不正メールの送信防止とボット感染検知の検討

040427493　間宮領一
渡邊研究室

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．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（図1）．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のという報告がある．

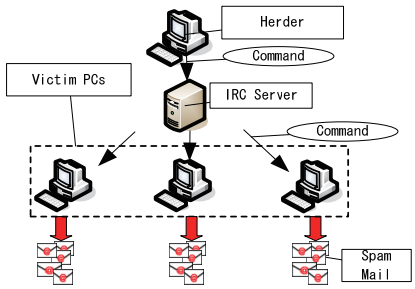


図1. スパムボット

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，クライアントから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手法を検討した．

ボットに感染したPCには，以下のようなメール送信パターンがある．

①　ユーザがメーラを用いて正常にメールを送信する．
②　ボットがMAPIをフックして，メーラからアドレス情報を取得する．その後，独自のSMTPエンジンによりメールを送信する．
③　ボットがMAPIをフックして，メーラを使用してメールを送信する．

一般にメールを送信する際，SMTPポート25，587を使用する．そこでパーソナルファイアウォール（PFW）でポート制御を行い，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可能である．しかし，この機能だけでは③の場合に対処できない．

そこで提案方式では，SMTPポート25，587を常に遮断しておき，更にあらかじめ使用するメーラを登録しておく．また，ボットがIRCサーバと通信する際のポートの約50%が6660から6669であるので，当該ポートの通信も監視する[1]．メールサーバにログオンするために使用するMAPI関数を監視し，起動したのが登録したメーラかどうか確認する．次にメーラを呼び出したのが正しいユーザかどうかをプロセスツリーにより確認する．上位プロセスがexplorerの場合は正常と判断し，ポートを開放し通信し通信終了後ポートを再度遮断する．これ以外の場合は全て不正とみなし，ポートを開放しないままユーザに警告をする（図2）．警告する際，IRCサーバとの通信が確認された場合は，ボットに感染している恐れがあるという警告を出す．

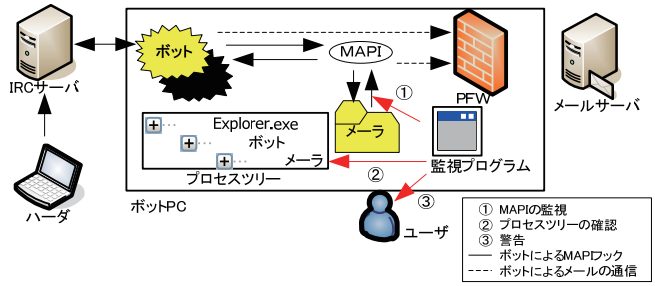


図2. 提案手法

4.　むすび

プロセスツリーから，メール通信を行ったのが正しいユーザかボットかを判断することにより，不正にメール通信が行われることを防止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．

参考文献

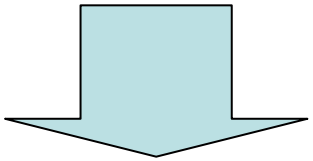
[1] 釘崎 裕司，笠原 義晃，堀 良彰，櫻井 幸一：トラフィック解析に基づくボット検知手法，第37回 コンピュータセキュリティ（CSEC）研究発表会(2007)

