CGNを対象としたホストIDを用いたフィルタリング機構の検証

大野夏希[1] 井上 朋哉[2] 宮川 晋[2,3] 篠田 陽一[2,4]

概要：IPv4 アドレス枯渇に伴い、インターネット接続サービスを提供する通信事業者は、保有しているIPv4 アドレスを有効利用するため、アドレス共有技術の導入を進めている。アドレスを共有する方法として、通信事業者が NAT を行う CGN が提案されている。CGN を適用した場合、インターネットにおいてキャリア内ネットワークのホストは、CGN が保有するグローバル IP アドレスによって識別される。インターネット上のサーバがキャリア内ネットワークのホストをフィルタリングした場合、同じアドレスを共有しているホストからの通信が不可能となる。この問題は、インターネット上のサーバにおいて、キャリア内ネットワークのホストを識別したフィルタリングを行うことによって解決する。キャリア内ネットワークのホストを識別する手法として、ホスト ID が提案されている。本研究では、ホスト ID を扱う CGN とファイアウォールを実装し、ホスト ID によるフィルタリングについて検証を行った。結果、ホスト ID を用いることによって、適切なフィルタリングが可能となった。しかし、ホスト ID を付与した通信は、現状のインターネットで利用することは困難であることが示された。

Verification of Filtering Mechanism using Host ID for CGN

Natsuki Ohno[1] Tomoya Inoue[2] Shin Miyakawa[2,3] Yoichi Shinoda[2,4]

1. はじめに

2011 年 2 月に、IPv4 アドレスを管理する Internet Assigned Numbers Authority(IANA) にて新規に割り当て可能な IPv4 アドレスの在庫が枯渇した。これにより、インターネット接続サービスを提供する通信事業者は、IPv4 を用いた接続サービスを提供するために必要なグローバル IPv4 アドレスの新規割り当てを受けることが不可能となった。IPv4 アドレスの枯渇を懸念して、IPv6 が考案された。しかし、運用者の技術や知識の蓄積、ソフトウェアの IPv6 対応などが充分ではないため、IPv6 の導入は難航している。このことから、しばらくの間インターネットは IPv4 ネットワークと IPv6 ネットワークが共存する環境となると考えられる。通信事業者が、今後グローバル IPv4 アドレスの新規割り当てなしに、新たなサービスの展開が可能な IPv4 ネットワークを提供するためには、現在保有しているグローバル IPv4 アドレスを有効利用する必要がある。

通信事業者によって Network Address Translation(NAT) を行う Carrier Grade NAT(CGN) [1] が、グローバル IPv4 アドレスを有効利用するための方法として提案されている。CGN は、グローバル IPv4 アドレスを複数のホストで共有する。そのため、キャリア内ネットワークのホスト (以下、キャリア内ホスト) がインターネット上のサーバ (以下、キャリア外サーバ) でフィルタリングされた場合、同じアドレスを共有するホストもフィルタリングされる事が挙げられる。CGN におけるフィルタリングの問題を解消するために、キャリア内ホストをキャリア外サーバで一意に識別する手法として、通信にホスト ID と呼ばれる識別

1 北陸先端科学技術大学院大学 情報科学研究科
Japan Advanced Institute of Science and Technology, School of Information Science
2 北陸先端科学技術大学院大学 高信頼ネットワークイノベーションセンター
Japan Advanced Institute of Science and Technology, Dependable Network Innovation Center
3 NTT コミュニケーションズ株式会社 先端 IP アーキテクチャセンタ
NTT Communications, Innovative Architecture Center
4 北陸先端科学技術大学院大学 情報社会基盤研究センター
Japan Advanced Institute of Science and Technology, Research Center for Advanced Computing Infrastructure

