scan 攻撃検知システムの誤検知の調査

有馬竜昭† 小埜勇貴†† 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検知された攻撃者について調査を行い，誤検知かどうかの検討結果を述べる．

Investigation of False Negative of Scan Attack Detection System

TATSUAKI ARIMA† YUKI ONO†† 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 against it.
We are developing system that supports discovery of symptom of scan attack for network administrator. In this paper, we investigate into attacker detected by using Scan Attack Detection System, and we describe result of an investigation whether false negative.

1. はじめに

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，インターネット上での電子決算など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．そのため，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．

我々は，scan 攻撃の徴候と思われる異常なパケット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]．攻撃の遮断を行う前に，現在の scan 攻撃検知システムの誤検知を調査する必要がある．

本論文では，2 章で関連研究について、3 章で scan 攻撃検知システムについて，4 章で検知システムの誤検知の調査について，5 章で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
††大分大学工学部知能情報システム工学科
Department of Computer Science and Intelligent Systems, Oita 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. 関連研究

フリーソフトの IDS(Intrusion Detection System)である snort[2]では、プリプロセッサにより scan 攻撃の検知を行っている．ステルススキャンと呼ばれる，ホストのログに残らない scan 攻撃の検知が可能である．しかし，scan 攻撃の判断基準が「単位時間当たりのコネクション要求回数のみ」であるため，Web クローラやプロキシを使用している場合，アクセス回数が閾値を超えてしまい誤検知が増えてしまうことや，攻撃者がパケットの送信間隔を大きくすることで容易に回避を行える．

また，Bro IDS[3]は，コネクションの状態を監視し，送信したパケットに対する応答がないものまたは拒否を行なったものを計数する．その計数値が閾値を超えた場合に scan 攻撃だと判断する．このため snort に比べて誤検知は少ない．しかし TCP half open 攻撃，smurf 攻撃等の送信元 IP アドレスを偽装する攻撃に対して偽装された送信元を攻撃者と誤検知する可能性がある．Bro IDS は IDP(Intrusion Detection and Prevention system)の機能も持っているおり，設定によりアクセスを禁止することもできる．

3. scan 攻撃検知システム

3.1 システム構成

本システムの構成を図 3.1 に示す．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する．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 攻撃の遮断が可能である．今回，誤検知の調査を目的とするため遮断を行わなかった．

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 3.2).

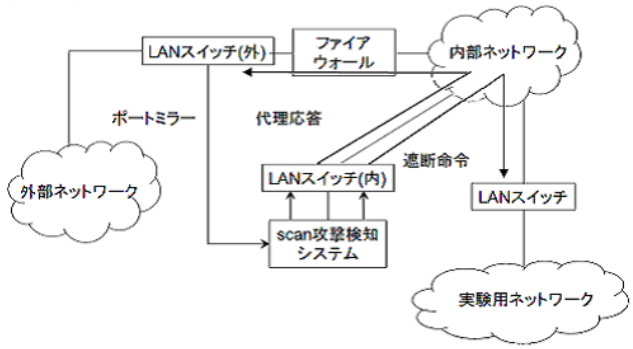

図 3.1 scan 攻撃検知システム構成図

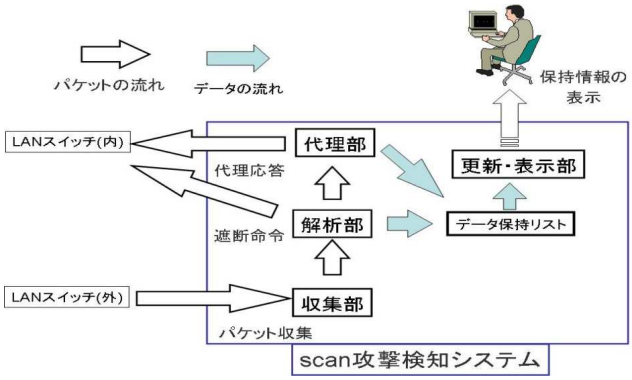

図 3.2 scan 攻撃検知システム内部構成

以下では，それぞれの構成部分について述べる．

- **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する．

- **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 3.2 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システムは保持しており，ログに出力することで管理者に攻撃者の情報を提示する．提示する情報を図 3.3 に示す．1 行目は攻撃者の IP アドレスや検知時刻等を示す．2 行目以降は，攻撃者と判定するのに用いたパケットの情報を示している．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 3.3 実際のログ（一部）

