IPv4/IPv6デュアルスタック環境における DNSを用いたIPv6機器発見の手法とその回避策の一考察

曽我 一喜[1]　桝田 秀夫[2]

概要：IPv4 アドレスの在庫の枯渇に伴い，IPv6 導入の動きが活発になり，一つの通信ノードに IPv4 アドレスと IPv6 アドレスの両方が設定される IPv4/IPv6 デュアルスタック環境が一般的になりつつある．そういった環境では，サービス運用の観点などから，一つの FQDN に対して A レコードと AAAA レコードの複数のレコードが対応づけられることが一般的になる．一方，インターネットでは，接続されている脆弱な機器を探索するために，ポートスキャンが広く行われている．IPv4 に比べて膨大なアドレス空間を持つ IPv6 では，接続されている機器を外部から発見することは困難である．本稿では，デュアルスタック環境において，DNS を用いて IPv6 機器を発見しポートスキャン攻撃を可能とする手法とその回避策を考察する．

キーワード：IPv4，IPv6，デュアルスタック，DNS，逆引き

Considerations on Remote Detection of Active IPv6 Addresses under IPv4/IPv6 Dual-stack Environment using DNS

Abstract: With a trigger of the IPv4 address exhaustion, IPv4/IPv6 dual-stack that both IPv4 and IPv6 addresses are set to one communication node will become general. From a viewpoint of the service operation, it becomes general that both A record and AAAA record are associated with one FQDN. On the other side, port-scanning is usually done to detect vulnerable host over the Internet. It is difficult that detection active host in IPv6 networks, because IPv6 provides a significantly larger address space than IPv4. This paper considers remote detection of active IPv6 addresses under IPv4/IPv6 Dual-stack environment using DNS.

Keywords: IPv4,IPv6,Dual-stack,DNS,reverse lookup

1. はじめに

IPv4[1] アドレスの在庫の枯渇に伴い，IPv6[2] 導入の動きが活発になっている．しかし，IPv6 は IPv4 との互換性がないために，IPv4 が広く利用されている現状では，IPv4 と IPv6 を共存させながら段階的に IPv6 への移行が行われている．IPv4 と IPv6 を共存は，一つのデバイスに IPv4 と IPv6 という仕様の異なるプロトコルスタックを両方実装するデュアルスタック方式 [3]，IPv6 専用ノードと IPv4 専用ノードの通信を可能にするアドレス/プロトコル変換方式 [4]，といった方式により実現されている．

また，インターネットに接続された機器は，ネットワーク経由での攻撃に常に晒されている．ポートスキャンをきっかけに攻撃対象を外部から発見する行為は日常的に行われており，問題となっている．さらに IPv4 ネットワークでは，アドレス空間が狭い上アドレスの利用状況が非常に密であることから，IPv4 アドレスの全数探索によってアクティブなホストを発見しようとする手法がよく見られる．それに対し，IPv6 ネットワークではホスト部が下位 64bit 分であることが一般的で，アドレス空間が広い上アドレスの利用状況が非常に疎であるため，同様の手法によってアクティブな IPv6 アドレスを得ることは非常に困難であり，ポートスキャンを受ける可能性は低いと考えられる．

1 京都工芸繊維大学大学院工芸科学研究科情報工学専攻
Graduate School of Information Science，Kyoto Institute of Technology
2 京都工芸繊維大学 情報科学センター
Center for Information Science，Kyoto Institute of Technology

© 2013 Information Processing Society of Japan

しかし，近年の Windows や MacOS X，Linux などの OS では，デュアルスタック方式に対応しているものがほとんどであり，同一のホストに IPv4 アドレスと IPv6 アドレスの両方が割り当てられている状況が当たり前になりつつある．

ネットワーク上のホストが接続要求を受けてコネクションを確立する際，通信相手を確認するために，DNS（Domain Name System）によって，IP アドレスから FQDN（Fully Qualified Domain Name）を問い合わせる逆引きを行い，相手の FQDN に応じたアクセス制限を行うといったことがよく行われている．さらに，得られた FQDN から IP アドレスを問い合わせる正引きを行って，逆引きの情報と対応しているかどうかを確認することも行われている．FQDN の正引きでは，IPv4 アドレスを問い合わせる場合は A レコード，IPv6 アドレスを問い合わせる場合は AAAA レコードを指定し，これらの問い合わせは OS のリゾルバの設定によって，順次行われる．そのため，デュアルスタック方式のホストでは，一つの FQDN に対して，A と AAAA のリソースレコードの両方が割り当てられている．