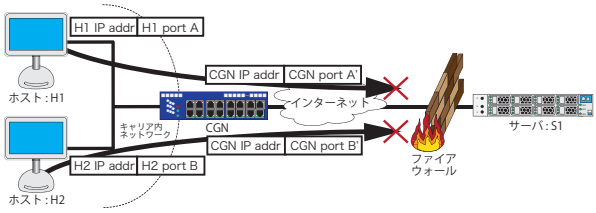

図 1 CGN を含むネットワークでファイアウォールを利用した場合

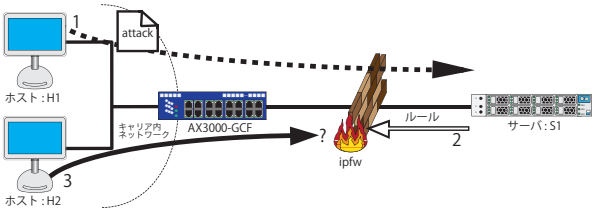

図 2 一般的な CGN を用いた通信:検証環境と検証方法

子を付与する方法が提案されている [2]。

本稿ではホスト ID に基づくフィルタリングを行うことにより、キャリア内ホストごとのフィルタリングが可能となるか検証を行った。また、ホスト ID を用いた通信が実際のインターネットにおいて使用可能であるか検証を行った。

2. CGN を用いる際の問題点

ホストを特定する識別子として利用されている IPv4 アドレスは、フィルタリングを行う際にもホストの識別のために利用される。キャリア内ホストから、キャリア外サーバへの通信は、インターネットにおいて CGN が持つグローバル IPv4 アドレスからの通信と観察される。そのため、送信元 IP アドレスを利用する一般的なフィルタリングでは、同じ IPv4 アドレスを共有しているホストからの通信にもフィルタリングの設定が反映されてしまう。図 1 は CGN を含むネットワークで IP アドレスベースのファイアウォールを用いた場合の説明である。キャリア内ネットワークからインターネットへの通信は、CGN によって送信元 IPv4 アドレスが CGN のグローバル IPv4 アドレスへ変換される。サーバ S1 では、ホスト H1 からの通信も、H2 からの通信も同じ IPv4 アドレスからの通信となる。つまり、IP アドレスベースのファイアウォールを用い H1 からの通信をフィルタリングした場合、H2 からの通信にもフィルタリングの設定が反映されてしまう。

CGN が持つグローバル IPv4 アドレスがフィルタリングされた場合、そのアドレスを保有する通信事業者が対処を行う必要がある。そのため通信事業者からは、共有されているグローバル IPv4 アドレスでフィルタリングを行うのではなく、キャリア内ホストごとにフィルタリングを行って欲しいという要求がある。また、サーバの運用者は、意図しないホストをフィルタリングしてしまうことによって、新たな顧客を得る機会を損失する可能性があるため、意図したホストのみフィルタリングしたいという要求がある。これらの要求を満たすためには、キャリア内ホストを識別し、フィルタリングを行う方法が必要となる。

3. 事前実験

3.1 一般的な CGN を用いた通信

前述の CGN の問題点は、RFC1631 [3] における NAT の定義に従って動作する CGN を経由した通信へのフィルタリングについてである。CGN を経由した通信では、実際に前述の通りフィルタリングが行われることを確認する必要がある。そこで、一般に使用されている CGN を経由した通信にフィルタリングを行った場合、フィルタリングの対象として意図しないホストにもフィルタリングが反映されることを確認した。

3.2 一般的な CGN を用いた通信の検証環境と検証方法

一般的な CGN を経由した通信を検証するために、図 2 のような検証環境を用意した。CGN にはホスト H1、H2 を接続し、キャリア内ホストとして設定した。サーバ S1 では、IP アドレスベースのフィルタリングを行うファイアウォールである ipfw(FreeBSD) を用意した。CGN は、A10 社の AX3000-GCF を用いた。これは、キャリア向けに販売されている CGN 製品である。破線矢印が攻撃による通信を、実線矢印が正当な通信を、白抜き矢印がフィルタリングルールの追加を表す。

