2012年度 修士論文

IPv6アドレス割り当てポリシーの観測に基づく脅威予測とその対策

提出日：2013年2月1日

指導：後藤滋樹教授

早稲田大学 基幹理工学研究科 情報理工学専攻
学籍番号：5111B063-6

髙田 雄太

目次

図一覧

表一覧

第 1 章

序論

1.1 研究の背景

Internet Protocol version 4 (IPv4) アドレスの枯渇が問題となっている．2011 年 2 月 3 日，インターネット上で利用されるアドレス資源をグローバルに管理する IANA (Internet Assigned Numbers Authority) において，新規に割り振りできる IPv4 アドレスが無くなった [1].

この問題への対応策の一つとして，Internet Protocol version 6 (IPv6) アドレスへの移行が挙げられる．IPv6 は，IPv4 よりも大きなアドレス空間を使用できるように設計されており，IPv4 アドレス枯渇問題を抜本的に解決する案として考案された．典型的なサブネットとして 64 ビット，すなわち 2 の 64 乗 (約 1800 京) の範囲をホストが利用でき，IPv4 サブネットと比べて実際に利用するホストの密度が大幅に低下する．

この広大なアドレス空間のため，IP アドレスを用いてインターネット上のホストを探索するホストスキャンは困難になった．しかし，ホストへの IPv6 アドレス配布や運用方法には一定の規則 (ポリシー) が存在するため，使用する IPv6 アドレスに偏りが生じ，実際には IPv6 アドレスの空間である 128 ビットよりも小さなアドレス空間しか用いられていない問題が存在する [8, 9, 22].

ホストスキャンで感染先を探索するワームは，感染ホストの IP アドレスから同じサブネット内の数値的 (トポロジ的) に近いホストから順に，または遠隔のネットワークに対してランダムに感染拡大していく [10, 11]．ワームによる IPv6 ネットワークへのスキャンは IPv4 と比べて減少傾向にあるが，いずれ IPv6 ネットワークにおいてもインテリジェントにスキャンする方法が確立される恐れがある．また，IPv6 アドレスのネットワークへの導入においては，組織や団体によっては既に運用レベルにあるところや，試行錯誤中の実験レベルにあるところが

あり，IPv6 ネットワークの対応状況は様々である．未だに脆弱な状態にある IPv6 ネットワークも存在しており，セキュアな IPv6 導入を保証するための対策を講じる必要がある．

1.2　研究の目的

本研究は，IPv6 パケットを観測して分析することで，IPv6 アドレス割り当てポリシーの存在を明らかにし，各ポリシーの特徴を示す．その結果を活用することで，新たに考えられる脅威を予測し，IPv6 アドレス割り当てのベストプラクティスを導く．提案するベストプラクティスを導入することで，本来外部に公開していないはずのサーバホストやクライアントホストに対するホストスキャンを緩和することができる．本研究において使用した実地データは，APAN (Asia Pacific Advanced Network) において IPv6 パケットをキャプチャしたデータを用いた．

1.3　論文の構成

本論文は以下の章により構成される．

第 1 章 序論

本論文の概要について述べる．

第 2 章 IPv6

IPv6 を紹介する．

第 3 章 IPv6 アドレス割り当て方法

IPv6 アドレスをホストに割り当てる方法を説明する．

第 4 章 ホストスキャン

IP アドレスを用いてホスト探索するホストスキャンを解説する．

第 5 章 観測実験

IPv6 アドレス割り当てポリシーの調査を目的とした観測実験とその結果の考察を行う．

第 6 章 脅威と対策

観測実験の結果を受けて，新たに考えられる脅威とその対策について述べる．

第 7 章 結論

本論文の結論を述べるとともに，残された課題を示す．

第 2 章

IPv6

2.1 IPv4アドレス枯渇問題とIPv6アドレスへの移行

Internet Protocol version 4 (IPv4) アドレスの枯渇が問題となっている．2011 年 2 月 3 日にインターネット上で利用されるアドレス資源をグローバルに管理する IANA において，新規に割り振りできる IPv4 アドレスが無くなった [1]．IPv4 アドレスを割り振れなくなると，新規サービス事業者の参入や個人ユーザのインターネットへの新規加入ができなくなり，インターネットの普及や拡大が停止してしまう．

この問題への対応策として，以下の 3 つが挙げられる．

- IPv4 アドレスの効率的な利用
- IPv4 アドレスの移転／売買
- IPv6 アドレスへの移行

1 つ目の IPv4 アドレスの効率的な利用は，LAN 内のノードにはプライベート IP アドレスを割り当て，インターネットに接続するときだけグローバル IP アドレスを使用することができる NAT (Network Address Translation) を活用したり，更に ISP (Internet Service Provider) が NAT を採用する CGN (Carrier Grade NAT) を活用したりする方法である．しかし，NAT には 1 つのグローバル IP アドレスに対して張ることができる TCP セッション数に上限がある問題や多段 NAT によってアプリケーションに支障を来す問題がある．

2 つ目の IPv4 アドレスの移転／売買は，使用していないアドレスブロックを回収して再利用したり，IP アドレスブロックを売買することで IP アドレスを取得したりする方法である．

また，今まで事実上許可されていなかった[1]ARIN の IPv4 アドレスの APNIC への移転という RIR (Regional Internet Registry) を越えた IPv4 アドレス移転が実現した [2].

上記 2 つの対応策は，比較的着手が容易であるものの効果は限定的であり，いずれ IP アドレスが不足するのは容易に予測できる．一方，3 つ目の IPv6 アドレスへの移行は、IPv4 アドレスよりも大きなアドレス空間を使用できるように設計されており，IPv4 アドレス枯渇問題を抜本的に解決する案として考案された．32 ビットのアドレス空間から 128 ビットのアドレス空間になり，アドレス数は約 43 億から約 340 澗 (澗=10^{36}) に増えた．IPv6 は，恒久的な対応策といえる一方で，コストが掛かるとともに，普及が不十分であるという問題を抱えている．しかし，2012 年 6 月 6 日には世界中で恒久的かつ商用に IPv6 アドレスの使用を推進する World IPv6 Launch [3] が行われ，Web サービス事業者やプロバイダ (ISP)，ホームルータベンダによる積極的な IPv6 アドレスの普及活動が行なわれているため，IPv6 アドレスの普及は時間の問題である．

[1]IPv4 アドレスは，世界 5 地域 (北米地域: ARIN, 欧州・中東・中央アジア地域: RIPE NCC, アジア・太平洋地域: APNIC, ラテンアメリカ地域: LACNIC, アフリカ地域: AfriNIC) を代表する RIR に分けられて管理されており，これまで RIR を跨いだ IPv4 アドレス移転は事実上許可されていなかった．2011 年に APNIC が，RIR を越えた IPv4 アドレス移転についてのポリシーを承認したが，他地域で同様のポリシーが存在しなかったため，RIR を越えた IPv4 アドレス移転はできなかった．

2.2　IPv6 と IPv4 の比較

IPv6 と IPv4 の仕様の比較を表 2.1 に示す．

表 2.1: IPv6 と IPv4 の比較

	IPv6	**IPv4**
アドレス空間	128 ビット	32 ビット
典型的なサブネット	64 ビット	8 ビット
アドレス表記	コロン (e.g. 2001:db8::1234:5678:90ab:cdef)	ドット (e.g. 192.168.0.1)
パケットヘッダ	固定 40 バイト	20 バイト＋α (可変)
アドレス割り当て	NIC ごとに複数 IP アドレスを 割り当て可能	NIC ごとに単一 IP アドレスのみを 割り当て可能[2]
拡張ヘッダ	あり	なし
中継ノードフラグメント	なし	あり
NAT	なし (エンドツーエンドを想定)	あり
アドレスの自動生成	DHCPv6, ICMPv6 RA	DHCP
アドレス形式	ユニキャスト，マルチキャスト， エニーキャスト	ユニキャスト，マルチキャスト， エニーキャスト，ブロードキャスト

