scan 攻撃の検知とその遮断について

有馬竜昭† 熊谷悠平††
永山聖希† 吉田和幸†††

scan 攻撃とは，攻撃者が攻撃対象ネットワーク内の情報（存在するホストやサービスなど）を収集する行為である．攻撃者は scan 攻撃により得た情報から，“パスワードクラッキング”などの具体的な破壊行為を実行するかもしれない．そのため，scan 攻撃は“事前攻撃”と捉えることができる．この事前攻撃の徴候を早期発見することで，対策を講じることが可能になる．
本研究室では，“scan 攻撃”の徴候を発見し，管理者を支援するシステムの開発を行ってきた．本論文では，本研究室が開発した scan 攻撃検知システムにより攻撃者の検知を行い，経路制御を用いた scan 攻撃の遮断と LAN スイッチの ACL を用いた scan 攻撃の遮断について述べる．

Detection and interception of scan attack

TATSUAKI ARIMA† YUHEI KUMAGAI††
TOSHIKI NAGAYAMA† KAZUYUKI YOSHIDA†††

Scan attack is what attacker collects information (existence of host, service, etc.) in the network. Attacker may execute actual ravage such as password cracking after the scan attack. Therefore, the scan attack can be treated as "Prior attack". If prior attack can be detected in early stage, we can take measures.

We are developing system that supports discovery of symptom of scan attack for network administrator. In this paper, we describe interception of scan attack by using routing and interception of scan attack by using LAN switch’s ACL after detection system detect scan attack.

1. はじめに

1.1 研究背景

インターネットの普及に伴い，ネットワークを通して WEB ページの閲覧や電子メールなどのコミュニケーションツール，インターネット上での電子決算などの様々な情報がやり取りされるようになってきた．

このように多くの情報を扱う一方で，ネットワークを利用した不正行為も多く存在する．例えば，システムの脆弱性を突くものや，ネットワークやホストの存在等を探索するものと様々である．これらの脅威への対処はネットワークの管理者が行うものであり，安全性の高いネットワークを維持するために，ファイアウォール，侵入検知システム(IDS)の導入などの対策を行っている．

このように，ネットワークを用いた不正行為への対策などの導入により，ネットワーク管理者への負担が増すと考えられる．

1.2 研究目的

我々は，攻撃者が攻撃対象であるネットワーク内の情報（ホストやサービスなどの存在確認）の収集を目的とした scan 攻撃と呼ばれる攻撃の検知を行う．攻撃者は scan 攻撃を行った後に，パスワードクラッキングなどの攻撃を行うであろう．このことから，scan 攻撃は攻撃の前に行う攻撃であり，scan 攻撃の徴候を早期発見することができれば，scan 攻撃後の攻撃に対する対策を講じることが可能である．

我々は，scan 攻撃の徴候を発見することで管理者への支援を行うシステムの開発を行ってきた[1].

本論文では，2 章で scan 攻撃検知システムについて述べ，3 章で経路制御を用いた攻撃の遮断と LAN スイッチの ACL を用いた攻撃の遮断の 2 種類の遮断について比較，考察を行う．4 章ではまとめと今後の課題について述べる．

†大分大学大学院工学研究科知能情報システム工学専攻
Department of Computer Science and Intelligent Systems, Oita University
††大分大学工学部（現在，広島大学大学院総合科学研究科）
Department of Computer Science and Intelligent Systems, Oita University
(Now he is at Graduate School of Integrated Arts and Science, Hiroshima University)
†††大分大学学術情報拠点情報基盤センター
Center for Academic Information and Library Services, Oita University

2. scan 攻撃検知システム

2.1 システム構成

本システムを防御対象ネットワークの境界に設置することで，ネットワーク全体のトラフィックを監視し，scan 攻撃を検知することが可能となる(図 2.1)．本システムはファイアウォールの外側にある LAN スイッチでポートミラーリングを行うことでパケットを取得し，ファイアウォールの外側にあるため，ファイアウォールで遮断しているポートなどへの scan 攻撃などを検知することが可能になる．また，実験用ネットワークを準備し，内部ネットワークと実験用ネットワークとの間にある LAN スイッチに対し遮断命令を出すことで，検知した scan 攻撃を遮断する．遮断に関して，２つの手法を用いて遮断を行う．経路表を用いた scan 攻撃の遮断については，学内ネットワーク全体を保護対象としており，ACL を用いた遮断については，実験用ネットワークを保護対象としている．２つの手法を用いた遮断について，第 3 章で説明する．

