社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（17）
2006－CSEC－32（17）
2006／3／16

IPid を用いた NAT 検知手法の考察

高橋 輝壮[*]　甲斐 俊文[**]　篠原 克幸[***]

[*]工学院大学 大学院 工学研究科 情報学専攻
[**]松下電工株式会社 先行技術開発研究所
[***]工学院大学 工学部 情報工学科

あらまし　接続許可が与えられていない PC を社内ネットワークに接続することは，悪意のあるユーザが個人情報を窃取し，悪意がないユーザであってもウィルスによる混乱を招く恐れがある．そのため接続する PC の MAC アドレスを予め登録するなど，ネットワーク内で未承諾 PC の接続を検知する技術が開発されている．しかし NAT（Network Address Translator）を利用することで検知を逃れることができるという問題点があり，これを防ぐためには NAT 検知技術が必要である．本稿では IPid を用いた NAT 検知に関する課題を整理し，それらを克服する手法を提案する．また，パケット観測数と NAT 判定の正答率についてシミュレーションにより評価する．

A consideration of a NAT detection technique using IPid

Teruaki TAKAHASHI[*],　Toshifumi KAI[**]　and　Katsuyuki SHINOHARA[***]

[*]Department of Infomatics, Graduate School of Engineering Science, Kogakuin University
[**]Advanced Technologies Development Laboratory, Matsushita Electric Works, Ltd.
[***]Computer Science and Communication Engineering, Kogakuin University

Abstract　When a PC which the connection is not being granted the permission is connected with an in-house network, a malicious user might thieve private information, even if a user not malicious, confusion might be caused by the virus. Therefore, some technologies that detect unapproved PC connection in the network as the MAC addresses of all connected PC are registered beforehand are developed. However, there is a problem that it is possible to escape from detection by using NAT (Network Address Translator), and the NAT detection technology is necessary to prevent this. We arrange the problem concerning the NAT detection using IPid in this text, and we propose a technique for overcoming them. In addition, we evaluate the number of observations of packets and the correct answer rate of the NAT judgment by the simulation.

1. はじめに

近年，企業ネットワークには個人情報漏洩とウィルス・ワーム感染の問題がある．これらの問題が起きる要因の一つに社外からの持込み PC がある．例えば持込んだ個人の PC を社内ネットワークに接続して情報を窃取するケースがある．また，個人の持込み PC は社用 PC と違い一般にウィルス対策が甘く，ウィルスに感染した状態で社内ネットワークに接続し，トラブルを引き起こす恐れがある．

そうした問題への対策として Intra POLICE[1]のような未承諾 PC を検知するための製品がある．この類の製品はPCのMACアドレスやその他の情報を登録して社内ネットワークに接続できる PC を制限し，承諾された PC のみが接続できる環境を構築する．しかし，接続許可されたPCにNAT（Network Address Translator）[2]機能を導入したり，新たに NAT ルータを設置することで，許可されていない PC を社内ネットワークに接続できてしまう．承諾された PC 自体が NAT として動作する場合，NAT として動作する PC や NAT の内側に接続された PC を検知することはできない．NAT 機能は設定に関する知識さえあれば導入可能であるため，モラルの低いユーザが管理者に無断で NAT 機能を利用する可能性がある．

そこで我々はBellovinらが提案しているIPヘッダのIdentificationフィールド（以下，IPid）を用いた通信ホスト台数検知技術[3]に着目し，検証プログラムを作成して基本的な挙動確認を行った[4]．さらに本稿では NAT 検知に関する課題を整理し，課題克服のためにオペレーティングシステム識別技術[5][6]の応用法や IPid の能動観測について述べ，IPid を用いた NAT 検知に関する新手法を提案する．新手法についてはシミュレーションにより評価する．