不正メールの送信防止とボット感染検知の検討

渡邊研究室
間宮 領一

研究背景

- ボットという新しいタイプのウィルスが増加
- 世界の電子メールの60～70%がスパムメール
  - 約70%がボットによるものと言われている

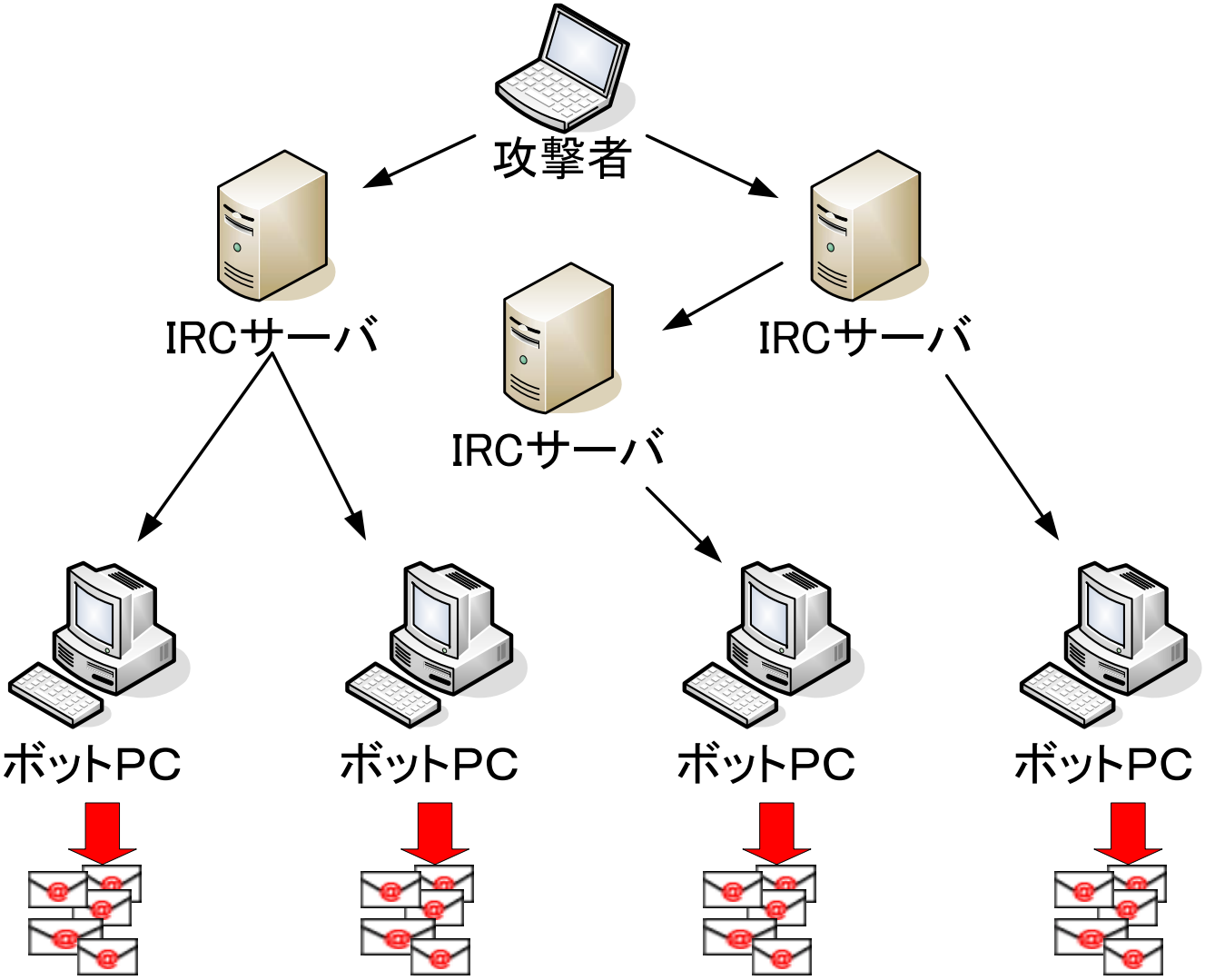


フィッシング，ウィルス添付，クリック詐欺など

ボットとは

- ボット
  - ウィルスの一種で感染PCを外部からコントロール可能にする悪意あるプログラム
- 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
- C/S(Client/Server)型ボットネット
  - IRC(Internet Relay Chat)サーバを使用してボットに命令