本システムは『収集部』『解析部』『代理部』『更新・表示部』という 4 つのサブシステムで構成されている(図 2.2)．

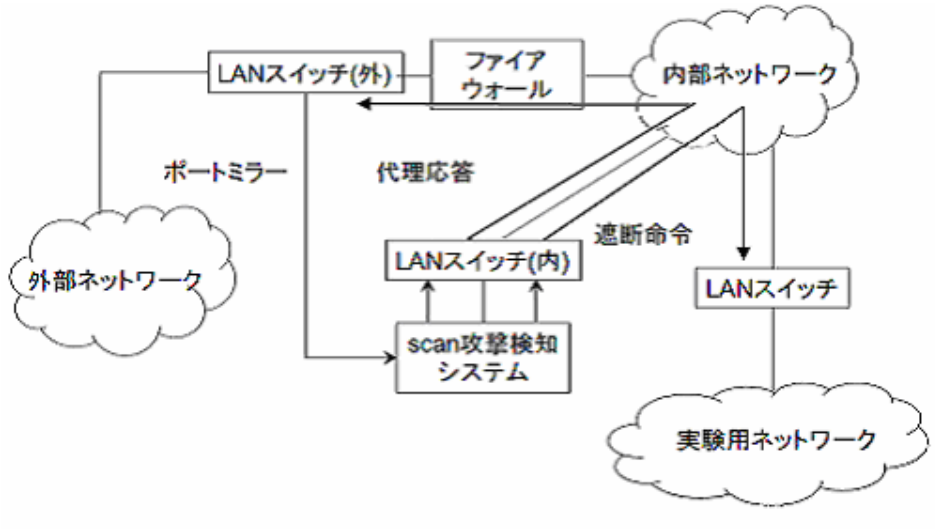

図 2. 1 scan 攻撃検知システム概要図

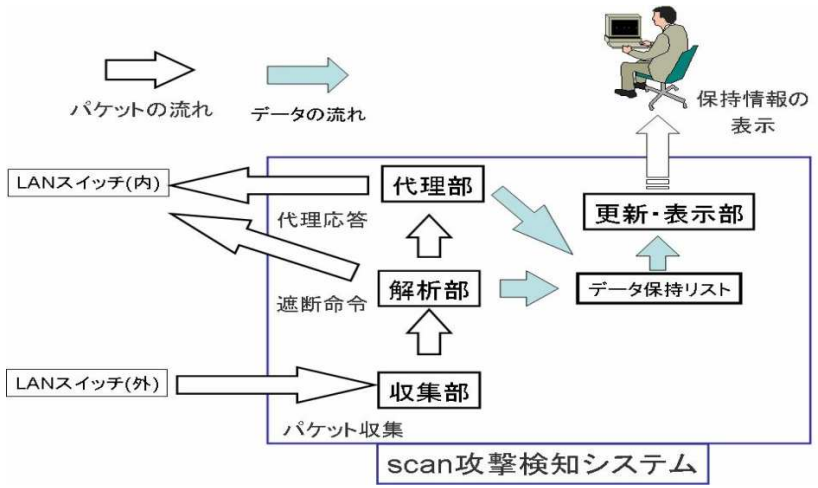

図 2. 2 scan 攻撃検知システム内部構成

以下では，それぞれの構成部分についての説明を行う．

- **収集部**

収集部では対象ネットワークを流れるトラフィックを収集し，解析部へと送る．現在のシステムでは，LAN スイッチのポートミラーリングを用いて対象ネットワークのパケットを収集している．