大きな違いは，アドレス空間の他に，エンドツーエンド通信の実現のため NAT の導入を想定していない点や，NIC ごとに複数の IP アドレスを割り当てられる点，アドレスの自動生成に DHCPv6 に加え，ICMPv6 による生成機能 (後述) がある点が挙げられる．

2.3　アドレス表記

アドレス長が 128 ビットある IPv6 アドレスは，16 ビットずつ 8 つに区切ってそれぞれを 16 進数で表記し，コロンで (:) 区切る．例えば次のようになる．

2001:0db8:0000:0000:1234:5678:90ab:cdef

しかし，IPv4 と比べ表記が長くなりがちなので，IPv6 には圧縮表記が用意されている．例えば，16 ビット区切りの中で，先につく 0 は省略することができる．上記の例は次のようになる．

[2]IPv4 においても 1 つの NIC に複数 IP アドレスを割り当てることは可能だが，一般的に単一 IP アドレスのみを割り当てる．

2001:db8:0:0:1234:5678:90ab:cdef

16 ビット区切りが連続して 0 である場合，これをコロン 2 つ (::) で置き換えることができる．この形式を用いると，上記のアドレスは次のようになる．

2001:db8::1234:5678:90ab:cdef

しかし，連続コロンはアドレス内の 1 箇所でしか用いることができない．

2.4　プレフィックス表記

IPv6 におけるプレフィックスは，IPv4 のクラスレスドメイン間経路制御 (Classless InterDomain Routing: CIDR) と非常に似ており，表 2.2 に示すように，IPv6 アドレスの上位ビットはサブネットや特定のアドレスタイプを表している．これをグローバルルーティングプレフィックスという．プレフィックス表記は，IPv6 アドレス末尾にスラッシュ (/) とプレフィックスのビット長を数字で付け加えて書かれる．現在割り当てられている予約済みのプレフィックス，リンクローカルアドレスやマルチキャストアドレス等の特殊なアドレスを表 2.2 に示す．

表 2.2: 割り当て済みプレフィックス

種別	プレフィックス	アドレス空間の割合
予約済み	::0/8	1/256
グローバルユニキャスト	2000::/3	1/8
ユニークローカルユニキャスト	FC00::/7	
プライベートな管理用	FD00::/8	
リンクローカルユニキャスト	FE80::/10	1/1024
マルチキャスト	FF00::/8	1/256

その他，表 2.2 に示されていないアドレスの範囲は，現時点ではすべて予約済みか未割り当てになっている．最新の割り当て状況は，IANA のページ [4] で公開されている．

2.5　グローバルユニキャストアドレス

全インターネットで一意な IPv6 アドレスを，グローバルユニキャストアドレスという．グローバルユニキャストアドレスのプレフィックスは，2000::/3 と決まっている．また，グローバルユニキャストアドレス空間の割り当ては，IANA のページ [5] で公開されている．グローバルユニキャストアドレスのフォーマットを図 2.1 に示す．

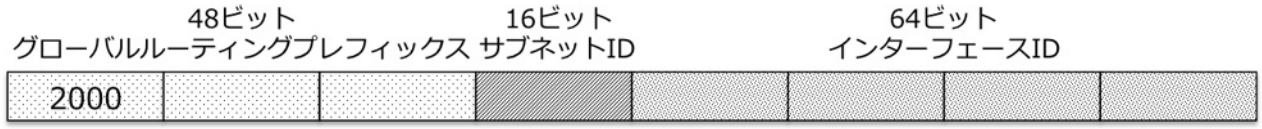

図 2.1: グローバルユニキャストアドレスのフォーマット

グローバルルーティングプレフィックスは，サイトに割り当てられたアドレス範囲を識別する．これは RIR もしくは ISP が割り当てるようになっており，階層的な構造を持っている．サイトは通常 RIR や ISP から /48 プレフィックスが割り当てられ，サイト管理者は 65536 個のサブネットを作成することができる．サブネット ID は，サイト内の 65536 個のリンクを識別する．インターフェース ID は，サブネット上のインターフェースを識別するもので，サブネット内で一意でなければならない[3]．

[3] グローバルルーティングプレフィックスとサブネット ID をあわせてサブネットプレフィックスといい，1 ビット刻みで設定可能だが，一般的に 64 ビット長のプレフィックスを使用するため，本研究では /64 プレフィックスと 64 ビットのインターフェース ID を扱う．

第 3 章

IPv6 アドレス割り当て方法

ホストへの IPv6 アドレスの割り当て方法には，自動設定による割り当てと手動設定による割り当てが存在しており，一定の規則に基づき割り当てられるアドレスが存在することが知られている．本章では，IPv6 アドレスの割り当て方法について述べる．

3.1 IPv6 アドレス上位 64 ビット

IPv6 アドレスの上位 64 ビットは，2.5 節で記述したように階層的に管理されている．サイトの管理者は，割り当てられた/48 プレフィックスからサブネット ID を決定し，最終的に/64 プレフィックスを RA (Router Advertisement) メッセージ (ICMPv6 によるメッセージ) でホストに通知する．RA メッセージは，ルータから定期的に全ノードマルチキャストアドレス宛に，もしくはホスト側から RS (Router Solicitation) メッセージを受けた際に送信される．IPv4 では，アドレスの自動設定に必要な情報を主に DHCP を使用して取得するが，IPv6 ではその情報を RA メッセージから取得する．RA メッセージに含まれる情報として，プレフィックスの他，デフォルトゲートウェイや MTU などがある．

3.2 IPv6 アドレス下位 64 ビット

IPv6 アドレスの下位 64 ビットは，インターフェース ID と呼ばれる同一サブネット上でインターフェースを特定できる識別子である．インターフェース ID の設定には，ホストによる自動設定もしくはユーザによる手動設定が存在する．

3.2.1　SLAAC によるアドレス

インターフェース ID を自動で設定する方法の一つに，EUI-64 (Extended Universal Identifier) フォーマット [6] と呼ばれるホストの MAC アドレスを用いてインターフェース ID を生成する方法がある．EUI-64 は， IEEE (Institute of Electrical and Electronics Engineers) が定めた一意な識別子で，48 ビットの MAC アドレスの先頭から 7 ビット目のビットの補数を取った後，上位 24 ビットと下位 24 ビットに分け，その間に “FFFE” を挿入することで，64 ビットのインターフェース ID とする．EUI-64 フォーマットに従ったインターフェース ID の生成を図 3.1 に示す．

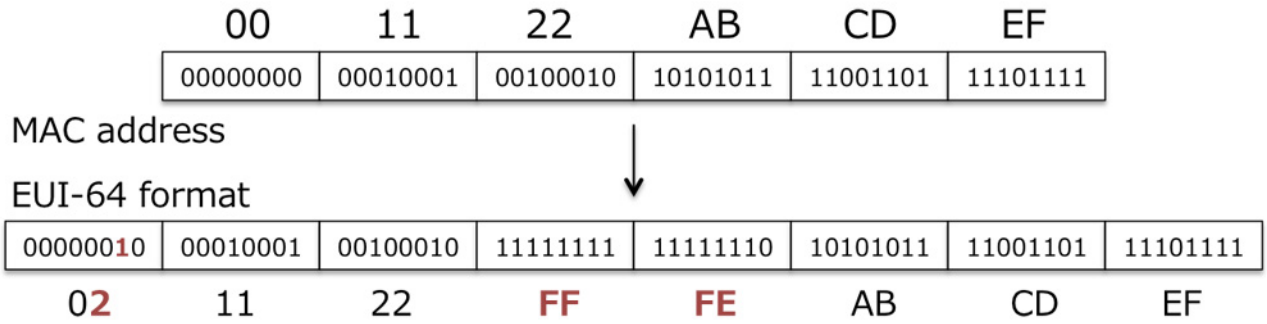

図 3.1: EUI-64 フォーマットに従ったインターフェース ID の生成

ホストは，RA で /64 プレフィックス情報を取得した後，生成したインターフェース ID と組み合わせることでグローバルユニキャストアドレスとする．これを SLAAC (Stateless Address Auto Configuration) [14] という．SLAAC によるアドレスは，リンク上にルータが存在しており，RA による SLAAC がオンである場合，自動的にホストに割り当てられる．SLAAC による IPv6 アドレスの割り当てを図 3.2 に示す．