ボットネットの動作



現状

- ボットの検出数
  - 亜種が1日に20～30種類が出現している
- 2006年下半期のシマンテックによる調査
  - 全世界のボット感染PCは6,049,594台
  - 指令サーバは4,746台
- フィッシング攻撃について
  - ブロックしたフィッシングメッセージは15億件検出(100/秒)
  - フィッシングメールを166,248件検出

既存技術による対策

- OP25B(Outbound Port25 Blocking)
  - 契約外のISPのメールサーバを使用したメール通信に使用するポート25番の通信を拒否
  - ユーザ認証機能を使用したSMTPポート587番の通信を提供

- アンチウィルスソフト
  - パターンマッチングによるウィルス検知が主流
  - パーソナルファイアウォールによる通信制御

既存技術の問題点

- OP25B
  - ボットには情報収集機能がある
  - 正規のユーザを装って通信されてしまう

- アンチウィルスソフト
  - 攻撃者はボットをアンチウィルスソフトにより検証してから拡散している
  - 新種や亜種のウィルスには対応できない

対策の着目点

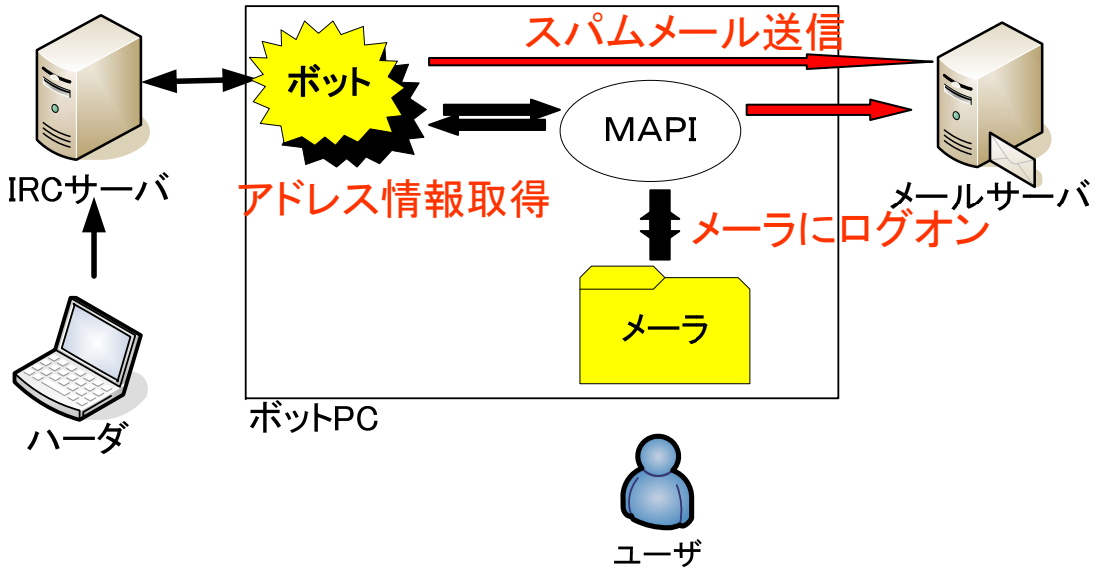
- 従来のスパムメール対策
  - サーバ側などにフィルタを設置するなどネットワーク側での対策がほとんど
- ボットの特徴
  - ボットは命令を受けるまで行動しない
  - 感染を防ぐのは難しい
- 提案では
  - 対策をクライアント側に組み込むことによりボット感染PCからの2次被害を防ぐ
  - 従来の技術を併用することにより高い効果が得られる

ボットのメール送信パターン

- MAPI(Messeging API)
  - Windows上で電子メール機能を扱うための関数郡

① MAPIをフック(処理の横取り)をしてアドレス情報を取得した後，独自のSMTPエンジンによりメールを送信する.

② MAPIをフックしてメーラにアクセス後，そのメーラを使用してメールを送信する.