第 1 章では本稿の概要について述べた．第 2 章では NAT 検知に関連する研究として，Bellovin らが提案している通信ホスト台数検知技術について我々の分析した内容を述べる．第 3 章では IPid の特性やトラフィックの特性について調査，実験を行ったので報告する．第 4 章では NAT 検知技術の課題を整理した．第 5 章では我々が提案する IPid 間の関連性分析手法について述べ，パケット観測数と NAT 判定の正答率についてシミュレーションにより評価したのでその結果を報告する．第 6 章ではまとめと今後の課題について述べる．

本稿では NAT に関する領域として，NAT に未承諾 PC が接続される側を内側，管理されている社内ネット

ワーク側を外側とする．

図1は悪意のあるユーザが不正にNATルータを設置して個人情報を窃取したり，持込み PC がウィルスに感染していたことによる情報漏洩やネットワークへ感染拡大したりする様子を表している．

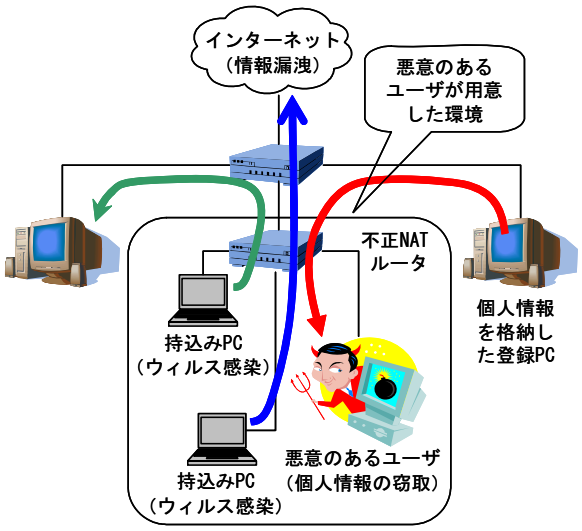

図1　不正 NAT と持込み PC の脅威

2. NAT 検知に関する関連研究

我々は Bellovin らが提案している通信ホスト台数検知技術を NAT 検知に応用できるかどうか分析を行った．そして，基本的な動作確認を行うために検証プログラムを作成し，検証実験を行った[4].

本章では次章以降の内容を考慮し，我々が分析した通信ホスト台数検知技術の概要，前提条件，用いたパラメータ，IPid 分類処理，検証実験の概要と結果について述べる．

2.1. 通信ホスト台数検知技術の概要

通信ホスト台数検知技術[3]はパケットの IP ヘッダの Identification フィールド（以下，IPid）を用いて NAT の内側に存在するホスト数をカウントする技術である．パケットを観測した順に IP ヘッダ内の IPid を抽出し，構成した IPid 列を分類条件を用いて走査し要素間の相関関係を調べる．

我々は通信ホスト台数検知技術を分析し，IPid について前提条件とパラメータを設定した．また通信ホスト数をカウントするために用いる IPid 分類処理を具体的に策定したので説明する．

2.1.1. 前提条件

IPid に書き込まれる値は，1 ずつ増加することを前提とする．IPid は 16bit のフィールドであり，かつ 0 を取ることはない．したがって i 番目に到着したパケットの IPid は以下の式になる．

$$IPid(i) = i \bmod 65535 + 1 \qquad (i = 0,1,\cdots)$$

そして，$IPid(i)$ を格納する配列をシーケンスと呼ぶ．キャプチャしたパケットの IPid を抽出し，IPid 分類処理（後述）を用いて該当するシーケンス $Seq(n)$　$(n = 1,2,\cdots)$ に追加していく．n の最大値 N がシーケンス数となり，NAT の内側に接続されているホスト数になる．ホスト数が 2 以上になった時点でその送信元アドレスを持つノードは NAT と判定する．

