不正メールの送信防止とボット感染検知の検討

間宮 領一

ボットネットを使用したスパムメールの大量発生が問題となっている．ボットは攻撃者からの命令を受けて初めて行動を開始するため，検出するのが難しいという特徴がある．本研究ではポートの制御を行うことにより，正規のユーザのメールの通信だけを許可し，ボットによるスパムメール送信を防止し，ボットによる 2 次被害を防止する．

Transmission prevention of illegal mail and examination of Bot infection detection

Ryouichi Mamiya

A large amount of generation of the spam mail that uses Bottonet becomes a problem.There is a feature that it is difficult to detect it because Bot starts on a course of action only after the instruction of the attacker is received. I admit only the communication of the email of an authorized user in this study by controlling the port and prevent the spam mail transmission of a message by the bot and prevent the second damage by the bot

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．ボットは攻撃者の命令を受けて始めて活動を開始するため，感染していることに気がつきにくいという特徴がある．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いわれている．世界の電子メールの 60～70%がスパムメールで，その内の 70%がボットネットによるものと言われ，ウィルス，スパイウェア，フィッシング，ワンクリック詐欺などの様々な脅威の媒介となっている[1].

ボットの感染者は一般のユーザが多い．その理由とし OS や各ソフトウェアのアップデートを行わない，サポート切れ OS の使用，アンチウィルスソフトの未導入などといったユーザが多いことがあげられる．国内の ISP ユーザでは 40 人から 50 人に 1 人がボットに感染しているといわれている．

従来のウィルスである大量メール送信型

ワームでは，DNS(ドメインネームシステム)に登録された正統なメールサーバに対してウィルスを添付したメールを中継させて拡散するものを第一世代，正統なメールサーバを介さず独自の SMTP エンジンを持ち，活動時に DNS サーバに MX レコード型 DNS クリエパケットを送信するものを第二世代，A レコード型 DNS クリエパケットのみを使用してメールサーバの名前解決をするものを第三世代と呼んでおり，これらはボットネットでも使用されている[2].

第一世代の対策として，メールサーバに対してのアンチウィルスソフトの導入，第二，第三世代では ISP(インターネットサービスプロバイダ)による契約外のメールサーバを使用したメール通信を拒否する，OP25B(Outbound Port 25 Blocking)の実施によりインターネット上のスパムメールが大きく軽減した．しかしボットは亜種が日々大量に出現しているためアンチウィルスソフトでは対策が追いつかない．ボットはスパムメールを送信するだけでなく，感染したコンピュータの情報収集をする　機能を持っている場合もあるため，OP25B ではボットネットによるスパムメールを根絶できていない.

本稿では，ボットが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に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送信を遮断する方式を提案する．IRC ポートも同時に監視し，メール送信時に IRC との通信が行われている場合，ボットに感染している恐れがあることをユーザに警告する.

表 1:ボット検出数(2006 年 11 月 24 日～2007 年 3 月末日)

	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

以降，2 章で OP25B とアンチウィルスソフトについて述べる．3 章では API フックにより正常なメールの判断を行い，ポート制御によりメールの送信制御を行う方式についての説明する．4 章で今後の検討課題を述べる．5 章でまとめる.

2. 既存技術とその課題

2.1 アンチウィルスソフト

ウィルス対策ベンダーなどが提供しているアンチウィルスソフトは，パターンマッチング方式によりボットに感染しているコンピュータからボットを取り除く．しかし，定義ファイルに情報のあるボットに対しては問題なく対応が出来るが，定義ファイルに情報のないボットには対応できない.

ボットはオープンソースになっており，1 日あたり約 20 種類の新種のボットが出現している(表 1)[3]．また，検知されるのを防ぐため定期的にボットがアップデートされるなど，アンチウィルスソフトでは対応しきれないという問題がある.

2.2 OP25B(Outbound Port25 Blocking)

OP25B とは，ISP（インターネットサービスプロバイダー）による対策で，ISP の会員のコンピュータから外部の契約外 ISP のメールサーバを使用したメール送信を防止するためのスパムメール対策技術である[4].

