ウィルスの内部感染拡大を防ぐための協調的 HTTP フィルタリングの実現

佐藤　陽一　　品川　高廣　　吉澤　康文

東京農工大学　工学部　情報コミュニケーション工学科

１．はじめに

インターネットの発展につれて,Web サーバに代表されるインターネットサーバも数多く稼動するようになってきた.しかし今日のインターネットでは，Blaster のようにウィルスによるサーバへの攻撃が頻繁に行われており,サーバを保護する仕組みがますます重要となっている.

本稿では，大学や企業などの大規模な組織内で動作しているインターネットサーバを対象として，組織の管理者が組織内のサーバを一括して保護するためのシステムについて述べる．本稿では特に Web サーバを対象として，HTTP を狙った攻撃からの保護を目的とする.

本稿で提案するシステムでは，組織内のネットワークで稼働中の Web サーバを保護するために，ルータにおいて HTTP のプロトコルのレベルでフィルタリングする．また，組織内の一台のサーバがウィルスに感染することによって,組織の内部へと感染が広まってしまう内部感染を防ぐために，ルータ間でフィルタリングすべき内容に関する情報を連携し，必要に応じて動的にフィルタ設定を更新出来るようにする．これによって感染の範囲を最小限に抑える.

２．現在の問題点

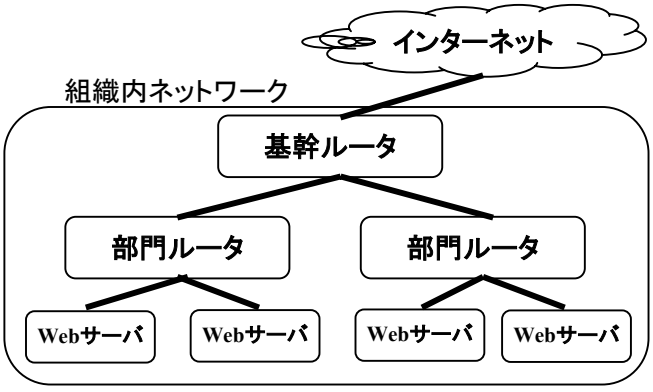

図１　想定する組織内ネットワーク

大規模な組織では，例えば図１に示すように,基幹ルータと呼ばれる装置によって，組織内ネットワークがインターネットに接続されている.組織内ネットワークでは，部門ごとにそれぞれルータを設置して，部門内のネットワークを基幹ルータに接続している．また，各部門ではそれぞれ Web サーバなどを独自に稼動させている.これは大学内であれば，研究室ごとに Web サーバを運営している状況に相当する.

従来の保護の手法には，以下のような問題点がある．第一に，パケットフィルタによるフィルタリングでは，保護の単位がポート単位なので，HTTP プロトコルを通じた Web サーバに対する攻撃などのように，稼動中のサービスを狙った攻撃を防ぐことが難しい．第二に，組織全体の管理者は一般にインターネットとの接続部分でのみフィルタリングを行なっている場合が多く，同じ組織内の別のマシンに対する攻撃がフィルタリングされない場合が多い．そのため，ウィルスに感染したノートパソコンを接続するなどによって，いったん組織内のマシンが感染してしまうと，組織全体のマシンに感染が広まってしまう内部感染が発生する可能性がある.第三に,フィルタリングの設定は管理者が手動で行っており,管理者が新しくフィルタリングの設定に追加するべき設定を考えてからフィルタリングの設定を変更していては,攻撃に対して迅速に対応することが難しい.

３．協調的 HTTP フィルタリング

本稿で提案するシステムでは，以下に述べる３つの手法によって，ウィルスなどの内部感染を防止する.

（１）HTTP プロトコルの中身を見て,攻撃の際によく含まれる文字列との比較により,フィルタリングを行なう.
（２）Web サーバが返すエラーの内容を分析して,新しい攻撃を自動で認識し,動的にフィルタを設定する.
（３）ルータ間で連携してエラー情報,フィルタ設定の情報をやりとりし,感染の拡大を最小限に抑える.

Cooperative HTTP Filtering For Preventing Virus From Spreading Over Local Networks.
Yoichi Sato, Takahiro Shinagawa, Yasufumi Yoshizawa.
Department of Computer, Information and Communication Sciences, Tokyo University of Agriculture and Technology.