提案技術

- 必要時にポート開放/遮断
  - パーソナルファイアウォールによりSMTPポート25，587番を常に遮断しておく
  - 正常なユーザがメール送信の要求をしたときのみポートを開放する
  - 通信終了後ポートを遮断する
  - IRC通信を確認し感染している場合ユーザに警告

これらの動作を行うための監視プログラムを作成

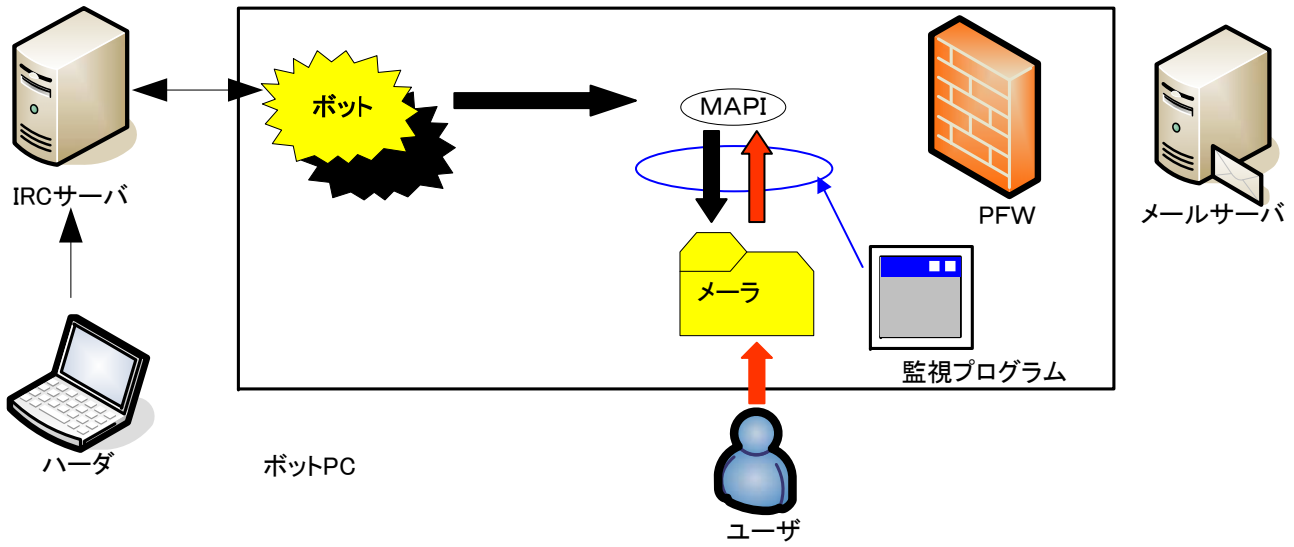
提案技術 – 監視プログラムの動作 –

- 監視プログラム起動時
  - パーソナルファイアウォールにより常にポートを遮断
  - ユーザが使用するメーラを登録
  - MAPIの監視を開始
  - IRCポートの監視を開始
- 使用するMAPI関数
  - 19種類ある関数のうち以下の2種類を使用

セッション名	機能
MAPILogon	メールサーバへログオン．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．

