福井大学 工学部 研究報告 第52巻 第1号 2004年3月
Mem. Fac. Eng. Univ. Fukui, Vol. 52, No. 1 (March 2004)

CATVインターネット網におけるポートスキャン検出システムの作成と事例報告

村上 雅彦* 小高 知宏** 小倉 久和**

The Case Report of the Portscan Detection System in a CATV Internet

Masahiko MURAKAMI*, Tomohiro ODAKA** and Hisakazu OGURA**

(Received February 20, 2004)

In this paper, we report design and implementation of a portscan detection system for the CATV internet network. The portscan detection system runs on the UNIX operating system. We report the example run of the portscan detection system on the computer connected to the CATV internet network for two months. Our detection system was able to detect portscan and unusual access preswming on the Microsoft Windows operating system security hole (MS03-049).

Key Words : Portscan, CATV Internet Network, Portscan Detection System

1. はじめに

現在，コンピュータネットワークは社会においてめざましい発展を遂げている．しかし，コンピュータネットワークが社会の中で普及するにつれて，ネットワークを介してのコンピュータへの侵入は大きな問題となっている．一般家庭にもADSLやケーブルテレビなどの常時接続環境が整い始め，セキュリティが甘いコンピュータは一般家庭の個人のものも攻撃の対象となっているだけでなく，侵入されることにより他のコンピュータへの攻撃の踏み台として利用されることもある．そのため，侵入者を自動で検出するシステムの構築の必要性がある．本論文では侵入行為の準備行為にあたるポートスキャンを検出するシステムを作成し，CATVインターネット網に接続したマシンで運用した事例を報告する．

ポートスキャンは標的となるマシンに実害のない攻撃であるが，確実に悪意があるととられる行為であり，不正アクセスのなかでも頻繁に行われる攻撃である．本研究ではインターネットで使用されているTCP/IPプロトコルを対象としている．ネットワーク上を流れるパケットに共通して存在するヘッダ部分を解析する．そして，このヘッダ部分の情報を，あらかじめシステムがデータベースにもっているセキュリティ上問題のある特徴(シグネチャ)と比較することで侵入者の検出を行う．ネットワークを流れるパケットとしてIPデータグラム，TCPセグメントを取得し，そのヘッダ部分をリアルタイムに解析することにより侵入者の企てを検出し未然に防ぐことができると考える．

本研究でのポートスキャン検出システムはUNIX系OS上で動作するように構築した．プログラム言語はC言語を使用した．システムはpcapライブラリ[1]を使用することで指定されたネットワークインタフェースからパケットを取得してパケットの付加情報を解析する．その付加情報を蓄積し解析することでポートスキャンの検出を行う．

実験は本研究室のプロキシサーバであるoglab-netを使用した．これにより実際の一般的常時接続環境でのポートスキャンの検出を試みた。その結果、ftp, http などのポートに対するアクセスがあり，実際にポートスキャンを検出することができた．また，特定のポートでの異常なトラフィックの増加を観測す

* 大学院工学研究科知能システム工学専攻
** 知能システム工学科
* Human and Artificial Intelligent Systems Course, Graduate School of Engineering
** Dept. of Human and Artificial Intelligent Systems

ることができた.

本論文の構成として、2 章では侵入方法とその検出法について述べる。3 章では本研究で作成したシステムの概要，動作，実装について説明する。5 章では、本研究で作成したシステムを使用した実験とその結果について述べる。6 章では、実験および本研究に対する考察を述べる。

2. 侵入検出について

2.1 侵入検出の原理

侵入者が行う侵入行為を検出する方法として大きく分けて，ミスユース検出方法とアノーマリ検出方法がある[2]．ミスユース検出方法は，不正な行為をあらかじめ定義しておき，システムに対してなされた行為がそれにあてはまるかどうかで不正な行為であるかどうか判断する．アノーマリ検出方法は，正常な行為をあらかじめ定義しておき，それに該当しない行為を不正な行為であると判断する．侵入検出において，侵入行為にあたらないものまでを侵入行為として検出してしまうことを「フォールスポジティブ」,侵入行為を侵入行為として検出しないことを「フォールスネガティブ」と呼ぶ.

