IPv6 インターネットを攻撃経路とするセキュリティ問題についての一考察

須藤　年章†

†インターネットマルチフィード株式会社
100-0004　東京都千代田区大手町 1-5-1 大手町ファーストスクエア　イーストタワー2F
sudo@mfeed.ad.jp

あらまし 2011年4月,日本を含めアジア太平洋地域では通常の申請により割り振り可能であるIPv4アドレスの在庫がなくなる「IPv4アドレス枯渇」となった.それに伴い様々なサービスでIPv6対応がすすみ,一般ユーザー向けアクセスラインサービスでもIPv6アドレスが標準で利用可能になるなどIPv6を利用できる通信環境が整備されはじめている.このようなインターネット環境の変化は,フィッシング,スパムやマルウェア感染などのセキュリティ問題へも影響を与える.本稿では,IPv6インターネットを攻撃経路とする攻撃データとMWS2011 DATAset[2]の攻撃通信データの関連性を分析し,IPv6網を利用した攻撃の現状と今後の影響について解析する.

Consideration of security problem to assume the IPv6 Internet to be attack route

Toshiaki Sudoh†

†Internet Mulifeed Corporation
OTEMACHI 1st.SQUARE EAST TOWER ,2F 1-5-1,Otemachi,Chiyoda-ku,Tokyo 100-0004,Japan
sudo@mfeed.ad.jp

Abstract It became ″IPv4 address dryness″ in which the IPv4 address that was able to be the allotment became out of stock by usual application in Asia Pacific region including Japan in April, 2011. The communication environment under which IPv6 can be used as it becomes possible for the IPv6 correspondence to proceed by various services along with it, and to use the IPv6 address by the standard even in the access line service for the average user begins to be maintained. The change in such an electronic environment influences the security problems such as the fishing, spam, and the malware infection. In this text, the relativity of the attack communication data of attack data and MWS2011 DATAset[2] of which the attack route is the IPv6 Internet is analyzed, and the current state of the attack using the IPv6 net and the influence in the future are analyzed.

1　はじめに

IPv4 アドレスの枯渇に伴いそれまで実験的要素が強かったIPv6アドレスを利用した一般ユーザー向けのサービスが展開され始めた.また利用者が気づくことなくIPv6 ネットワークに接続される場合も多いため,多くのセキュリティ問題を生む可能性が高く,対策も困難になる.本稿では,IPv6 インターネットを攻撃経路とする攻撃データとMWS2011 DATAset[2]の攻撃通信データの関連性を分析し,IPv6 網を利用した攻撃の現状と,今後の影響について解析する.

2　インターネット接続環境の変化

インターネットを利用する際にネットワーク上の各端末やネットワーク機器には,個々の機器を識別するために IP アドレスが設定される.現状は IPv4アドレスが一般的であるが,1981 年 9 月に仕様公開後インターネットを利用したサービスの普及による IP アドレスの消費量の急増に伴い CIDR,NAT などの手法により延命策が取られてきたが,2011 年 2 月 3 日にIANA にプールされていた IPv4 アドレスは枯渇し,2011 年 4 月 15 日には,APNIC でも通常の申請により割り当て可能である IPv4 アドレスの在庫がなくなった.IPv4 に替わる IPv6 アドレスは 1995 年から,1998 年にかけて仕様が決められ,1999 年 7 月に IANA による IPv6 アドレスの割り当てが開始されたが,実験的な利用でしか用いられず,ISPによるIPv6を利用した接続サービスは提供されてはいたが,ほとんど普及していない状況だった.

2.1　接続サービス

日本国内では一部の ISP で商用サービス,試験サービスが提供されていたが,2011 年に入り,一般コンシューマユーザー向けのサービス展開が始まり,今後の利用者の拡大が想定される.

2.2　端末環境

各 OS の IPv6 への対応は,1998 年移行 UNIX 系の OS への実装が行われ,2006 年頃には主要な実装は完了している.Windows 系の OS についても 1998 年以降テストが行われており 2001 年に WindowsXP SP1 と WindowsServer 2003 から正式版として対応が行われ,基本機能として実装されている.また近年利用者数が急増している携帯端末類をはじめ多くの装置が IPv6 対応している.

