「マルチメディア，分散，協調とモバイル
(DICOMO2013) シンポジウム」 平成25年7月

IPv4/v6アドレス混在環境におけるネットワークセキュリティ

村田 大輔[†1] 東 結香[†1] 大平 健司[†1] 猪俣 敦夫[†2] 藤川 和利[†2]

概要：今日においてインターネットは重要な社会基盤となっており，インターネットを構成しているコンピュータなどの機器が悪意ある攻撃を受けてしまうと，その被害は甚大なものとなってしまう。その影響は金銭トラブルのみならず，社会生命への影響など大きなトラブルへと発展する可能性もある。現在のインターネットは，様々なデバイス，アプリケーション，サービスが相互にネットワークを介して利用されている。便利になった反面，IPv4 アドレスの枯渇が問題となり，本格的な IPv4/v6 共存時代へと動いている。IPv4 は登場とともに長い運用期間を経て技術・経験が確立されてきたが，IPv6 ではその知見がほとんど無い。そのため，本稿では，IPv6 の本格的な利用を前に，IPv6 環境での脅威の発見と対策を行うことを目的に，実験環境を構築し，トラフィックを収集・解析することとした。

Network security in a IPv4-IPv6 address mixed network

Daisuke Murata[†1] Yuka Higashi[†1] Kenji Ohira[†1] Atsuo Inomata[†2] Kazutoshi Fujikawa[†2]

1. はじめに

現在，主にインターネットの通信で使用されているプロトコルである IPv4 はアドレス枯渇問題をはじめとする様々な問題が表面化している。一方，これらの問題については早くから指摘がなされており，アドレス空間を拡張した IPv6 が開発されている。今後，IPv4 の枯渇により IPv6 のみでしかインターネットへアクセスが出来ない端末が発生するとも考えられる。そのような端末に対してもサービスを提供できるようにサービスネットワークの IPv6 対応は必要となってくる。IPv6 は，その拡張により事実上は無限に近い個数のアドレスで構成されるため，IPv4 と比べて悪意ある攻撃が成功する可能性は低いと考えられている。しかし，IPv6 では IPv4 と異なり 1 つの NIC に対し，多数のアドレス割り当てを可能としているため，潤沢なアドレスの中から，意図的に複数のアドレスを用いて攻撃が行われることも予測される。IPv6 はアドレス空間が 128 ビットで構成されているため，アドレス空間が 32 ビットしかない現行の IPv4 端末と直接の通信ができない。ただし，IPv6 は IPv4 との共存を考慮した設計がなされている [1]。また現在，IPv6 を利用する場合は IPv4 と併用したデュアルスタックネットワークを構成して利用することが一般的である。そのほかにも，IPv4/IPv6 トランスレータなどの利用など，IPv6 を取り巻く環境では既存の IPv4 のみの環境とは異なる性質が多々発生する。また，現時点で IPv6 環境の運用における知見は少なく，IPv4 専用の環境と比べどのような点がセキュリティリスクとなり，問題がどこにあるのかを検証するため実機実験を行うこととした。現在，安全な IPv6 ネットワーク環境での運用のために，世界的にセキュリティに対する取り組みや研究が行われている [2–7]。しかし，それらは IPv4 での運用から得られた経験的なものや，シミュレーションでの結果，実機を用いた場合でも各論文の著者らが閉じたネットワークで意図的に攻撃パケットを配信し，得られた知見を述べているものがほとんどである [8,9]。本論文では，これらの問題を解決することを目的とし，実機を用い，IPv4/v6 アドレス混在環境におけるネットワークセキュリティを調査するための実験トポロジを構築し，実証実験を実施した結果を報告する。

†1 現在，奈良先端科学技術大学院大学 情報科学研究科
Presently with Graduate School of Information Science, Nara Institute of Science and Technology
†2 現在，奈良先端科学技術大学院大学 総合情報基盤センター
Presently with Information Initiative Center, Nara Institute of Science and Technology