ミスユース検出方法は，行われる行為が，既知の侵入行為に該当する行為であるかどうかを検出する方法である．その行為が侵入行為であるかどうかの判断を行うために，その行為と侵入行為を特徴付けるデータとの比較を行う．それによって侵入行為の判断をする．また，その行為を特徴付けるデータを「シグネチャ」という.

ミスユース検出方法は「シグネチャ」がセキュリティの侵入行為にあたる行為以外を検出する場合は「フォールスポジティブ」になり，セキュリティの侵入行為にあたる行為を検出しない場合，つまり侵入行為にあった適切な「シグネチャ」がない場合は「フォールスネガティブ」になる.

アノーマリ検出方法は,通常の行為でないものを検出する方法である．侵入行為は通常は行われない行為にあたると仮定される．つまり，通常でない(異常な)行為が検出されれば侵入行為であると判断できる．この方法は，通常の行動を知っていなければならないので，ユーザ毎の特徴を表したもの（プロファイル）を持っていなければならない．さらに，短期間ではユーザ毎の特徴をつかめないので，ある程度の準備期間が要る.

本研究では，ミスユース検出方法を用いて侵入者の検出を行う．ミスユース検出方法ではシグネチャが必要である．今回はこのシグネチャを「アクセスされたポートの数」とした．侵入者からのポートへのアクセスの数を数え，その数があらかじめ設定したある値(閾値)を越えた時点で侵入と判断する．また，通常，サービス提供側であるサーバにはクライアントに対してサービスを提供するために待ち受けをしているウェルノンポートがある．侵入者はサーバが提供しているサービスでシステム上の欠陥を持ったものを探している．よって，サービスを提供するためのポートであるウェルノンポートへの複数のアクセスはポートスキャンである可能性が非常に高い．そこで，ウェルノンポートの中で，サービス提供をしていないポートへのアクセスであっても，複数のアクセスがあった場合，あらかじめ設定した閾値を越えなくてもポートスキャンであるとする.

2.2 検出方法

ポートスキャンを検出するには，自身のコンピュータのポートに対してのアクセスを監視する必要がある．つまり，どのポートに対して，いつ，どこから，どれだけのアクセス数があったかを数える.つまり，IP データグラムの送信元 IP アドレスや TCP セグメントの宛先ポート番号の情報を取得することが必要である．これにより，自身のコンピュータのどのポートが狙われているかを把握することができる．閾値の設定は，どのような環境で使用しているコンピュータでシステムを動作させるかによって異なる．何らかのサービスを提供しているコンピュータであれば，閾値の設定は高い値になる．Web サービスを提供しているコンピュータであれば 80 番ポートに対してのアクセスがあるのは当然である．しかし，普段のアクセス数を大きく越すようなアクセスがあった場合には異常である可能性もある．このような場合の閾値の設定は正常な状態のアクセス数の情報が必要になるため難しい．また，何もサービスを提供していないコンピュータならば,閾値は低くなり、閾値がゼロとなる場合もある.

2.3 システムの設計方針

本システムでは,pcap ライブラリを使用する.pcap ライブラリは Van Jacobson 氏らの開発したライブラリである．pcap ライブラリを使用することでネットワークインターフェースが手に入れることのできるパケットのヘッダ情報を，データとして手に入れることができる．取得するパケットは，図 1 のような構造をしている[3].ヘッダ情報の中から宛先 IP アドレス，送信元 IP アドレス，宛先ポート番号，Control Bits の情報を取得する．パケットから取得した情報からウェルノウンポートに対するアクセスを解析し

ポートスキャンの検出を行う．本システムでは，自身のコンピュータのウェルノウンポートに対して送信されたパケットのみを対象をする．ウェルノウンポートはサービスを提供するために使用されるので，そこから侵入される可能性が高いからである．本論文では、CATV のインターネット網に接続されたコンピュータを使用している．このコンピュータはサービスを提供していないので，閾値はゼロの設定とする．