ログの見方を図 3.4 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．攻撃のタイプを表 3.1，接続状態を表 3.2 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 3.4 ログの表記例

表 3.1 攻撃のタイプ分類

タイプ	攻撃の検知タイプ
1	代理応答による確認
2	接続状態が未解決
3	短期集中的な scan 攻撃

表 3.2 接続状態

接続状態	状態の説明
SYNSENT	内部からの接続要求
REV_SYN	外部からの接続要求
SYN_RECV	接続要求の応答待ち
EST	接続確立
DELWAIT	接続終了
UNSOLVED	接続未解決状態
CAMOUFLAGE	代理応答による接続要求
RSTSCAN	代理応答に RST 返信
EXIST	代理応答に応答あり
ABSENT	代理応答の応答待ち

3.2 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．

3.2.1 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．

3.2.2 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、ファイアウォールにより止められるため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 3.3)．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 3.3 コネクション状態の遷移

コネクション状態(ホストあり)						
		登録なし	接続要求の応答待ち	接続確立	接続終了	接続未解決
フラグオプション	SYN	接続要求の応答待ち				
	FIN	接続未解決	接続未解決	接続終了		
	RST	接続未解決	接続未解決	接続終了		
	ACK	接続未解決	接続確立			
コネクション状態(ホストなし)						
		登録なし	代理応答の応答待ち	代理応答に RST 返信	代理応答に応答あり	
フラグオプション	SYN	代理応答の応答待ち				
	FIN	接続未解決	接続未解決		接続終了	
	RST	接続未解決	代理応答に RST 返信		接続終了	
	ACK	接続未解決	代理応答に応答あり			

※斜線部は状態が変化しないことを示す

表 3.3 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．

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．

コネクション状態が終了状態の場合，コネクション状態をリセットするために一定時間を経過すると登録なし状態に変更する．

3.2.3 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．

4. scan 攻撃検知システムの誤検知の調査

4.1 設置環境

システムの使用している PC の OS とハードウェア性能は以下のとおりである．

- OS ： Red Hat Enterprise Linux 5
- CPU ： Intel (R) XEON(TM) E5620
- メモリ ：2.4Gbyte

また，外部ネットワークからの通信が禁止されているポート番号を除外している．

除外ポート：80,135～139,445,443

これらのポートは主に LAN 内部で使用するポートであるため，LAN 外部からのすべてのアクセスをファイアウォールなどで除外することが推奨されている．また，HTTP・HTTPS サーバ以外への 80・443 ポートに対するアクセスは通常されないため，これらのポートへのアクセスを禁止した．

最後に本システムでは，攻撃者の検知基準は以下のように判断している[5].

- 代理応答による存在確認が 3 回を超えた
- TCP コネクションの未解決状態が 5 回を超えた
- 1 秒間に 10 回以上のコネクション要求を送信

代理応答による確認では，送信元からの ACK フラグが 1 のパケットが帰ってこない場合でも計数している．

4.2 運用期間

システムを動作させた期間は 2011 年 10 月 24 日 14:00～2011 年 10 月 26 日 3：00 の間動作させた．

4.3 運用結果

検知基準により検知した攻撃者の総数や分類をまとめたものが表 4.1 である．攻撃者の総数は 4565 件検出した．ここで表記している件数は本システムで検知された送信元 IP アドレス数のことを示している．