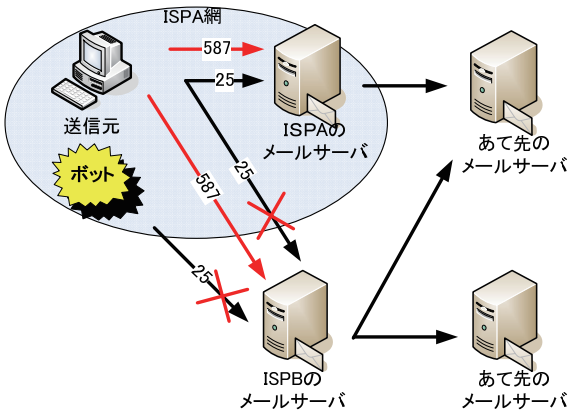

図 1：OP25B の詳細

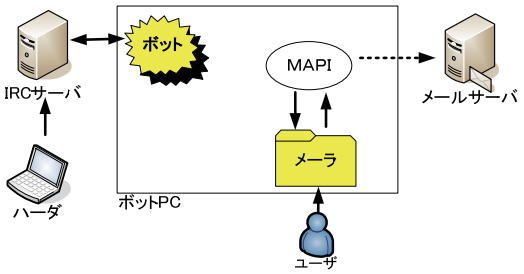

図 2：ユーザによるメーラを用いたメール送信

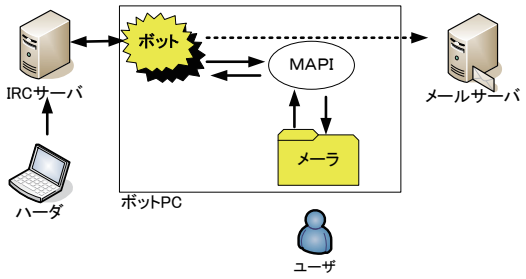

図 3：ボットによる独自の SMTP エンジンを用いたメール送信

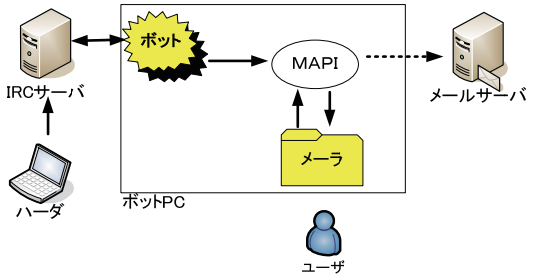

図 4:ボットによるメーラを用いたメール送信

図 1 に OP25B の詳細を示す．通常メールでは送信の際に SMTP ポート 25 番が使用される．ISPA の会員である端末から A のメールサーバへのポート 25 番の通信は許可される．A の会員が ISPB のメールアドレスを持っていて，B のメールサーバを使用したポート 25 番の通信を行いたい場合では通信がブロックされてしまう．この場合では，サブミッションポートと呼ばれるポート 587 番を使用しユーザ認証を行うことにより ISPA の会員が ISPB のメールサーバを使用したポート 25 番の通信を可能にする．この技術により，ボットが独自の SMTP エンジンを使用してのポート 25 番の通信は遮断することが出来る．しかし，ボットに感染しているコンピュータはメーラを用いてユーザが契約しているメールサーバへスパムメールを送信したり，情報収集機能をもつボットがパスワードなどを取得し，正規のユーザを装ってメールを送信したりした場合には対応できない．

3. 提案方式

本提案では，MAPI を監視しプロセスの確認を行うことにより，送信されようとしているメールが正常なものかどうかを判断し，ポート制御を行うことにより不正なメールがクライアントから送信されないようにする．以降，3.1 でクライアントからのメール送信の分類を示す．3.2 でポート制御のための，パーソナルファイアウォールの利用法について述べる．3.3 でプロセスツリーについて述べる．3.4 で IRC の通信をどのように監視するかを述べる．3.5 でシステムの動作を述べる．