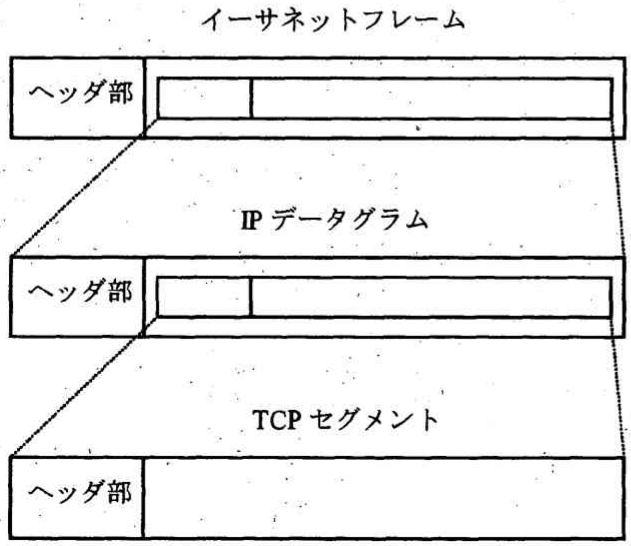

図 1　パケット構成図

ットのヘッダ情報を，データとして手に入れることができる．そして，イーサネットフレーム，IP データグラム，TCP セグメント，UDP データグラムなど，それぞれのヘッダ部分の情報を pcap が用意した構造体に格納する．パケットを取得する毎にこれらの処理を行う．

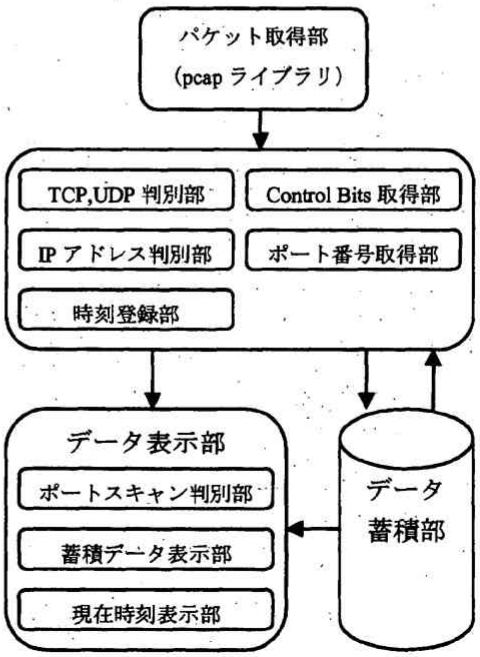

図 2　システムの構成

3.　システム設計と実装

3.1 システムの概要

本研究では，ネットワーク経由でのシステムへの侵入において，準備行為として行なわれるポートスキャンを検出するプログラム(portscan)を作成する．このプログラムは UNIX 系 OS 上で動作するものである．使い方は

./portscan ネットワークインタフェース名

のようにコマンドラインにネットワークインターフェースを指定することで動作する．プログラムの終了は Ctrl-C である．

このシステムのおおまかな動作は，まず，コマンドライン引数で指定したネットワークインターフェースがネットワーク上のパケットを手に入れる．次に，そのパケットからヘッダ情報を取り出し，ポートスキャンを判断するための情報を蓄積する．そして，蓄積した情報によりポートスキャンであると判断する．システムの動作の結果としてポートスキャンに関する情報を標準出力に表示する．

このシステムの構成は図 2 のようになっている．

パケット取得部は pcap ライブラリを使用しパケ

パケット取得部で得られた情報はパケット処理部に渡り，ポートスキャン判別に必要である IP アドレス，Control Bits のフラグの種類， TCP と UDP のどちらであるか，宛先ポート番号などの情報を処理する．これらの情報はデータ蓄積部とデータ表示部に渡される．