そこで本稿では，デュアルスタック方式と DNS サービスとの連携により IPv6 機器を発見しポートスキャン攻撃を可能とする手法とその回避策を考察する．

2. ポートスキャンについて

2.1 ポートスキャンの概要

TCP/IP を利用したネットワーク通信では，IP アドレスにより通信相手となるホストを指定する．そのホスト上で動作している複数のネットワークを利用するアプリケーションを指定するためには，0〜65535 までのポート番号が使われる．ポートとはアプリケーションが使用する仮想的な接続口であり，それぞれのサービスの種類によって，アプリケーションが使用するポート番号は基本的に指定されている．

ポートスキャンとは，対象ホストのコネクション確立要求を受け付けるポート番号を見つ出す行為である．最も簡単な方法は，対象ホストの全ポートに対して，接続要求を行う．また，各 IP アドレスごとにアプリケーションがよく使用するポート番号に接続要求を送信し，アクティブなホストを見つけ出す行為が同時に行われることもある．

2.2 IPv4 でのポートスキャン

IPv4 ネットワークでは，IPv4 のアドレス空間が全体でも 2^{32}（= 約 43 億）個と狭いこと，IPv4 アドレスの利用状況が非常に密であることから，IPv4 アドレスの全数探索によってアクティブなホストを発見しようとする手法がよく見られる．

2.3 IPv6 でのポートスキャン

IPv6 ネットワークでは，IPv6 のアドレス空間が 2^{128}（= 約 340 澗）個と非常に広いこと，ホスト部が下位 64bit 分であることが一般的で，アドレスの利用状況が非常に疎であることから，IPv4 ネットワークでの手法と同様の手法によってアクティブな IPv6 アドレスを得ることは非常に困難であり，ポートスキャンを受ける可能性は低いと考えられる．

仮に，100Mbps の速度で 512byte/ホストでスキャンパケットを送出するとすれば，約 6 時間ですべての IPv4 アドレスに対する送信が完了できるが，IPv6 アドレスの場合，単一のサブネット (/64) の中だけだとしても約 280 万年ほどかかることになる．

3. 発見手法

アクティブな IPv6 アドレスの発見手法について述べる．

3.1 既知の発見手法

文献 [5] では，以下のような発見手法が述べられている．

3.1.1 アドレスの推測

IPv6 アドレスの下位 64bit に覚えやすいアドレスや，サービスのポート番号をそのまま使ったアドレスは推測されやすい．（::10,::53 など）また，MAC アドレスから IPv6 アドレスを生成している場合，NIC のベンダ ID を調べれば探索範囲を狭められる．

3.1.2 不正 RA による発見

IPv6 で追加されたステートレスアドレス自動設定の際に，攻撃者が不正な RA (Router Advertisement) を送出することで通信の内容を盗聴でき，アクティブな IPv6 アドレスを発見できる．この手法は攻撃者が既にローカルネットに侵入していることが前提となっている．

3.2 提案する発見手法

IPv4/IPv6 デュアルスタック環境では一つの FQDN に対して A レコードと AAAA レコードの両方が割り当てられていることが一般的である．そこで，デュアルスタック方式と DNS との連携により，IPv6 機器を発見する手法を述べる．（図 1）

