端末からの不正メール送信を防止するための検討

050427585　平田祐二
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．ボットとは悪性のプログラムであり，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，ボットが組織化したボットネットからのスパムメール送信を防止するため，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

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．

攻撃者(Herder)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).

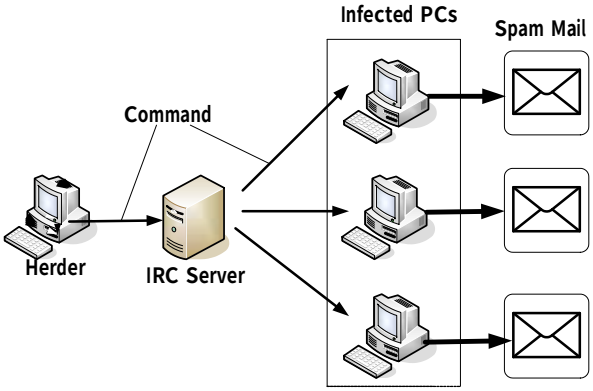


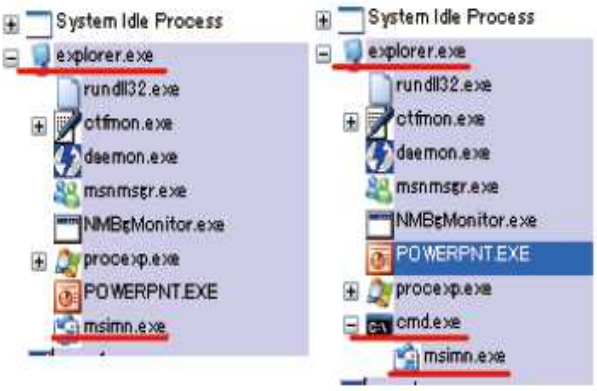
図 1.　ボットネットによるスパムメール送信

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 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．また，サーバを踏み台にしてスパムメールを送信するので，Herder を見つけることが困難とされている．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. 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初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送信を遮断する手法を検討した．

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を用いる．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．しかしボットに感染していると，メーラを呼び出す上位プロセスが正常時とは異なるはずである．メーラの上位プロセスが explorer.exe と確認できた場合にのみ正常と判断し，異なった場合はボットなどの不正なプログラムが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．



(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ための対策として，プロセスツリーを監視し，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検討した．今後はこの手法の有効性を確認する．