データ蓄積部では，パケット処理部から渡されたデータを蓄積し，データ表示部からの要求があった場合にはデータ表示部に蓄積したデータを渡す．

データ表示部では，パケット処理部から渡された情報とデータ蓄積部の情報からポートスキャンであるかを判断する．ポートスキャンであると判断した場合はデータ蓄積部の情報と現在時刻を表示する．そうでない場合は何もしない．

3.2 システムの実装

今回作成したシステムの構成を説明する．

システムは，パケットを取得する毎に packet_print 関数を呼び出す．packet_print 関数は，パケットからヘッダ情報を取り出し，その情報を pcap ライブラリで用意されている構造体(iph, tcph, udph)に格納し，ポートスキャンを判別する関数(synscan 関数，

ackscan 関数，finscan 関数，nullscan 関数，xmasscan 関数，udpscan 関数)を順に呼び出す処理を実行する．システムの構成は図 3 のようになっている．

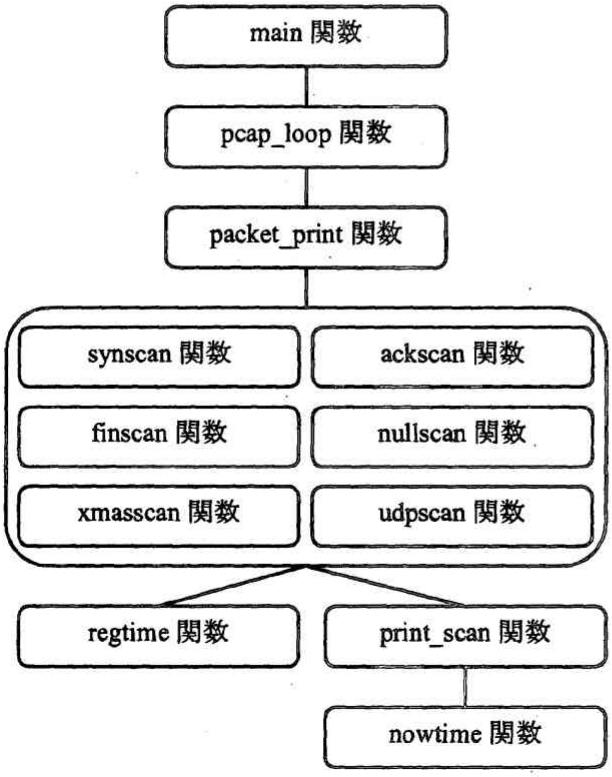

図 3　システム構成

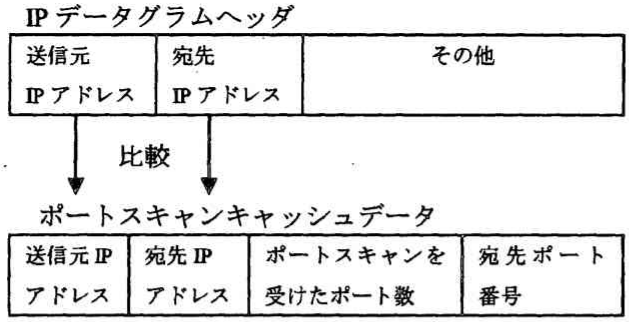

図 4　フラグチェック

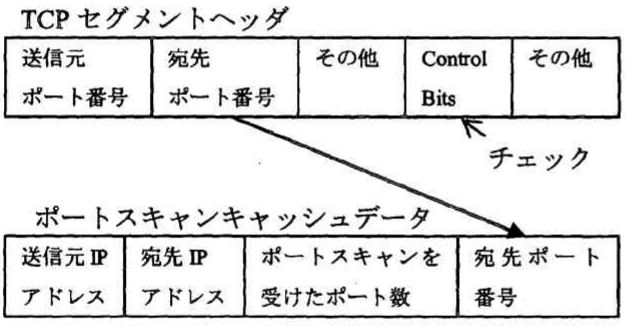

図 5　IP アドレスの比較

次に，ポートスキャンを判別する関数について説明する．どの関数も処理がほぼ同様なので，synscan 関数を例に説明する．

まず，図 4 のように，TCP セグメントの Control Bits が TH_SYN であるかを判別する．TH_SYN であった場合のみ処理が続行され，図 5 のように，送信元 IP アドレスと宛先 IP アドレスの組み合わせが，IP データグラムとポートスキャンキャッシュデータで同じであるかを判断する．