手順 1. IPv4 ネットワークでアクティブな IPv4 アドレスを探索する．

手順 2. 手順 1 で見つけた IPv4 アドレスで逆引きを行い，そのアドレスに対する FQDN を得る．

手順 3. 手順 2 で得た FQDN で正引きを行い，その FQDN に対する IPv6 アドレスを得る．

手順 4. 手順 3 で得た IPv6 アドレスに対して，ポートスキャンを実行する．

© 2013 Information Processing Society of Japan

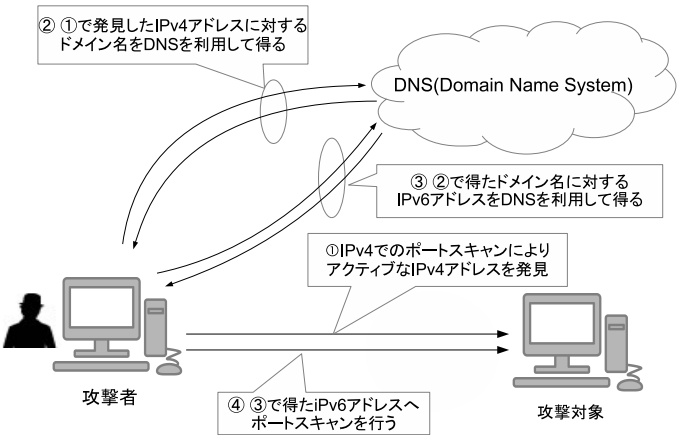

図 1　発見手法

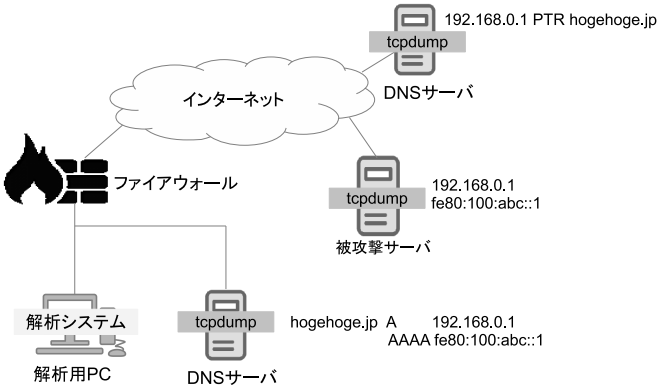

図 2　観測環境

表 1　inetd で待ち受けている主なポート

ポート番号	サービス名
21	ftp
23	telnet
80	http
445	Microsoft-DS
1433	MSSQL server
3306	MySQL database system
3389	Windows Based Terminal server
5900	VNC remote desktop protocol

4.　観測環境

3.2 章で述べた発見手法が実際に存在しているかを確認するための観測方法について述べる．図 2 は観測環境の概要である．

被攻撃サーバ

故意に攻撃を受けるサーバである．IPv4 アドレスと IPv6 アドレスの両方を持つ．IPv4 のポートスキャンでよく攻撃されるポートへのアクセスには，接続だけを行い，一定時間後にタイムアウトするスクリプトを inetd で稼働させている．表 1 に inetd で待ち受けている主なポートを示す．

DNS サーバ

被攻撃サーバのアドレスに対応した FQDN を解決するサーバである．ネットワークの環境上，正引きと逆引きに応答するサーバは別々である．

被攻撃サーバ，DNS サーバそれぞれで tcpdump を行う．DNS サーバの tcpdump のログから 3.2 章で述べた動作の DNS クエリを抜き出し，その後に被攻撃サーバへ攻撃がないかを，被攻撃サーバの tcpdump のログから調べる．

5.　回避策の検討

3.2 章で述べた手法でアクティブな IPv6 アドレスが発見されたときに，攻撃を回避する方法を検討する．

5.1　回避策に対する要求

回避策に対しては，以下のような要求が考えられる．

要求 1　攻撃を回避できること

IPv6 機器を発見された際に，攻撃を回避できる．または，IPv6 機器を発見されないことが求められる．

要求 2　容易に導入できること

不特定多数の利用者が IPv6 機器を利用すると考えると，IPv6 機器の管理者側だけで導入できる技術が求められる．

要求 3　通常の使用に影響がないこと

回避策の導入により，使用できなくなったり，使用に制限がかかるサービスなどが無いことが求められる．

5.2　関連研究

文献 [6] では，Mobile IPv6 を応用した回避策が提案されている．この回避策が 5.1 節の要求を満たすか考察すると以下のようになる．

要求 1 に関して

要求 1 は満たす．

要求 2 に関して

クライアントの Mobile IPv6 への対応が必須であるため，要求を満たさない．

要求 3 に関して

この論文の中でも述べられているように，通信の遅延が大きいことが問題であるため，要求を満たさない．

このように要求 2 と要求 3 に関しては問題があり，特に要求 3 に関しての問題はサービスの運用という観点から考えた場合，小さくない問題であると考えられる．そこで次節では，他の IPv6 技術を使った回避策について検討する．