参考文献

[1] 間宮領一，渡邊晃：不正メールの送信とボット感染検知

端末からの不正メール送信を防止するための検討

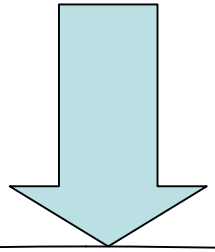
渡邊研究室

050427585

平田　祐二

研究背景

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

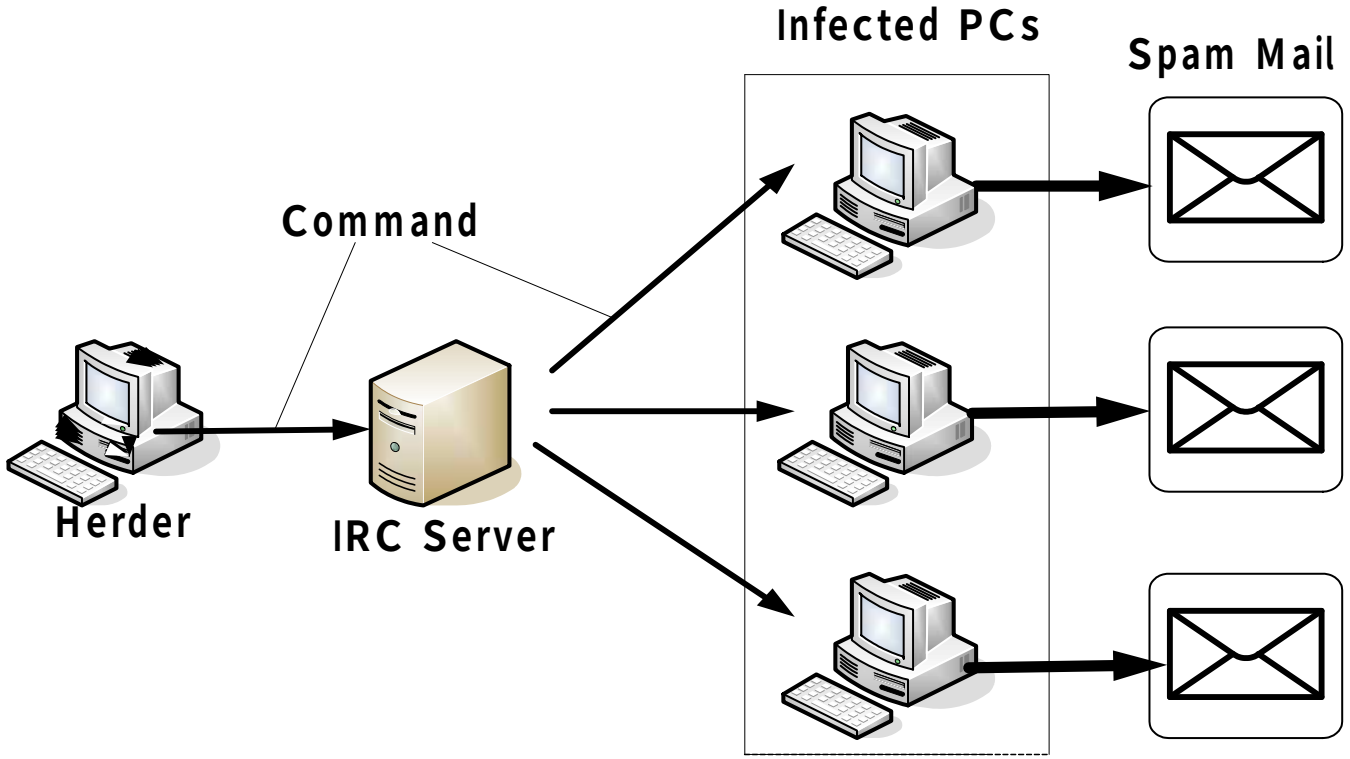


DoS攻撃，スパムメールの大量送信，個人情報流出

ボットとは

- ボット
  - ウィルスの一種
  - 攻撃者の意のままにコントロールされるPC
  - 愉快犯から犯罪目的
  - 感染したことに気づきにくい
- 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
  - 数千～数万台で構成