- **解析部**

解析部では収集部から渡されたパケットのヘッダ情報から以下の 5 つのデータを抽出し，scan 攻撃かの判定を行う．

- 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
- TCP フラグ

代理応答を行う必要のあるパケットを発見した場合，そのパケットの情報を代理部に送る．scan 攻撃の判定方法は 2.2 節で説明する．

また，一定時間以内に同じ IP アドレスから一定回数以上の SYN パケットが送信されると，実験用に準備された LAN スイッチに対して遮断命令を送信する．

- **代理部**

代理部では解析部から渡されたデータより代理応答パケットの送信判定を行い，代

理応答パケットを送信する必要がある場合に送信する．

- **更新・表示部**

更新・表示部では解析部によって scan 攻撃を行っていると判定されたホストに関する情報を管理者に提示する．提示する情報は，送信元ホストが攻撃者である『攻撃者リスト』と検知基準には達していないがコネクションの状態が異常なもの，または未使用の IP アドレスやポートにアクセスしてきた『未解決リスト』の 2 つである．二つのリストの提示方法は以下の図のようになっている(図 2.3)．また，保持している情報を確認し，必要であれば保持している情報の削除や攻撃者の判定を行う．

```
123.211.159.222 type: 1 Tue Dec 22 17:29:37 2009
54608 -> 133.37.96.54 26804 state:8 EXIST Tue Dec 22 17:29:37 2009
53013 -> 133.37.96.54 26804 state:8 EXIST Tue Dec 22 17:28:21 2009
50319 -> 133.37.96.54 26804 state:8 EXIST Tue Dec 22 17:21:12 2009
```

図 2.3 実際のログ（一部）

ログの見方を図 2.4 に示す．1 行目に送信元 IP アドレスと攻撃者が行った攻撃，検知時刻が来る．2 行目以降には送信元ポート番号，宛先 IP アドレス・ポート番号接続の状態，接続時刻の順になっている．攻撃のタイプを図 2.5，接続の状態を図 2.6 に示す．

送信元 IP アドレス	攻撃のタイプ		検知時刻	
送信元ポート番号	宛先 IP アドレス	宛先ポート番号	接続状態	接続時刻

図 2.4 ログの表記例

type:1	代理応答による確認
type:2	接続状態が未解決
type:3	短期集中的なscan攻撃

図 2.5 攻撃のタイプ分類

SYNSENT	内部からSYN送信
REV_SYN	外部からSYN送信
EST	接続確立
DELWAIT	接続終了
UNSOLVED	接続未解決状態
RSTSCAN	代理応答にRST返信
EXIST	代理応答に応答あり
ABSENT	代理応答に応答なし

図 2.6 接続状態

2.2 scan 攻撃検知手法

本システムで使用している scan 攻撃の検知手法について説明する．本システムでは，検知した条件により攻撃を 3 つに分類し，管理者攻撃者の情報を提示する．以下それぞれの説明を行う．

2.2.1 代理応答に対する応答の送信回数

本システムは，代理応答を用いることで宛先の存在しないホストへ SYN フラグが 1 のパケットを送信してきた送信元の存在確認を行う[4]．また，代理応答を行う際の宛先 IP アドレスは未使用の IP アドレスまたはポートである．そのため，代理応答に対し，応答である ACK フラグが 1 のパケットを送信してきた場合，その送信元が scan 攻撃を行っていると判断できる．応答がないまたは RST フラグが 1 のパケットを送信してきた際には，送信元の偽装を疑うことができる．

2.2.2 TCP コネクションの未解決状態数

一般ユーザが外部へ公開しているサーバ以外に対してアクセスすることはほとんどない．また，scan 攻撃を行っていると考えられる攻撃者は，サーバの使用状況などを探るためにパケットを送信しているため，パケットの送信回数と比較してコネクションの確立数は少なくなる．このことから，本システムではコネクションの確立ができなかった回数を計数することで scan 攻撃を検知する．実際には，システムに登録のない状態で SYN フラグが 1 のパケットが到着した場合，コネクションの状態を接続確認状態とし，システムに登録する(表 2.1)．それ以外であればコネクション状態を未解決状態とした後，登録する．その後は，システムに登録されているコネクションの状態と到着したパケットの TCP フラグオプションを元に，コネクション状態を変更していく．

表 2.1 コネクション状態の遷移

		コネクション状態				
		登録なし	接続確認	接続確立	終了	未解決
フラグオプション	SYN	接続確認				
	FIN	未解決	未解決	終了		
	RST	未解決	未解決	終了		
	ACK	未解決	接続確立			

＊斜線部は状態が変化しないことを示す

表 2.1 では上の行に存在する TCP フラグオプションの優先度が高く設定されている．また，斜線部分はなにも行わない設定になっている．そのため，SYN/ACK パケットのように複数のフラグオプションが 1 となり送信されてきた場合，優先度の高い方のフラグオプションと同じ扱いを受け，接続確認状態であれば状態を変更せず次に ACK パケットが来ることを期待する．また，コネクション状態が接続確認状態で一定時間以上が経過した際には，未解決状態としてコネクションの状態を変更する．これは，学内から SYN/ACK パケットを送信した後，何もパケットが返されないことを想定している．