表 4.1 検知数

代理応答による存在確認	0 件
TCP コネクションの未解決状態数	4475 件
1 秒間のコネクション送信回数	90 件
重複	0 件
総数	4565 件

また，TCP コネクションの未解決状態数と 1 秒間のコネクション送信回数で検知された攻撃者のログの一部を以下に示す（図 4.1，4.2）.

```
189.38.1.167 type: 2 Mon Oct 24 15:33:40 2011
 2490 -> 133.37.56.196 22 UNSOLVED Mon Oct 24 15:33:40
 4047 -> 133.37.144.196 22 ABSENT Mon Oct 24 14:28:28
 3989 -> 133.37.148.196 22 ABSENT Mon Oct 24 14:28:27
 3985 -> 133.37.145.196 22 ABSENT Mon Oct 24 14:28:27
 3911 -> 133.37.149.196 22 ABSENT Mon Oct 24 14:28:31
```

図 4.1 TCP コネクション未解決状態数の検知例

```
41.178.237.57 type: 3 Mon Oct 24 15:51:01 2011
 4315 -> 133.37.57.16 23 REV_SYN Mon Oct 24 15:51:01
 4309 -> 133.37.57.10 23 REV_SYN Mon Oct 24 15:51:01
 4308 -> 133.37.57.9 23 REV_SYN Mon Oct 24 15:51:01
 4305 -> 133.37.57.6 23 REV_SYN Mon Oct 24 15:51:01
 4304 -> 133.37.57.5 23 REV_SYN Mon Oct 24 15:51:01
 4307 -> 133.37.57.8 23 REV_SYN Mon Oct 24 15:51:01
 4306 -> 133.37.57.7 23 REV_SYN Mon Oct 24 15:51:01
 4303 -> 133.37.57.4 23 REV_SYN Mon Oct 24 15:51:01
 4302 -> 133.37.57.3 23 REV_SYN Mon Oct 24 15:51:01
 4301 -> 133.37.57.2 23 REV_SYN Mon Oct 24 15:51:01
```

図 4.2 1 秒間のコネクション要求回数の検知例

4.4 Scan 攻撃検知システム誤検知の調査

4.4.1 調査の流れ

調査で使用するログは，攻撃者と判断する元となったパケットの情報を知るために，3.1 節の更新・表示部で提示する攻撃者ログを使用する.

攻撃者の宛先（攻撃対象）ＩＰアドレス・ポートについて以下の４つのパターンに分類する．攻撃者リストのログを用い，分類別に scan 攻撃の特徴を踏まえて調査する.

- 複数の宛先ＩＰアドレス・複数の宛先ポート
- 複数の宛先ＩＰアドレス・単一の宛先ポート
- 単一の宛先ＩＰアドレス・複数の宛先ポート
- 単一の宛先ＩＰアドレス・単一の宛先ポート

４つのパターンの検知例を以下に示す（図 4.3，4.4，4.5，4.6）.

```
91.121.95.168 type: 2 Mon Oct 24 16:38:56 2011
 113 -> 133.37.64.106 63695 UNSOLVED Mon Oct 24 16:38:56
 22 -> 133.37.130.76 32911 RSTSCAN Mon Oct 24 16:38:14
 22 -> 133.37.148.9 35076 RSTSCAN Mon Oct 24 16:37:59
 22 -> 133.37.206.13 47818 RSTSCAN Mon Oct 24 16:36:27
 22 -> 133.37.254.1 29373 RSTSCAN Mon Oct 24 16:34:35
```

図 4.3 複数の宛先ＩＰアドレス・複数の宛先ポート

```
213.151.174.158 type: 2 Mon Oct 24 16:39:45 2011
 40831 -> 133.37.13.183 22 ABSENT Mon Oct 24 16:39:45
 49972 -> 133.37.203.131 22 ABSENT Mon Oct 24 16:35:58
 42365 -> 133.37.144.147 22 ABSENT Mon Oct 24 16:32:24
 58037 -> 133.37.32.26 22 ABSENT Mon Oct 24 16:26:47
 37012 -> 133.37.207.106 22 ABSENT Mon Oct 24 16:19:48
```

