透過プロキシーシステムを用いたHTTPフィルタリングの効果について

伊藤 求[†]，伴 好弘[†]，鳩野 逸生[†]

和文抄録 本報告では，学内から学外透過プロキシをL4スイッチとWebキャッシュサーバを用いて実現するとともに，組織外部から内部のWWWサーバへのアクセスに対しても，内部→外部の場合と同様な逆透過プロキシを導入したことを特徴とする神戸大学における透過プロキシシステムについて述べる．導入後，学内のWWWサーバは1台もアタックの被害にあっておらず， 神戸大学のネットワークセキュリティ維持に大きな効果があったことを確認した．

HTTP Filtering with Rule Based Reverse Transparent Proxy System

Motomu ITO[‡‡] Yoshihiro BAN[‡‡] and Itsuo HATONO[‡‡]

Abstract This paper deals with a rule based reverse transparent proxy system for HTTP access. To protect the attacks to WWW servers in Kobe University from the outside networks, we develop a transparent proxy system that consists of two web cache servers for LAN to WAN and WAN to LAN http access by using a layer 4 switch, respectively. From Dec. 2001, the developed system has filtered almost http attacks from WAN and no damaged WWW servers have been found in Kobe University. This result suggests that the system is much effective to protect WWW servers from the attacks.

1. はじめに

近年，WWW(World Wide Web) を用いた情報発信および情報収集は，大学における研究教育活動にとっても必要不可欠なものになってきており，学内に数多くのWWWサーバが存在している．これは，近年，ソフトウェアパッケージ技術の進歩によりWWWサーバソフトウエアの導入が飛躍的に簡単になったことによるものである．一方，コンピュータウイルス，ワーム，クラッカーによるWWWサーバへの攻撃は増加の一途をたどっている．これらの攻撃を防ぐには，サーバソフトウェアを適切に設定することと，ソフトウェア自体のアップデートなど，日々のメンテナンスが必要であるが，放置されているサーバが多いのも事実である．また，このようなユーザサイドの問題もさる事ながら，ソフトウェアの設計仕様や情報公開対応の遅れなど，ユーザの手が届かないところで発生する脆弱性によって引き起こされる被害が顕在化してきている．

また，Webブラウザを利用するクライアントに関しても，閲覧するだけで被害を及ぼすページが数多く存在することが知られている．さらに，クライアントがコンピュータウイルスに感染した場合，他のWWWサーバを攻撃するタイプのものも存在しており，学内ネットワーク運用に関して大きな問題の一つとなっている．WWWサーバと同様に，クライアントにおいても適切なソフトウエアのアップデートが行われていれば多くの場合回避できるが，完璧なメンテナンスをユーザに期待することは事実上困難である．

以上のような状況に鑑み，本報告では，神戸大学が昨年度導入したWWW透過プロキシシステムについて述べる．本システムは，通常，組織内部から外部を閲覧する場合に用いられる透過プロキシ [1] をL4スイッチとWebキャッシュサーバを用いて実現するとともに，組織外部から内部のサーバへのアクセスに対しても，内部→外部の場合と同様な逆透過プロキシを導入したことを特徴とする．これにより，内部に設置されたWWWサーバを外部からの攻撃から守るとともに，アクセスログ収集による問題発生時の解析が迅速化できる．

2. HTTPアクセスのためのセキュリティ防護方策の要件

一般にネットワークのセキュリティを守るためには，Firewallを用いた通信制限を設ける手法がとられる．これは，外部ネットワークと内部ネットワークの間にFirewallを設置し，そこで外部からの通信

[*]神戸大学総合情報処理センター
[‡‡]Information Processing Center, Kobe Univ.

要求に必要なポートだけを開き通信を行うというものである. すなわち, Firewall においては，ポートのON/OFF 制御のみ可能であり，WWW などのネットワークサービスへのサービス要求の内容に対してアクセス制御を実現することは困難である.

ネットワークのセキュリティを守るための代表的な方法として，内部のネットワークを外部ネットワークと完全に遮断して構築し, 外部ネットワークへの全ての通信は Firewall や代理サーバを介して通して行うという手法が存在する. しかし, この手法はユーザに対する制約が大きくなるとともに, 外部と通信するためにはネットワーク管理者, ユーザ双方に設定登録作業が発生し, ヒューマンエラーによるサービス障害という潜在的な問題を抱えることになる. またサービスに制限が多いということによりネットワークサービスの利用をやめてしまうという悲劇的な結果にもつながる可能性もあるため, できる限りユーザへの負担を低減しつつネットワークセキュリティを一定のレベルで保つ必要がある.