図 3.2: SLAAC による IPv6 アドレスの割り当て

しかし，SLAAC によるアドレスは下位 64 ビットにインターフェース固有の識別子である

MAC アドレスを用いているため，個人のインターネットアクセスを追跡 (トラッキング) できてしまう問題が存在する．

3.2.2　プライバシーアドレス

SLAAC による IPv6 アドレスのトラッキング問題を解決するため考えられたインターフェース ID の自動設定方法として，プライバシーアドレス [15, 21] がある．プライバシーアドレスは，インターフェース ID の生成に MAC アドレスを使用せず，短い一定期間 (1 時間から 1 日) で使い捨てるランダムな値を生成し，インターフェース ID として使用する．Web サーバや FTP サーバのようなサーバ側のホストには，一意に定まる固定したアドレスが必要であるが，ブラウザや FTP クライアントを利用するようなクライアント側のホストでは，同じアドレスは必ずしも必要ではないため，プライバシーアドレスを用いることができる．

3.2.3　その他のアドレス

SLAAC およびプライバシーアドレスは自動設定による割り当て方法だが，手動設定によるアドレス割り当て方法 [8, 9] も存在する．これは一定の規則に基づいた割り当て方法であり，典型的な IPv6 サブネットのアドレス空間 64 ビットよりも小さいアドレス空間であることがわかる．SLAAC およびプライバシーアドレスを含めた IPv6 アドレス下位 64 ビットの割り当て方法とそれぞれのアドレス空間を表 3.1 に示す．

表 3.1: IPv6 アドレス下位 64 ビットの割り当て方法

	割り当て方法	割り合て例	アドレス空間
自動設定	MAC アドレスを用いたアドレス (SLAAC)	2001:db8::1234:56ff:fe78:90ab	OUI[1]を固定すると 2^{24}
	プライバシーアドレス (Privacy)	2001:db8::1f9a:a208:394b:2b7e	2^{64}
手動設定	下位 64 ビットに IPv4 アドレスを用いたアドレス (IPv4-based)	2001:db8::192:168:0:1	2^{32}
	末尾 16 ビットを除くすべてにゼロを用いた省略記法のアドレス (Low-byte)	2001:db8::1	2^{16}
	上記以外の手動で設定したアドレス (Manual)	2001:db8::db8:db8	2^{64}

[1]OUI (Organizationally Unique Identifier) とは，IEEE によってネットワーク製品の製造者に割り当てられる MAC アドレス上位 24 ビットのこと．

Low-byte は，IPv6 アドレスの下位 16 ビットのみを使用した圧縮表記を利用した一番アドレス空間が小さくなる割り当て方法である．IPv4-based は，IPv6 アドレスの下位 64 ビット (16 ビット区切りを 4 つ使用) に IPv4 アドレスを用いる割り当て方法である．上記以外の割り当て方法のアドレスを，DHCPv6 によって自動的に割り当てられた，もしくはユーザによって手動で割り当てられたと考え，Manual に分類した．

その他，下位 64 ビットだけでなく上位 64 ビットも含めたアドレス空間におけるアドレス割り当て方法として，beef や dead といった単語や 1111 といった連続値を使用したアドレス (Wordy) や移行技術や共存技術を利用する際に割り当てられるアドレス (6to4 [16], ISATAP [17], Teredo [18]) が挙げられる．また，表 3.1 の割り当て方法はそれぞれ独立した方法だが，Wordy および 6to4 については，表 3.1 の割り当て方法と重複して出現する可能性[2]がある．

[2]例えば，2001:db8::beef は，Low-byte および Wordy となり，プレフィックスが 2002::/16 の IPv6 アドレスは，6to4 を利用しているため，2002:db8::1111 は，6to4, Low-byte そして Wordy となる．

第 4 章

ホストスキャン

本章では，IP アドレスを用いてネットワーク上のホストを探索するホストスキャンとその対策について記述する．

4.1 ホストスキャン

一般的な管理下にあるホストの存在を確認する方法は，対象ホストの IP アドレスを用いて ICMP エコー要求 (ping コマンド) を送信し，ICMP エコー応答を確認する方法がある．この方法を悪用し，管理下にないホストの存在を IP アドレスを増加させながら ICMP エコー要求を送信することで確認する方法をホストスキャンといい，攻撃目標や踏み台とするホストを探索するために行われる．

ホストスキャンによって存在が確認されたホストに対しては，次にポートスキャンによる実行されているサービスの確認が行われる．ポートスキャンによって実行されているサービスの確認が行われた後，そのサービスに対する脆弱性を悪用した攻撃が実施され不正アクセスにつながる．

ホストスキャンが有効な理由は，対象とするネットワークが決まっている場合，非常に短い時間で行うことができるからである．IPv4 では IP アドレスのアドレス空間は 32 ビットであり，典型的な IPv4 サブネットのアドレス空間は 8 ビットであるため，IPv4 サブネットのホスト密度は高い．サブネット内の全ホストを対象としても ping コマンドの試行回数は，2^8 の 256 回で済む．すなわち，1 秒 1 試行だとすると 5 分以内に終了する．一方，IPv6 では IP アドレスのアドレス空間は 128 ビットであり，典型的な IPv6 サブネットのアドレス空間は 64 ビットであるため，IPv6 サブネットのホスト密度は非常に低い．サブネット内の全ホストを対象と

すると ping コマンドの試行回数は，2^{64} の約 1800 京 (京=10^{16}) 回と現実時間では終わらない回数になる．従って，IPv6 ネットワークへのホストスキャンは実質的に不可能とされてきた．しかし，3 章で記述したように，IPv6 アドレスにはアドレスの割り当て方法が存在することが知られており，実際には 64 ビットよりも小さいアドレス空間内の IP アドレスが割り当てられているため，必ずしも IPv6 ホストスキャンは不可能とは言い切れない [9]．

4.2　ホストスキャンへの対策

ホストスキャンやポートスキャンは，攻撃や感染の前兆であることは間違いないが，それらを完全に検知し防御するのは非常に難しい．しかし，スキャンを完全に防御するのではなく，緩和する対策としては，FW (Firewall) によるフィルタリングや不要なサービスの停止が挙げられる．その他，IDS/IPS といったセキュリティアプライアンスを導入することで，しきい値を超える通信量の検知や，通信パターンを分析し，不審な通信パターンを検出する方法がある．

しかし，上記の対策は一般的に従来の IPv4 ネットワークにおいて施されているもので，IPv6 ネットワークに対しては FW の設定忘れや設定不足により，フィルタリングが行われていなかったり，既存のセキュリティアプライアンスが IPv6 に対応していなかったりといった現状がある．本研究は，IPv6 におけるホストスキャンに対する検討を行う．

第 5 章

ポリシーの観測

本章では，IPv6 パケットを観測することで IPv6 アドレスの割り当て方法の存在確認とその割り当て方法に特徴がないか，ネットワークによって割り当て方法にポリシーがないか調査し，得た結果を基に考察する．

5.1 観測実験の概要

5.1.1 観測方法

本研究では，APAN (Asia Pacific Advanced Network) の観測点にて 2012 年 7 月 16 日から 2012 年 10 月 15 日までの 3ヶ月間，送信元ポートもしくは宛先ポートに 25, 53, 80 が利用されている通信を対象に IPv6 パケットの先頭 96 バイトを tcpdump [25] を用いてキャプチャした．