提案技術 – MAPIの監視 –

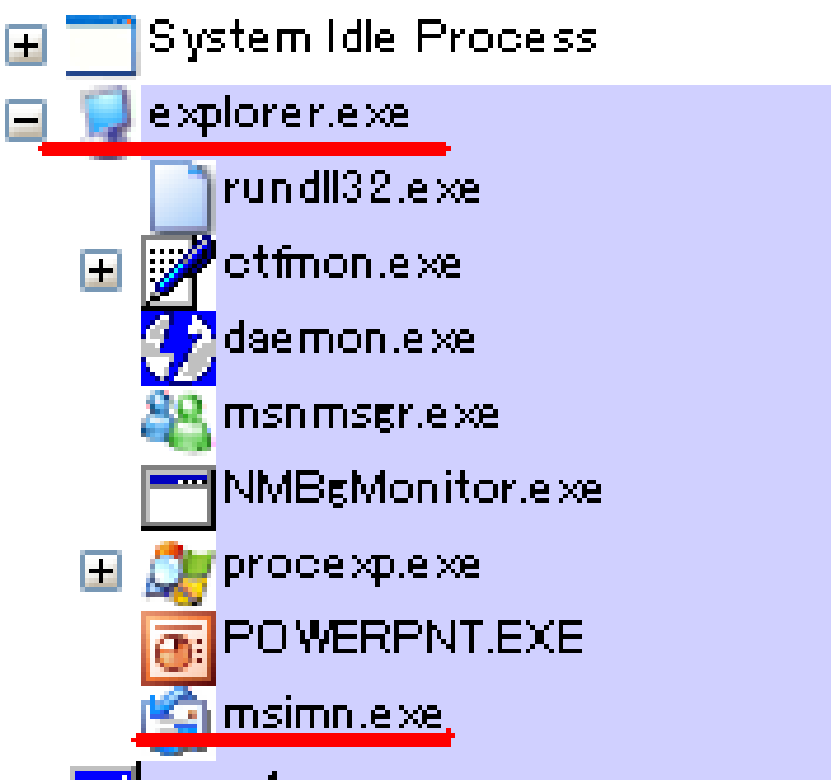
- MAPILogonを監視
  - MAPILogonが呼び出されたときメーラが起動したことが確認できる
  - 登録されているメーラと一致するか確認する
  - 登録されたメーラでなかった場合不正な動作と認識



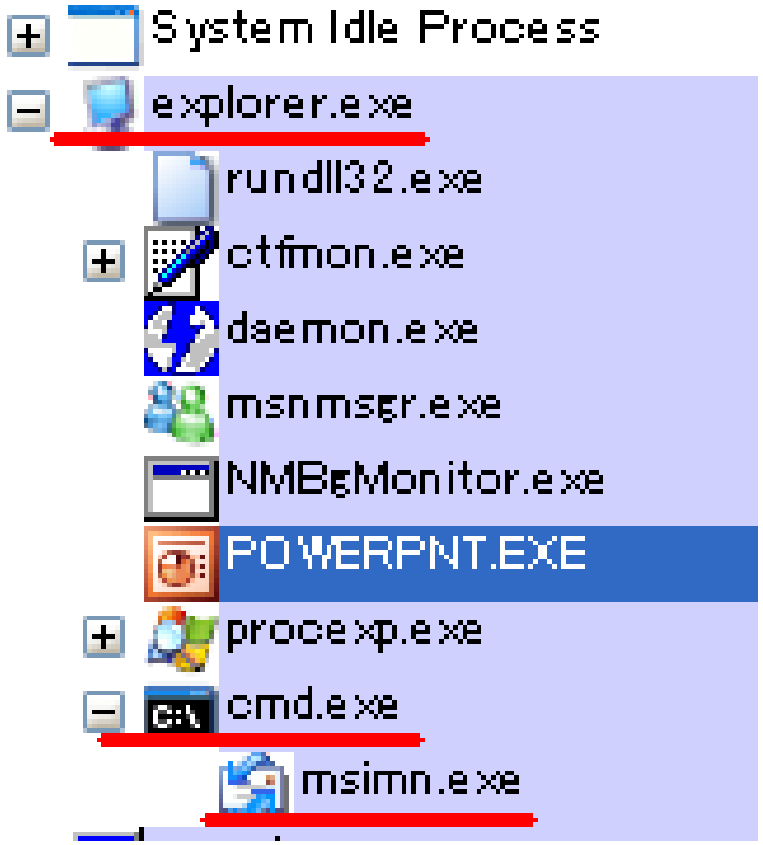
提案技術 – プロセスの監視 –

- メーラの起動が確認されたとき
  - メーラにログオンしたのがユーザか否かをプロセスツリーにより確認
- プロセスツリーとは
  - 各プロセスの関係をツリー上で表現
  - アプリケーションの上位プロセスは正常時は必ずexplorer.exeである
  - ボットがログオンしているならメーラの上位プロセスはボットである