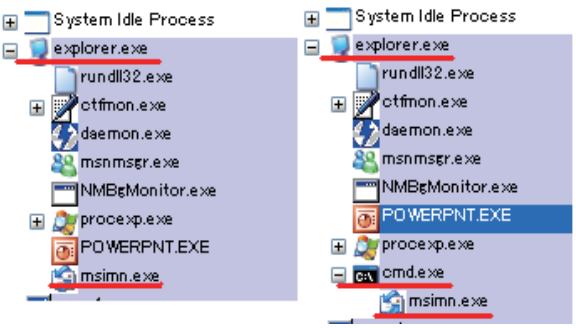

図 5：プロセスツリーによる上位プロセスの確認

3.1　メール送信の分類

MIAP(Messaging API)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，保存するための関数郡である[5].一般的に Windows では MAPI によりメールを送信する.

ボットに感染しているコンピュータがメールを送信する際，以下のようなメール送信パターンがある.

- ユーザがメーラを用いて正常にメールを送信する(図 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，ボット独自の SMTP エンジンによりメールを送信する(図 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(図 4).

3.2　パーソナルファイアウォールの利用

アンチウィルスソフトの機能としてパーソナルファイアウォールが含まれているものがある．これによりユーザのコンピュータに対して危険のある通信や，ユーザが通信をしたくないプロトコルを任意に遮断するなどの設定が可能である．また細かいポート制御が出来るものもある.

一般にメールを送信する際，SMTP ポート 25，587 番を使用する．提案方式では，パーソナルファイアウォールのポート制御機能を利用して常に SMTP ポートを遮断しておく．メーラを呼び出したのが正常なユーザかどうかを確認できた場合にだけ，ポートを開放し通信終了後にポートを再度遮断する．この方法により不正なメールの送信を確実に防止する.

3.3　プロセスツリー

3.2 で述べたメーラを呼び出したのが正常なユーザかどうかを判断するために，プロセスツリーを監視する．プロセスツリーとは，実行中のプロセスをツリー上に表現したものである．今回はプロセスツリーを可視化するアプリケーションである Process Explorer v11.04 を使用した[6].アプリケーションが実行されたとき，通常は explorer.exe が上位プロセスとなる．ボットが MAPI をフックしてメーラにアクセスした場合，メーラの上位プロセスがボットとなると考えられる(図 5)．プロセスツリーによりメーラの上位プロセスが，explorer.exe と確認できた場合は正常と判断し，違った場合は不正なプログラムが実行したということが確認できる.

3.4　IRC 通信の監視

ボットは攻撃者から命令を受け取るために，司令塔となるマシン C&C(Command & Control)サーバに接続を試みる．C&C サーバは IRC(Internet Relay Chat)が使われることが一般的である．IRC は IRC サーバと IRC クライアントで構成され，ユーザは IRC クライアントを使用し IRC サーバに接続する．サーバを介して，クライアント同士がテキストデータを交換することにより会話

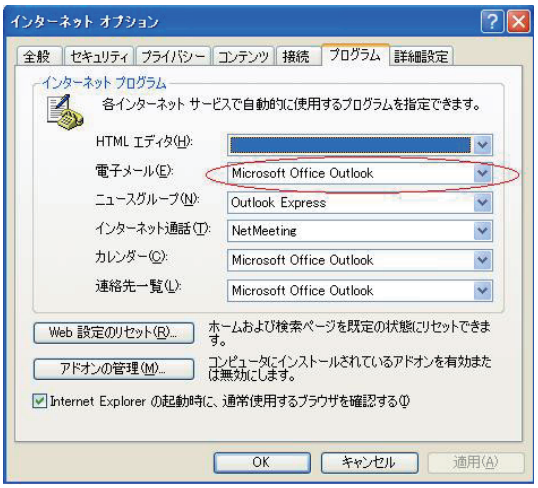

図 6：インターネットオプションによるメーラ登録

を行う.IRC はマルチキャスト配送なので，容易に多数のボットに指令を送ることが可能である[7]．フリーのサーバソフトが数多く出回っているため一般のユーザでもチャットシステムを作成することが出来る．