5.1.2 観測データ

5.1.1 項で取得したデータから IPv6 アドレスを抽出し，表 5.1 に示した正規表現を用いて割り当て方法の分類を行った．同時にポート番号も抽出し，IPv6 アドレスと関連付けて保存した．また，備考にある各割り当て方法における特徴的な値も抽出した．

正規表現で機械的に分類したため，手動で設定したアドレスであっても SLAAC や Privacy に分類されたり，自動で設定したアドレスであっても偶然 Word が生成され，Wordy に分類されたりする可能性がある．また，本研究はグローバルネットワークにおける観測であるため，表 2.2 におけるグローバルユニキャストのプレフィックス (2000::/3) を含む IPv6 アドレスのみを対象とした．

表 5.1: IPv6 アドレス割り当て方法の分類

割り当て方法	正規表現	備考
SLAAC	ff:fe[0-9a-f]{2}:[0-9a-f]{0,4}$	別途 OUI を抽出した
Privacy	:[0-9a-f]{2,4}:[0-9a-f]{3,4}:[0-9a-f]{3,4}:[0-9a-f]{3,4}$:[0-9a-f]{3,4}:[0-9a-f]{2,4}:[0-9a-f]{3,4}:[0-9a-f]{3,4}$:[0-9a-f]{3,4}:[0-9a-f]{3,4}:[0-9a-f]{2,4}:[0-9a-f]{3,4}$:[0-9a-f]{3,4}:[0-9a-f]{3,4}:[0-9a-f]{3,4}:[0-9a-f]{2,4}$	一箇所のみ 2 桁を許容した
Low-byte	::([0-9a-f]{1,4})$	別途 Low-byte の値を抽出した
IPv4-based	((:(\d|\d\d|1\d\d|2[0-4]\d|25[0-5])){4})$	
Wordy	add, beef, cafe, dead, face, 0000, 1111, aaaa, ffff 等	
6to4	^2002((:[0-9a-f]{1,4}){2})	
Teredo	^2000	
ISATAP	:5efe((:[0-9a-f]{1,4}){2})$	
Manual	上記以外	

観測期間中に観測した IPv6 アドレスの概要を表 5.2 に示す.

表 5.2: 観測データ概要

すべての IPv6 アドレス数	5,183,962
ユニーク IPv6 アドレス数	2,788,288
ユニーク /64 プレフィックス数	296,866
whois 情報未登録ユニーク /64 プレフィックス数	53,936

本研究では，IPv6 アドレスを管理している AS を調べるため，whois コマンドを利用した．whois サーバは，“whois.radb.net” を使い，複数の whois 情報を取得できた場合[1]は、一番最初の情報を採用した．“whois.radb.net” に whois 情報が登録されていなかった場合は，更に “whois.apnic.net” に対しても whois コマンドを試みて，それでも未登録であった場合は “UNKNOWN（not allocated）” とした．表 5.2 からは，20% 弱が whois 情報未登録であったことがわかる.

[1]例えば，6to4 のプレフィックス 2002::/16 は，複数の whois 情報が取得できる.

5.2　観測結果

5.2.1　IPv6 アドレス数の遷移

3ヶ月を 6 つの半月の期間に分け，期間ごとに観測した/64 プレフィックスの累積とユニーク IPv6 アドレスの数をそれぞれ図 5.1，図 5.2 に示す．ユニークな IPv6 アドレスは半月の期間ごとにカウントした．つまり同じアドレスが異なる半月に出現する場合には，それぞれの半月の期間において 1 つのアドレスとなる．

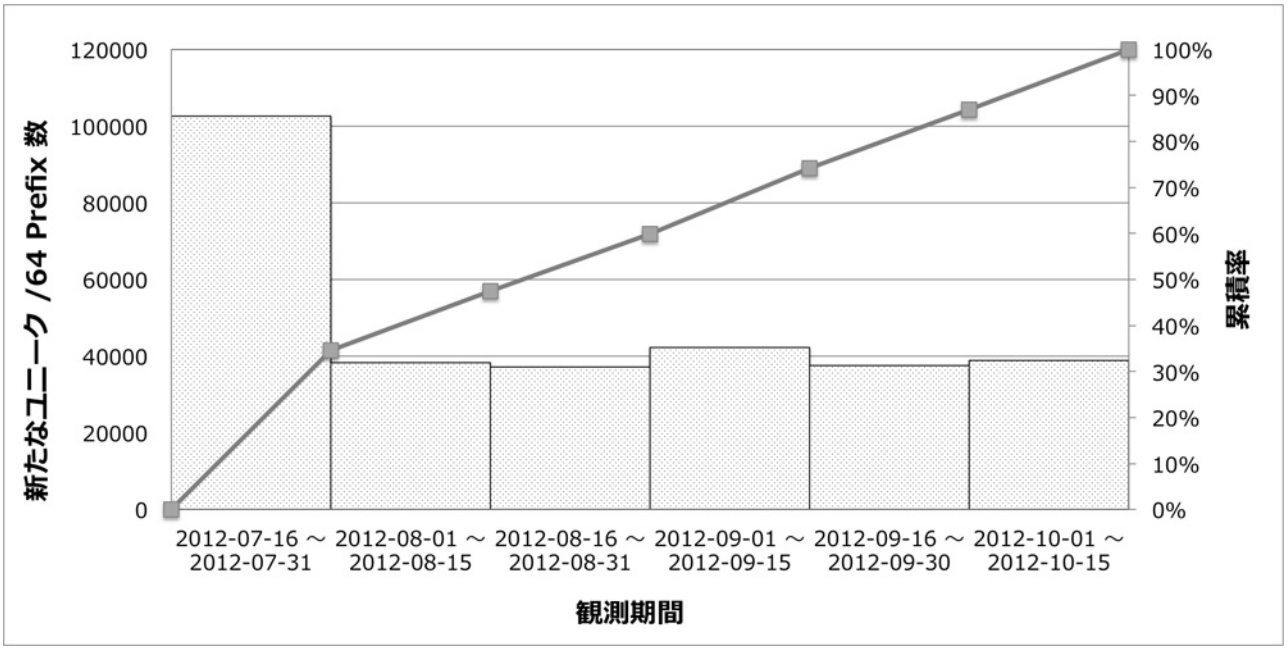

図 5.1: 半月ごとの/64 プレフィックス数の累積

図 5.1 から，/64 プレフィックスは時間が経過するにつれ種類および数は増加し，平均して半月に約 40,000 個のユニーク/64 プレフィックスを観測したことがわかる．

また，図 5.2 からは，観測期間中どの半月においても，約 40 万〜60 万個のユニーク IPv6 アドレスを観測し，ユニークアドレス数をすべてのアドレス数で割ったアドレスのユニーク率は 50% を超えていた．