2.1.2. パラメータ

IPid 分類処理で用いるパラメータとその意味を表 1 にまとめた．

表1　IPid 分類処理で用いるパラメータ

パラメータ	意味
$diff$	$IPid(i) > IPid(i-1)$ のとき $diff = IPid(i) - IPid(i-1)$ $IPid(i) \le IPid(i-1)$ のとき $diff = 65535 + IPid(i) - IPid(i-1)$
$gaplim$	$Seq(n)$ に $IPid(i)$ を格納するための $diff$ の上限 $(1 \le gaplim \le 65535)$

Bellovin らはパケットの到着時間間隔もパラメータとして用いていたが，検証実験を簡単にするために本稿では以上のパラメータのみを用いることとした．

2.1.3. IPid 分類処理

IPid を対応するシーケンスに分類・格納する IPid 分類処理について述べる．図 2 に IPid 分類処理のアルゴリズムを示す．

```
（ステップ 1）初期化
  Seq(0) を確保し，Seq(0) の要素全てを 0 に初期化する．
（ステップ 2）IPid 分類処理
 for ( n = 0 ;  n < N ;  n = n + 1 ) {
    diff = IPid(i) − IPid(i − 1)
    if ( diff ≤ 0 )
       diff = 65535 + IPid(i) − IPid(i − 1)
    if ( gaplim ≥ diff ) {
       Seq(n) に IPid(i) を追加
       n = n − 1
       break
    }
    else
       continue
 }
 if  n = N  then
    新たにシーケンスを作成し IPid を追加
```

図2　IPid 分類処理アルゴリズム

ステップ 1 を実行しステップ 2 を繰り返し実行することで一試行が完了する．パケットが到着する毎にステップ 2 を試行し，該当するシーケンス $Seq(n)$ に $IPid(i)$ を格納していく．シーケンス数 N が 2 以上になった時点でその送信元アドレスのホストは NAT ルータだと判定する．

2.2. 検証実験の概要と結果

我々は通信ホスト台数検知技術の挙動を確認するために，検証プログラムを作成し検証実験を行った．

通信ホストが 1 台のとき，1 台の通信ホストと判定するか, NAT と誤判定するかどうかを検証した. また，通信ホストが 2 台のとき，NAT と判定するかどうかを検証した．

検証実験の結果，簡単な環境下では正常に通信ホスト台数検知技術は NAT 検知技術として応用できることが分かった．

3. IPid の特性及びトラフィックの特性

本稿では NAT 検知のために IP ヘッダの Identification フィールド（以下，IPid）を用いる．また，NAT の外側のインタフェースから流出するパケットを観測して IPid を抽出し，既に記録している IPid との相関関係から NAT 判定を行う．そこで我々は IPid の特性や NAT から流出するトラフィックに関して調査を行った．

本章では IPid の目的と一般性質，オペレーティングシステム（以下, OS）毎にセットされる IPid の規則性，ローカル通信が与える IPid への影響, NAT から流出するトラフィックの特性について述べる．

3.1. IPid の目的と一般性質

IPid は経路途中でパケットが分割化された際，パケットの宛先ホストが分割化されたパケットを再構築する際に参照する 16 ビット（0～65535）の識別子である．IPid にはパケットの送信元ホストでユニークな値がセットされる．もし経路途中のルータでパケットが分割化されると，IPid は分割化されたパケットで共有される．また，ルータを経由してパケットが宛先ホストに届いたとしても，IPid は変更されない．

3.2. OS 毎の IPid の特性

IPid は送信ホストの OS によってセットされる値の規則性に相違が現れる[5][6]. 表 2 に OS と IPid 値の取り方の対応を示す．

表2　OS 毎の IPid の規則性

OS	IPid の規則性
Windows	1 ずつ増加する
OpenBSD	ランダムに変化する
Linux	セッションが確立されるまではランダムに変化する 確立したセッション毎に 1 ずつ増加する ICMP パケットは 0 に初期化する
FreeBSD	1 ずつ増加する
NetBSD	1 ずつ増加する
Solaris	1 ずつ増加する
AIX	1 ずつ増加する