攻撃者はボットに命令を出すために，公開されている IRC サーバを使用するか，あらかじめボットに感染させた IRC サーバを使用する．またボット自身にサーバの機能を持たせ，IRC サーバとして使用する場合もある．また攻撃者は複数の IRC を使用しているため，ひとつの IRC サーバを止められてもボットネットが停止することはない．

近年では IRC サーバは専用サーバを使用する場合が多くなってきている．ボットが利用する IRC サーバのポートは TCP6660～6669 番が約半数を占めている．しかし，今日では HTTP ポート 80 番や 8080 番を使用した IRC の通信が確認されている[8]．また最近のボットは Web 経由による攻撃，ファイルのダウンロード，ボットのアップデートが増加傾向にある．

提案方式では，ボットに感染していることを検知するために IRC ポートの通信を監視する．ポート 6660～6669 番を監視し，このポートの通信が行われているときに MAPI による不正メール送信が確認された場合，ユーザに警告を出す．ただし，この方法では半数の IRC 通信しか検知できない．今回は他のポートに関しては，警告は出せないが不正メールの送信は防止することが出来る．

表 2：主な MAPI 関数

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．
MAPILogoff	メールサーバからログオフ．MAPILogon にて返ってきたセッションハンドルを指定．
MAPISendMail	MapiMessage 構造体のメールコンテンツを送信．

3.5　提案方式の動作

不正メールの送信を防止しボット感染を検知する方法として MAPI のフック，プロセスツリーの検査，IRC 通信の監視を行う監視プログラムを作成する．

監視プログラムはコンピュータが起動したときと同時に起動する．起動後にユーザに使用するメーラを選択させ登録を行う．メーラの登録方法としては Windows のインターネットオプションを使用する(図 6)．ここでは MAPI 対応メーラのみ選択できる．次に IRC 通信の監視を始める．

MAPI を使用するために mapi32.dll を解析した結果,MAPI 関数は 19 種類確認できた．その中でメール送信に使用される関数は表 2 に示す．MAPILogon，MAPISendMail，