このような観点と, 神戸大学における WWW の利用状況を考慮すると, HTTP アクセスにおけるセキュリティ防護策は，学内の WWW サーバおよび Web ブラウザ側のどちらも現状の設定を変更せずに運用可能であることが求められる.

3. 神戸大学における透過プロキシシステムの概要

以上のような状況を考慮し，神戸大学では，学内から学外への WWW サーバへのアクセスおよび学外からの学内の WWW サーバのアクセスの両方に対して, 透過プロキシを導入した. **Fig. 1** に構成の概要を示す. 前述したように，本プロキシシステムは，(1) 内部・外部 http アクセス用プロキシと, (2) 外部・内部 http アクセス用プロキシから構成される. 以下に, 構成の詳細について述べる.

4. 透過プロキシシステムの構成

Fig. 1 に示すように， 2 台の Web キャッシュ装置はそれぞれ, WAN-LAN に対するキャッシュ, LAN-WAN に対するキャッシュとして動作している. これらの Web キャッシュ装置は, キャンパスネットワークの対外接続部分にレイヤ 4 スイッチと呼ばれる， 通過するパケットをアクセスするポート別にスイッチングできるネットワーク装置を介して間接的に接続している. 使用機材を **Table 1** に示す.

4.1 システムの特徴

提案システムの備える特徴としては前述した通りであるが， 列挙すると以下のようになる。

Table 1 List of equipments in the trasparent proxy system.

Equipment name	Product name
Layer 4 Switch	Alteon 180e
Cache Server	CacheFlow6000x2

(1) **提案するシステムを通過するパケットのうち, http に関するものを選択して代理応答処理を行う.**
この特徴により, レイヤ 4 スイッチにより http 以外のアクセスが Web キャッシュを通過しないため, http 以外のアクセスに関するスループットの低下を最小限に抑えることが可能である.

(2) **ユーザレベルからみるとキャッシュの存在を意識する必要がない.**
WAN 側と LAN 側の双方向で完全な透過キャッシュ動作を実現しているため, ユーザレベルでは本システムの存在を一切意識する必要がない.

(3) **URL に対してルールベースのフィルタリングが可能である.**
この特徴は IP レイヤで行われるパケットフィルタではなく,URL に対して設定ルールに従ったフィルタリングを実行することを実現している. この機能を用いることで, Nimda などが行う WWW サーバに対する攻撃をブロックすることが可能である. また,

(4) **提案システムは基本的に Web キャッシュであるので, 冗長な web アクセスに対して代理応答することで, ネットワークの利用効率を向上させるする効果を持つ.**

従来のブラウザからのアクセスを効率化することを目指としたキャッシュ機能に加えて, 学内の WWW サーバに対する学外からのアクセスも Web キャッシュによる代理アクセスに置き換えることを実現している. そのため学外からの大量のアクセスに対して, WWW サーバが極端な過負荷状態に陥ることを抑制できる.

このように, 提案システムでは単純なパケットフィルタリングでは処理できない Web サーバへのアタックを URL フィルタリングを実現することで, 防止することを可能にしてる.

5. フィールドテストとその結果

本システムを 2001 年 9 月に構築し, 本稼働に必要な基礎データの取得を目的に 9 月 21 日から 27 日までの間フィールドテストを行った. 実験当時, 透過キャッ