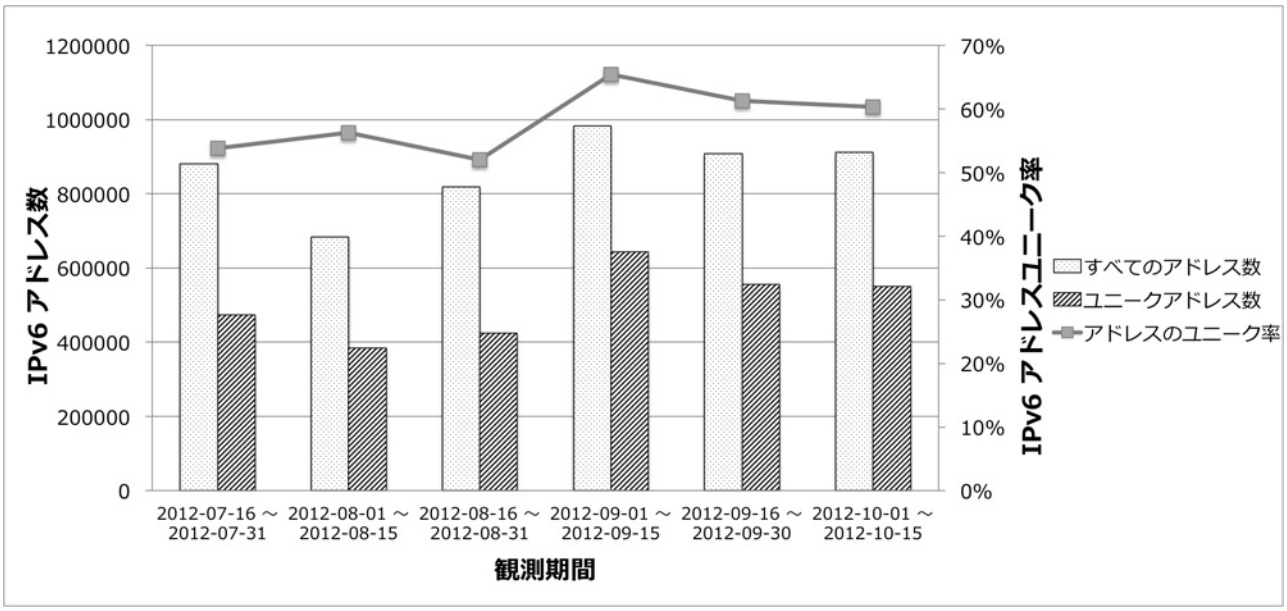

図 5.2: 半月ごとのユニーク IPv6 アドレスの遷移

5.2.2　IPv6 アドレス割り当て方法

観測期間を通して観測した IPv6 アドレスの割り当て方法の割合を表 5.3 に示す.

表 5.3: 観測期間中の IPv6 アドレス割り当て方法の割合

割り当て方法	個数	割合 [%]
Privacy	2,436,929	87.40
6to4	233,577	8.38
Manual	171,663	6.16
SLAAC	67,961	2.44
Low-byte	61,350	2.20
Wordy	52,542	1.88
ISATAP	47,310	1.70
IPv4-based	3,075	0.11

Privacy の割合が 90% 弱を占めており，Manual の割合は 6%，SLAAC, Low-byte の割合は 2% 強であった.

次に，半月ごとに観測した IPv6 アドレスの割り当て方法の割合を図 5.3 に示す.

図 5.3 から，観測期間中どの半月においても，IPv6 アドレス割り当て方法の割合に大きな変動はないことがわかる．また，表 5.3 と図 5.3 を比べて，表 5.3 の方が Privacy の割合が高く，その他の割り当て方法の割合は低い．その原因は，半月ごとの観測では、期間をまたいだ

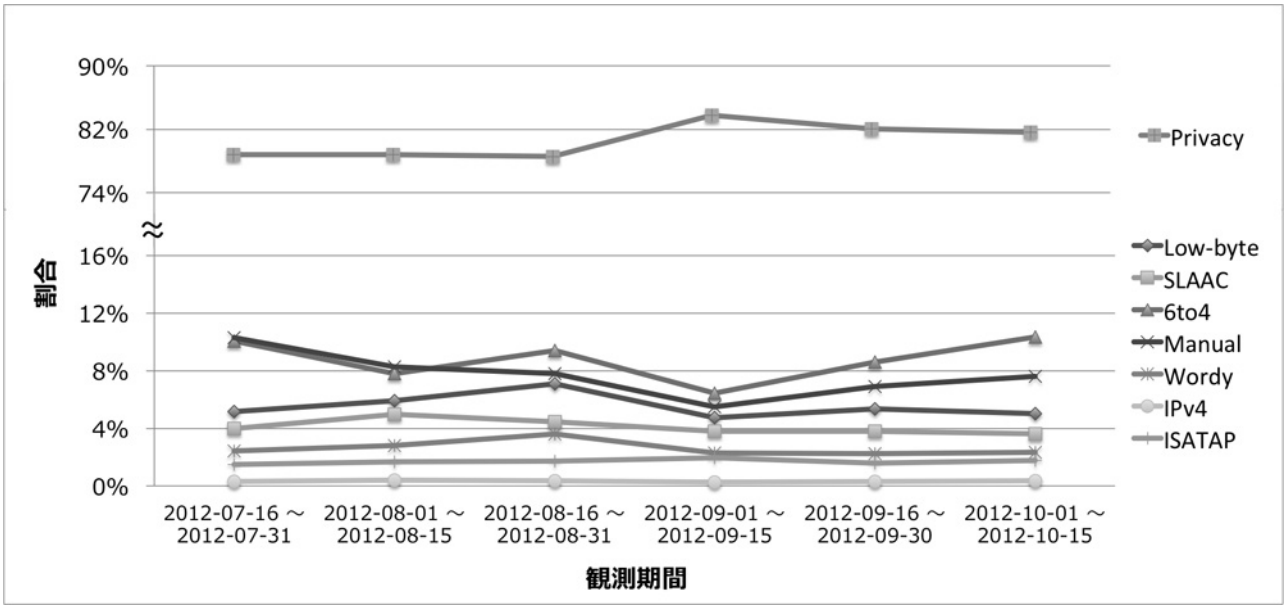

図 5.3: 半月ごとの IPv6 アドレス割り当て方法の割合

IPv6 アドレスの重複を許容したからである．Privacy は一定期間が経過するとアドレスが更新されるので重複せず，割合が上がり，Privacy 以外の割り当て方法は，IPv6 アドレスが変化しないため，重複して割合が下がったと考えられる．

5.2.3　ポートごとの IPv6 アドレス割り当てポリシー

ポートごとに観測したユニーク IPv6 アドレス数を表 5.4 に，ポートごとの IPv6 アドレス割り当て方法の割合を図 5.4 に示す．eph25, eph53, eph80 はそれぞれ，ポート 25 と通信しているポート，ポート 53 と通信しているポート，ポート 80 と通信しているポートを表す．

表 5.4: ポートごとに観測したユニーク IPv6 アドレス数

ポート	個数	割合 [%]
25	1,050	0.04
53	17,127	0.61
80	51,725	1.85
eph25	1,623	0.06
eph53	144,065	5.14
eph80	2,587,439	92.31