IP アドレスの組み合わせが同じであった場合，図 6 のように処理される．TCP セグメントの宛先ポート番号(th_dport)が以前にアクセスされたかどうかを判断している．以前アクセスがない場合のみアクセスされたという情報が更新される．さらに、そのポートに何回アクセスがあったかを数え，その情報も更新される．その後，regtime 関数と print_scan 関数を呼び出す．regtime 関数は現在の時刻をポートスキャンキャッシュデータに格納する処理を行う関数である．print_scan 関数はポートスキャンキャッシュデータの内容を標準出力に送る関数である．

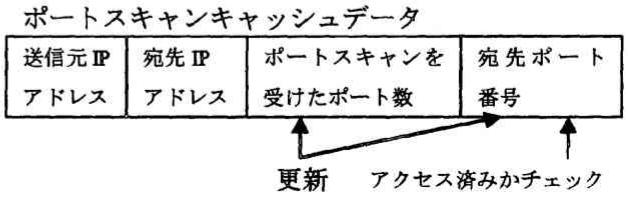

図 6　ポート番号のチャックと情報の更新

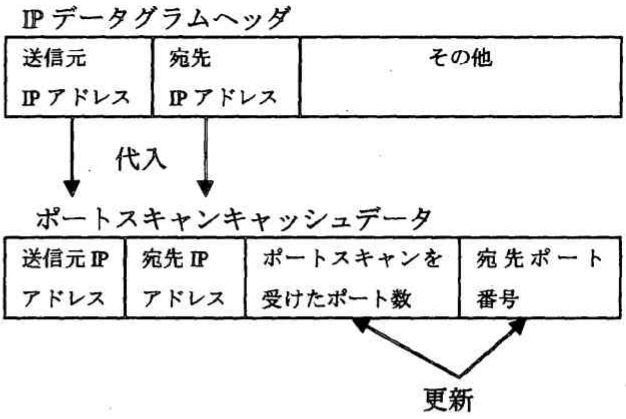

図 7　IP アドレスとポート番号の情報の更新

IP アドレスの組み合わせが同じでない場合，図 7 のように，IP データグラムの送信元 IP アドレスと宛先 IP アドレスの組み合わせをポートスキャンキャッシュデータに格納する．また，TCP セグメントの宛先ポート番号(th_dport)の情報よりポートスキャンキャッシュデータのポートがアクセスされたどうかの情報（dstport）とアクセス数の情報を更新する．その後，regtime 関数と print_scan 関数を呼び出

す．実際に用意したポートスキャン用データ構造体 portscan は以下に示すものである．

```
struct{
  unsigned long int ipaddr ; //送信元 IP アドレス
  unsigned long int ipdest ; //宛先 IP アドレス
  int nmbrport ; //ポートスキャンを受けたポートの種類の数
  int port[MAXPORT] ; //宛先ポート番号
  char pro[MAXPORT][5] ; //TCP か UDP
  char flag[MAXPORT][5] ; //flag は何か
  int time[MAXPORT][3] ; //ポートがスキャンされた時刻
} portscan[MAXENTRY] ;//MAXENTRY 個の要素数からなる配列
```

4. ポートスキャン検出実験結果

この実験の目的は，一般的な常時接続環境にあるコンピュータが侵入などのセキュリティ面から見て，一体どのような状況にあるのかを調べることである．

実験は，本システムを常時接続環境にあるコンピュータ(直接接続されたコンピュータ)で長期的に稼動させ，その結果から常時接続環境で使用されるコンピュータのおかれる状況を見るものである。