ボットネットによるスパムメール送信

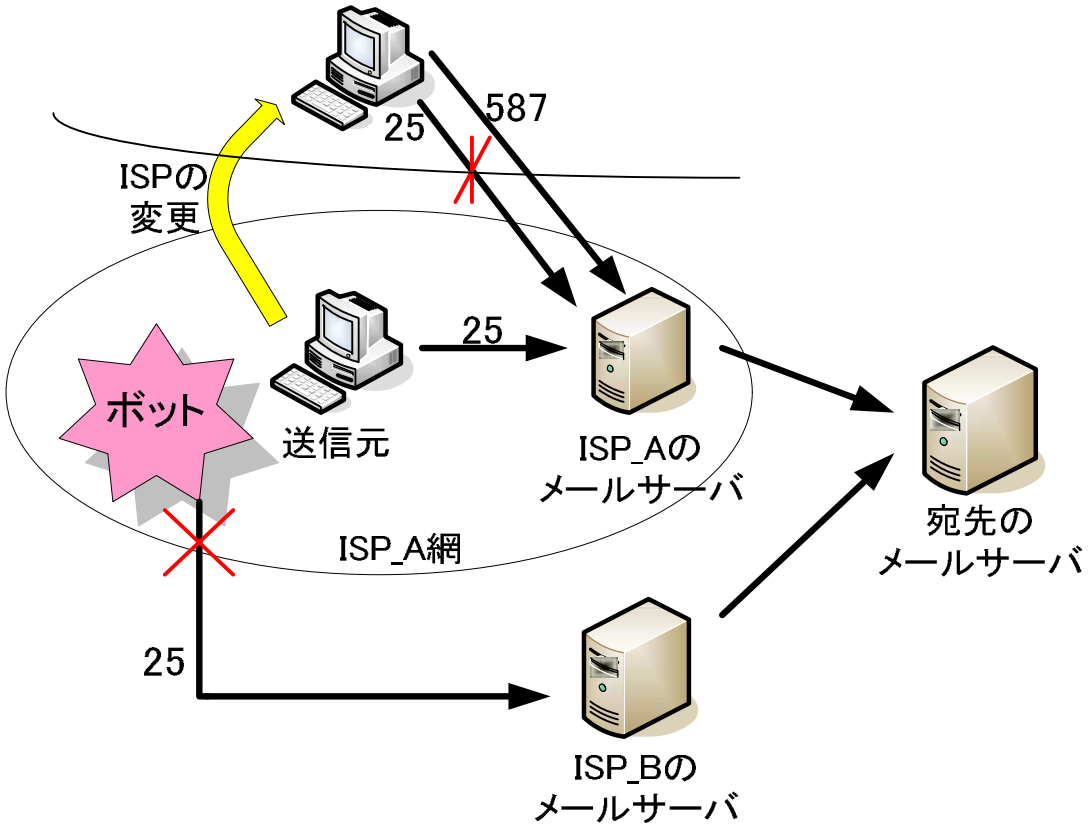


- **ボットネットを根絶することは難しい**
  - IRC Serverの冗長化
  - Serverを踏み台にしてスパムメールを送信する

IRC; Internet Relay Chat

既存技術による対策

- アンチウィルスソフト
  - クライアントで実施
  - パターンマッチング方式によりボットを取り除く
- OP25B(Outbound Port25 Blocking)
  - プロバイダで実施
  - 契約外ISPのメールサーバを使用したSMTPポート25番の通信を拒否
  - ユーザ認証機能付きのSMTPポート587番による通信サービス



既存技術の課題

- アンチウイルスソフト
  - 定義ファイルに情報のないボットに対応できない
  - 新種のボットが数多く出回っている（1日あたり約20種類）

  →定義ファイルの更新が間に合わない
- OP25B
  - ボットに感染したコンピュータが，ユーザの契約しているメールサーバへスパムメールを送信した場合には送信を防止できない．
  - 情報収集機能を持つボットには，ポート587番を使用してもスパムメール送信を防止できない．

提案方式

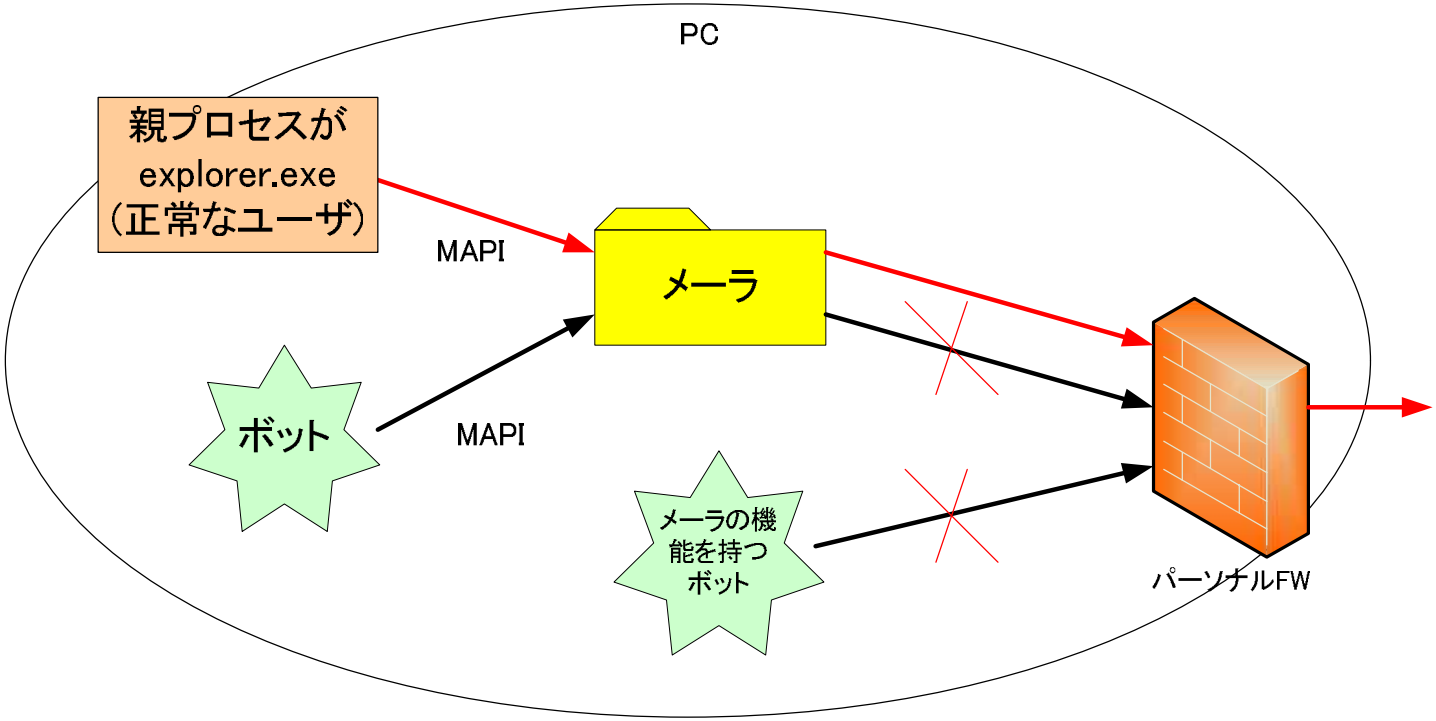
- クライアント側での対策
  - ボットは亜種や新種が多く存在する
  - ボットの感染は避けられない
  - 二次災害を防止する