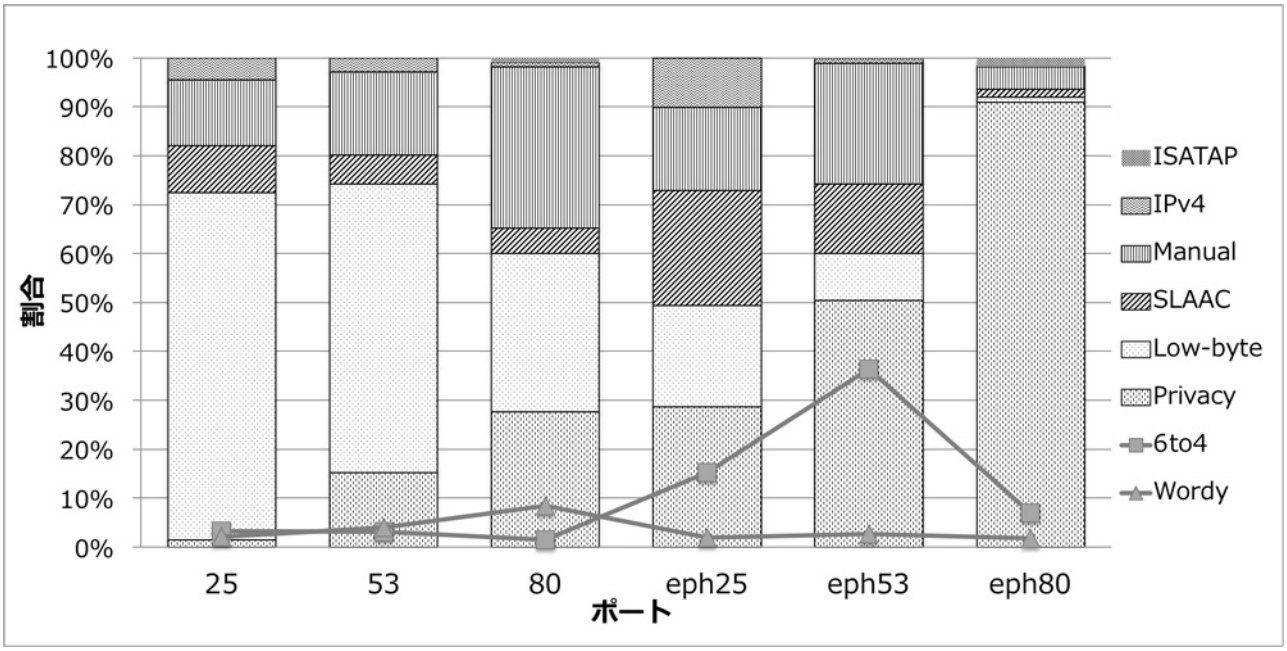

図 5.4: ポートごとの IPv6 アドレス割り当て方法の割合

表 5.4 から，90 % 以上の IPv6 アドレスが，eph80 で観測されていることがわかる．すなわち，主に IPv6 アドレスは，ユーザがブラウザを用いて Web 通信を行うために利用されていると考えられる．

図 5.4 からは，25, 53, 80 は Low-byte や Manual が 60% 以上を占め，eph25, eph53 は，Low-byte の割合は下がり，Privacy や SLAAC の割合が上がっていることがわかる．eph80 は，Privacy が 90% を占めており，ブラウザを利用したユーザの IPv6 アドレスはほとんど Privacy であることがわかる．

表 5.4 と図 5.4 の二つの結果から，Privacy の一定期間にアドレスが更新される性質を考慮すると，eph80 の IPv6 アドレスに Privacy が多く採用されたことにより，eph80 のユニーク IPv6 アドレス数が 90% 以上を占めたと考えられる．一方で，80, eph53 のように Privacy の割合は高いのにも関わらず，eph80 ほどユニーク IPv6 アドレスを観測できなかったのは，5.1.2 項で記述したように，手動で設定したアドレスであっても Privacy に分類された可能性があるからである．80, eph53 は，Manual の割合が比較的高いことからも，本来 Manual であるアドレスを Privacy と誤って分類した可能性がある．

5.2.4　AS ごとの IPv6 アドレス割り当てポリシー

表 5.3 で多くの割合を占めた Privacy, Manual, SLAAC, Low-byte を軸に，AS ごとに割合を計算した結果を図 5.5 に示す．

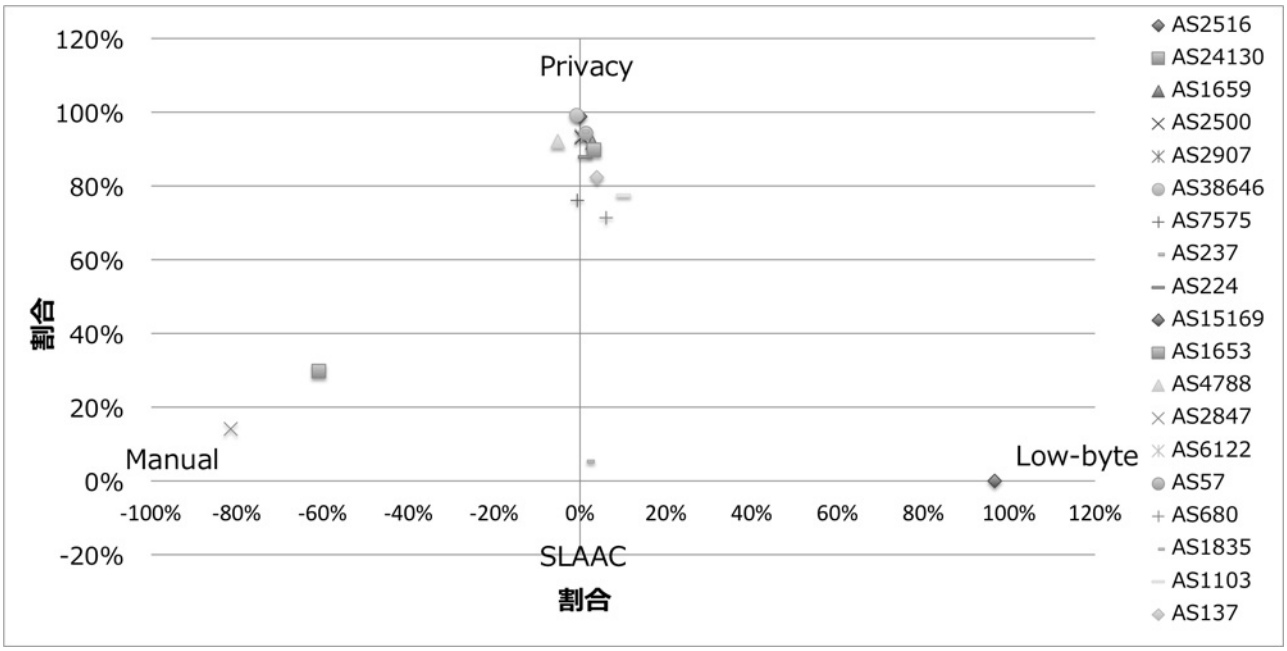

図 5.5: AS ごとの IPv6 アドレスの割り当て方法の割合

図 5.5 からは，ほとんどの AS が Privacy による割り当てポリシーを採用している一方で，中には Manual, SLAAC, Low-byte による割り当てポリシーを採用している AS も存在していることがわかる．

5.2.5　IPv6 アドレス割り当て方法の特徴

Low-byte, SLAAC, Wordy における特徴を集計した結果をそれぞれ表 5.5, 5.6, 5.7 に示す．

表 5.5: Low-byte における値の割合

Low-byte	個数	割合 [%]
1	7,522	12.26
2	6,150	10.02
3	1,187	1.93
10	884	1.44
4	702	1.14

表 5.6: SLAAC における OUI の割合

OUI	個数	割合 [%]
C80AA9	2,029	2.99
000C29	1,729	2.54
003048	1,617	2.38
005056	1,588	2.34
002590	1,230	1.81

表 5.7: Wordy における Word の割合

Word	個数	割合 [%]
ffff	24,101	45.87
1ce	6,844	13.03
add	5,349	10.18
dad	5,022	9.56
bed	3,992	7.60

Low-byte で使用されている値としては，1 および 2 が多い．SLAAC で使用されている MAC アドレスの OUI には偏りが見られなかった．Wordy で使用されている Word は，“ffff” が半分近く占めている．これは，“ffff” を含むプレフィックスを用いた IPv6 アドレスが多く存在したからである．

5.3　既存研究

本研究と同様，IPv6 アドレス割り当て方法を観測した研究 [13] が存在する．2008 年 4 月時点での IPv6 アドレス割り当て方法の割合を，表 5.8, 5.9 として示している．しかし，本研究は World IPv6 Launch によって様々な組織や企業が IPv6 アドレスの商用を開始した，より実運用に近い環境での観測結果を示しており，IPv6 アドレスの割り当て方法から考えられる脅威と対策を提案しているため新規性があると考えている．実際に，表 5.8, 5.9 の結果は，Privacy の割合が 10% 未満だが，本研究の結果は，表 5.3 にあるように Privacy が 90% 弱と大きく異なった．

表 5.8: ホストの IPv6 アドレス割り当て方法

割り当て方法	割合 [%]
SLAAC	50
IPv4-based	20
Teredo	10
Low-byte	8
Privacy	6
Wordy	＜ 1
Others	＜ 1

表 5.9: ルータの IPv6 アドレス割り当て方法

割り当て方法	割合 [%]
Low-byte	70
IPv4-based	5
SLAAC	1
Wordy	＜ 1
Privacy	＜ 1
Teredo	＜ 1
Others	＜ 1