2.3　サービス,コンテンツ

2011 年に入り,接続サービスの IPv6 対応に伴い ISP や企業ホームページの IPv6 対応が進んだが,ほとんどのネットサービスは IPv6 対応は行われていない.一部 IPv6 に対応しているサービスにおいても,IPv6 ネイティブの通信環境ではすべてのサービス,ページで完全なサービスは提供されず,基本的に IPv4,IPv6 のデュアルスタック環境が前提条件となっており,IPv4での通信で補完される必要があるものがほとんどである

3　IPv6 の攻撃利用可能性

IPv6 接続環境が整ってくるに従い新たな脅威が発生することが想定される.新たなアプリケーション,新たなサービスが利用されはじめるときには必ずプロトコル,サービスそのものの脆弱性だけではなく,セキュリティ対策の準備遅れ,想定外の通信や利用方法,利用者の盲点など,さまざまな問題が発生する.IPv6 について現段階で想定される攻撃利用対象まとめると以下のようになる.

- プロトコル実装における脆弱性
- アプリケーションの脆弱性
- マルウェアダウンロード,リダイレクト経路、情報流出経路としてIPv6の利用

この中で現状では攻撃経路としてIPv6が利用される場合が多いと想定される。

3.1　攻撃経路としての IPv6 の利用可能性

本稿では,MWS2011 DATAset[2]を用い,攻撃経路としての IPv6 の利用可能性の現状について考察する.

3.1.1　名前解決に関する実装

IPv6 を使用する場合でも,インターネットサービスを利用する上で DNS による名前解決は基本機能として重要な役割を果たす.これは一般サービスに限った話ではなく,マルウェア感染や情報漏えいなどの攻撃においても同じである.特に IPv6 の普及に伴い IPv4,IPv6 のデュアルスタック環境が今後のユーザー環境の基本形態になると想定されるが,その環境においては名前解決の挙動により,IPv4 を利用して通信を行うのか,IPv6 を利用して通信を行うのかが変わる.またこの実装は OS や装置毎に異なる.したがってデュアルスタック環境での名前解決についての各種実装について次の二点を注意することがある.

- 問い合わせリソースレコードの順序
- トランスポート対応

問い合わせリソースレコードの順序が A,AAAA どちらが先か,その結果をどう利用するかや、名前解決時に利用するプロトコルが IPv4 か IPv6 かそしてどちらが優先されるかが実装により事なる.図 1にデュアルスタック環境での DNS の提供形態を示す.

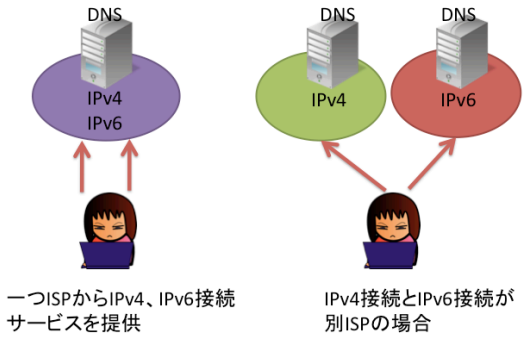

図 1　デュアルスタック環境での DNS

通常は IPv4 接続も IPv6 接続も同一の ISP から提供を受ける形態が想定されるため,エンドユーザーが利用する DNS サーバーも同一の ISP のものを利用することになる.ただし,IPv4 と IPv6 の接続サービスが別の ISP から提供される形態もあるのでその場合は IPv4 用の DNS と IPv6 用の DNS が異なる ISP から提供される場合がある.このような接続サービス提供形態と次に示す各 OS の実装の組み合わせにより複雑な問題を生む可能性がある.図 2 に IPv4,IPv6 デュアルスタック環境での各 OS の名前解決挙動について示す.