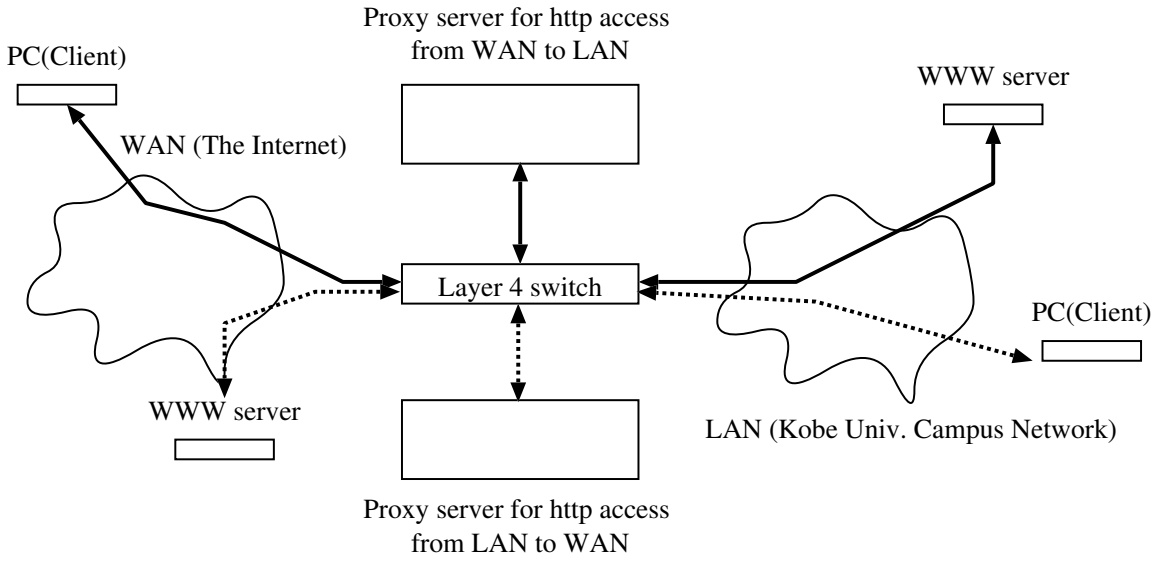

Fig. 1 Transparent proxy system in Kobe Univ.

Table 2 Number of filtered Nimda's attcks.

Date	No. of filtered Nimda's attacks	Filtering rate	Total no. of http access
2002.9.21	1,617,361	51 %	3,181,225
2002.9.22	2,872,865	43 %	6,682,643
2002.9.23	1,476,004	33 %	4,469,101
2002.9.24	788,551	45 %	1,742,782
2002.9.25	1,045,134	45 %	2,345,690
2002.9.26	1,169,305	39 %	3,016,361
2002.9.27	751,954	26 %	2,906.555

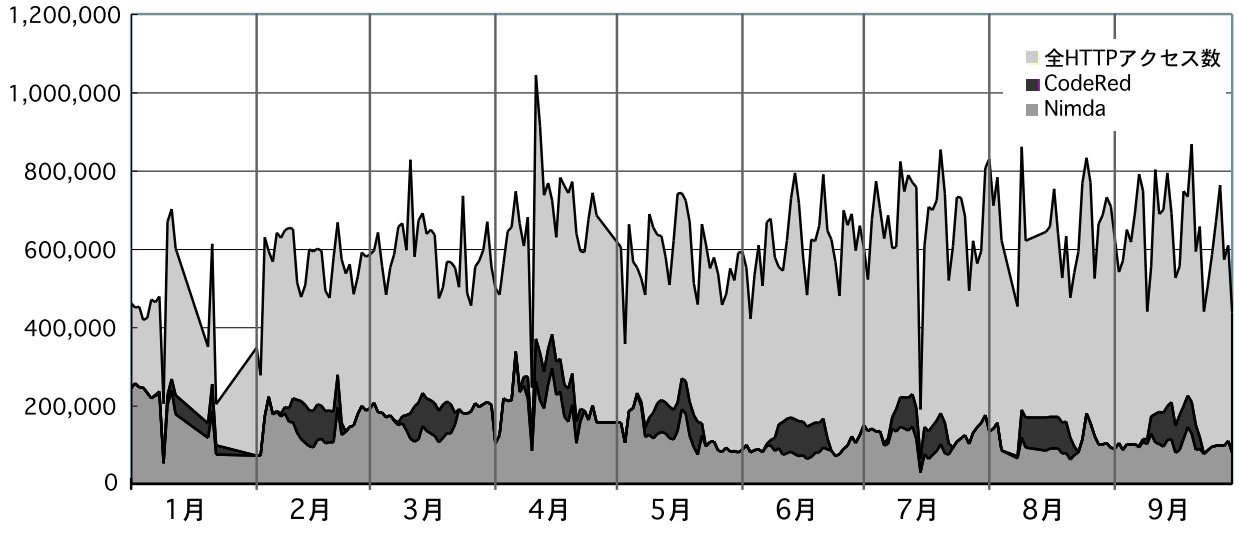

Fig. 2 No. of http access from WAN to LAN and filtering rate of Nimda's attacks.