IPv6 ネットワークにおけるインテリジェントワームの感染拡大を解析した研究 [10, 11] では，ワームが IPv6 ネットワークにも対応していることを示しているが，感染拡大対象はローカルネットワークにおける IPv6 アドレスであり，本研究のようにグローバルネットワークにおける IPv6 アドレスの特定方法ではない．

その他，DNS の AAAA レコードを用いたワームの感染拡大をシミュレートした研究 [12] や P2P アプリケーションにおけるトラッカーでの IPv6 アドレス収集，サーバログからの IPv6 アドレス収集を指摘した研究 [10] があるが，本研究では特別なリソースを用いず IPv6 アドレス割り当てポリシーから IPv6 アドレスを特定できることを指摘している．

また，IPv6 ネットワークに対応したホストスキャンツール [26, 28, 27] が存在する．これらのツールは，指定した IPv6 アドレスに対して高速なスキャンを実現するツールであり，広大な IPv6 アドレス空間をより小さくすることで効率的にスキャンするヒューリスティックな手法はサポートしていない．

最後に，上記研究を踏まえ，IPv6 ホストスキャンの可能性についてまとめた IETF Internet-draft [9] が存在する．具体的な IPv6 アドレスの収集方法や IPv6 ホストスキャンの方法ついて述べているが，IPv6 アドレスの割り当て方法の割合データとして表 5.8, 5.9 を利用していることに加え，本研究のように実際に観測や実験は行っていない．

第 6 章

脅威と対策

本章では，観測結果から考えられる脅威を述べるとともに，その脅威を緩和する対策を考案する．

6.1 脅威

6.1.1 ポートや AS の割り当てポリシーを利用したホストスキャン

観測結果から，ポートごとにアドレス割り当てポリシーが存在することがわかった．

ポート 25, 53, 80

ウェルノウンポートを使用しているホストは公開サーバホストであると予想でき，Low-byte によるアドレスが比較的多く，Low-byte の値は ::1, ::2 が多い．すなわち，人間が覚えやすいアドレスを使用していることがわかる．

ポート eph25, eph53

SMTP サーバおよび DNS キャッシュサーバといったサーバホストであると予想でき，SLAAC によるアドレス，プライバシーアドレスが比較的多い．

ポート eph80

ブラウザを使用しているクライアントホストであると予想でき，プライバシーアドレスが多い．

上記のポリシーに従って，簡易なホストスキャンシミュレーションを行った．スキャン対象とする IPv6 アドレスは，観測データとする．ホストスキャンシミュレーションの際に使用す

る /64 プレフィックスは，Alexa top sites の接続性をチェックしているページ [23] から IPv6 アドレスを取得し，そこから圧縮表記にならない/64 プレフィックスのみを利用した．ページ内において，Date が “2012-10-15_0001” の “valid AAAA records” から抽出した結果，2,839 個の /64 プレフィックスを得た．抽出した /64 プレフィックスを用いて，::1, ::2 を含めた::ffff までの値を範囲とした Low-byte，表 5.6 の 5 つの OUI を含む SLAAC，そして Privacy を観測データから抽出し，その数をヒット数とした．ヒット率は，ヒット数をスキャンの試行回数 (表 3.1 のアドレス空間) で割った値である．

ホストスキャンのシミュレーション結果を表 6.1 に示す．

表 6.1: ホストスキャンのシミュレーション結果

割り当て方法	ヒット数	ヒット率
Low-byte	2,690	$2690/2^{16} = 4.10 \times 10^{-2}$
SLAAC	1,079	$1079/(5 \times 2^{24}) = 1.29 \times 10^{-5}$
Privacy	4,340	$4340/2^{64} = 2.35 \times 10^{-16}$

Privacy は，IPv6 の典型的なサブネットのアドレス空間 64 ビットに対するスキャンと同等であるが，ヒット率が非常に低いことに加え，一定期間にインターフェース ID が更新されるため，プライバシーアドレスへのスキャンは非現実的であることがわかる．

Privacy と比較して，Low-byte や SLAAC のヒット率は高く，スキャンは現実的であることがわかる．SLAAC においては，明確に機能をオフにしないと自動設定によりアドレスが割り当てられるため，プライバシーアドレスで外部と通信していたとしても，SLAAC によるアドレスも割り当てられてしまう．本研究では観測データを用いたため，外部と通信している際に使用される IPv6 アドレスのみがスキャン対象だが，潜在的に割り当てられている SLAAC によるアドレスを考慮すると，ヒット率は多少上がると考えられる．

6.1.2　連鎖的な IPv6 アドレスの特定

観測結果から，AS ごとにアドレス割り当てポリシーが存在することがわかった．任意の AS において， Low-byte や SLAAC による割り当てポリシーに従い，連続する値をアドレスに割り当てると，1 つアドレスが特定された際に、AS 内の他のアドレスも芋づる式に特定される可能性がある．アドレス特定への戦略を立てやすくなり，意図して外部に公開していないホストが攻撃される恐れがある．

しかし，外部からは AS ごとにどういった割り当てポリシーを採用しているか容易には分からない．割り当てポリシーの特定は，ある程度のスキャンが必要であるため，6.2 節の対策を講じることで防ぐことができる．

6.2　対策

6.2.1　IPv6 アドレス割り当てのベストプラクティス

ホストの利用目的に応じて，IPv6 アドレスを次のように適切に割り当てることが推奨される．公開サーバホストに対しては，人間が覚えやすい Low-byte によるアドレスを割り当てる．非公開サーバホストに対しては，SLAAC によるアドレスをオフにし，複雑なアドレスを手動で固定設定する．クライアントホストには，SLAAC によるアドレスをオフにし，プライバシーアドレスを割り当てる．

SLAAC によるアドレスをオフする方法には，ルータ側で SLAAC によるアドレス配布をオフにする，もしくはホスト側で SLAAC をオフにする方法がある．IPv6 では一つの NIC に複数の IP アドレスを割り当てることができるため，プライバシーアドレスを使用していても，SLAAC によるアドレスが割り当てられている可能性がある．自動的に割り当てられる SLAAC によるアドレスは，ホストスキャンに対して応答してしまうため注意が必要である．

6.2.2　IPv6 ホストスキャンへの対策

従来の IPv4 ネットワークと同様もしくは修正を加えた対策を IPv6 ネットワークにも施す必要がある．

適切な IPv6 用の FW 設定

IPv6 アドレスは，IPv4 アドレスに比べて表記が長くなりがちなので，FW への設定ミスも多くなる．公開サーバホストに対して人間が覚えやすい Low-byte によるアドレスを割り当てることで，設定ミスは減少すると考えられる．

また，FW の設定においては，IPv4 と同様のセキュリティポリシーでは不適切である．例えば，すべての ICMP パケットを破棄するような設定を行うと，パス MTU 問題[1]と

[1]IPv6 では，中継ノードでパケットをフラグメント化をせず，代わりに送信元が行う．従って，特定の経路が搬送できる最大のサイズでパケットを送信できるよう保証するため，通信の前に経路の MTU を調整する (パス

いった障害が発生してしまう．IPv6 では思わぬ障害につながるため，RFC [20] 等を参考に注意して設定する必要がある．

IPv6 に対応したセキュリティアプライアンスの導入

IPv6 にも対応した IDS/IPS の導入，OSS (Open Source Software)[2] の使用が挙げられる．

MTU 探索) 必要がある．パス MTU 問題とは，ICMPv6 の “packet too big” メッセージをフィルリングされてしまうと，パス MTU 探索が動作しなくなるという問題のことである．