2. 脅威と対策手法

IPv4 は，1981 年の仕様公開から今まで約 30 年以上にわたって利用されてきており，その長い運用期間をもって，適宜，セキュリティ問題への対応等を進めてきた歴史がある。それに対し，IPv6 では，これまで大規模な利用や運用が行われた経験が十分にないため，IPv6 におけるセキュリティ上の課題及びその対策は，実態ベースでは広く共有されていない部分が多い。セキュリティを考慮しない場合の IPv6 への対応方法は，基本的に各機器や OS を IPv6 に対応させ，IPv6 アドレスの取得・割り当てするだけでよい。このレベルの知見は現時点でも十分に蓄積されており，IPv6 インターネ ットに接続できる環境であれば，単純に IPv6 対応が可能となる。ただし，今日でのネットワークは大量に送信される SPAM メールと呼ばれる unsolicited commercial email (UCE) や unsolicited bulk email (UBE)，ポートスキャンなどといった迷惑行為からシステムを防御する仕組みが必要となる。更に IPv4 から IPv6 への移行期には，様々な手法で共存環境が構築されることが予想される。その中でも 6to4 [10], Teredo [11], 6rd [12], ISATAP [13] といったトンネリング技術はセキュリティ上大きな穴となりうる。6to4 リレールータは世界中に多く存在するが，管理主体は存在せず，ボランティアベースの運用である。そのため，6to4 リレーエニーキャストプレフィックス (192.88.99.0/24), 6to4 アドレス (2002::/16) への経路広告の正当性を保証する仕組みが無く，悪意ある運用がなされる危険性がある。更に，IPv4 アドレスと 6to4 アドレスの検査が正しく実施されない場合は，攻撃者の IP アドレスを隠蔽した形で，IPv6 ノードへの攻撃を行うことなどが可能となる。なお，Teredo サーバも，クライアントの Teredo サーバを悪意のある Teredo サーバに置き換えることで，DNS 偽装と同等の振る舞いが行え，Teredo リレーは，対象の IPv6 ノードから近い Teredo リレーが選択されるため，悪意ある Teredo リレーによる通信傍受が可能となる。また，6to4, 6rd, ISATAP は， IPv6 アドレスににトンネルの端点となるルータの IPv4 アドレスを埋め込む形で利用される。この場合，宛先と送信元 IPv6 アドレスを偽造することで、自動トンネルによるループ構成となるなど，トンネリング技術を利用する場合の問題も発生する。また，IPv4 アドレスの枯渇に伴い，特にモバイル環境では 1 年程度で IPv6 だけで通信する端末が出てくることも考えられる。これから近い将来起こるであろう IPv6 本格利用時代に向けて，IPv6 を安全に使っていくことが出来るようにするためには，IPv6 対応にあたって現在の IPv4 と同等のセキュリティを確保するための手法を確認することが大事である。

2.1 既存調査

文献 [2] では，企業ネットワークの DMZ において IPv6 ネットワーク環境を導入するにあたって必要なネットワークモデルの提案を行っている。デュアルスタック，パラレルスタックおよびトランスレータ利用におけるサービスモデルの提案とその特徴を挙げ，それぞれのメリット・デメリットを提案しているが，実際の運用知見が十分に述べられていない。また，今後長きにわたるであろう共存状況におけるモデル提示および対策が述べられておらず，IPv4 から IPv6 への移行時に必要となる要素が不足している。

文献 [3] では，エンドノード（クライアント・サーバノード），ネットワーク機器（ルータ・L2 スイッチ等），セキュリティ機器（IDS / IPS，ファイアウォール）に対する脅威と対策を考え，緊急性が高く、広範囲に影響が広がるものに関しては実機を用いて攻撃の有効性の検証をし，その他の案件に関しては机上検証を行っている。同様に，文献 [5] などにおいてもこれらはあくまで想定される各シナリオに対してのみ検証を行っており，『インターネット全体の運用』という点では精査できていないと考える。