→スパムメールの送信防止に着目している

- 提案内容
  - 常にSMTPポート25, 587番を遮断
  - MAPI(Messaging API)を監視
  - プロセスツリーを監視

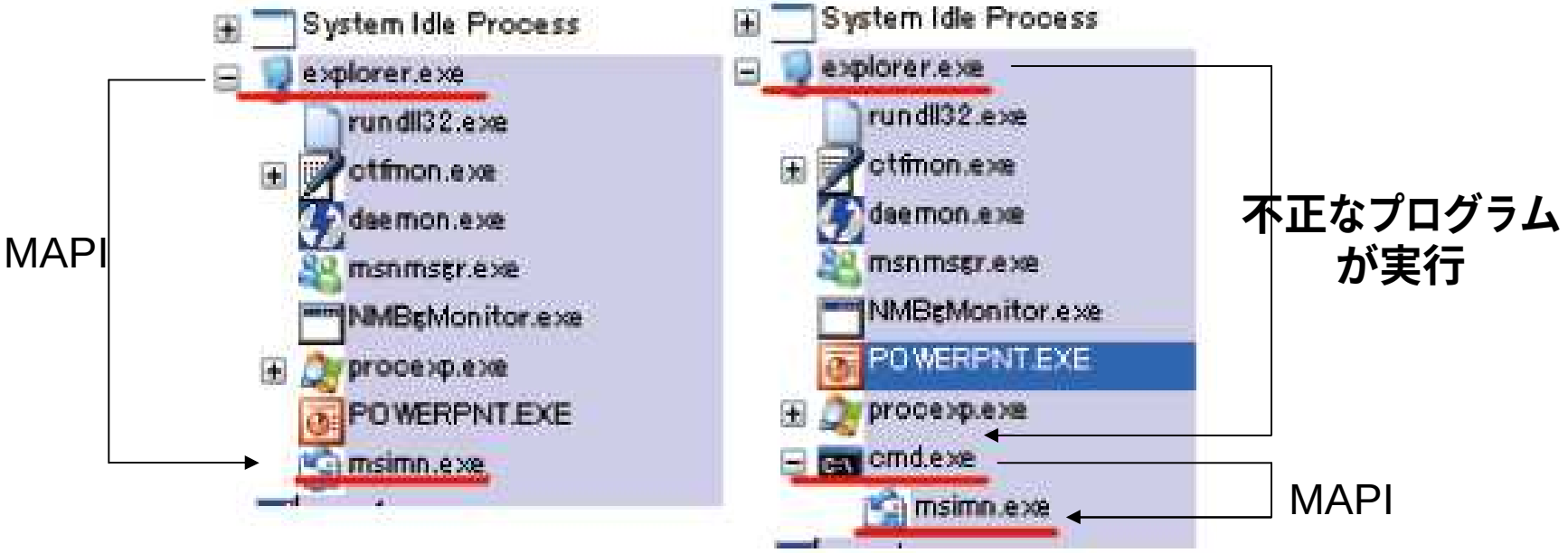
MAPIの監視

- MAPIとはWindows上で電子メールを扱うための関数郡で，一般的にWindowsではMAPIを用いてメールを送信する
- メーラを呼び出したのが正常なユーザと判断した場合
  →ポートを開放しメール送信を許可．送信終了後にポートを再度遮断