Windows や FreeBSD，Solaris などは IPid の値を 1 ずつ増加しながらパケットヘッダにセットするが，OpenBSD はランダムな値を IPid にセットし，Linux はセッションごとに IPid の値が 1 ずつ増加しながら IPid をセットする．図 3 は NAT の外側で観測した IPid の値が①1 ずつ増加，②ランダムに変化，③セッション毎に 1 ずつ増加する過程を表している．

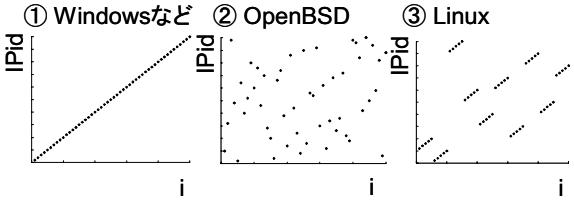

図3　OS 毎の IPid 変化特性

3.3. ローカル通信

パケットを送信するホストの OS が Windows の場合，IPid を 1 ずつ増加させながらパケットヘッダにセットしていくが，NAT の外側でパケットを観測した場合，NAT の内側で行われるローカル通信によって IPid の値が 1 ずつ増加しないことがある．

その原因としてホスト PC 内部でのループバック通信や NAT の内側だけで通信が行われていたと考えられる．それらの通信が行われた場合，その分 IPid の値は増加する．したがって NAT の外側で IPid を観測しても 1 ずつ増加しないことがある．ローカル通信が多発するような環境では $IPid(i-1)$ に比べて $IPid(i)$ が急増し，IPid が 65535 を超えて 1 に戻ると逆に減ってしまう可能性がある．

3.4. トラフィックの特性

我々は IPid とローカル通信の関係について分析するために，NAT ルータの内側から流出してくるパケットを観測し，トラフィックの特性について調査した．

3.4.1. 分析に用いるパラメータ

NAT 検知を想定したパケット間の関係を分析するために，表 3 のパラメータを用いた．

表3　トラフィック特性の分析に用いるパラメータ

パラメータ	意味
L	ローカル通信の発生確率 1 台の通信ホストを NAT と判定することに起因
D	連続送信確率 N 台の通信ホストを 1 台の通信ホストと判定することに起因

L は通信ホストがローカル通信を発生する確率を表している．ローカル通信は 1 台の通信ホストを NAT と判定してしまう一要因である．そこでローカル通信の頻度を計測するためにこのパラメータを導入する．また D は同一ホストがパケットを連続して送信する確率を表している．同一ホストが連続してパケットを送信し続けるということは，複数台の通信ホストを 1 台の通信ホストと判定してしまう一要因となる．そこで実環境での同一ホストのパケット連続送信確率を計測するためにこのパラメータを導入する．

3.4.2. 計測結果

パケットの観測は本学 2 研究室を対象に行った．計測結果を表 4 に示す．

表4　各研究室のパケット観測結果

	L		D
研究室 1	PC1	0.32	0.97
	PC2	0.00	
	PC3	0.72	
	PC4	0.38	
	PC5	0.30	
研究室 2	PC1	0.04	0.98
	PC2	0.52	
	PC3	0.23	

表 4 の結果から, ある通信ホストが NAT の外側のホストと通信する場合，連続して外部ホストと通信をする確率が高いことが確認できた．また，ローカル通信の頻度も通信ホストによって様々だが比較的高くなる場合があることが分かった．

4. NAT 検知技術の課題整理

前章までに NAT 検知に関する既存技術と IPid の特性，トラフィックの特性について我々が調査，実験した内容を述べた．本章ではそれらを踏まえ，NAT 検知に関する課題の整理を行う．まず IPid を用いた NAT 検知技術の課題について述べ，IPid のランダム性を分離するアプローチや能動観測手法について述べる．