前節にて，IPv6 ネットワーク環境においての『インターネット全体の運用』の方針を示す知見が不足していることを述べた。そこで，本研究では，より実際のインターネット環境での運用に際しての知見を得るために，実際のインターネットを介したシステムが通信した実トラフィックを取得・解析するための，パケット取得用の仮想マシンを作成する。

2.2 関連研究

本研究は，ハニーポットと呼ばれる研究領域に分類される。関連する研究として The Honeynet Project [14] が挙げられる。また，Library of Malware Traffic Patterns [15] といった不正なトラフィックを公開しているものもある。

The Honeynet Project は，悪意ある第三者が攻撃に用いたツールや，攻撃の戦略などから得られた情報を公開し，実際の攻撃から学ぶことを理念として活動している。しかし，The Honeynet Project の報告は主に不正アクセスに対する啓蒙を行っており，その監視手法について明白な部分が少ない。また攻撃者の行動内容を NFS や SMB を用いて記録する方針をとっているが，侵入者がネットワークへのトラフィックを監視した場合，侵入したホストが Honeypot であると検知できる。このため，The Honeynet Project の目的は，ホストに侵入する前の攻撃者の行動を監視することにあると思われる。本研究ではホストに侵入した後の攻撃者の行動に着目し，監視を行い，行動を観測することとする。

3. 実証実験

3.1 実験トポロジの構築

IPv4, IPv6 およびデュアルスタックネットワーク環境における脅威や攻撃方法を確認するために，インターネット上での通信トラフィックを取得する環境を各 IPv4, IPv6 およびデュアルスタックネットワーク環境に構築した。その簡易モデルを以下の図 **1** に示す。

今回は，これらで取得したパケットを解析し，IPv4, IPv6 およびデュアルスタックネットワーク環境におけるそれぞれの特徴を確認することとする。また，得られた結果を用いて，上記で述べたような脅威からシステムを防御する仕組みを検討することとした。

3.2 実験の方針

間近に迫る IPv6 本格利用時代に向けて，IPv6 を安心して使っていくことが出来るようにするためには，IPv4 と同等のセキュリティを担保する必要がある。そのために，本実験では，実機を用いて実際のインターネットにおけるトラフィックを，IPv4 Native, IPv6 Native, デュアルスタックそれぞれのネットワークに接続したマシンで観測し，各ネットワーク毎の変化状況を取得する。そして，得られたデータを元に，各方式の特徴をまとめ，IPv6 ネットワーク環境における運用知見を見いだすこととする。これにより，実際に IPv6 が提供されている環境での振る舞いを観測することができ，机上の議論や経験則ではなく，実際の傾向に基づいた知見が得られると言える。