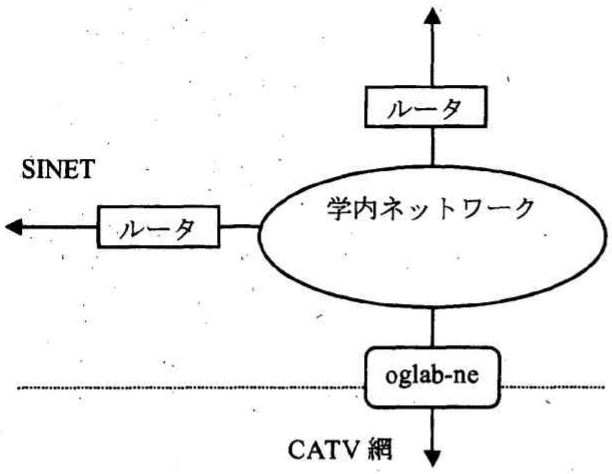

図 8　oglab-net ネットワーク接続図

4.1 oglab-net の実験環境

本研究室のプロキシサーバとし利用されている oglab-net でシステムを稼動させた．図 8 に oglab-net のネットワーク接続図を示す．oglab-net は学外に直接接続されているマシンなので，ポートスキャンを受ける可能性がある．本研究室の HTTP プロキシサーバ)である．このプロキシサーバ(oglab-net)においてポートスキャンの検出を試みた．

4.2 ポートスキャン検出実験の結果

10 月 1 日から 11 月 30 日までの実験結果を表 1 に示す．表 1 は，10 月，11 月のウェルノウンポートの対するアクセス数が多いものを表している．

1 日あたりに数件のポートスキャンとみられるアクセスがあった．ftp(21)に対しては 1 日に 1 から 10 件ほどのアクセスがあり，平均して 1 日あたり 3.7 件のアクセスがあった．ftp はネットワークを利用してファイルの転送を行うプロトコルである．smtp(25)に対しては、最大 33 件のアクセスがあった。1 日あたりでは 2 件ほどになっている．smtp はメールをやり取りするためのプロトコルである。サーバとサーバの間、クライアントからサーバへのメールの転送に使用される．http(80)に対しては多い場合には 1 日に 12 件のアクセスがみられた．平均して 1 日あたり 2 件ほどのアクセスがあった．http は web サーバとクライアントのデータの転送に使用されるプロトコルである．rtsp(554)に対しては 1 日あたり 2.5 件ほどのアクセスがあった．これは，動画などがストリーミング配信されることが多くなったことにより，rtsp(554)の利用が高まったためと思われる．

これらの他にも https，ssh ポートなどに対しても数件のアクセスがみられた．これらのアクセスが全て悪意をもったものであるとは断定できないが，これらウェルノウンポートに対してアセセスしてくることは正常なアクセスとは言いがたい．また，139 番ポートの Windows のファイル共有，プリンタ共有などに使うポートにアクセスがみられた．多い場合では，図 9 のように，11 月 11 日に最大で 150 件を越えるアクセスがある日もあった．この日の前後は目立って 139 番ポートに対するアクセスが増加している．これは，日本時間の 11 月 12 日に Microsoft によって公開されたセキュリティホール（Workstation サービスのバッファ オーバーランにより、コードが実行される (828749) (MS03-049)）[4] を狙ったものと考えられる．他のポートに対するアクセスと比べて明らかに目立って数が多くい．これらのアクセスには Windows ユーザが知らずに(悪意なく)送信してしまったものも含まれていると考えられるが，これらの中には悪意をもったものも存在すると考えられる．このポートを使用してトロイの木馬型ウイルスを仕掛けられる事例も多くある．139 番ポートは，NetBIOS を利用したファイル・プリンタ共有のために使用される[5]．