4.1. IPid を用いた NAT 検知技術の課題

前章までに挙げた通信ホスト台数検知技術，OS 毎の IPid の規則性，ローカル通信，トラフィックの特性から次の NAT 検知技術の課題を洗い出した．

1. OS 毎の IPid の規則性
2. $gaplim \geq diff$ の限界
3. パケットの到着時間間隔の影響
4. 受動観測の限界

1 は通信ホスト台数検知技術では OpenBSD や Linux が送信するパケットの IPid を正しく分析できないことを意味している．IPid がランダムに変化する場合，IPid を分析しても有益な情報が得られない．またセッション毎にシーケンシャルな IPid 列が発生する場合，1 台の通信ホストを NAT と誤判定してしまう．

2 は通信ホスト台数検知技術がローカル通信に対応していないことを意味している．ローカル通信が頻繁に発生するような対象を観測する場合，$gaplim \geq diff$ の条件だけでは対応できない．

3 は $IPid(i)$ と $IPid(i-1)$ の到着時間間隔を考慮した場合，IPid 分類処理に影響することを意味している．Bellovin らの提案している通信ホスト台数検知技術は元々パケットの到着時間間隔と IPid の相関を考慮した技術だった．しかし，NAT の内側のホストがしばらく通信を行わないと，通信ホスト台数検知技術では 1 台の通信ホストを 2 台のホストと誤って判定してしまう．

4 は承諾済み PC 自身が NAT ルータとして動作した場合に問題が発生することを意味している．通信ホスト台数検知技術は，ネットワーク上に流れるパケットをキャプチャすることにより IPid を観測することが前提である．したがってこのような受動的な観測手法のみでは NAT ルータとして動作する承諾済み PC の NAT 機能と, その内側に接続されるホストを検知できない．

4.2. IPid のランダム性分離

OpenBSD や Linux のように，IPid を一貫してシーケンシャルに増加しないものがある．そこで我々はパケットを送信したホストの OS を識別する技術[5][6]を用いることにする．これにより IPid を用いた NAT 検知の対象とそうでないものを分離することができる．図 4 は IPid のランダム性を分離する例をフローとして表したものである．

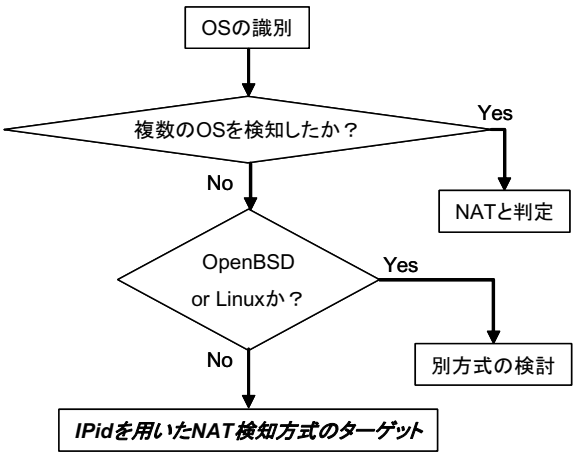

図4　IPid のランダム性分離フロー

まず OS 識別技術によってパケットの送信元ホストが単一 OS のみ検知されるかどうかを調べ，複数の OS が検知された場合はその時点で NAT と判定する. 単一 OS のみ検知された場合，OpenBSD や Linux の挙動が確認できるかを調べる．もしパケットが OpenBSD や Linux から送信されたものとして検知された場合，IPid 以外の情報を用いた NAT 検知方式について検討しなければならないが，そうでないならば我々の IPid を用いた NAT 検知方式の対象とする．

比較的整備された社内ネットワークでは，承諾していない OS を使用した PC の接続を検知した場合，それを異常な状態として扱うことができる．そのため OS 識別技術単体でも未承諾 PC の検知に応用できる．

4.3. 能動観測手法

社内ネットワークで前述した NAT 検知技術を導入したとしても，承諾済み PC 自身が NAT ルータとして動作する場合，NAT ルータや内側に接続されている通信ホストを検知することはできない. これは NAT 検知技術がネットワーク上を流れるパケットを受動的に観測していることが原因である．