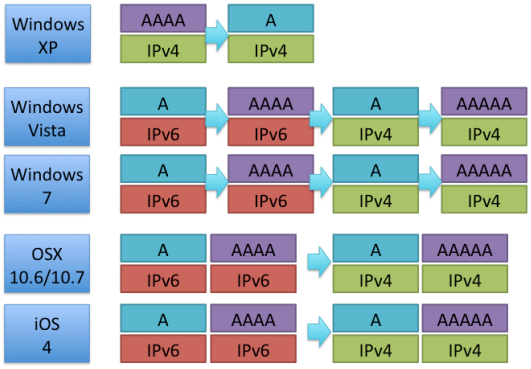

図 2　デュアルスタック環境での各 OS の名前解決の挙動

- windows XPは,IPv6トランスポートでの名前解決機能が実装されていない.そのためトランスポートはかならずIPv4側を利用することになる.クエリタイプはAAAAが先に問い合わされる.
- WindowsVistaとWindows7はトランスポートはIPv6優先,クエリタイプはAレコード問い合わせ後,NXDOAMINでない場合は続けてAAAAレコードの問い合わせを送信する.その結果AAAAレコードの応答が得られた場合には,IPv6で通信を行おうとする.
- OSX,iOSは,IPv6優先,A優先だが,実際にはIPv6トランスポートでA,AAAAがほぼ同時に送出されAAAAの応答があればIPv6通信を行うという挙動である.

このような実装であるため,エンドユーザーも,提供 ISP も実際の通信の挙動を把握することが非

常に困難になることが想定される.つまり感染経路,攻撃経路が IPv4 経由なのか IPv6 経由なのか,またはそれの混在なのかを分析する必要があり,両方のネットワークに対して対策を施す必要が発生する.また DNS を利用したブラックリストやセキュリティ対策なども,エンドユーザーがどちらの DNS を利用するかが端末の挙動に左右されてしまうため,意図した通りのセキュリティ対策が行えなくなるなどの問題を生む可能性がある.そのためこの点を攻撃者側のメリットとして捉えられる可能性がある.

4 データセットから得られる悪性サイトの IPv6 利用度解析

4.1 解析シーケンス

MWS2011 DATAset[2]の攻撃通信データの中から IPv6 網経由で影響がある通信先を解析する.MWS2011 DATAset[2]の攻撃通信データには,ダウンロード元の IP アドレス情報しかないため,IPv6 の利用状況を解析するために,各 IP アドレスを別途準備した悪性 FQDN データベースを利用することで,FQDN 情報に変換し,その FQDN 情報について AAAA レコードの設定状況を調査する.図 3 に変換シーケンスを示す.

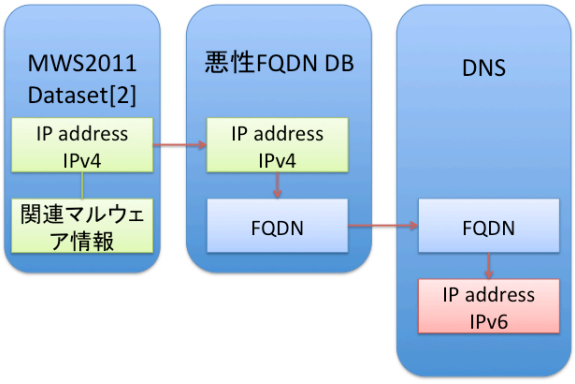

図 3 変換シーケンス

4.2 解析結果

表 1 に解析結果を示す.

表 1 解析結果

対象データ期間	2009/5 ～2011/1
総 IP 数	263769
FQDN 変換可能 IP 数	1104
AAAA 登録 FQDN	3

総 IP 数は 263769 個存在したが,FQDN に変換できたものは 1104 個で全 IP の 0.041%であった.これは下記のように MWS2011 DATAset[2]のデータに含まれる攻撃対象が下記のようなものが多く,変換に利用した悪性 FQDN データベースとの間に差異があることが原因と想定される.

- ダウンロード元の情報がIPアドレスで直接指定されている
- 攻撃種別が隣接スキャン等でダウンロード元を指定した上で感染させるものではないものが多い

4.2.1 該当 FQDN について

IPv6 利用が想定される結果が得られた 3 件の FQDN に関するデータを表 2 に示す.