本検証では、UDP echo サーバと、UDP echo クライアントを用いて通信を発生させた。サーバが攻撃パケットを受け取った場合、攻撃パケットと同じ送信元 IP アドレス持つパケットを破棄するフィルタリングルールを ipfw に動的に追加するプログラムを作成し、検証に用いた。これは、フィルタリングルールの追加を動的に行うことによって、ヒューマンエラによる検証の失敗を無くすために作成した。本検証において、攻撃を検知することは目的ではない。しかし、どのような通信をフィルタリングするか決定するためには、攻撃がどのようなものであるのか定義しなくてはならない。そこで、echo データの中身が”*attack*”という文字列を含む通信を攻撃と定義した。

検証方法は、まず H1 が攻撃を行う。その後、H1、H2 から通信を行い、通信の可否の確認を行う。

3.3 一般的な CGN を用いた通信の検証結果

前述した検証環境を用いて、検証を行った。表 1 は、攻撃に対するフィルタリングルールが追加された後の、ホストから S1 への通信の可否である。H1 から攻撃を行った場合、H1 から S1、H2 から S1 への通信が不可能となることを確認した。この結果から、キャリア内ホストから攻撃があり、キャリア外サーバが IP アドレスベースのフィルタリングを行うと、同じ IP アドレスを共有するキャリア内

表 1 フィルタリングルール追加後の
ホストから S1 への通信の可否

ホスト	S1 への通信
H1(攻撃者)	×
H2	×

ホストもフィルタリングされてしまうことが示された。

CGN の問題点が一般的な CGN でも発生することを確認した。この問題を解決するために、キャリア内ホストを識別し、フィルタリングを行う方法が必要である。次の章では、解決する方法についての考察、検証そして検証の結果から実際の利用について検討を行う。

4. ホスト ID を用いた通信の検証

4.1 提案されている手法

キャリア内ネットワークからインターネットへ転送されるパケットに、ホスト ID と呼ばれる識別子を付与することによって、インターネットからキャリア内ホストを識別する方法が複数提案されている [4]。ホスト ID を付与する場所の案は、アプリケーションメッセージや TCP オプション、IP オプションなどがある。しかし、IP 層より上位の層でホスト ID を埋め込むものは、そのプロトコルを用いた通信でしか用いることが出来ない。例えば、TCP ヘッダのオプションにホスト ID を埋め込む方法が提案されている。しかし、この方法だけでは UDP を用いた通信の際に、キャリア内ホストを識別する事が出来ない。そのため、汎用的にホスト ID を使うためには、IP ヘッダにホスト ID を埋め込む必要がある。

4.2 IP オプションを用いたホスト ID の付与

IP ヘッダにホスト ID を付与するために、IP オプションを用いる方法がある。図 3 は IP ヘッダへホスト ID を埋め込むための、オプションフィールドの構造である。Type フィールドは、IP オプションの種類を示す。ホスト ID オプションは、Type が正式に定義されていない。既に RFC に定義されている IP オプションの Type を用いた場合、検証において誤った結果となる原因となる可能性がある。そのため、本検証では RFC で定義されていない Type 番号である 31 をホスト ID の Type と定義した [5] [6] [7] [8] [9] [10] [11]。Length フィールドはオプションの長さを示す。ホスト ID オプションは、可変長のフィールドが存在するため、Length フィールドは一定の値ではない。Num フィールドは多段 NAT が行われた場合に対応するための値である。Reserved フィールドは常に 0 の値が用いられる。IdTyp フィールドはホスト ID がどの形式のアドレスを使用しているのかを示す。ホスト ID は、IPv4 アドレス、IPv6 アドレス、GRE キー、IPv6 フローラベルなどが用いられる。TIdTyp フィールドはトンネル ID がど

