2008－IOT－2 (2)
2008／7／24

# 長期的スキャニングを対象とした スキャン攻撃検知システムの評価

兒玉 清幸[†1] 藤原 健志[†2] 大塚 賢治[†1] 吉田 和幸[‡]
†1大分大学大学院工学研究科 †2大分大学工学部 ‡大分大学学術情報拠点情報基盤センター

**あらまし** 近年，インターネットの普及に伴い，ネットワークを通して様々な情報のやり取りが行われている．管理者は管理対象となるネットワークを常に安全に保つためにトラフィックやパケットの監視を行う必要がある．しかしながら，帯域幅を小さく絞った不正アクセスは，通常の通信パケットの中に埋もれてしまい，その検出は容易なことではない．そこで，我々はこのような長期的スキャニングを検知することを目的としてシステムの開発を行ってきた．本論文では，開発したシステムの長期的スキャニング検出能力について評価する．

# Evaluation of Scan Attack Detection System for Long-term Scanning

Kiyoyuki Kodama[†] Takeshi Fujiwara[†] Kenji Otsuka[†] and Kazuyuki Yoshida[‡]
†Department of Compute Science and Intelligent Systems, Oita University
‡Center for Science Information and Library Services, Oita University

**Abstract** Recently, as the Internet spreads, various information is exchanged through the Internet. To keep network safely and securely, network administrators should monitor traffic and the packet. However, it's not easy to detect illegal accesses with small bandwidth. We are developing Attack Detection System for Long-term Scanning. In this paper, we evaluate the system to detect Long-term Scanning.

## 1. はじめに

### 1.1 研究背景

近年，インターネットの普及に伴い，ネットワークを通して様々な情報のやり取りが行われている．一方で，ネットワークを利用した不正通信も多く存在する．それは，あるシステムの脆弱性を突くものであったり，ネットワークやホストの存在を探索（スキャン）するものであったりと様々である．これらの脅威はインターネットが正常に利用されることを前提とした設計思想がもたらしたものであり，その不正通信への対処は，各ホストの管理者や各ネットワークの管理者に委ねられている．ゆえに，ネットワーク管理者は安全性の高いネットワークを実現するために，ファイアウォール，侵入検知システム(IDS)やトラフィックの監視ツールを導入することが必要とされる．

しかし，帯域をしぼってやってくる不正通信が正常な通信の中に埋もれてしまい発見が困難となることがある．

### 1.2 研究目的

我々はスキャニングの疑いのある通信をグラフ化し，ネットワーク管理者に攻撃の状況を提示するシステムの開発を行ってきた[1]．本システムは，上述した正常な通信の中に埋もれてしまう“長期的・低帯域のスキャン”を検出し，ネットワーク管理者にその兆候を提

示することを目的としている．

本稿では，スキャン攻撃検知システムが用いている“長期的・低帯域のスキャン”の検出アルゴリズムの有功性を検証し評価する．

## 2. スキャン攻撃

### 2.1 スキャン攻撃とは

本研究で検知対象としているスキャン攻撃とは，攻撃者がターゲットのネットワークの各 IP アドレスに対して特定のサービス要求を行なったり，特定のホストに対して様々なサービスを要求したりすることである．これを行うことで，攻撃者はターゲットのネットワークにおけるホストの有無や各ホストで動作しているサービス，ＯＳの種類やバージョンなどを特定できる．これらの情報は，DoS(Denial of Services)攻撃やバックドアを仕掛ける際に利用される．

### 2.2 特徴による分類

本稿では，スキャン攻撃をトラフィック量という観点から以下の２つに分類する．

- **短期的スキャン攻撃**
  使用可能な帯域をすべて使って短時間にスキャンを行う．
- **長期的スキャン攻撃**
  帯域幅を絞って長時間に亘りスキャンする．

短期的スキャン攻撃は，大量のトラフィックを発生させるので，トラフィック量に閾値を設けた監視プログラムなどで検知することが可能である．しかし，長期的スキャン攻撃の場合は同種の検知手法を適用することが難しい．攻撃により発生するトラフィックが少量のため，閾値を高く設定した場合は検知することができない（False Negative）．また，閾値を低く設定した場合は正常な通信が不正と判断される“誤検知（False Positive）”が発生する．つまり，トラフィックに閾値を用いる手法では長期的スキャン攻撃と正常な通信との区別することができない．

本システムでは，長期的スキャン攻撃を検知対象としている．本格的な攻撃を受ける前に，管理者が特定のポートを閉じる，特定の IP アドレスからの通信を遮断するなどの対策を打つことができれば，ネットワークを管理運用する上で有益であると考えられる．