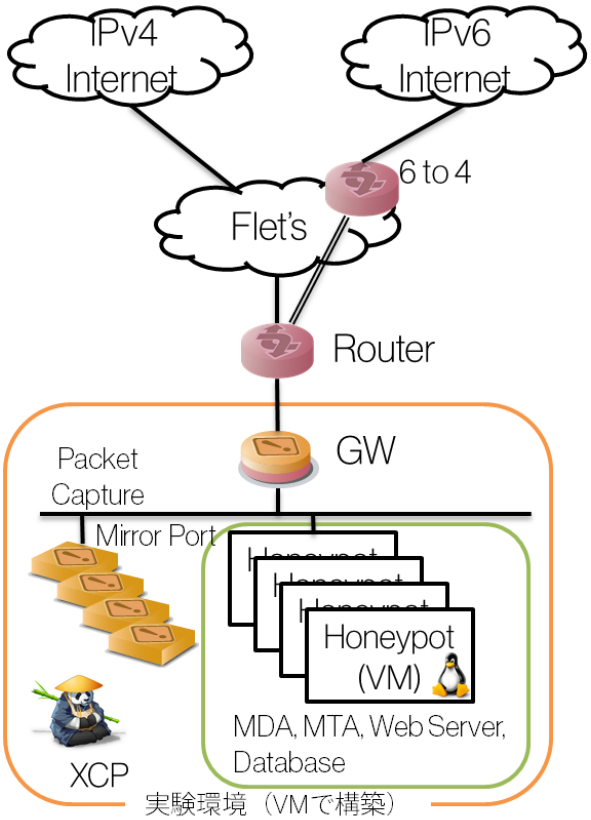

図 **1** 実験環境のモデル構造

本実験では，可能な限りインターネット上における実際のパケットを取得する必要がある。既存のハニーポットでは，攻撃側にハニーポットと検知された瞬間に攻撃対象から外されてしまうことがある。これではデータを観測することができないため，今回は OS やソフトウェアのバージョンをあえて落とし，構築途中で放置されたであろうサーバを模した環境を構築し，これをハニーポットとして使うことにした。なお，クライアント環境ではなく，HTTP や SMTP，FTP，SSH などのサービスを提供するサーバ環境として実験を行うこととする。それぞれの検証用サーバは Xen Cloud Platform [16] 上に仮想マシンとして構成し，ほぼ同等の OS・ソフトウェア構成で環境を構築し，それらがどのような攻撃を受けるかを，パケットを受信し観測する。仮想マシンを採用した理由は，何か問題が発生したときにリモートから操作しやすいこと，ならびに攻撃されたサーバのイメージを取得しやすいこと，原本のイメージと攻撃されたサーバのイメージとの差分が取りやすいこと，スナップショットで容易に過去の状態に戻せることなど，情報収集の容易性を考慮した点が挙げられる。気を付けなければならないこととして，攻撃を受けた実験用サーバが乗っ取られ，次に加害者とならない様に対策を取る必要も出てくる。今回は，システムを監視し，必要に応じて人為的にサーバを止めるという手段で実験を行った。この手法では，人間による攻撃には対応できないが，適宜，仮想マシンのイメージを元に戻し，攻撃されていないサーバとして，以降も続くであろう機械的な攻撃に対して，パケットをとり続けることとした。

3.3 実験シナリオ

ここで本論文での実験内容について述べる。今回使用する実験環境の構成の概略図を図 **2** に示す。このネットワーク環境は，文献 [17] にて構築されたネットワーク環境を参考としている。実験環境はグローバルの IPv4 専用ネットワーク，IPv6 専用ネットワーク，デュアルスタックネットワークセグメントにそれぞれサーバを設置するものとする。これらはハニーポットとして，外部からのパケットを全て防御せずに収集する。実験シナリオは以下の通りである。

(1) VM 上にサーバとゲートウェイのイメージを作成する
(2) サーバが送受信したパケットをゲートウェイでミラーし，別途保存する
(3) サーバを運用し，1 日毎にスナップショットを保存する
(4) ミラーしたデータとスナップショットのイメージを確認する
(5) 完全に乗っ取りが行われたことが確認できた場合は手動でサーバをシャットダウンし，ログを確認する

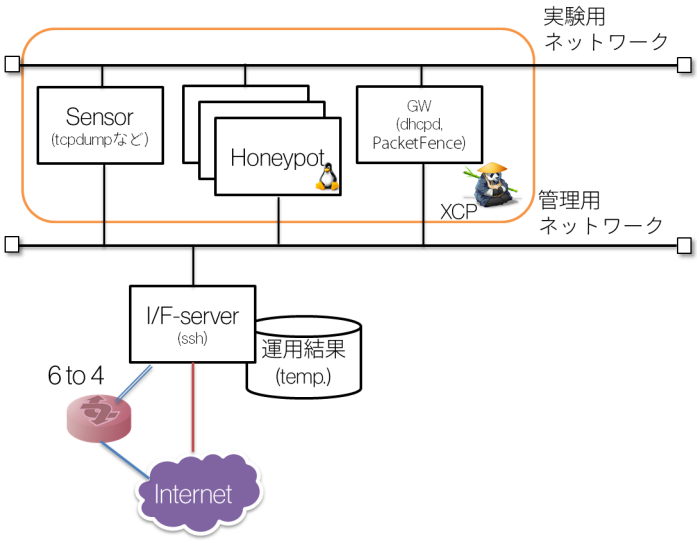

図 2　実験環境概略図

実験で得られた観測結果を用いて，シングルスタックとデュアルスタックでの変化や，IPv4 と IPv6 での変化などを取得することとし，そこから今後の IPv6 環境構築における知見を示すことを目標とする。