- 正常なユーザと判断するためにプロセスツリーを用いる



プロセスツリー

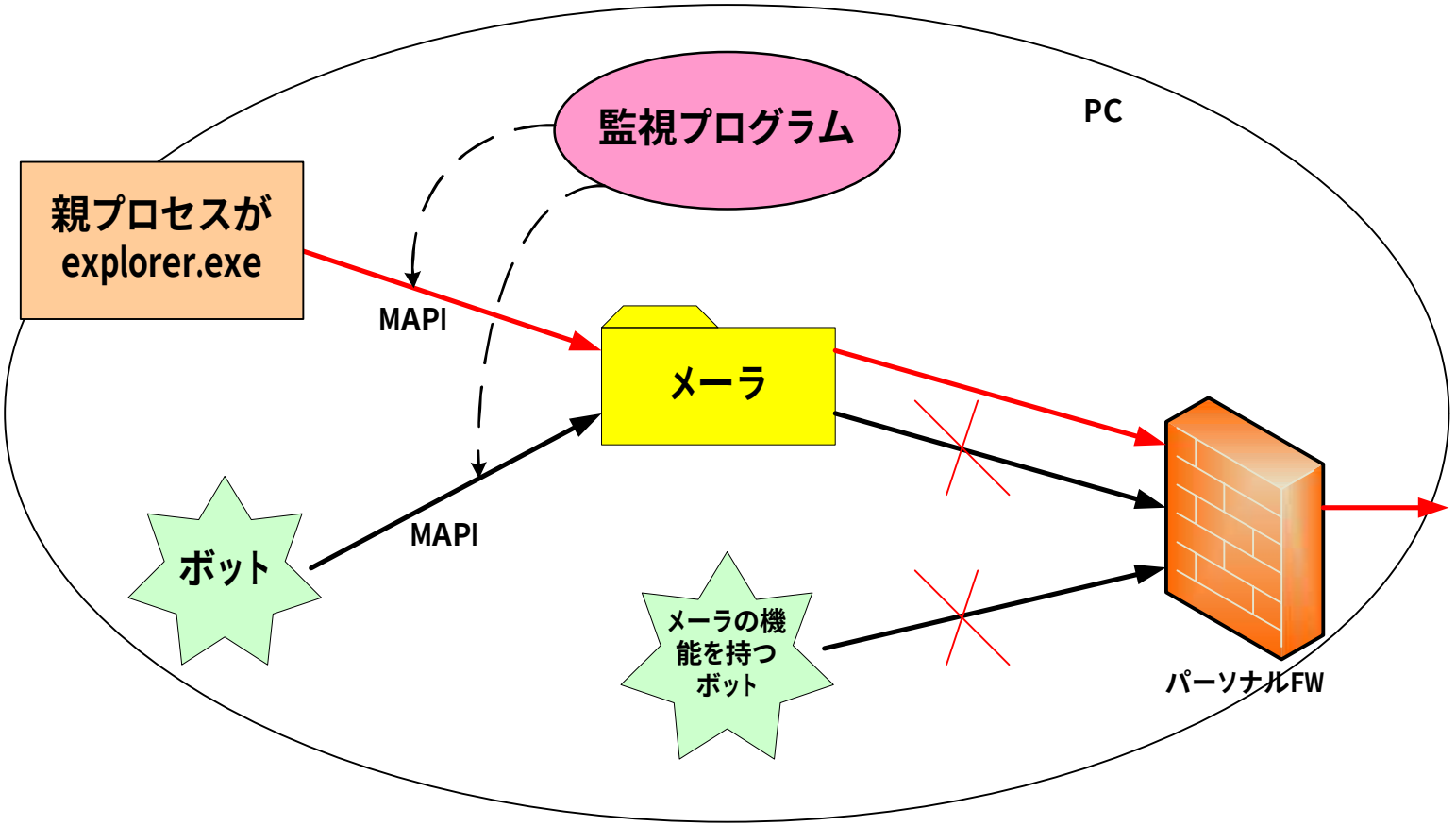
- 実行中のプロセスをツリー状に可視化したもの
  - 正常なメーラの親プロセスはexplorer.exe
- MAPIによるメーラ呼び出し時にメーラの親プロセスを確認
  - メーラの親プロセスがexplorer.exe
    →正常な実行と判断
  - メーラの親プロセスがexplorer.exe以外
    →不正なプログラムがメーラを呼び出したものと判断