2.2.3 1 秒間のコネクション要求送信回数

短期間でのコネクション要求を大量送信してくる送信元は scan 攻撃や攻撃を行っている可能性が考えられる．これは，一般のユーザが一度に大量のコネクション要求を送信してくることは考えにくいためである．

この場合，送信元は DoS 攻撃によるサービス不能状態の期待や scan 攻撃による探索行動が考えられる．こうしたパケットの大量送信に関しては実際にその送信元がパケットを送信していない可能性があるが，実際に大量のパケットが送信されるという状況が発生している．そのため，遮断などの処置を行い余計なパケットを遮断することが必要となる．

3. ２つの手法による scan 攻撃の遮断

3.1 scan 攻撃遮断の概要

scan 攻撃の遮断に関して２つの遮断プログラムを実装した．一つは，経路表を用いた遮断プログラムで，もう一つは LAN スイッチの ACL を用いた遮断プログラムである．

本章では，それぞれのプログラムを動かし得られた結果より，２つの手法について比較，考察する．

今回遮断に用いた LAN スイッチは，Alaxala AX3640S-24T2XW を使用した[5].

3.2 経路表を用いた遮断

scan 攻撃は，接続要求である SYN パケットを攻撃対象に送信し，その SYN パケットに対する確認応答である ACK パケットにより，攻撃対象のネットワークの状況を知る．そのため，攻撃者に対して ACK パケットを返さないことで，攻撃者がネットワークの状況を知ることを防ぐことが可能である．

攻撃者宛のパケットを NULL インタフェースへ集めるように経路を設定し，それを用い学内に配送することで, scan 攻撃に対する LAN からの応答パケットを破棄し, scan 攻撃を防ぐ．

図 3.1 は遮断で使用した LAN スイッチでの静的経路の登録例である．検知システムが攻撃者を検知すると, telnet を用いて検知 IP アドレスを静的経路に next hop を NULL インタフェース（図 3.1 の null 0）として登録する．そうすることで，攻撃者宛のパケットは全て NULL インタフェースで破棄される．

```
#config
# ip route 192.0.2.30 255.255.255.255 null 0
# ip route 198.51.100.1 255.255.255.255.null 0
# ip route 203.0.113.3 255.255.255.255.null 0
# exit
```

図 3.1 静的経路への登録の例

3.3 LAN スイッチの ACL を用いた遮断

アクセスコントロールリスト(ACL)は，LAN スイッチのインタフェースに適用することにより，そのインタフェース上で特定のホストの通信を許可したり，拒否したりすることができる．通信アクセスの拒否，許可の基準として，特定の MAC アドレス，IP アドレス，またはポート番号をその対象にできる．scan 攻撃検知後，攻撃者の IP アドレスを ACL に登録することで，攻撃者の送信パケットを遮断する．

今回使用した LAN スイッチは実験ネットワーク(133.37.0.0/21，10 名程度の利用者のいるネットワーク)と学内 LAN 基幹スイッチとの間に設置してあるので，実験ネットワーク宛の scan 攻撃のみを遮断する．

検知システムから攻撃者の IP アドレスを受け取り，telnet を用いてスイッチの ACL に対して遮断する命令を送信することで攻撃者の登録が行われる．図 3.2 は遮断で使

用した LAN スイッチでの ACL の登録例である．適応インタフェースを設定し，ACL を生成した後に，遮断条件を登録する．ACL に登録可能な IP アドレス数は最大 255 件であり，255 件を超えたときに ACL の初期化を行い，256 件目の攻撃者の登録を続ける．

```
#config
# interface gigabitethernet 0/24
# ip access-list input test
# no ip access-list standard test
# ip access-list standard test
# 1024 permit any
# 1 deny host 192.0.2.30
# 2 deny host 198.51.100.1
# 3 deny host 203.0.113.3
# exit
```

図 3.2 ACL への遮断登録の例

3.4 遮断の検証

3.4.1 経路表を用いた遮断結果

経路表を用いた遮断による遮断パケットを確認するため，学内ネットワークから攻撃者宛の ACK パケットを集める．静的経路の next hop を NULL インタフェースではなく，ACK パケットを収集するための PC の IP アドレス(133.37.222.113)に指定することで，ACK パケット収集用の PC の tcpdump のログにより遮断パケットを確認する．