そこで我々は承諾済み PC 自身が NAT ルータとして動作する場合，ping アプリケーションを利用して NAT ルータのパケットを能動的に観測することにする．図 4 は NAT 検知機能が受動観測を行うだけでなく，NAT ルータとして動作する Windows マシンに ICMP Echo Request を送信し，NAT ルータから返信される ICMP Echo Reply の IPid を分析している様子を表している．

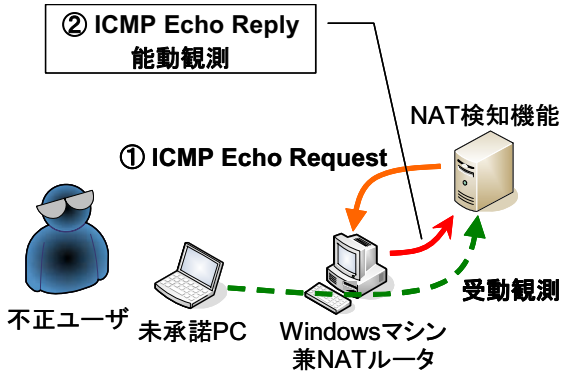

図5　受動観測と ping による能動観測

能動観測の場合も OS 識別技術と同様に，比較的整備された社内ネットワークでは ICMP パケットを破棄するような PC があったとしても，ICMP Echo Reply を返さない PC は異常だと判定できる．したがって悪意のあるユーザが IPid を隠蔽しようと試みても，未承諾 PC の接続の可能性を示すことができる．

5. IPid 間の関連性分析手法

前章の IPid を用いた NAT 検知におけるローカル通信とパケットの到着時間間隔についての課題を克服するために，我々はローカル通信をある程度許容でき，パケットの到着時間間隔に依存しない IPid 間の関連性分析手法を提案する．

本章では IPid 間の関連性分析手法の概要と評価方法，シミュレーション結果について述べる．

5.1. 提案手法の概要

IPid 間の関連性分析手法（以下，提案手法）は通信ホスト台数検知技術と同様にパケットを観測した順に IPid を抽出し，IPid 列を構成する．さらに表 1 のパラメータを用いて IPid 列の要素間の相関関係を調べる．図 6 はパケットの到着順 *i* と IPid 値を示した提案手法の例である．

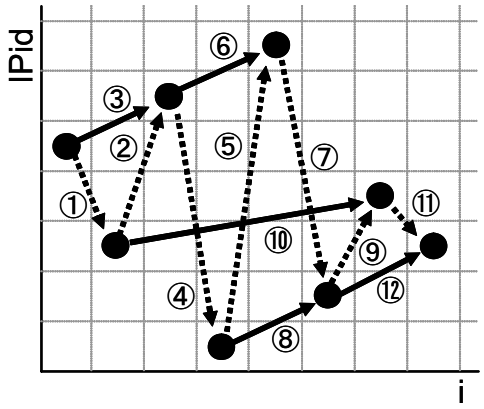

図6　IPid 間の関連性分析手法の例

提案手法は $gaplim \geq diff$ を用いて 2 つの出力結果を得る．1 つは図 6 の破線矢印（①，②，④，⑤，⑦，⑨，⑪）である．破線矢印は $gaplim < diff$ により発生する．他方，実線矢印（③，⑥，⑧，⑩，⑫）は破線矢印によって繰り返し遷移していく IPid が $gaplim \geq diff$ の条件を満たす場所に戻ってきたときに発生する．

以降，簡便のために破線矢印を BA（Broken line Arrow），実線矢印を SA（Solid line Arrow）と略記する．

BA だけでなく SA を導入することによってローカル通信の問題を緩和することができる．また提案手法は到着したパケット順に IPid を抽出し作成した IPid 列を解析するだけなので，パケットの到着時間間隔に依存しない．