表 2 該当 FQDN

No	FQDN	該当データ	Malware
1	A	2009/8 2009/9	Cryp_Neb-2
2	B	2009/5	ALLAPLE.IK
3	C	2010/8 2010/9 2010/11 2010/12	WORM_DOWNAD.AD

各 FQDN に関する情報を以下に解析する.

4.2.1.1 FQDN A

2009 年 8 月に検出された IP アドレスであるが,現在もドメインは存在し,IP アドレスも同一セグメント内のアドレスに変化しただけである.該当のサイトはスイスのバーチャルホスティングサービスを利用して構築されており,一般のサイ

トが立ち上がっている.したがって,このホスティングサービスが IPv6 に対応したため,自動的にこの FQDN についても AAAA レコードが設定されたようである.AAAA レコードの設定時期が不明なため影響度は不明である.

4.2.1.2 FQDN B

2009 年 5 月に検出された IP アドレスであるが,現在もドメインは存在する.IPv4 アドレスは大きくかわっているが,当時も現在も中国のホストの IPv4 アドレスのままであるが,現状は攻撃には利用されていない.IPv6 アドレスはブラジルの ISP のものである.またドメイン自体もブラジルのドメインであるため,IPv6 アドレスは意図せず設定されたものである可能性が高い.

4.2.1.3 FQDN C

2010 年 8 月から 12 月の間に観測された IP アドレスであるが,現在もドメインは存在する.IPv4 アドレスは変化しており,検出時はアメリカの ISP のアドレスであったが,現在はオランダのホスティングサービスのアドレスになっている.IPv6 アドレスも同じオランダの IP アドレスである.この IPv6 アドレスもオランダのホスティングサービスに移行時に意図せず設定されたものであると想定される.

4.3 各種ブラックリスト解析

比較を行うために一般に公開されているドメインベースのブラックリストの情報に対して同様の解析を行った. 3 種類のブラックリストについて登録されている FQDN に AAAA レコードが設定されているかどうか解析した結果を表 3 に示す.

表 3 ブラックリスト解析結果

list	種別	総登録数	AAAA 登録数	
Blacklist1	フィッシング	4465	34	0.8%
Blacklist2	マルウェア	14049	23	0.2%
Blacklist3	マルウェア	2260	31	1.4%

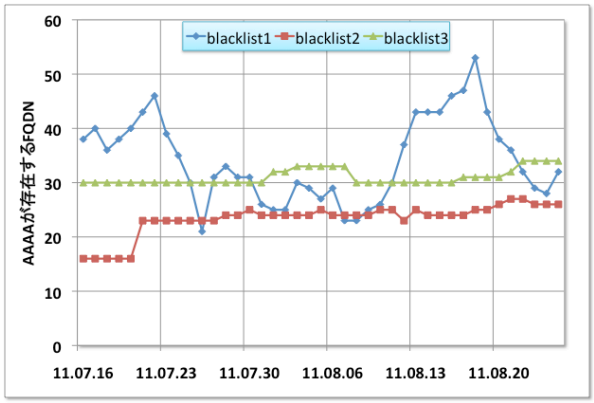

図 4 AAAA レコード設定のある FQDN の登録件数の推移

総登録件数に対する割合は 0.2%から 1.4%程度あり,いずれも 30 件前後であるが,これら 3 つのブラックリスト間での AAAA レコード登録のある FQDN の共通性は 1 件のみであった.

次に 1 日毎の AAAA レコード設定のある FQDN の登録数の 1 ヶ月間の推移を図 4 に示す.フィッシングサイト中心の blacklist1 は日変動が大きいが,その他のリストは一定している.このリストはフィッシングサイトの中心のブラックリスト登録件数が多い.フィッシングやマルウェア感染のためのランディングページは一般のホスティングサービス上に置かれることが多いため,それらのサービスの IPv6 対応が進んでいるため,新規に登録される FQDN が AAAA 設定されている場合が多いため,このような変動があるものと想定される.