提案技術 – プロセスの監視 –



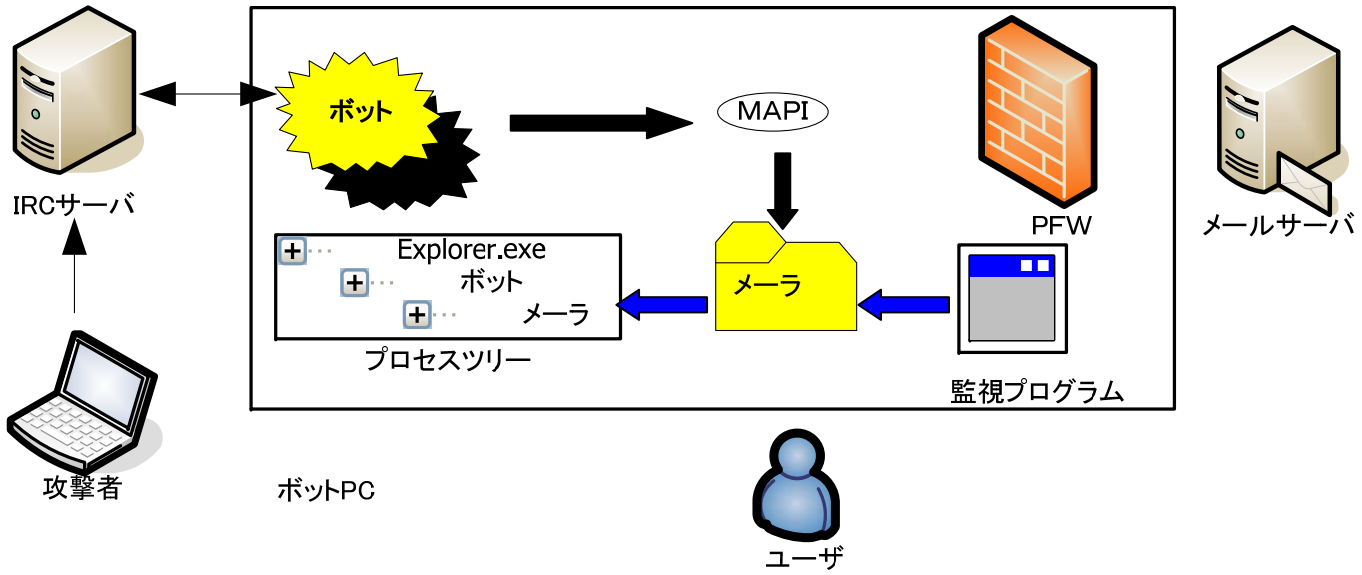
正常時



不正時

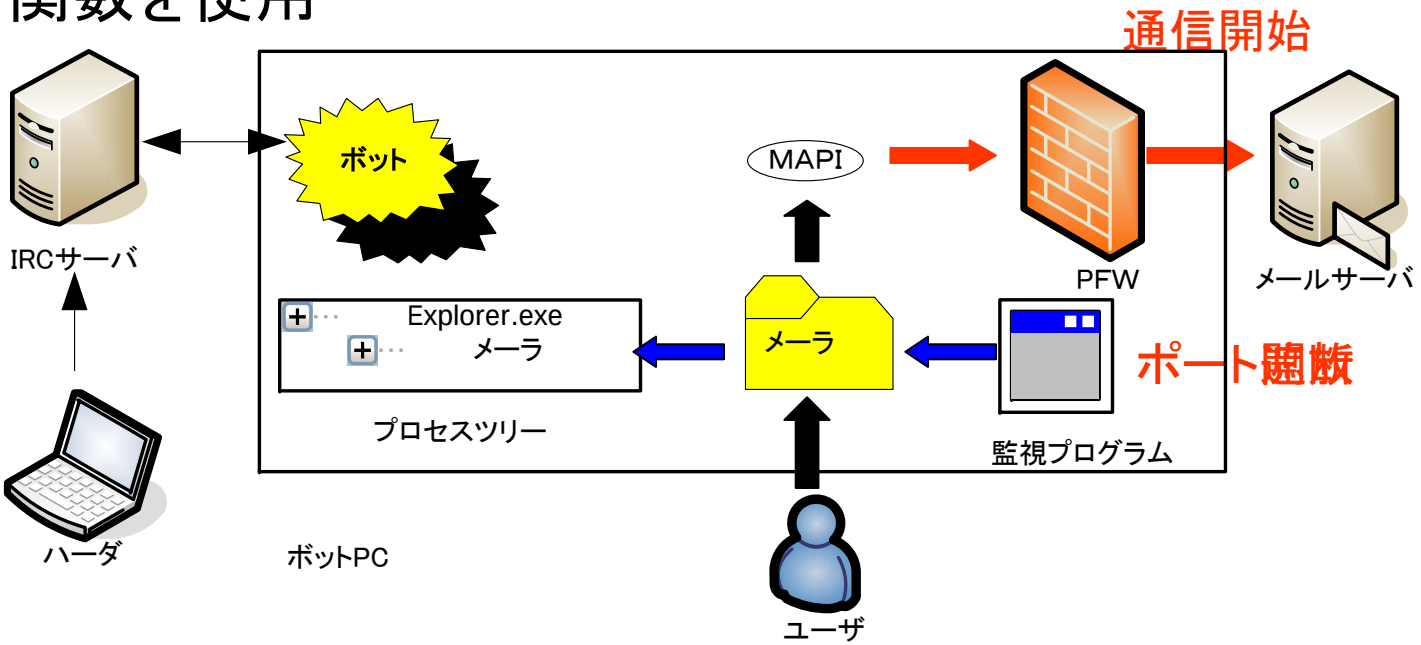
提案技術 – プロセスの監視 –

- メーラの上位プロセス
  - 正常な場合は次の手順へ
  - メーラの上位プロセスがexplorerでなければ不正と認識



提案技術 – ポート制御 –

- MAPISendMailの監視
  - メール送信要求があったときポートを開放する
  - 通信が終了したことが確認された場合にポートを遮断する
  - 通信終了確認はSFXSMTPSender クラスのコールバック関数を使用



提案技術 – IRC通信の監視 –

- 不正な動作
  - メーラ起動時に登録メーラと確認できなかったとき
  - メーラの上位プロセスがexplorerでない
- IRCの通信
  - ポート6660～6669を監視する
  - ボットネットによるIRC通信の約半数がポート6667である
  - ボットがIRC通信を行うとき一定間隔で通信が行われる
  - ボットの通信と疑わしい場合にユーザに「ボットに感染している可能性が高い」と警告を出す

むすび

- まとめ
  - ボット感染PCからのスパムメール送信対策として正規のユーザを判断しポートの制御による通信制御の検討を行った
- 今後の課題
  - この提案の有効性を確かめるための実装

補足：ボット検出数

	トータル		平均/日
	件数	種類	種類
検出数	974,999	31,082	350
未知		1,711	20

出典：サイバークリーンセンター

（2006年11月24日～2007年3月末日）

補足：IRC通信の監視

- IRCサーバへの接続の際の動作
  - クライアントはNICK，USERコマンドをサーバに送信
  - サーバは両方のコマンドを受け取ったのちにクライアントを登録する
  - クライアントはチャンネルに参加するためJOINコマンドを送信
  - IRCはニックネームの重複やサーバ負荷や疑わしいクライアントの接続を防ぐため接続拒否をすることがある
- NICK→(ERROR)→NICK→(ERROR)→．．．
- NICK→USER→(ERROR)→NICK→USER→(ERROR)→．．．

以上の動作が起こることが考えられる