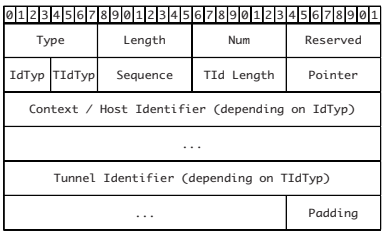

図 3 ホスト ID オプションの構造

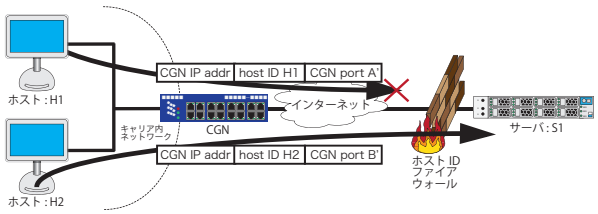

図 4 ホスト ID を用いたフィルタリング機構の動作

のアドレス、ID を利用しているのかを示す。トンネル ID は、IPv4 アドレス、IPv6 アドレス、MPLS VPN ID などが用いられる。Sequence フィールドは、ホスト ID を付与した際に割り当てられる値である。TId Length フィールドは、トンネル ID の長さを示す。pointer フィールドは、ホスト ID、トンネル ID、padding フィールドの長さを足し合わせた値である。Context/Host Idenrifier フィールドはホスト ID が入る。このフィールドは可変長となっている。Tunnel Identifier フィールドは、トンネル ID が入る。このフィールドは可変長となっている。

4.3 ホスト ID を用いたフィルタリング機構

ホスト ID を用いたフィルタリングを行うために、2 つの構成要素から成る機構を設計、実装した。1 つは、キャリア内ネットワークからインターネットへ通信を転送する際に、IP ヘッダにホスト ID を付与する機能を持った CGN である。もう 1 つはホスト ID を基にフィルタリングを行うホスト ID ファイアウォールである。

図 4 はホスト ID を用いたフィルタリング機構の動作についての説明である。キャリア内ネットワークに存在するホスト H1、H2 がサーバ S1 へアクセスを行う。その際 CGN が、キャリア内ネットワークからインターネットへ転送される通信の送信元 IPv4 アドレスを、CGN のインターネット側のインターフェースに付けられた IPv4 アドレスに変換する。この時、CGN は IP オプションにホスト ID を付与する。ホスト ID には、キャリア内ネットワークで用いられていた IPv4 アドレスを用いる。キャリア外サーバにおいて、ホスト ID を参照することによって、キャリア内ホスト H1 と H2 を識別することが可能になると考えられる。

IP オプションを用いたホスト ID は提案段階である。現段階において、ホスト ID を扱うことが可能な製品は存在

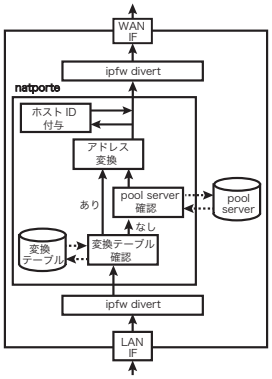

図 5 キャリア内ネットワークからインターネットへパケットの転送を行う natporte の挙動

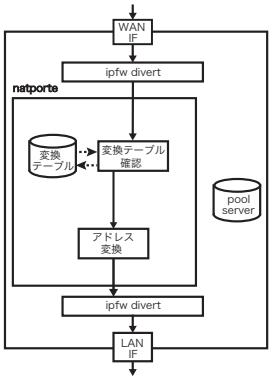

図 6 インターネットからキャリア内ネットワークへパケットの転送を行う natporte の挙動

しない。そこで、ホスト ID を用いたフィルタリング機構の検証を行うために 2 つのソフトウェアを実装した。実装したソフトウェアの詳細を後述する。

4.3.1 natporte

natporte はホスト ID 付与機能を持つソフトウェア CGN である。図 5 は、キャリア内ネットワークからインターネットへパケットの転送を行う natporte の挙動である。キャリア内ネットワークに接続されたインターフェース LAN IF がパケットを受信すると、ipfw の divert socket によって、パケットは natporte プログラムの中へ転送される。転送されたパケットは、中の情報を調べられ、変換テーブルに登録されているのか確認される。登録された情報があった場合、変換テーブルから得た情報を用いて、アドレス変換が行われる。登録された情報がなかった場合、割り当て可能なアドレスとポート番号を pool server に問い合わせる。そして、pool server から得た情報を用いてアドレス変換を行う。この時、変換テーブルに変換の際用いた情報の登録を行なう。ホスト ID の付与機能が有効となっている場合は、IP オプションにホスト ID を付与する。その後、インターネットへ接続されたインターフェース WAN IF から、パケットを送信する。