© 2013 Information Processing Society of Japan

5.3 提案する回避策

IPv6 の技術を利用し，回避策を提案する．

5.3.1 IPv6 Privacy Extensions の利用

ステートレスアドレス自動設定 [7] では，IPv6 アドレスの上位 64bit はルータから取得し，インタフェース ID と呼ばれる下位 64bit はホスト自身で生成する．インタフェース ID は一意であるため，このアドレスを使用しているとホストを容易に特定されてしまう．そこで，IPv6 Privacy Extensions[8] では，インタフェース ID をランダムに決定してアドレスを生成し，それらの有効期間を短くすることでアドレスから特定のホストを特定される危険性を減らす．

要求 1 に関して

一定期間毎にアドレスを変更できるため，通常の攻撃は回避できると考えられる．しかし，既に確立された接続は変更前のアドレスで通信するため，一度接続してアドレスを得た攻撃者は，そのアドレスを使用して攻撃を継続できるという問題がある．

要求 2 に関して

要求 2 は満たしていると考えられる．ただ，DNS の設定は Dynamic DNS[9] などを利用して，対応する必要がある．

要求 3 に関して

導入することによって，通常の使用に影響が出ることはない．よって，要求 3 は満たす．

5.3.2 DHCPv6 の利用

IPv4 での DHCP と同様に，IPv6 にも DHCPv6[10] が用意されている．アドレスのリースタイムを短くすることで，定期的にアドレスの変更が可能となる．

要求 1 に関して

アドレスの衝突や DHCP で割り振るアドレスの数によっては有効な回避策にならないことが問題であり，要求 1 を満たしているとは言えない．

要求 2 に関して

要求 2 は満たしていると考えられる． 5.3.1 と同様，DNS の設定は Dynamic DNS などを利用して，対応する必要がある．

要求 3 に関して

要求 3 は満たす．

6. 考察

3.2 章で述べた発見手法による攻撃は，2013 年 6 月から観測を開始しているが今のところ観測されていない．

回避策としては， 5.1 節の要求 1 を満たすことが最重要だと考えられるが， 5.3.1 項で挙げた方法は，要求 1 に対して問題を抱えている．しかし，全く満たさないという訳ではなく，サービス運用の観点から重要だと考えられる要求 2 と要求 3 は満たすため，これらの方法とパケットフィルタなどでの防御を行うのが，現状では最も好ましいと考えられる． 5.3.2 項で挙げた方法は，要求 1 に関する問題が大きいため，他の技術との連携や応用などを考えなければならない．

7. まとめ

本稿では，デュアルスタック環境において，DNS を利用することでアクティブな IPv6 アドレスを発見する方法を提案し，その回避策について検討した．今後は，さらに有効な回避策を考えるとともに，IPv6 ネットワーク上での攻撃の動向に注目していきたい．

参考文献

[1] RFC 791, Internet Protocol, http://www. ietf. org/rfc/rfc791. txt
[2] RFC 2460, Internet Protocol , Version 6 (IPv6)Specification, http://www. ietf. org/rfc/rfc2460. txt
[3] RFC 4241, A Model of IPv6/IPv4 Dual Stack Internet Access Service, http://www. ietf. org/rfc/rfc4241. txt
[4] RFC 3142, An IPv6-to-IPv4 Transport Relay Translator, http://www. ietf. org/rfc/rfc3142. txt
[5] Convery and D. Miller: IPv6 and IPv4 Threat Comparison and Best-PracticeEvaluation (v1.0), 2004, http://www.seanconvery.com/v6-v4-threats.pdf
[6] 日下貴義，角将高，馬場達也，稲田勉: Mobile IPv6 技術を応用した輻輳型 DoS 攻撃回避方式の提案，情報処理学会， 研究報告コンピュータセキュリティ (CSEC), 2004-CSEC-26(17), pp. 105-112, 2004.
[7] RFC 2462, IPv6 Stateless Address Autoconfiguration, http://www. ietf. org/rfc/rfc2462. txt
[8] RFC 3041, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, http://www. ietf. org/rfc/rfc3041. txt
[9] RFC 2136, Dynamic Updates in the Domain Name System (DNS UPDATE), http://tools. ietf. org/html/rfc2136
[10] RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), http://tools. ietf. org/html/rfc3315

© 2013 Information Processing Society of Japan