### 2.3 スキャンツール

現在，様々なスキャンツールがインターネット上や書籍などで公開されている[3]．以下に幾つか例を示す．

- fping[3]
  WindowsNT または UNIX で動作する Ping スイープツール．通常の Ping より高速かつ効率よく動作するため大量の IP アドレスを調べることが可能である．gping[3]を利用してアドレスリストを作成できる．
- nmap[3]
  強力なポートスキャナであり，ステルススキャン，広域スキャン，フィンガープリンティングと呼ばれる OS を推測する機能などを有する．この GUI 版として NMapWin[3]も存在する．

このように，インターネットが普及した現在では誰でも容易にスキャンツールを入手できる環境にあり，バックドアや DoS 攻撃などの生成ツールも多く公開されている．ゆえに,それらを使ってネットワークを通してハッキングを仕掛けてくるケースも少なくない．先ほど述べたように，攻撃者はターゲットを攻撃する際に，その前段階でスキャン攻撃を行うことが多く，そのスキャン攻撃の段階でそれらを特定し，特定の IP アドレスやサービスをブロックできればメリットが大きい．

## 3. 長期的スキャン攻撃検知システム

### 3.1 システムの概要

本システムは外部ネットワークから行われるスキャ

ン攻撃の検知を目的とする．本システムで対象とするスキャン攻撃は低帯域で長時間に渡って行われる長期的スキャン攻撃である．本システムの構成図を以下に示す．

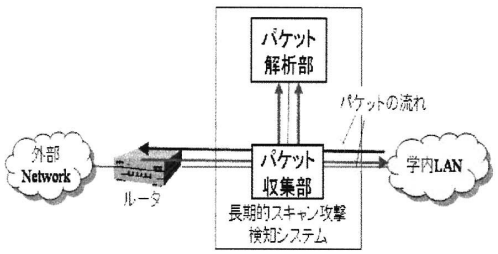


**図 1　スキャン攻撃検知システムの概念図**

### 3.1.1　パケット収集部

対象ネットワークを流れるトラフィックを収集し，パケット解析部へと送るために．従来のシステムでは，LANスイッチのsflow機能を用いていた[1][2]．今回は，LAN スイッチのポートミラーリングを用いてパケットを収集した．

### 3.1.2 パケット解析部

パケット解析部は，パケット収集部から渡されたデータのヘッダから以下の４つのデータを抽出し，長期的スキャン攻撃の疑いがあるかどうか判定を行う．

- ソース IP アドレス
- ソースポート番号
- 宛先 IP アドレス
- 宛先ポート番号

上記の情報を元に，ネットワーク管理者に長期的スキャン攻撃の可能性を提示する．

### 3.2 長期的スキャン攻撃の検知手法

2.2 節で述べたように，長期的スキャン攻撃は低帯域幅で長期間に亘るトラフィックが発生するという特徴がある．そこで，本システムではスキャン攻撃を区別するために，時間区間ごとにソース IP アドレスの出現の有無をスキャン攻撃の評価基準として利用する．

時間区間ごとのソース IP アドレスの有無をある期間に亘って集計することで，スキャン攻撃の判定を行う．このようにすることで，対象区間で同一ホストが大量のトラフィックを発生させた場合も，区間内では，１としてカウントされる．概念図を以下に示す．これによりトラフィック量自体を集計することに比べて記憶量を大幅に圧縮することが可能になり，長期間の集計が可能となる．

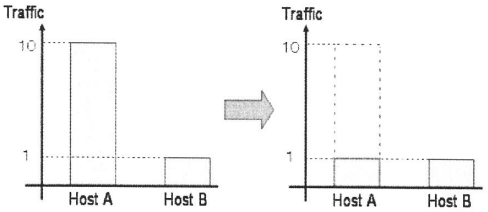


**図 2 区間ごとの出現のカウントの概念図**

区間ごとにカウントしたトラフィックを一定期間集計し，ホストごとに合計値を計算する．集計期間内で長期間に亘って出現するホストほど合計値が大きくなり，短時間で通信が終了するホストほど合計値が小さくなる．本検出アルゴリズムでは，集計期間内のホストごとの出現数を長期的スキャン攻撃の指標としている．つまり，出現頻度が高いホストほど，長期的スキャン攻撃の疑いが強いと判定する．