5.2. 提案手法の評価

提案手法は出力する BA，SA が NAT 判定の資源となる．我々はシミュレーションを行い，どのような環境が BA，SA を発生させるのか，SA が発生するまでのパケット観測数はどのように変化するのか，その指標を明らかにした．

5.2.1. 評価方法

シミュレーションではローカル通信の発生確率 L と同一 PC の連続送信確率 D を用いてパケット観測数 1～10000 の IPid 列を擬似的に作成した．そして提案手法を用いて擬似的に発生した IPid を解析し，BA，SA を発生させた．本稿では SA が発生した時点で NAT と判定することにした．

評価項目毎に入力したパラメータを表 5 に示す．

表5　入力パラメータ

評価項目	L	D	gaplim	通信ホスト
①D の特性	0.00	0.00～0.99	64	2 台
				3 台
②L の特性	0.00～0.99	0.00		1 台
③正答率	0.90	0.98		1，2 台
	0.99			

評価項目①は D を変化させたときに SA が発生するまでのパケット観測数はどのように変化するのかを検証した．また通信ホストを増やした場合も同様に検証した．

評価項目②は L を変化させたときに SA が発生するまでのパケット観測数はどのように変化するのかを検証した．

評価項目③は表 4 を参考に D=0.98 としたときの NAT 判定の正答率について検証した．NAT 判定の正答率とは，ある観測時点で通信ホストが 1 台の場合生成する IPid 列から SA が発生しない確率，通信ホストが 2 台の場合生成する 2 つの IPid 列から SA を発生する確率のことである．

評価項目①～③についてパケット観測数（1～10000）それぞれ 100 回ずつ IPid 列を生成し試行した．次に示す結果はそれらの平均値である．また gaplim には Bellovin らが用いている値（=64）[3]を入力した．

5.2.2. シミュレーション結果

評価項目①のシミュレーション結果から，NAT の内側に通信ホストが複数台接続されていたとしても，SA が発生するまでにある程度パケット観測が必要であることが分かった．評価項目①のシミュレーション結果の一部を表 6 に示す．

表6　SA が発生するまでの平均パケット観測数（L=0.00）

D	0.50	0.90	0.95	0.99
通信ホスト2台	15	111	250	1695
通信ホスト3台	13	93	215	1395

表 6 から D が高い環境ほど，SA が発生するまでに要するパケット観測数が増えることが分かった．さらに通信ホストの台数が増えると SA が発生するまでのパケット観測数が減少することが分かる．

評価項目②のシミュレーション結果から L が高い環境でパケットを観測し続けると，通信ホストが 1 台であっても SA が発生し始めることが分かった．評価項目②のシミュレーション結果の一部を表 7 に示す．

表7　SA が発生するまでの平均パケット観測数（D=0.00）

L	0.85	0.90	0.95	0.99
通信ホスト 1 台	9905	6503	3189	617

表 7 から L が高い環境ほど，SA が発生するまでに要するパケット観測数が減少することが分かる．

最後に評価項目③のシミュレーション結果を図 7，図 8 に示す．

図 7 は L=0.90, D=0.98 のときのパケット観測数に対する NAT 判定の正答率を表している．これは通信ホスト 1 台のときの結果と 2 台のときの結果を合成し，正答率の遷移を分析しやすいように近似したものである．

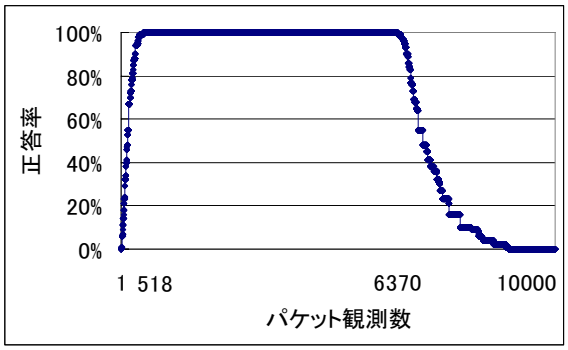

図7　NAT 判定の正答率（L=0.90，D=0.98）

通信ホスト 2 台から生成された 2 つの IPid 列からは，パケット観測数が 518 になるまで SA の発生率は 100%未満だった．また，通信ホスト 1 台から生成された IPid 列からはパケット観測数が 6370 を超えたあたりから SA が発生し，正答率が 100%から減少している．この結果から高精度に NAT 判定を行うためにはパケット観測数の上限と下限を意識しなければならないことが分かった．