経路表を用いた scan 攻撃の遮断期間は，2011 年 5 月 10 日 16:40 から 2011 年 5 月 13 日 14:40 の約 3 日間である．

静的経路の登録を行った LAN スイッチから，登録された攻撃者の IP アドレスを取得した．（図 3.3）図 3.3 の①のアドレスと tcpdump のログから，攻撃者宛のパケットを取得した結果，収集用 PC の tcpdump のログから攻撃者宛の ACK パケットを確認した．（図 3.4）

経路表を用いた遮断に関して，3 日間の総攻撃検知数は 3544 であり，学内からの ACK パケットを遮断された攻撃者の IP アドレス数は 258 である．

```
ip route 27.50.134.133 255.255.255.255 133.37.222.113
ip route 27.118.11.12 255.255.255.255 133.37.222.113
ip route 27.118.12.46 255.255.255.255 133.37.222.113    ①
ip route 27.118.13.3 255.255.255.255 133.37.222.113
ip route 27.188.139.156 255.255.255.255 133.37.222.113
```

図 3.3 静的経路登録状況一部

```
08:44:01.768735 IP 133.37.216.6.443 > 27.118.12.46.4616: S 3227517272:3227517272 ack
08:44:04.591084 IP 133.37.216.6.443 > 27.118.12.46.4616: S 3227517272:3227517272 ack
08:44:05.654088 IP 133.37.216.6.443 > 27.118.12.46.4616: S 3227517272:3227517272 ack
```

図 3.4 27.118.12.46 への ACK 送信状況の一部

3.4.2 ACL を用いた遮断結果

ACL の遮断状況を出力したログから，パケットの遮断された攻撃者が存在するかを確認する．ACL を用いた scan 攻撃の遮断期間は，2011 年 5 月 6 日 19:00 から 2011 年 5 月 9 日 19:00 の 3 日間である．図 3.5 は，5 月 6 日の 19:00 から 22:14 の間適用していた ACL の遮断状況ログである．

```
Date 2011/05/06 22:14:56 JST
Using Port:0/24 in
Standard IP access-list:test
        deny host 76.21.105.248
            matched packets          :          0
        deny host 119.62.128.113
            matched packets          :          0
        deny host 125.88.105.43
            matched packets          :          1    ①
        deny host 113.161.71.62
            matched packets          :          0
        permit any
            matched packets          :     125446
        implicitly denied packets:          0
```

図 3.5 ACL の遮断状況ログの一部

図 3.5 の①から，IP アドレスが 50.62.12.185 の攻撃者のパケットが遮断されていることが分かる．

次に，学内ネットワークと外部ネットワークとの境界面にある LAN スイッチの tcpdump から得たログを解析し，遮断が確認された 50.62.12.185 の実験環境へのパケットの送信状況を見る（図 3.6）．図 3.6 の①から，ACL へ遮断登録している間に，実験環境である 133.37.0.0/21 へパケットが送信されていることが分かる．

```
20:20:13.014377 IP 125.88.105.43.59310 > 133.37.207.94.2200: S
20:25:04.368055 IP 125.88.105.43.51740 > 133.37.57.118.22: S
20:25:52.562964 IP 125.88.105.43.45565 > 133.37.208.131.2: S
20:38:32.958381 IP 125.88.105.43.54974 > 133.37.223.157.1: S
20:42:30.729666 IP 125.88.105.43.50829 > 133.37.4.36.22: S    ①
20:44:49.753382 IP 125.88.105.43.58135 > 133.37.98.208.2200: S
```

図 3.6 50.62.12.185 から実験環境への送信状況

ACL を用いた遮断に関して，約 3 日間の総攻撃検知数は 1896 であり，検知後に実験環境へ scan 攻撃を行った送信先 IP アドレスは 13 であった．

3.5 考察

経路表を用いた scan 攻撃の遮断について，総攻撃検知数 3544 の内，検知後に学内からの ACK パケットを遮断された攻撃者の IP アドレス数は 258 である．経路表を用いた遮断は，攻撃者への ACK パケットを遮断することから，攻撃者が SYN パケットを用いた scan 攻撃に対して有効である．