図 6 は、インターネットからキャリア内ネットワークへパケットの転送を行う natporte の挙動である。WAN IF がパケットを受信すると、ipfw の divert socket によって、パケットは natporte プログラムの中へ転送される。転送されたパケットは、中の情報を調べられ、変換テーブルと比較される。変換テーブルから得た情報を用いて、アドレス変換が行われる。その後、LAN IF から、パケットを送信する。natporte では、TCP、UDP、ICMP を用いた通信に、ホスト ID を付与することが可能である。

4.3.2 natching firewall

natching firewall は、ホスト ID を参照してフィルタリングを行うファイアウォールである。図 7 は、natching firewall の挙動である。インターフェースで受信されたパケットは、ipfw の divert socket によって、natching firewall のプログラムへ引き込まれる。プログラムの中では、受信したパケットのホスト ID と、破棄するホスト ID のリストを比較する。ホスト ID がリストに含まれている場合、プログラムは何もしないことによって、事実上このパケットは破棄される。ホスト ID がリストに含まれていない場合、プログラムはパケットをサーバへ転送する。このような実装により、ホスト ID によるフィルタリングを可能とした。

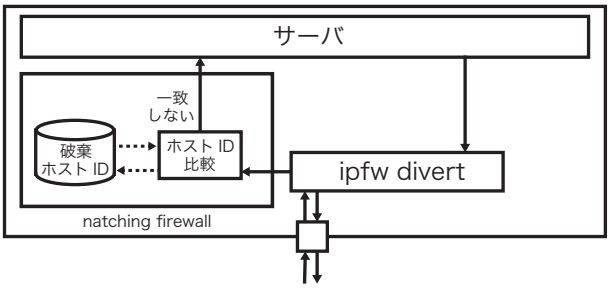

図 7 natching firewall の挙動

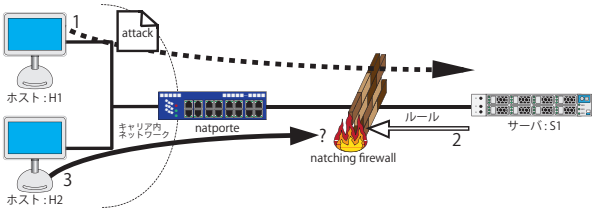

図 8 ホスト ID を用いたフィルタリング機構：検証環境と検証方法

4.4 ホスト ID を用いたフィルタリング機構の検証

4.4.1 ホスト ID を用いたフィルタリング機構の検証環境と検証方法

ホスト ID を用いたフィルタリング機構の検証を行うために、図 8 のような検証環境を用意した。natporte には 3 台のホストを接続した。natporte のキャリア内ホストとして、ホスト H1、H2 を設定した。また、キャリア外サーバとして、サーバ S1 を設定した。破線矢印は攻撃による通信を、実践矢印は正当な通信を、白抜き矢印はフィルタリングルールの追加を表す。

本検証では、UDP echo サーバと、UDP echo クライアントを用いて通信を発生させた。S1 が攻撃パケットを受け取った場合、攻撃パケットと同じホスト ID を持つパケットを破棄するフィルタリングルールを natching firewall に動的に追加するプログラムを作成し、検証に用いた。これは、フィルタリングルールの追加を動的に行うことによって、ヒューマンエラによる検証の失敗を無くすために作成した。本検証において、攻撃を検知することは目的ではない。しかし、どのような通信をフィルタリングするか決定するためには、攻撃がどのようなものであるのか定義しなくてはならない。本検証では、echo データの中身が”*attack*”という文字列を含む通信を攻撃と定義した。