図 8 は L=0.99, D=0.98 のときのパケット観測数に対する NAT 判定の正答率を表している．図 7 と同様に通信ホスト 1 台のときの結果と 2 台のときの結果を合成し，正答率の遷移を分析しやすいように近似している．

図 8 からパケット観測数が 557 を超えると正答率が減少しているのが分かる．したがって L が非常に高い環境で高精度に NAT 判定を行うためには，パケット観測数の上限を低く設定しなければならないことが分かった．

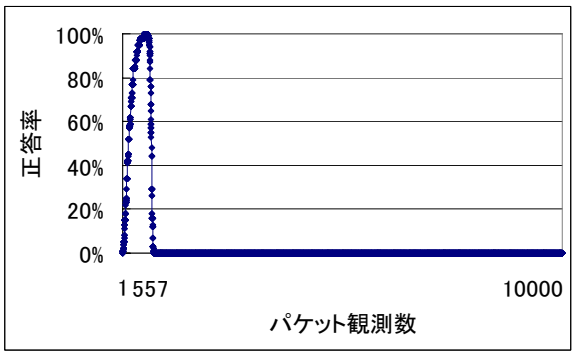

図8　NAT 判定の正答率（L=0.99，D=0.98）

6. おわりに

本稿では NAT 検知技術として既存技術の通信ホスト台数検知技術を NAT 検知技術に応用することについて述べた．また，IPid の特性とトラフィックの特性から NAT 検知に関する問題点を洗い出し，OS 識別技術や IPid の能動観測を NAT 検知に応用することについて述べた．さらに，ローカル通信やパケットの到着時間間隔の問題を克服するために IPid 間の関連性分析手法を提案し，実環境のローカル通信の発生確率と連続送信確率という側面から提案手法の性質を明らかにしようと試みた．その結果，使用環境によって SA が発生するまでのパケットの観測数と NAT 判定の正答率に影響を及ぼすことが分かった．

IPid を用いた NAT 検知の課題として，本稿の提案手法では使用環境を分析し，その上で入力パラメータ gaplim を分析しチューニングすること，OpenBSD や Linux のような IPid のランダム性に対応することが挙げられる．さらに，NAT に IPid を改変するアプリケーションゲートウェイのような機能を追加して未承諾 PC を接続する場合や，悪意のあるユーザが故意に IPid をランダムに変化させるような場合に対して対策を講じることが挙げられる．

参考文献

[1] Intra POLICE. http://www.netcocoon.com/jp/intrapolice/overview/index.html

[2] K. Egevang, Cray Communications, P. Francis and NTT. “The IP Network Address Translator (NAT) RFC1631.” May 1994.

[3] Steven M. Bellovin. “A Technique for Counting NATted Hosts.” Proc. IMW'02, Nov. 2002.

[4] 高橋 輝壮，河原 隆，甲斐 俊文，篠原 克幸．“IPid を用いた NAT 検知技術に関する研究.” 2006 年度 暗号と情報セキュリティシンポジウム SCIS2006. Jan. 2006.

[5] Toby Miller. “Passive OS Fingerprinting: Details and Techniques.” http://madchat.org/reseau/portscanning/passiveos.pdf

[6] Toby Miller. “Passive OS Fingerprinting: Details and Techniques (Part 2).” http://madchat.org/reseau/portscanning/passiveos2.pdf