ACL を用いた scan 攻撃の遮断について，総攻撃検知数 1896 の内，検知後に実験ネットワークに対して攻撃を行った送信元 IP アドレス数は 13 であった．ACL は，遮断 IP アドレスを 255 件までしか登録できないことから，登録数が 255 件になる前に ACL の登録数を初期化し，新たに IP アドレスの登録を行う．このことから，ACL を初期化する直前に登録された攻撃者は，すぐに初期化されてしまい遮断時間が短い．

２つの手法を比較してみると，初めに攻撃者登録件数から，経路表を用いた場合 8000 件攻撃者を登録できるが，ACL は 255 件であることから遮断数に限りがある．また，ACL の初期化より，初期化前に登録された攻撃者のパケットは遮断時間が短いことから，遮断が不十分な場合があるかもしれない．

次に，手法による遮断方法の違いに関して比較すると，経路表を用いた遮断では，攻撃者への ACK パケットを遮断することから，攻撃者のパケットを学内に通してしまう．ACL を用いた遮断の場合，学内ネットワークと学外との境界 LAN スイッチで遮断を行うことで，攻撃者パケットを学内に入る前に遮断できる．このことから，経路表を用いた遮断に比べ ACL を用いた遮断の場合は，学内ネットワークに攻撃者パケットが通らないので，ネットワーク資源の浪費を抑えられる．

次に，遮断機器の設置場所を考えた場合，経路表を用いた遮断では，経路表を用いて学外へのパケットを遮断するので，設置場所の自由度が高い．一方，ACL を用いた遮断では，遮断する LAN スイッチをパケットが通過しなければ遮断できない．

表 3.7 2 つの遮断方法の比較表

	経路表による遮断	ACL による遮断
総攻撃検知数	3544	1896
遮断 IP アドレス数	258	13
攻撃者の最大登録件数	学内 LAN の OSPF では 8000 件扱える	255
遮断対象パケット	攻撃者宛の応答パケット	攻撃者の送信パケット
遮断機器の設置場所	遮断を行うネットワーク内	保護ネットワークと外部との境界

4. まとめと今後の課題

4.1 まとめ

２つの手法を用いて scan 攻撃の遮断を行い，２つの手法を比較し，考察した．

今回 ACL を用いた遮断に関して，研究室内の実験環境のみの遮断であった一方，経路表を用いた遮断では大学全体を対象とした．そのため ACL による遮断では，総攻撃検知数 1896 の中で遮断の確認された IP アドレス数は 13 となった．

経路表による遮断に関して，総攻撃検知数 3544 の中で学内からの ACK パケットを遮断された攻撃者の IP アドレス数は 258 であった．未使用 IP アドレスからは ACK パケットは送信されない，または遮断されたことによる攻撃の停止から，学内からの ACK パケットを遮断された攻撃者の IP アドレス数は 258 となったと考えられる．

4.2 今後の課題

(1) 誤検知した場合に備え，攻撃者の遮断継続時間の検討が必要である．また，遮断登録数による LAN スイッチへの負荷とのバランスも含めて遮断継続時間を考えなければならない．

(2) ACL を用いた遮断に関しては，学外との境界にある LAN スイッチを用いて遮断を行い，実験環境だけではなく学内全体に対する scan 攻撃を遮断したい．

参考文献

[1] 衣笠雄気，大塚賢治，兒玉清幸，吉田和幸，“TCP コネクション要求回数の計数による攻撃者の検知”，インターネットと運用技術(IOT2008)シンポジウム，pp.39-46，2008.
[2] 大塚賢治，藤原健志，吉田和幸，“TCP コネクション確立の偽装とその計数による scan 攻撃検知システムとその運用について”，マルチメディア，分散，協調とモバイル(DICOMO2009)シンポジウム，pp.1285-1290，2009.
[3] 永山聖希，大塚賢治，藤原健志，吉田和幸，“TCP コネクション確立とその計数による攻撃者検知について”，電気関係学会九州支部連合大会，（第 62 回連合大会），03-1P-03，2009.
[4] 永山聖希，大塚賢治，藤原健志，吉田和幸，“代理応答を用いた scan 攻撃検知システムの運用と短期 scan 攻撃の遮断について”，マルチメディア，分散，協調とモバイル(DICOMO2010)シンポジウム，pp.1136-1145，2010.
[5] アラクサラネットワークス株式会社，AX3600S 製品マニュアル，
http://www.alaxala.com/jp/techinfo/manual/index.html#AX3600S