シュの性能を評価する目的でテストを行っていたが, 偶然に Nimda ウィルスの感染が急速に広がり, それに伴って Web サーバに対する不正アクセスが確認されたので, 急遽 Web キャッシュ装置に URL フィルタの設定を行うこととなった. この URL フィルタは http のアクセスの際に用いる URL に対して正規表現を用いたフィルタリングを実現している. 本システムでは学外のからの Web アクセスは学内の Web サーバへ直接サクセスすることはなく, キャッシュサーバが代理でアクセスする形をとる. したがって, Nimda など不正アクセスを行う際に規則性のある URL を用いて攻撃してくる場合, これを検知するルールの設定を行うことで, キャッシュサーバが Web サーバに代わり攻撃をブロックすることが可能となる. 今回 Nimda のアクセスに対するルールの設定を行い, その結果, 本システムが Nimda などの不正アクセスに対して非常に有効な機能を果たしたことが確認できた. そのときに取得された WAN-LAN に対する Web キャッシュの総アクセス数と URL フィルタによりブロックされた Nimda の不正アクセス数の対比を **Table 2** に示す.

Table 2 に示すように, 当時学外からの Web アクセスのうち約半数が Nimda による不正アクセスであることが分かる. この Nimda を原因とする大量な不正アクセスのため, 多くの機関で Web サービスの停止や, 過剰なトラフィックのため他のサービスの停止にまで追い込まれたところが少なからず存在したいたが, 本学の場合このシステムが稼働していたため, 学内の Web サーバをはじめ他のネットワークサービスを停止することなく運用を継続するが可能であった.

また, このシステムは学内から学外にある Web サーバに対する不正アクセスに対しても同様に機能するため, 学内のクライアント PC などが Nimda などのコンピュータウィルスやワームに感染しても学外への被害の拡大を阻止することが可能である. 他の特徴として, 昨今 IIS[2] の脆弱性を狙った不正アクセスが社会問題化してきている. 多くの場合サービスと提供しているコンテンツが IIS に強く結び付いたものが多いため, 現時点では他の Web サーバに乗り換えることが難しい場合も少なくない. このような場合, 本システムでは Web サーバをネットワークシステムレベルで防御しようとする考えのため, これらの Web サーバが持つ潜在的な脆弱性による問題を顕在化させることを防止させることが可能と考える.

本報告では Web サービスと Nimda を取り上げたが, これらのウィルスやワームが Web サーバに対して行う攻撃のうち, 規則性のあるものに関しては, ルールベースの URL フィルタは極めて有効に機能することが確認できた.

これと同様に感染力が強く, 急速に感染範囲を広げるコンピュータウィルスが原因となって引き起こす, 2 次的な攻撃は他のネットワークサービスにも起きることは想像に固くない. その場合であっても本システムと同様な手法で被害を低減できるサービスも存在すると考える.

また, 本システムでは, 全 http アクセスに対するログを収集しているが, 前述の WWW サーバ攻撃機能を持ったウイルス感染端末の早期発見に大きな効果があった.

6. おわりに

本報告では, 学内から学外透過プロキシを L4 スイッチと Web キャッシュサーバを用いて実現するとともに, 組織外部から内部のサーバへのアクセスに対しても, 内部→外部の場合と同様な逆透過プロキシを導入したことを特徴とする神戸大学における透過プロキシシステムについて述べた. 導入後, 学内の WWW サーバは 1 台もアタックの被害にあっておらず, 神戸大学のネットワークセキュリティ維持に大きな効果があったことを確認した.

現在の問題として, 現在のシステムは, フィルタリングルールがあってはじめて有効であることからも分かる通り, WWW を用いた攻撃をできるだけ早期に察知し, 速やかにフィルタルールに反映させることが鍵となる. 将来的には, CERT 等からでる報告から自動的にフィルタリングルーツを生成し, インストールすることが必要になると思われる. また, 本システムは, 冗長構成になっておらず, キャッシュサーバがストールした場合, キャッシュおよびフィルタリング機能が利用できなくなることと, 今後対外接続が増速された場合, キャッシュサーバが通信ボトルネックになる可能性がある. 今後は, さらに L4 スイッチを導入することにより, システムの冗長化を計っていく必要があると思われる.

参考文献

[1] http://www.squid-cache.org/
[2] http://www.microsoft.com/