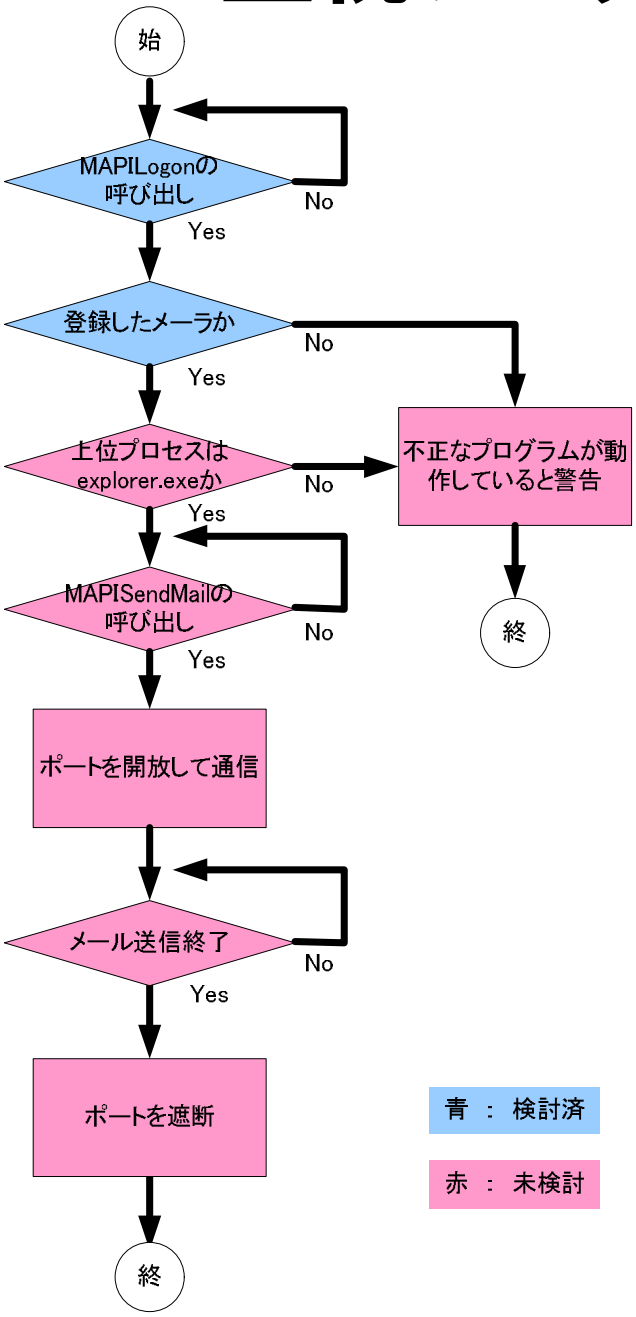
1.正常時　　2.異常時

提案方式の動作

- 常にSMTPポート25,587番を遮断
  - メーラの機能を持つボットのメール送信を遮断
- MAPIを監視しメーラの呼び出し元を確認
  - プロセスツリーを用いる
- メーラの親プロセスがexplorer.exeの場合にSMTPポートを開放（それ以外の場合は遮断したまま）



監視プログラムのフローチャート



- 本提案では，登録したメーラと呼び出し元のメーラが一致するかの確認まで，実装と検討が進んでいる．
- 登録したメーラと呼び出し元のメーラを確認する
  - 一致した場合

