6S-09　ポートスキャン検出を利用した動的なパケットフィルタリングシステムの設計*

小林 文彦†　西山 裕之†　溝口 文雄†

東京理科大学 理工学部‡

1　はじめに

現在、インターネットへの常時接続サービスが安価に提供され、中小企業、一般家庭ユーザーも多く利用するようになってきている。多くの企業は、ネットワークセキュリティ対策としてファイアウォールを導入しているが、一般家庭、中小企業レベルでは、導入、運営を行えていないのが現状である。多くの場合、ルータのパケットフィルタリング機能を利用し、フィルタリングの設定を行なっていることが考えられるが、全く知識のないユーザーが適切に設定できるものではない。設定ミス等により、必ずしもユーザーの望む働きをそのままの状態で保証できるわけではなく、ユーザーは常に不正アクセスの危険にさらされている。

本論文では、ユーザーのコンピューター上で、不正アクセス者が攻撃対象を調査する際に行なうポートスキャンを検出し、このスキャン元に対して専用のフィルタリングルールをユーザーに代わって自動的に設定、更新するシステムの設計を行なった。本システムにより、ユーザーはセキュリティを意識することなく、不正アクセスに対するセキュリティを高めることが可能となる。

2　設計方針

従来、不正アクセスの防御策としてファイアウォールを導入することが一般的である。ファイアウォールは、防御策として確かに有効な手段であるといえるが、それはセキュリティーポリシーにのっとった正しい設定と、日々の運用によるところが大きい。ファイアウォールは、あらかじめ設定した通りに忠実に実行するが、ポートスキャンなどの攻撃を検出することはできない。ログから攻撃を見つけ出すことは、困難な作業であり、攻撃を受けてから短時間で対策を施すことは難しいという問題点がある。ファイアウォールは、導入、運用にコスト、専門知識が必要であることから、専門のシステム管理者がいない状況では導入は難しい。特に現在の常時接続サービスが普及し始めたことで、一般家庭でもインターネットへの常時接続を行なっている。現在はルータによるパケットフィルタリングの設定を行ないセキュリティを高めていると思われるが、専門の知識がないユーザーが設定することを考慮するとセキュリティを保てるとはいえない。不正アクセス者は、最終目標となるコンピューターを攻撃するためにいくつもの踏台となるコンピューターを使用するため、格好の標的となっている。不正アクセス者の行動を考えてみると、攻撃の第一段階として、インターネットの広範囲に渡ってポートスキャンと呼ばれる調査を行うと考えられる。ポートスキャンは、コンピューターのOS、サービスなどを調べるもので、この情報を元に不正アクセス者は、攻撃対象を定め実際の攻撃に移行する。したがって、ポートスキャンをしてきたIPアドレスには不正アクセスを試みる悪意のあるパケットがくる可能性が高く最も注意しなくてはならないことが分かる。スキャン元のIPアドレスに対して短時間で、このIPに行き来するパケットを遮断する対策を施すことで、不正アクセス者がそのIPで攻撃を仕掛けてきてもすぐには不正アクセスできない。このため数多くある他のコンピューターにターゲットを移すと考えられ、セキュリティが保たれる。このようなツールは、UNIXにおいていくつか提供されているが、一般ユーザーを対象に考えた場合、UNIXの導入することは現実的ではない。そこで、本論文では一般的に使用されているWindows2000を対象とし、リアルタイムなポートスキャン検出[1]とその対応策となるパケットフィルタリングルールを自動的に追加、更新可能なシステムを設計する。

3　システム構成

本システムは，ポートスキャン検出部とフィルタリングルール制御部の二つから構成される．このシステ

*Design for dynamic packet filtering system which uses port scanning detection

†Fumihiko KOBAYASHI, Hiroyuki NISHIYAMA, Fumio MIZOGUCHI

‡Faculty of Sci. and Tech. Science University of Tokyo

ム構成を図1に示す。悪意を持ったユーザーが、ポートスキャンによりコンピューターを調べたときポートスキャン検出部によって、ポートスキャンをされたことを検出する。検出結果からスキャン元のIPアドレスを特定し、このIPアドレスをフィルタリングルール制御部に送る。フィルタリングルール制御部は、送られてきたIPアドレスに対してフィルタリングルールを生成し追加、更新を行なう。パケットフィルタリングには、Windows2000に標準搭載されているルーティング&リモートアクセスサービス（RRAS）を使用する。