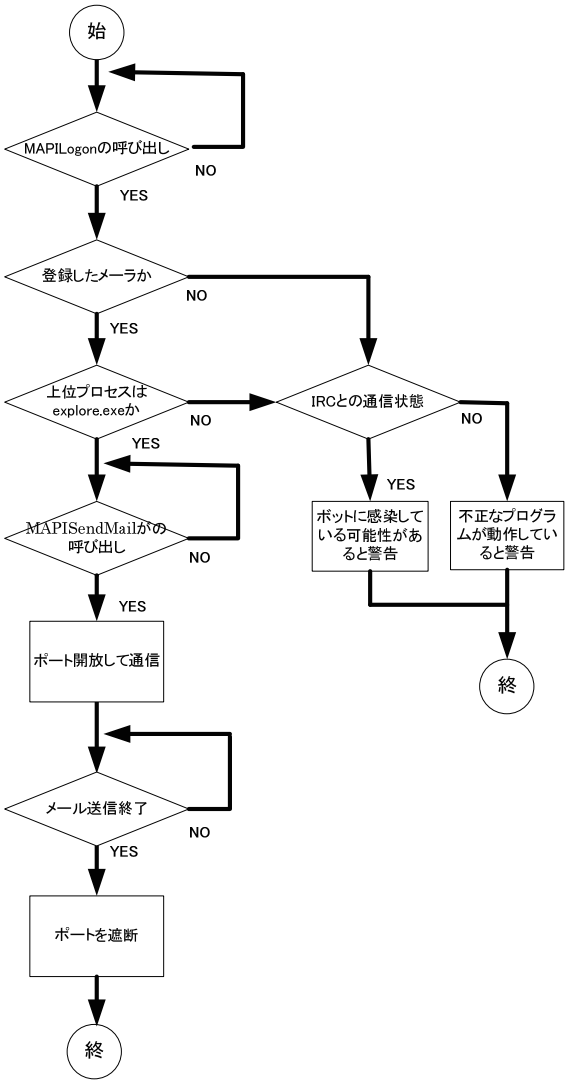

図 7：監視プログラムの動作

MAPILogoff の 3 種類である．監視プログラムでは，MAPILogon と MAPISendMail を使用する．

監視プログラム起動時に MAPILogon と MAPISendMail の監視を始める．MAPILogon が呼び出された時に，メーラが起動したことと判断できるため，呼び出し下のプログラムがあらかじめ登録しておいたメーラと一致するかを確認する．登録したメーラと一致しなかった場合は不正とみなし，IRC と通信状態か否かを確認し，通信状態ならばユーザに対してボットに感染している恐れがあるという警告を出す．呼び出し下のプログラムがあらかじめ登録しておいたメーラと一致した場合は，メーラの上位プロセスをプロセスツリーにより確認する．メーラの上位プロセスが explorer.exe の場合は，MAPISendMail が呼び出されるのを待つ．メールの通信要求がされるときに MAPISendMail が呼び出されるので，この時点で SMTP ポートを開放し通信を終了したら再びポートを遮断する．メーラの上位プロセスが explorer.exe でない別のプログラムだった場合，IRC と通信状態か否かを確認し，通信状態ならばユーザに対してボットに感染している恐れがあるという警告を出す．また，IRC と通信状態出なかった場合は，不正な動作があったという警告を出し，ポートは開かない(図 7)．

以上によりボットに感染したコンピュータからスパムメールが送信されることを防ぎ，ユーザに対して危険にさらされていることを知らせる事が出来る．

4. 今後の検討課題

本稿では不正なメール送信が行われるのを防ぎ，IRC と通信状態かを確認することによりボットに感染していることをユーザに警告する対策を提案した．この提案により不正メールの送信は防止でき，IRC 通信の監視によりボットに感染の恐れがあることをユーザに知らせることが出来る．しかし，ボットネットで使われている IRC ポートの約半数分しか監視できないため，感染検知の点において完全ではない．このため，ボットに感染しているという確証を得るため IRC の通信監視が今後の検討課題である．また，現在ではほとんどのメーラが MAPI に

対応しているが，対応していないメーラや自作のメーラを使ったメールの通信を行いたい場合にポートが開放されずメールを送信することが出来ない問題がある．本研究では，使用するメーラが MAPI 対応である必要があるため今後この問題を検討していく．

5. まとめ

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し，ボットに感染していることをユーザに知らせるための手法を検討した．今後は検討課題も踏まえつつ，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]“ISS が実現する最新のメール・セキュリテ～ビジネスの可用性とセキュリティの両立～”
インターネットセキュリティシステム株式会社，井下田久幸 2007 年 6 月 21 日

[2] “ボットネットワーク対策について”
武藤泰雄，熊本大学総合情報基盤センター・コミュニケーション研究部
(http://www.cc.kumamoto-u.ac.jp/arcmit05/musambot.html)

[3] “Interop Tokyo 2007”
(http://internet.watch.impress.co.jp/cda/event/2007/06/14/16051.html)

[4] “Inbound/Outbound Port 25Blocking 実施 ISP”
(http://seclan.dll.jp/ccblk25.htm)

[5] “Japan MSDN”
(http://msdn.microsoft.com/library/ja/default.asp?url=/library/ja/vccore/html/_core_MAPI_Topics.asp)

[6] “Process Explorer v11.04”
(http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx)

[7] “An Inside Lool at Botnets”
Paul Barford , Vinod Yegneswaran, Advances in Information Security

[8] “Bot C&C Servers on Port 80”
(http://isc.sans.org/diary.html?storyid=1865)

謝辞

本研究を進めるにあたり，多大なるご指導，ご鞭撻を賜りました渡邊晃教授に心より感謝いたします．また有益なご助言，ご検討を頂きました渡邊研究室の皆さんに深く感謝いたします．