本実験の目的は，IPv6 環境においてセキュリティを保護しつつサービスを提供するための基本的な情報を収集するということにある。そのため今回の実験では，実際のインターネット環境において IPv4，IPv6，デュアルスタックという 3 タイプのネットワーク状況が異なる実機を用いて，データを収集した点が重要となっている。更に，ハニーポット側でスキャンプログラムを実行させていると，各コンポーネントのバージョンは古いにもかかわらず，システム自体が監視されているという攻撃者から見た時に不自然な状況が発生するため，スキャンされているということに気付かせないようにする必要がある。そのため，監視はパケットをミラーした別のマシンにて行うこととした。近年，不正アクセスは自動化される傾向にあり，侵入したホストから自動的に不正アクセスを行うツールが出現している。この状況を放置していると加害者となるため，自動化されたツールの外部に対する攻撃の流出の排除を行う必要がある。文献 [18] では模擬 DNS を用い，不正アクセスに対し偽の応答を返答することで，攻撃の流出を排除しているが，意図したアクセスが出来ず，その後の振る舞いが変わった事を示している。このように，環境に手を加えることで変化する動作についても加えて調べてゆきたい。

4. 考察

IPv6 アドレスの膨大さに起因し、一時アドレスを利用した攻撃については，リンクローカル側では NDPMon [19] を利用して，IP アドレスと MAC アドレスの対応付けを行うという対策を講じることで，対応できると考えている。また，外部からのパケットに関しては，プレフィックスを判断し，短時間に多数のアクセスが来た場合，一時的にプレフィックスを制限するなど試行を行い，運用に支障が無いかを判断してゆく必要があると考える。次に，移行時の混在環境や Pv6 ネットワーク環境の調査不足の点は，必要数に対して十分なグローバル IPv4 アドレスを提供できなくなるに伴い，IPv6 アドレスとの共存は深くなると考えられる。次第に IPv6 への移行が進むにつれ，運用知見は多く述べられると考えている。最後に，シングルスタック (IPv4/IPv6) とデュアルスタックおよび，IPv4 と IPv6 における通信状況の変化を取得する際に，全てのパケットを取ることが理想的ではあるが，量が膨大なもととなり，管理・解析が非常に大変なものとなる。そこでパケットのどの部分をスクランブルするのか、更には，本実験のような運用および攻撃によって変化したイメージをどう短時間で差分計算するか，攻撃ではなく通常の運用によって変化した部分との差異をどう出すのかが解決すべき課題となる。

5. おわりに

本研究では，IPv4/v6 アドレス混在環境におけるネットワークにおいて，シングルスタックおよびデュアルスタックの実トラフィックを収集する環境を構築した。今回，構築した環境において収集したデータを用いて，今後，解析を行い，これらの異なるネットワーク環境を持つトラフィックにどのような傾向があるか，また，デュアルスタックという IPv4 / IPv6 の二つの経路を持つマシンにおいて，パケットがどのように出て行くのかなど，IPv4 専用ネットワークとは異なる振る舞いを確認し，それらの特徴を確認することとする。

なお，今後，得られた情報をもとに，IPv6 環境において，セキュリティを保護しつつサービスを提供するための知見の公開を行う予定である。

6. 謝辞

最後に，本稿における環境構築および実験を行うにあたり，実験機材の提供など多大なるご支援，また，暖かいご激励とご鞭撻ならびに親切なご指導を頂いた NPO 日本ネットワークセキュリティ協会 (JNSA) WG の許 先明氏，二木 真明氏，加藤 雅彦氏に深く感謝申し上げます。