表 2　フィルタリングルール追加後の
ホストから S1 への通信の可否

ホスト	S1 への通信
H1(攻撃者)	×
H2	○

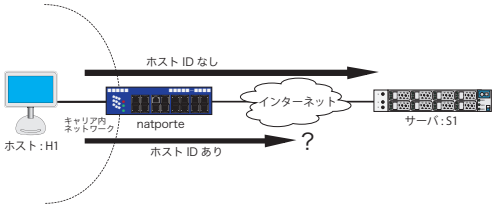

図 9　インターネットにおけるホスト ID の使用:検証環境と検証方法

検証方法は、まず H1 が、S1 へ攻撃を行う。その後、H2 から S1 へアクセスを行い、アクセス可否の確認を行う。

4.4.2　ホスト ID を用いたフィルタリング機構の検証結果と考察

前述した検証環境を用いて、検証を行った。表 2 は、攻撃に対するフィルタリングルール追加後のホストから S1 への通信の可否である。H1 から攻撃を行った場合、H1 から S1 への通信が不可能となり、H2 から S1 への通信は可能であることを確認した。この結果から、キャリア内ホストから攻撃を行った場合、攻撃を行ったホストのみフィルタリングされることを確認した。

CGN でホスト ID を付与することによって、キャリア外サーバから、キャリア内ネットワークにおけるホストの識別が可能となった。これにより、ホスト ID を用いたフィルタリング機構によって、意図したホストのみフィルタリング可能となることが示された。

4.5　インターネットにおけるホスト ID の使用の検証

4.5.1　現状のインターネットにおけるホスト ID の使用

ホスト ID を用いたフィルタリングの検証は、閉じたネットワークで検証を行った。実際のインターネットにおいて、CGN とサーバの間には、複数のルータが存在する。そこで、実際のインターネットにおいて、ホスト ID を付与した通信を行うことで、使用の可否について検証を行った。

4.5.2　インターネットにおけるホスト ID の使用の検証環境と検証方法

インターネットにおけるホスト ID の使用の検証を行うために、図 9 のような検証環境を用意した。natporte には、ホスト H1 を接続し、キャリア内ホストとして設定した。また、本検証において natporte は、北陸先端科学技術大学院大学のネットワークを介してインターネットへ接続した。サーバ S1 として、*www.yahoo.co.jp*、*www.ocn.ne.jp*、*jp.msn.com*、*www.biglobe.ne.jp* などのインターネット上で一般的に利用されている web サーバを利用した。実線矢印は、HTTP の get 通信である。

表 3　web サーバへの通信の可否

S1	ホスト ID 無効	ホスト ID 有効
www.biglobe.ne.jp	○	○
www.yahoo.co.jp	○	×
www.ocn.ne.jp	○	×
jp.msn.com	○	×

natporte は、ホスト ID 付与機能の有効、無効を切り替えることが可能である。まず natporte を、ホスト ID 付与機能無効と設定する。H1 は telnet を用いて、S1 と通信を行う。これにより、正常に通信が行えることを確認する。次に natporte を、ホスト ID 付与機能有効と設定する。H1 は telnet を用いて S1 に接続し、それによって通信の可否を確認を行う。

4.5.3　インターネットにおけるホスト ID の使用の検証結果と考察

前述した検証環境を用いて、検証を行った。表 3 は、各 web サーバへの通信の可否である。natporte のホスト ID 付与機能を無効にした場合、全ての Web サーバと正常な通信が可能であった。次に、ホスト ID 付与機能を有効にした場合、正常な通信が行えたのは *www.biglobe.ne.jp* のみであった。*www.yahoo.co.jp*、*www.ocn.ne.jp*、*jp.msn.com* との通信は不可能であった。

ホスト ID が付与されたパケットによる通信が不可能となる理由として、途中経路のルータによって、ホスト ID 付きのパケットが破棄された可能性が考えられる。その可能性を調査するために、traceroute を用いて経路を調べた。その結果、dix-ie や JPIX を経由した場合、ホスト ID が付与された通信が破棄されていることが外部観測によって判明した。この結果より、ホスト ID が付与された通信は、途中経路のルータにおいて破棄される場合が存在することが言える。

途中経路に存在するルータは、RFC の定義にそぐわないパケットを発見した場合、そのパケットを破棄する設定がなされている場合がある。これは、セキュリティ上の観点から投入される設定である。ホスト ID オプションは、RFC において正式に定義されておらず、また、Type フィールドの値に関しては、本稿で定義したものである。そのため、ルータにおいて RFC の定義にそぐわないパケットを見なされ、破棄されたと考えられる。