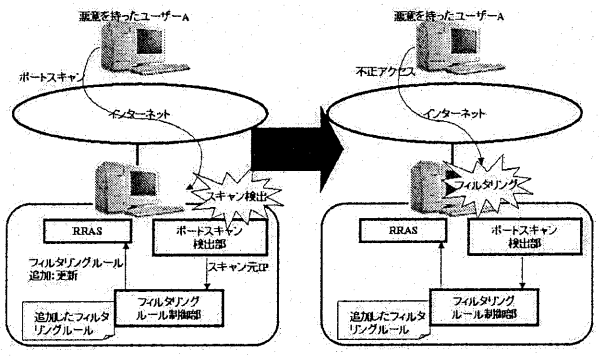

図 1: システム構成図

3.1 ポートスキャン検出部

ポートスキャン検出部によってポートスキャンのリアルタイム検出を行なう．検出するスキャンはTCPスキャンのFull-Connectionスキャン，Half-Connectionスキャンである．ポート137,138,139や，ポート23など危険があるポートへの接続を監視することでポートスキャンを検出する．

3.2 フィルタリングルール制御部

フィルタリングルール制御部は，ポートスキャン検出部からのフィルタリングルール追加依頼（攻撃元IPアドレス）を受け，RRASのフィルタリングルールを変更し，反映させる．RRASでは，次のときにフィルタリングルールのチェックを行なう．

- input：パケットが入ってくる時
- output：パケットが外に出ていく時

RRASは，netsh.exeコマンドを使用し，インターフェースに対するフィルタリングルールをフィルタタイプ（input,output）毎に設定し，フィルタの制御を行なう．例えば，自分のコンピュータのIPアドレスが192.168.0.10でIPアドレス：192.168.1.139からポートスキャンを受けた場合，次のコマンドを実行する．

```
netsh routing ip add filter ‘‘ローカル エリア接続’’ input
192.168.1.139 255.255.255.255
0.0.0.0 0.0.0.0 ANY
netsh routing ip set filter name=’’ ローカル エリア接続’’
filtertype=input action=forward
```

追加したフィルタリングルールは，ファイルに追加した日付と共に記録し、一定期間を過ぎると解除する．

スキャン元からのIPをフィルタリングするため，スキャン元から攻撃を仕掛けようとしてもコンピュータへのアクセスができないため未然に攻撃を防ぐことが可能となる．

4 システムの有効性

本システムでは，ポートスキャンのリアルタイム検出を行ない，フィルタリングルールを自動的に更新することを可能にした．フィルタリングはホームルータによって設定することが基本だが，使用用途にあったフィルタリングルールを設定できるとは限らない．ユーザーは，アクセスログの監視とその対策となるフィルタリングルールの追加を行なうことなく，ポートスキャンによって不正アクセス可能なコンピュータを探している不正アクセス者からの攻撃を自動的に防ぐことが可能となった．不正アクセス者は，少しでもセキュリティの弱いコンピュータを狙うことから，迅速なフィルタリング対策を行なうことで，別のコンピュータに攻撃対象を切替えると考えられる．本システムだけで，安全なフィルタリングをできるとは言えないが，ルーターによるフィルタリングの補助として使用することでユーザーの管理作業を軽減させられる．

5 おわりに

本稿では，ポートスキャン検出の検出結果を利用した動的なパケットフィルタリングシステムについて述べた．本システムによって，ユーザーが直接ログを監視し、フィルタリングルールを追加することなく不正アクセス者からの接続をフィルタリングをすることが可能である．

参考文献

[1] Vern Paxson, A System for Detecting Network Intruders in Real-Time, Seventh USENIX Security Symposium, SAN ANTONIO TEXAS, Jan 26-29, 1998.