[2]IPv6-Guard, 6Guard 等がある．

第 7 章

結論

7.1　まとめ

本研究では，IPv6 パケットを観測することで，IPv6 アドレス割り当てポリシーの存在を明らかにし，各ポリシーにおける特徴を示した．また，World IPv6 Launch 後，IPv6 アドレスの割り当て方法の割合は大きく変化していることがわかった．これらの観測結果を活用し，考えられる脅威の簡易シミュレーションを行った上で，その対策法を考案した．対策を施すことで，本来外部に公開していないはずのサーバホストやクライアントホストに対するホストスキャンを緩和することが期待できる．これらの対策は，IPv4 と IPv6 のそれぞれの特性を理解した上で施す必要があり，これからベストプラクティスやノウハウを蓄積していく必要がある．

7.2　今後の課題

本研究で残された今後の課題を以下に挙げる．

7.2.1　他ネットワークでの観測

AS ごとに IPv6 アドレス割り当てポリシーが異なったため，APAN 以外のネットワークで観測することで，また異なる特徴を得ることができると期待できる．

7.2.2　実環境でのホストスキャン

本研究では，ホストスキャンの対象として観測データを使用し，シミュレーションによる評価を行った．しかしシミュレーションでは，潜在的に割り当てられているアドレスの存在や，フィルタリングによるスキャンの失敗といった再現することができない要素がある．そういった要素を含め，実際に任意のネットワークを対象にホストスキャンを行うことで，IPv6 アドレス割り当てポリシーに基づくホストスキャンの有効性を示すことができると考えられる．

謝辞

本論文の作成にあたり，日ごろよりご指導をいただいた後藤滋樹教授に深く感謝致します．また，本研究を進めるにあたり，方針や貴重なご助言およびご協力をいただいた NTT ネットワーク基盤技術研究所の森達哉氏に心から感謝申し上げます．そして，通信データ収集に対する助言やともに研究について議論した千葉大紀氏に感謝致します．

最後に，多くの御協力をいただいた後藤研究室の皆様に感謝致します．

参考文献

[1] “IPv4アドレスの在庫枯渇に関して”, JPNIC, http://www.nic.ad.jp/ja/ip/ipv4pool/, Apr. 2011.

[2] “APNIC Processes First Inter-RIR IPv4 Transfer from ARIN,” APNIC, http://www.apnic.net/publications/news/2012/apnic-processes-first-inter-rir-ipv4-transfer-from-arin

[3] World IPv6 Launch, http://www.worldipv6launch.org/

[4] “Internet Protocol Version 6 Address Space,” IANA, http://www.iana.org/assignments/ipv6-address-space/, Aug. 2012.

[5] “IPv6 Global Unicast Address Assignments,” IANA, http://www.iana.org/assignments/ipv6-unicast-address-assignments/, Oct. 2012.

[6] “Guidelines for 64-bit Global Identifier (EUI-64) Registration Authority,” IEEE, http://standards.ieee.org/regauth/oui/tutorials/EUI64.html, Mar. 1997.

[7] “IPv6 技術検証協議会 セキュリティ評価・対策検証部会 最終報告書 概要編,” IPv6 技術検証協議会 セキュリティ評価・検証部会, http://ipv6tvc.org/documents/20121023Report.pdf, 参照 Oct. 23 2012.

[8] F. Gont, “Analysis: Vast IPv6 address space actually enables IPv6 attacks,” SerchSecurity, http://searchsecurity.techtarget.com/tip/Analysis-Vast-IPv6-address-space-actually-enables-IPv6-attacks, 参照 Jun. 15 2012.

[9] F. Gont, T. Chown, “Network Reconnaissance in IPv6 Networks,” Internet-Draft IETF, http://tools.ietf.org/html/draft-ietf-opsec-ipv6-host-scanning-00, Dec. 2012.

[10] S. Bellovin, B. Cheswick and A. Keromytis, “worm propagation strategies in an IPv6 Internet,” USENIX ;login:, pp.70–76, Feb. 2006.

[11] T. Liu, X. Guan, Q. Zheng, and Y. Qu, “A New Worm Exploiting IPv6 and IPv4-IPv6 Dual-Stack Networks: Experiment, Modeling, Simulation, and Defense,” IEEE Network, pp.22–29, Sep. 2009.

[12] A. Kamra, H. Feng, V. Misra and A.D. Keromytis, “The Effect of DNS Delays on Worm Propagation in an IPv6 Internet,” INFOCOM 2005, Mar. 2005.

[13] D. Malone, “Observations of IPv6 Addresses,” PAM2008, Apr. 2008.

[14] S. Thomson, T. Narten, “IPv6 Stateless Address Autoconfiguration,” IETF RFC2462, http://www.ietf.org/rfc/rfc2462.txt, Dec. 1998

[15] R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” IETF RFC3041, http://www.ietf.org/rfc/rfc3041.txt, Jan. 2001.

[16] B. Carpenter, “Connection of IPv6 Domains via IPv4 Clouds,” IETF RFC3056, http://www.ietf.org/rfc/rfc3056, Feb. 2001.

[17] F. Templin, T. Gleeson, M. Talwar, D. Thaler, “Intra-Site Automatic Tunnel Addressing Protocol (ISATAP),” IETF RFC4241, http://www.ietf.org/rfc/rfc4214, Oct. 2005.

[18] C. Huitema, “Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs),” IETF RFC4380, http://www.ietf.org/rfc/rfc4380, Feb. 2006.

[19] S. Thomson, T. Narten, T. Jinmei, “IPv6 Stateless Address Autoconfiguration,” IETF, http://www.ietf.org/rfc/rfc4862.txt, Sep. 2007.

[20] E. Davies, J. Mohacsi, “Recommendations for Filtering ICMPv6 Messages in Firewalls,” IETF RFC4890, http://www.ietf.org/rfc/rfc4869.txt, May 2007.

[21] T. Narten, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6,” IETF RFC4941, http://www.ietf.org/rfc/rfc4941.txt, Sep. 2007.

[22] T. Chown, “IPv6 Implications for Network Scanning,” IETF RFC5157, http://www.ietf.org/rfc/rfc5157.txt, Mar. 2008.

[23] D. Wing, “AAAA and IPv6 connectivity statistics,” employees.org, http://www.employees.org/~dwing/aaaa-stats/, 参照 Oct. 20 2012.

[24] S. Hagen, 市原 英也, 豊沢 聡, “IPv6 エッセンシャルズ 第 2 版,” オライリー・ジャパン, Jun. 2007.

[25] tcpdump,
http://www.tcpdump.org/

[26] G. Lyon, Nmap6,
http://nmap.org/6/

[27] CAIDA, scamper,
http://www.caida.org/tools/measurement/scamper/

[28] V. Hauser, THC-IPV6,
http://thc.org/thc-ipv6/

[29] phamvantoan, IPv6-Guard,
http://code.google.com/p/ipv6-guard/

[30] X. Weilin, 6Guard: a honeypot-based IPv6 attack detector,
http://www.honeynet.org/node/944

付録

IPv6 アドレス割り当て方法の分類における正規表現

表 5.1 の各割り当て方法における正規表現の説明を記述する．

SLAAC

88 ビット〜104 ビット目に “ff:fe” が使用されている IPv6 アドレス．

Privacy

下位 64 ビットの各 16 ビット区切りに，3〜4 桁の 0〜9，a〜f を使用した IPv6 アドレス．ランダム値生成の際に，偶然 0 が 2 回続き省略された場合を考慮し，16 ビット区切りの内一箇所のみ 2 桁を許容した．

Low-byte

末尾 16 ビット区切りのみに 1〜4 桁の 0〜9，a〜f を使用した IPv6 アドレス

IPv4-based

下位 64 ビットの各 16 ビット区切りに，1〜3 桁の 1〜255 を使用した IPv6 アドレス

Wordy

add, beef, cafe, dead, face, 0000, 1111, aaaa, ffff 等を含む IPv6 アドレス

6to4

プレフィックスが，2002:IPV4:ADDR::/48 である IPv6 アドレス．

Teredo

プレフィックスが，2000::/32 である IPv6 アドレス．

ISATAP

5efe:IPV4:ADDR で終わる IPv6 アドレス．