## 4. 検証実験

### 4.1 課題設定

本システムにおける長期的スキャン攻撃の検知手法に関する検証実験を行う．検証項目は以下の２項目である．

- 区間ごとの出現の数による攻撃分類効果
- 長期的スキャン攻撃の検知能力

なお，検証データは2008年5月28日に発生した全インバウンドトラフィックを用いた．

### 4.2 区間ごとの出現の数による攻撃分類効果

区間を設けてホストの出現の数を集計することにより，長期的スキャン攻撃の疑いがあるホストと短期的スキャン攻撃の疑いがあるホストを分類することができるかを検証した．

検証のために，検証データより以下の２つのファイルを作成した．

**ファイルA：**

検証データからホスト毎のトラフィック量を集計する．そのトラフィック総量の降順に順位付けを行っている．

**ファイルB：**

2008年5月28日の検証データに15分区間ごとでの出現の有無を集計する．その結果からホスト毎の出現回数の降順に順位付けを行っている．

上の２つのファイル間に存在するホストの関係に着目する．つまり，ファイルAで上位に順位付けされているホストがファイルBでは下位に順序付けられていることを確認する．以下に結果を示す．

**表 1 ファイルA中のホストの順位比較**

| | ファイルA 順位 | ファイルB 順位 |
|---|---|---|
| 221.186.113.140 | 1 | 1 |
| 203.209.145.186 | 2 | 27,722 |
| 133.243.232.68 | 3 | 4,728 |

（全ホスト数 : 286,832）

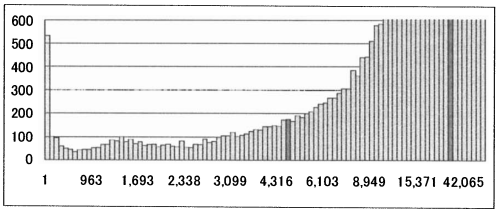


**図 3 ファイルB中の全体に占める位置**

表１より，ファイルA中で上位に順位付けされているホストがファイルB中では下位に順位付けされていることがわかる．なお，221.186.113.140は大量のトラフィックを24時間以上にわたり発生させていたため，両ファイル中で1位となっている．203.209.145.186と133.243.232.68が属する順位を図2中の赤色の要素で示す．

同様にファイルB中で上位に順位付けされているホストが，ファイルAでは下位に順序付けられていることを確認する．以下に結果を示す．

**表 2 ファイルB中のホストの順位比較**

| | ファイルA 順位 | ファイルB 順位 |
|---|---|---|
| 221.186.113.140 | 1 | 1 |
| 89.140.26.132 | 23,601 | 1 |
| 88.198.20.89 | 4,060 | 1 |

（全ホスト数 : 286,832）

表２より，ファイルB中で上位に順位付けされているホストがファイルA中では下位に順位付けされていることがわかる．これらのホストに対してDNSサーバに問い合わせを行い，ドメイン名を取得した．結果を以下に示す．

**表 3 IPアドレスとドメイン名の対応**

| IPアドレス | ドメイン名 |
|---|---|
| 221.186.113.140 | sv3.diskworks.co.jp |
| 89.140.26.132 | 89.140.26.132.static.user.ono.com |
| 88.198.20.89 | idoru.pl |

検証実験から区間ごとの出現の有無の集計を用いることにより，トラフィック総量が少ないが，長期間に亘って通信を行っているホストを上位に順位付けすることが可能であることがわかった．これにより，長期的スキャンの疑いがあるホストを検出可能といえる．

## 4.3 長期的スキャン攻撃の検知能力

### 4.3.1 パラメータの設定

本手法は以下のパラメータを設定する必要がある．

- 出現の有無を調べる時間区間
- 長期的スキャニングと判断する期間

検証実験では，時間区間を 10 分間，長期的と判断する時間区間を"12 時間"と設定した．10 分区間ごとの出現の有無を，12 時間に亘って集計し，その量が上位のものを“長期的スキャン攻撃の疑いが梅強いホスト”とする．

### 4.3.2 検証実験

2008 年 5 月 28 日の 0:00-12:00 までに発生した全インバウンドトラフィックに対して，本検知手法を適用した．その結果，386 個のホストが scan 攻撃の疑いのあるホストとして検知された．これらのホストに対して，トラフィック総量を求め解析した．結果を以下に示す (図 4，表 4)．なお，ヒストグラムに関しては，トラフィック量が 90,000 未満の要素のみを表示している．