図 4.4 複数の宛先ＩＰアドレス・単一の宛先ポート

```
58.253.94.21 type: 2 Mon Oct 24 17:14:02 2011
41264 -> 133.37.99.128 60430 ABSENT Mon Oct 24 17:14:02
41262 -> 133.37.99.128 60422 ABSENT Mon Oct 24 17:14:01
41252 -> 133.37.99.128 60355 ABSENT Mon Oct 24 17:13:11
41250 -> 133.37.99.128 60352 ABSENT Mon Oct 24 17:13:10
40706 -> 133.37.99.128 60034 ABSENT Mon Oct 24 17:01:39
```

図 4.5 単一の宛先ＩＰアドレス・複数の宛先ポート

```
217.68.69.203 type: 2 Mon Oct 24 17:10:19 2011
29182 -> 133.37.216.6 25 ABSENT Mon Oct 24 17:10:19
13598 -> 133.37.216.6 25 ABSENT Mon Oct 24 16:23:56
10270 -> 133.37.216.6 25 ABSENT Mon Oct 24 15:35:56
4691 -> 133.37.216.6 25 ABSENT Mon Oct 24 14:48:05
2407 -> 133.37.216.6 25 ABSENT Mon Oct 24 14:01:43
```

図 4.6 単一の宛先ＩＰアドレス・単一の宛先ポート

4.4.2 宛先ＩＰアドレス・ポートによる調査

攻撃者の宛先ＩＰアドレス・ポートについて 4 パターンに分類し，各タイプの攻撃者検知件数は以下（表 4.2）のようになった.

表 4.2 パケットの送信パターン

パケットの送信タイプ	検知数（件）
複数の宛先ＩＰアドレス・複数の宛先ポート	513
複数の宛先ＩＰアドレス・単一の宛先ポート	1810
単一の宛先ＩＰアドレス・複数の宛先ポート	170
単一の宛先ＩＰアドレス・単一の宛先ポート	2072
計	4565

A) 複数の宛先 IP アドレス・複数の宛先ポート

一般ユーザが複数の宛先ＩＰアドレス・複数のポートに対してパケットを送ることは通常では考えられないと思われるため，誤検知と考えず遮断時間を指定することでパケットを遮断してよいと考える.

B) 複数の宛先 IP アドレス・単一の宛先ポート

図 4.4 のように，攻撃者の目的が攻撃対象のネット

ワーク情報の収集が目的のために特定のポートが開いているか，複数の宛先ＩＰアドレスを調べていることから，このようなパケットの送信パターンは scan 攻撃と考えられる．複数の宛先ＩＰアドレス・単一の宛先ポートに対するパケットの送信について，宛先ポート毎に攻撃者検知数を見る（表 4.3）．その他は，宛先ポート毎の検知数が 20 件以下のものをまとめた．

表 4.3 宛先ポート番号ごとの攻撃者検知数

宛先ポート番号	検知数（件）
3389(Remote Desktop)	1552
22(SSH)	81
8080(HTTP)	52
23(telnet)	47
25(SMTP)	21
その他	57
計	1810

表 4.3 より，8080 番ポートは，オープンプロキシの探索[8]のため, 8080 番ポートの開いている宛先のポートスキャンをしていることが考えられる．25 番ポートに関しては，学内宛のメールはメールサーバ（ajimu1.net.oita-u.ac.jp）を中継するようになっており，宛先ポート番号が 25 番の学内宛のパケットはファイアウォールによって遮断されるが，メールの配信先を決定するために用いるＭＸレコードに学内のメールサーバを登録していたことがあったことからメールを送信しようとしたと考えられる．また，一度に複数の宛先ＩＰアドレスにメールを送った可能性が考えられるため誤検知の可能性がある.その他のポートには, 4899, 5900，5938 番ポートといった用途の割り当てられていないポート番号が見られた．