このように一般のブラックリストに登録されている悪性 FQDN にも AAAA レコードが登録されているものが 0.2%～1.2%と少ないながらも含まれていた.全体に対する割合は MWS2011 DATAset[2]に比べて約 100 倍であることから,前述のとおり登録されている FQDN のカテゴリーに差異があるものと想定される.

4.3.1.1 サイト解析

AAAA レコードに登録されている IPv6 アドレスの所在国を解析した結果を図 5 に示す.また

IPv4 アドレスベースでのサイト所在国を解析した結果を図 6 に示す。

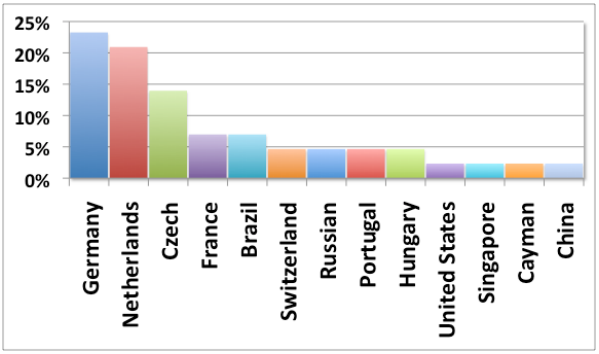

図 5 IPv6 ベースでのサイト所在国

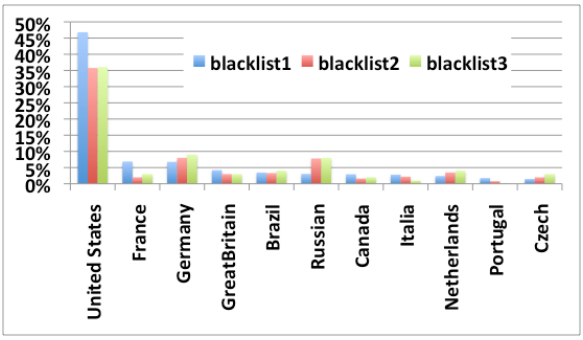

図 6 IPv4 ベースでのサイト所在国

IPv6 ベースではドイツ,オランダ,チェコ,フランスを始めとしたヨーロッパが大半をしめており,その他ブラジル,アメリカ,中国が含まれる.データセットの解析結果で得られた IPv6 アドレスもこれらの上位国に含まれている。IPv4でもこれらの国は上位にいるが、傾向が異なる部分も多く、これらの国の IPv6アドレスの利用率の高さ,利用されるホスティングサービスの IPv6 対応率の高さを示しているものと想定される.

5 結果分析

IPv6の攻撃利用に関しては、各種攻撃状況の解析結果から、基本的には意図的な利用はほとんど観測されておらず,攻撃に利用されているホスティングサービスやサービスプロバイダが強制的にIPv6に対応したため,攻撃者の意図とは関係なく悪性サイトがIPv6対応したり,IPv6通信を利用した攻撃が発生してしまている場合が大半をしめる状況であると想定される.

6 まとめ

攻撃の対象となるのは,より大きな成果を効率的に得るために,大きな脆弱性があるか,人気コンテンツやサービスがあり,多数のユーザーがあつまるものであるサービスやネットワークであるため,接続環境が整い始めただけの IPv6 ネットワークは未だに大きな攻撃対象とはなり得ない状況である.ただし新サービス導入期における,運用と利用者の混乱により人為的なセキュリティ対策の欠陥や脆弱性が発生し、その点が攻撃に利用される状況は過去の様々なサービスで繰り返されてきたことである.したがって IPv6 においてもこれらに備えるために早期に IPv6 ベースでのハニーポットや悪性サイト調査解析を行っていく必要があると想定される.

謝辞

本研究の一部は Telecom-ISAC Japan の支援を受け実施している. 本研究を進めるにあたり, 有益な助言と協力を頂いた Telecom-ISAC Japan の関係者各位に深く感謝致します.

参考文献

[1] 畑田充弘,他:マルウェア対策のための研究用データセット ～ MWS 2011 DATAsets ～ (MWS2011) (2011.10)