この結果は，いわゆる一般的な常時接続環境にあるコンピュータはポートスキャン，それに続く攻撃の脅威にさらされていることを示していると思われ

る．

表1　各ポートのアクセス数

ポートスキャンを受けた後，oglab-netに対して攻撃が加えられてはいない．これはoglab-netが不要なポートは開いておらず，セキュリティのパッチの適用などの管理がなされているからと考えられる．もし，セキュリティ対策をとっていないサーバであった場合は，すでに，攻撃がなされていたのではないかと考える．

	21	25	80	139	554	その他	合計
10月	92	52	48	155	9	85	441
11月	137	59	77	481	149	138	1041
合計	229	111	125	636	158	223	1482

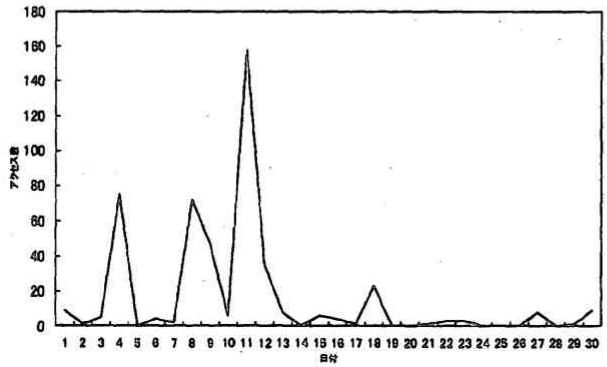

図9　11月の139番ポートへのアクセス数の変化

5. 考　察

今回の実験結果からも，明らかにポートスキャンであると見てとれるアクセスがあった．oglab-netは福井大学の一研究室のプロキシサーバであるが，最近一般家庭でも増加しているADSLやケーブルテレビでの常時接続環境と同じ環境にあると言える．これは，爆発的に広がっているコンピュータネットワークにおいてポートスキャンが日常的に行なわれている行為であるといえる．また，ポート毎のアクセス数の増加を見ても，新たにセキュリティホールが公開，発見された時期には，そのセキュリティホールを狙ったと思われるアクセスが増加している．この結果から，使用しているコンピュータについての情報やセキュリティに関する一般的な情報(ワーム，ウイルスなど)について常に注意を払っておく必要がると考える．そして，使用しているコンピュータがどういったネットワーク状況下におかれているかも把握しておく必要があると考える．これらの情報を把握しておくことで新たなセキュリティ情報にいち早く対処できると考える．139番ポートに関するセキュリティホールの場合も，対策として必要となるのはセキュリティパッチを適用するだけの作業である．しかし，セキュリティ情報への注意や作業を怠ったがためにデータが漏洩し，トロイの木馬などを仕掛けられてしまうこともある．また，oglab-netに限らず，インターネットに接続されたマシンはこのポートスキャンをいつ受けてもおかしくない状況にある．それは，管理下のマシンがLANなどのネットワークにおいて奥深いところに設置されていたとしても同じであると考える．そして，それらのマシンはポートスキャンのみならずその先に，侵入者による，トロイの木馬をしかける，DoS攻撃，バックドアをしかけるなどの行為によってデータの改竄，消去，漏洩，マシン停止といった実害がある．これらのような侵入者による実害のある行為がなされる前兆であるとポートスキャンを取らえると，プロキシサーバ上でポートスキャン検出プログラムを実行することは，侵入行為の検出の第1段階に値すると考える．

参考文献

[1]小高 知宏：基礎からわかる TCP/IP アナライザ作成とパケット解析 Linux/FreeBSD対応，オーム社，273（2001）．
[2] 山口 英　鈴木 裕信：bit別冊 情報セキュリティ，共立出版，2000年1月号別冊，352（2000）．
[3] 小高 知宏：TCP/IPで学ぶ コンピュータネットワークの基礎，森北出版株式会社，135（1996）．
[4]http://www.microsoft.com/japan/technet/security/bulletin/fq03-049.asp
[5] 久米原 栄：TCP/IP セキュリティ，ソフトバンクパブリッシング株式会社，501（2000）．