5.　今後の展望

ホスト ID を用いたフィルタリング機構を用いることによって、キャリア内ホストごとのフィルタリングが可能となることを検証によって示した。しかし、ホスト ID は一般的に用いられている IP オプションではないため、途中経路のルータで破棄されてしまう可能性がある。そのためホスト ID は、現状のインターネットでの使用が難しいと言

える。ホスト ID を使用するためには、周知や定義によって、使用可能な環境を整える必要がある。

本検証において、実際に利用する通信の中に識別子を付与した。通信に識別子を付与する方法の他に、問い合わせによって識別子を通知する方法も考えられる。それらの方法についての考察を行い、また検証を行うことによって、実際のインターネットにおいて使用の可否を確認する必要がある。

6. おわりに

CGN を用いた際、インターネット上のサーバにおいて、キャリア内ホストを識別する事が不可能となる。本稿では、これによりインターネット上のサーバにおいて適切なフィルタリングが行えないことを問題として提起した。そこで、CGN において通信にホスト ID と呼ばれる識別子を付与し、インターネット上のサーバで、ホスト ID に基づくフィルタリングを行うことにより、キャリア内ホストごとのフィルタリングが可能となるか検証を行った。また、ホスト ID を用いた通信が実際のインターネットにおいて使用可能であるか検証を行った。検証の結果、ホスト ID を用いることによって、キャリア内ホストを識別し、キャリア内ホストごとのフィルタリングを可能としたことが示された。しかし、現在のインターネットにおいて、IP オプションにホスト ID を付与した通信の使用は困難であることが判明した。なぜなら、RFC において定義されていない IP オプションを持つパケットを、破棄する設定となっているルータが途中経路に存在している可能性があるからである。そのため、ホスト ID を付与したパケットをインターネットで用いた場合、通信できない事例が発生した。ルータにとって未知の IP オプションを用いたパケットは、途中経路で破棄されてしまう可能性があるため、実際のインターネットでの使用は困難であることが判明した。

謝辞

本研究は、総務省による委託研究「IPv4 アドレスの枯渇に伴う情報セキュリティ等の課題への対応に関する実証実験の請負」の一部である。研究に関わった方々に感謝の意を表する。

参考文献

[1] S. Perreault, I. Yamagata, S. Miyakawa, A. Nakagawa, and H. Ashida. Common Requirements for Carrier-Grade NATs (CGNs). RFC 6888 (Best Current Practice), April 2013.

[2] Youming Wu, Hui Ji, Qi Chen, and Tina Tsou. IPv4 Header Option For User Identification In CGN Scenario, March 2011.

[3] K. Egevang and P. Francis. The IP Network Address Translator (NAT). RFC 1631 (Informational), May 1994. Obsoleted by RFC 3022.

[4] Mohammed Boucadair, Joseph Touch, Pierre Levis, and Reinaldo Penno. Analysis of Solution Candidates to Reveal a Host Identifier in Shared Address Deployments, September 2011.

[5] J. Postel. Internet Protocol. RFC 791 (INTERNET STANDARD), September 1981. Updated by RFCs 1349, 2474, 6864.

[6] J.C. Mogul, C.A. Kent, C. Partridge, and K. McCloghrie. IP MTU discovery options. RFC 1063, July 1988. Obsoleted by RFC 1191.

[7] S. Kent. U.S. Department of Defense Security Options for the Internet Protocol. RFC 1108 (Historic), November 1991.

[8] D. Katz. IP Router Alert Option. RFC 2113 (Proposed Standard), February 1997. Updated by RFCs 5350, 6398.

[9] B. Fenner. Experimental Values In IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers. RFC 4727 (Proposed Standard), November 2006.

[10] S. Floyd, M. Allman, A. Jain, and P. Sarolahti. Quick-Start for TCP and IP. RFC 4782 (Experimental), January 2007.

[11] C. Pignataro and F. Gont. Formally Deprecating Some IPv4 Options. RFC 6814 (Proposed Standard), November 2012.