3.1 HTTP フィルタリング

HTTP を利用した攻撃では,不正な GET メソッドを送ることにより,サーバでプログラムを実行させるなどの手法が用いられている.このような攻撃では,ほぼ共通の文字列を含む GET によるアクセスを行ってくるという特徴がある.

そこで,攻撃の際によく含まれる文字列をキーワード（以下 NGW(No Good Words)）として登録しておき,フィルタリングする.

また,サーバに対するバッファオーバーフロー攻撃を防ぐために，GET のサイズをチェックして,1KB より大きなものは破棄する.

3.2 動的フィルタリング

基幹ルータは，部門ルータからエラー等の情報を集めて分析し，新たな攻撃や内部感染を検知して,自動的に新しい NGW 設定を作る.Web サーバに対する攻撃は，複数のサーバに対して無差別に行なわれることが多いという点に着目し，同じ IP アドレスから送られた同じリクエストに対して，異なる複数のサーバがエラーを返した場合に，無差別攻撃の可能性が高いと判断し，攻撃かどうかを判定するために，そのリクエストを一時的な NGW リストに登録しておく.

この一時的な NGW をそのままフィルタリングしてしまうと，意図的に不正なリクエストを送ることによって，正しいリクエストもフィルタリングさせてしまう DoS 攻撃を受ける可能性がある．そこで，この一時的な NGW を含むリクエストが組織内のマシンから送られた時点で，ウィルス感染による攻撃が発生したと判断し，フィルタリングすべき NGW として登録する.

3.3 ルータ間の連携

基幹ルータが新しい NGW 設定を登録すると，その情報は部門ルータに伝えられる．部門ルータは,新しい NGW を受け取ると即座に登録し,次のアクセスからのフィルタリングに適用する.これにより，攻撃をより早く検知できるとともに,早い段階で部門ルータにおいてフィルタリングを行なうことにより，内部感染による感染の拡大を防ぐことが出来る.

４．性能測定

提案手法では，HTTP のプロトコルの内容分析や，新しい攻撃の検知，フィルタリングを行なうなどのためにオーバーヘッドが発生する．本性では，このオーバーヘッドを測定するための実験について述べる．この実験では，本稿で述べた方式によるフィルタリングを行なった場合と行なわなかった場合について，HTTP を用いたファイルのダウンロードにかかる時間を比較した．実験には 300byte から 203Kbyte までの７種類の大きさのファイルを使用した．実験に使用したマシンは，表１のとおりである.

表１　クライアント PC とルータ PC

CPU	Pentium4 2.4C GHz
メモリ	512Mbyte

実験結果を図１に示す.横軸はアクセスしたファイルのサイズ(単位:byte),縦軸はダウンロードにかかった時間を(単位：ms)を表している.

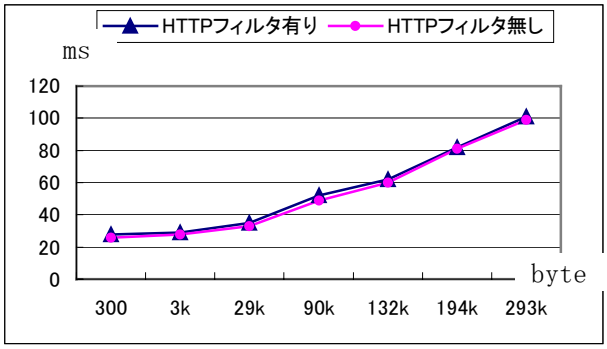

図１：HTTP フィルタのオーバーヘッド

フィルタリングをすることによる性能低下は,最大でも 90kbyte のファイルにアクセスした場合の７％程度であった.

５．終わりに

本稿では，大規模な組織内で動作する Web サーバを一括して保護することを目的とした強調的 HTTP フィルタリングの枠組みについて提案した．本稿で述べた手法では，(1)HTTP のレベルでのフィルタリング，(2)HTTP のエラー情報の分析によるフィルタリング設定の自動更新，(3)内部感染を防止するためのルータ間で連携したフィルタリング，などの手法により，ウィルスによる不正アクセスの被害を最小限に抑えることが出来る.

今後の課題としては，攻撃を認識するアルゴリズムに対する更なる検討などが挙げられる.

参考文献

[1] Stephen Thomas“HTTP プロトコル”SOFT BANK Publishing (2002)