C)　単一の宛先 IP アドレス・複数の宛先ポート

宛先ＩＰアドレス毎に攻撃者検知数を分け，検知数が多かった宛先ＩＰアドレスに逆引き行いホスト名を調べたが，ホスト名から宛先ＩＰアドレスの用途は分らなかった．また，宛先ポート番号を調べたところ，図 4.5 のように用途の割り当てられていないポート番号が多く，一度しかポートが使われていない．そのため，一般ユーザが用途不明の宛先ポートに対してパケットを送ることは通常では考えられないため，パケットを遮断してよいと考える．

D)　単一の宛先 IP アドレス・単一の宛先ポート

単一の宛先ＩＰアドレス・単一の宛先ポートに対してパケットを送信していることから，ネットワーク情報の収集を目的としていないことが考えられる．宛先ポート毎に攻撃者検知数を見る（表 4.4）．

表 4.4 宛先ポート毎の攻撃者検知数

宛先ポート番号	検知数（件）
6883(用途不明)	907
14705(用途不明)	514
6885(用途不明)	59
25(SMTP)	50
8014(Symantec)	47
その他	495
計	2072

表 4.4 から，宛先が 25 番ポートの検知者は，メールの配信先を決定するために用いるＭＸレコードに学内のメールサーバを登録していたことがあったことから誤検知と考えられる．8014 番ポートは，Symantec Endpoint Protection Manager とエンフォーサの通信のデフォルトポートであり，学内からであればサポートしているが学外からではサポートしていないことにより検知されため誤検知と考えられる．6883，6885，14705 番ポートは用途不明のポート番号であり，宛先ＩＰアドレスの逆引きでは誤検知と判断はできなかったが，送信元ポート番号を調べた結果，6969 番ポートといった bit torrent で使用されるポート番号が見られた．

5.　結論

攻撃者の宛先ＩＰアドレス・ポートについて 4 パターンに分類し，scan 攻撃検知システムの誤検知の調査を行った結果，複数の宛先ＩＰアドレス・特定の宛先ポート，特定の宛先ＩＰアドレス・特定の宛先ポートの 2 つのパターンに誤検知が見られた．誤検知と考えられる送信元の特徴として，宛先ポート 25，8014 番を使用していることが分かった．このことから，学内でよく使用されるポートの中で、学外からも使用するようなポートに注意する必要があり，検知システムの除外ポートに 25，8014 番ポートを設定する必要がある．

今後，攻撃者の 3 タイプ別に，攻撃者の宛先ＩＰアドレス・ポートについて分類した 4 パターンを含め検知条件を検討していく必要がある．

一般ユーザが通常では行わないパケットの送信が見られた．一般ユーザが通常では行わないようなパケット送信により検知した攻撃者のパケットは遮断を行う．攻撃者情報の保持時間やパケットの遮断時間は今後の検討課題である．

参考文献

1) 三鑰達真, 吉田和幸, ”長期的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”, 信学技報（IA2007-47）, 電子情報通信学会, pp.39-44, 2008.
2) Snort, http://www.snort.org/.
3) Bro, http://www.bro-ids.org/.
4) 大塚賢治, 兒玉清幸, 吉田和幸, ”偽装応答による scan 攻撃抑制システムの攻撃抑制効果について”, 情報処理学会火の国情報シンポジウム 2008 論文集, B-8-3,pp.1-8 (published by CD-ROM), 2008.
5) 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”, 情報処理学会マルチメディア, 分散, 協調とモバイル(DICOMO2009) シンポジウム論文集, pp.1285-1290, 2009.
6) 大塚賢治,”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”, 大分大学修士論文, 2009.
7) 永山聖希, 大塚賢治, 藤原健志, 吉田和幸, “scan 攻撃検知システムの遮断時間決定のための予備調査”, 火の国情報シンポジウム 2010 論文集, A-5-3, pp1-7 (published by CD-ROM), 2010.
8) プロキシを利用したメール等の不正中継について, 警視庁分析レポート, http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/20080229_PROXY.pdf, 2008.