**表 4 トラフィック総量による比較**

| | |
|---|---|
| 最大トラフィック総量 | 3,482,617 |
| 最小トラフィック総量 | 291 |
| 中央値 | 5,318 |

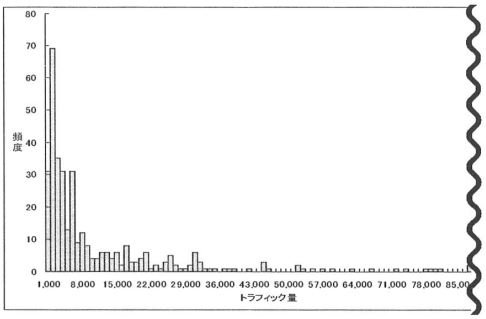


**図 4 検証結果を用いたヒストグラム**

図４と表４より，検出されたホストのトラフィック総量には偏りがあることがわかる．作成したヒストグラムを基に解析を行なった結果，トラフィック総量が 30,000 以下のホストが全体の 80%以上を占めていることがわかった．このトラフィック総量をモデルとして帯域幅を計算する．計算過程を以下に示す．

【仮定】:

・トラフィック全てが 62Byte(496bit)の SYN パケット

・回線利用率は 100%，通信障害などは発生しない

【帯域幅 X】:

$X = 496\text{bit} \times 30{,}000 \div (60 \times 60 \times 12))$

$= 14{,}880{,}000 \div 43{,}200 \fallingdotseq$ **344.4 bits / second**

上記の結果より，本手法では非常に低帯域の通信を検出可能であることがわかる．

### 4.3.3 検知例

本手法を適用して検知された長期的スキャン攻撃の検知例を図 5 に示す．

ホスト 89.140.26.132 は，学内の不特定多数のホストに対して 1,433 番ポート (MS-SQL) に対する要求を行なっていた．また，1 分間で平均 1.12 トラフィックという非常に低帯域な通信を行なっていることから，長期的スキャン攻撃の特徴が見て取れる．

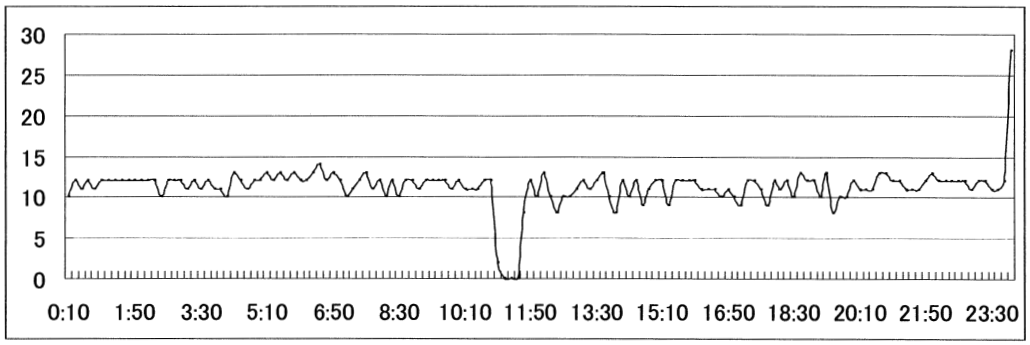


**図 5 ホスト“89.140.26.132”が発生させるトラフィック量の推移**

## 5. おわりに

### 5.1 まとめ

本稿では，我々が開発した長期的スキャン攻撃検知システムが用いている検知手法の有功性を検証し評価した．検証実験により，非常に低帯域のトラフィックを発生させるホストを検知することが可能であることがわかった．また，検知されたホスト群の中から実際に長期的スキャン攻撃を行なっているホストを確認することができた．これにより，本手法は長期的スキャン攻撃を検出する能力を有していると評価できる．

### 5.2 今後の課題

現行システムでは，長期的スキャン攻撃の疑いのあるホストの検出のみを行なっており，スキャン攻撃としての判断は管理者に依存している．今後は，この判断をシステムで自動化し，管理者への通知や通信の遮断などの“攻撃への対策”について検討していく．

## 参 考 文 献

[1] 三鑰達真，吉田和幸，“長期スキャンニングを対象としたスキャン攻撃検知システム”，インターネットアーキテクチャ研究会，電子情報通信学会，信学技報 Vol.107 No.449,pp.39-44，Jan.2008.

[2] AlaxalA Networks Corporation，“AX6700S AX6300S ソフトウェアマニュアル”，http://www.alaxala.com/jp/support/manuals/AX6300S/AX6300s_V10-6.zip

[3] IPUSIRON，ハッカーの教科書 完全版，矢崎雅之，株式会社データハウス，東京，2005.

[4] RRDtool : http://poplr.ee.ethz.ch/~oetiker/webtools/rrdtool

[5] RRDtool の利用 http://www.stackasterisk.jp/tech/systemManagement/snmp04_01.jsp