参考文献

[1] Gilligan, R. and Nordmark, E.: Transition Mechanisms for IPv6 Hosts and Routers, RFC2893 (2000). 入手先 ⟨http://www.ietf.org/rfc/rfc2893.txt⟩

[2] IPv6 普及・高度化推進協議会 セキュリティ WG: IPv6 対応セキュリティガイドライン (第 1.0 版) (2012). 入手先 ⟨http://www.v6pc.jp/jp/upload/pdf/swg-IPv6SecurityGauideline_v1.0.pdf⟩

[3] IPv6 技術検証協議会 セキュリティ評価・検証部会: 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 (2012). 入手先

⟨http://ipv6tvc.jp/documents/20121023Report.pdf⟩
[4] Doug Montgomery, Stephen Nightingale, Sheila Frankel and Mark Carson: A Profile for IPv6 in the U.S. Government Version 1.0 (2008). 入手先 ⟨http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf⟩
[5] Sheila Frankel, Richard Graveman, John Pearce and Mark Rooks: Guidelines for the Secure Deployment of IPv6 (2010). 入手先 ⟨http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf⟩
[6] DISR IPv6 Standards Technical Working Group: DoD IPv6 Standard Profiles For IPv6 Capable Products Version 5.0 (2010). 入手先 ⟨http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf⟩
[7] Beckman, T., Hann, D. and Thomas, K,: DoD IPv6 Generic Test Plan, Version 4 (2009). 入手先 ⟨http://jitc.fhu.disa.mil/adv_ip/register/docs/ipv6v4_may09.pdf⟩
[8] Kamra, A., H. Feng, V. Misra, and A.D. Keromytis.: The effect of DNS delays on worm propagation in an IPv6 Internet. in INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE. 2005.
[9] Ting, L., G. Xiaohong, Z. Qinghua, and Q. Yu,: A new worm exploiting IPv6 and IPv4-IPv6 dual-stack networks: experiment, modeling, simulation, and defense. Network, IEEE, 2009. 23(5): p. 22-29.
[10] Carpenter, B. and Moore, K.: Connection of IPv6 Domains via IPv4 Clouds, RFC2893 (2001). 入手先 ⟨http://www.ietf.org/rfc/rfc3056.txt⟩
[11] Huitema, C.: Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), RFC4380 (2006). 入手先 ⟨http://www.ietf.org/rfc/rfc4380.txt⟩
[12] Townsley, W. and Troan, O.: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification, RFC5969 (2010). 入手先 ⟨http://www.ietf.org/rfc/rfc5969.txt⟩
[13] Templin, F., Gleeson, T. and Thaler, D.: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), RFC5214 (2008). 入手先 ⟨http://www.ietf.org/rfc/rfc5214.txt⟩
[14] The Honeynet Project. 入手先 ⟨http://www.honeynet.org⟩
[15] DeepEnd Research: Library of Malware Traffic Patterns. 入手先 ⟨http://www.deependresearch.org/2013/04/library-of-malware-traffic-patterns.html?m=1⟩
[16] Xen Cloud Platform. 入手先 ⟨http://www.xen.org/products/cloudxen.html⟩
[17] 三輪信介，門林雄基，篠田陽一：小規模攻撃再現テストベッドによる動作記録データセットの生成．サイバークリーンセンター・情報処理学会，マルウェア対策研究人材育成ワークショップ 2009 (2009).
[18] 三輪信介，宮本大輔，櫨山寛章，井上大輔，門林雄基：模倣 DNS によるマルウェア隔離解析環境の解析能向上，サイバークリーンセンター・情報処理学会，マルウェア対策研究人材育成ワークショップ 2008 (2008).
[19] NDPMon — Main / About NDPMon. 入手先 ⟨http://ndpmon.sourceforge.net/⟩