    →プロセスツリーを検査する
  - 一致しなかった場合

    →不正なプログラムが動作しているとユーザにアラームをあげる

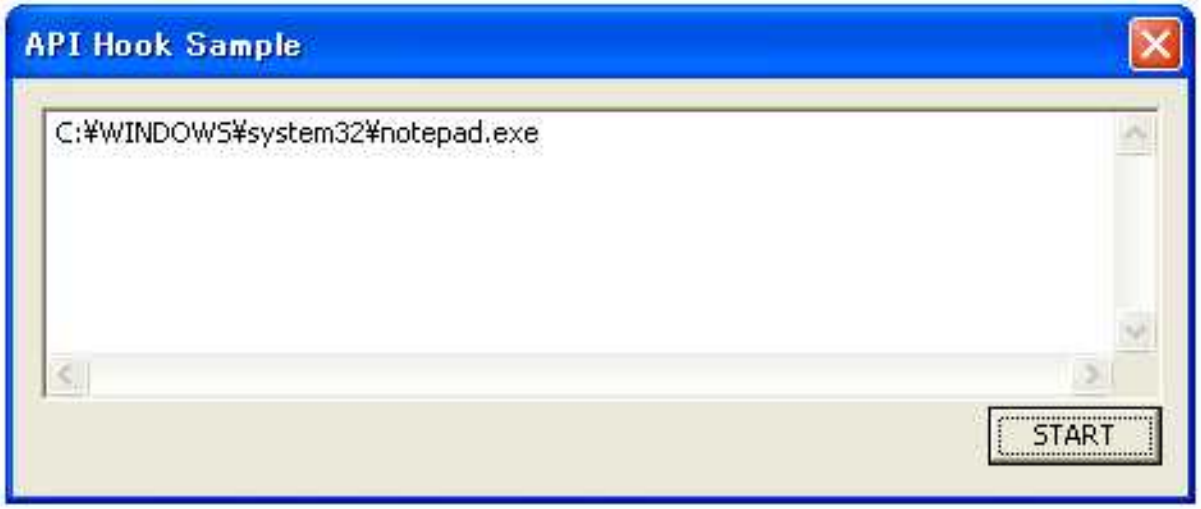
登録メーラの確認方法

- **レジストリを操作する**
  - **レジストリとはWindows系OS上の，システムやアプリケーションの設定を記録するデータベース**
  - HKEY_LOCAL_MACHINE¥SOFTWARE¥Clients¥Mail**キーに登録してあるメーラの値が格納されている**

1. RegOpenKeyEx　　**レジストリサブキーを開く**
2. RegQueryValueEx　**レジストリ値のデータを取得**
3. RegCloseKey　　**レジストリサブキーを閉じる**

呼び出し元メーラの確認方法　1

- MessageBox関数をフックし，呼び出し元のパスを表示することができるサンプルプログラムを利用する．
- フックとは，プログラムの特定の箇所に利用者が独自の処理を追加できる仕組みのことであり，主に機能追加や拡張などの手段として使われる．
- 開発環境はWindowsXP，コンパイラはVisual C++ .NET



サンプルプログラムの実行結果

参考URL： http://ruffnex.oc.to/kenji/text/api_hook/API_Hook.zip

呼び出し元メーラの確認方法 2

呼び出し元のパス：

C:¥WINDOWS¥system32¥notepad.exe

1. **拡張子ありのファイル名を取得**
   - **パスの先頭から’¥’，’:’，’/’を検索し，発見した時に次のポインタを保存する．この動作を**NULL**が検索されるまで繰り返す．**
   - notepad.exe**が取得できる**
2. **拡張子なしのファイル名を取得**
   - **拡張子ありのファイル名の先頭から’.’を検索し，最後に現れた’.’に**NULL**を代入する．**
   - notepad**が取得できる**

- MessageBox**関数を**MAPI**関数に書き換えることにより，呼び出し元メーラのプロセス名を得ることができる．**

むすび

- スパムメール送信防止としてクライアントでの対策を検討
  - プロセスツリーを監視し，メーラを呼び出したのが正常な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．
- 今後の課題
  - 提案方式の評価
  - 残された実装