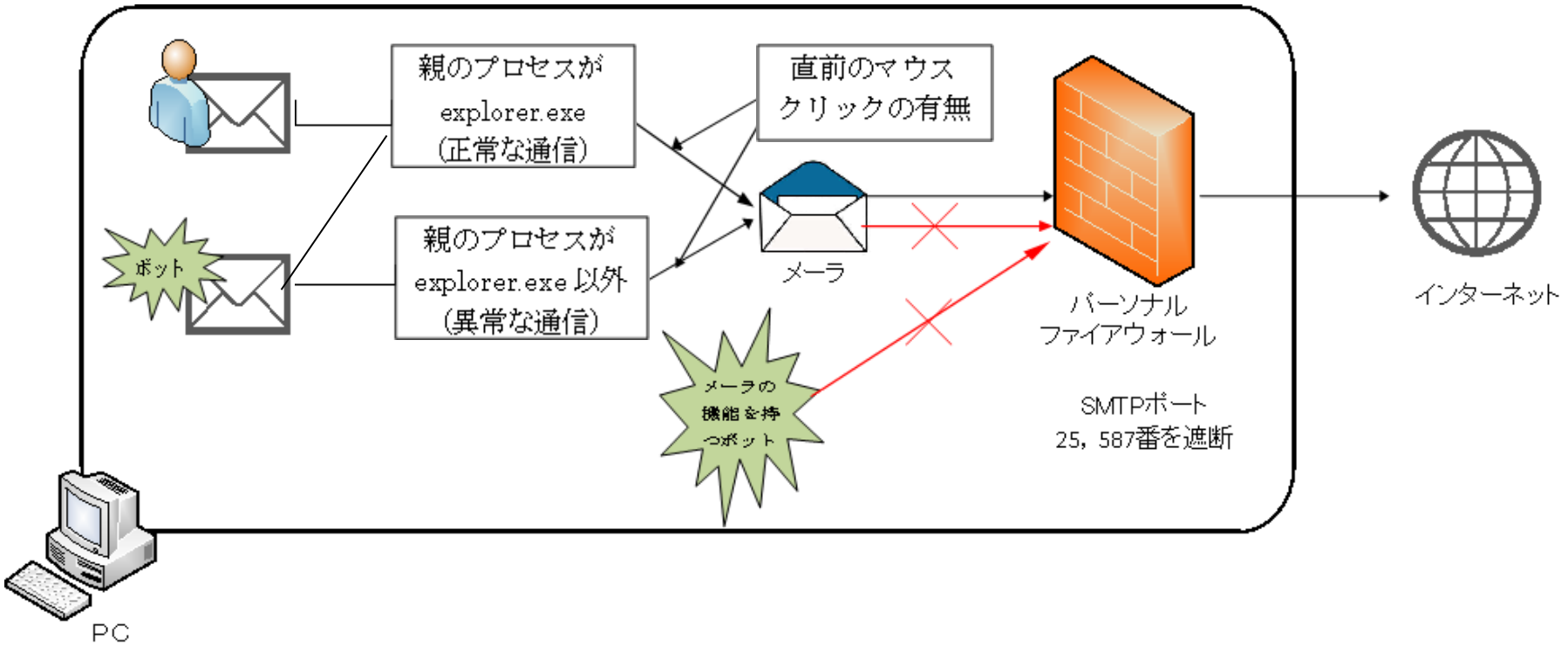
- ユーザによる直前のマウスクリックがあった場合

⇒正規ユーザの実行と判断

- 直前のマウスクリックがなかった場合

⇒不正なプログラムがメーラを呼び出したものと判断

提案方式の動作



1. 常にSMTPポートを遮断しておく
2. MAPIを監視しメーラの呼び出し元を確認する

—プロセスツリー，マウスクリックを監視

3. 正規ユーザ判断した場合のみ SMTPポートを開放する
4. メール送信後SMTPポートを再び遮断する

むすび

- スパムメール送信を防止するためクライアント側での対策を検討した

—MAPI関数をフックし，送信要求があった場合プロセスツリー，マウスクリックを監視し，正規ユーザかを確認する

—確認できた場合のみポートを開放しメールを送信する

- 今後の課題

—提案方式の有効性を確認するための実装をする