2005－DSM－36（3）
2005／3／18

組織内ネットワークにおける MACアドレストレースバックシステムの開発

續木　涼太†　　泉　裕††　　齋藤　彰一†　　塚田　晃司†

†和歌山大学　システム工学部　　††和歌山大学　システム情報学センター

内容梗概　　インターネットを利用したDoS(Denial of Service)攻撃，ウイルスやワームなどの障害が発生した場合，ネットワーク管理者は速やかにパケットの発信端末を特定し，対処する必要がある．本研究では管理者支援のために，組織内ネットワークにおいてMACアドレスのトレースバックを行うシステムを開発した．トレースバックを行うための情報を，管理VLAN上でのtelnet接続によりネットワーク機器から取得するものと，SNMPにより取得するものを構築した．本システムの利用により，パケットの発信端末の物理的な位置情報が特定可能となった．さらに，ネットワーク機器との接続を指すパッチリストと連携し，発信端末の存在する部屋名の表示も可能とした．

Development of MAC Address Traceback System for Internal Network

Ryota TSUZUKI †　　Yutaka IZUMI ††　　Shoichi SAITO †　　Koji TSUKADA †

†Faculty of Systems Engineering, Wakayama University
††Center for Information Science, Wakayama University

Abstract　　In these cases, DoS(Denial of Service) attack, problems of computer virus and worm, the network manager has to search the packet sender rapidly and deal with these prompems. We developed the system of MAC address traceback for internal network, to support the network managers. There are two ways to get the information for traceback from network equipments. Through management VLAN, telnet to switch and router and execute cpmmands, the other way is using SNMP. This system enable us to search the phisical place of the packet sender. And, combination with patch lists, this system is able to show room name.

1　はじめに

近年インターネットが普及し，一般企業・学術機関・政府機関等における利用率が高まっており，ネットワーク運用は必須になっている．現在利用されている多くのシステムおよびサービスはネットワークの利用を前提としているため，ネットワーク運用に障害が発生すると様々な弊害を生じる．このため，ネットワーク管理は年々重要性を増している．

上記の重要性が増すにつれ，インターネットに付随した問題が増加している．深刻な問題には，DoS（Denial of Service）攻撃，DDoS（Distributed DoS）攻撃，コンピュータウイルスやワーム，不正アクセス等がある．どの問題も，発信元となる端末の特定が，管理上不可欠

である．

上記の中で，ワームが発生した場合にネットワーク管理者が行う対策について述べる．ネットワーク管理者は発生した攻撃や通信から発信エリアを特定し，ネットワーク上からの隔離や経路上でのフィルタリングによって，攻撃となる通信を止める処置をとる．ネットワーク管理者は被害を局所化するために，問題が発生したネットワークや端末の位置情報を，可能な限り詳細に調べる必要がある．

端末をトレースバックする手法として一般的に使われるのが，traceroute（tracert）である．しかし，traceroute は IP アドレスを前提とした Layer-3 におけるネットワーク経路を表示するコマンドであり，ネットワーク管理者が位置情報を特定できるのはルーティングを行っている機器までである．さらに，近年 VLAN 技術が普及し，巨大な Layer-2 ネットワークが広く利用されているため，ルーティング機器を特定しても，端末の設置場所を特定するのは困難な場合が多い．仮に，特定したルーティング機器でネットワークの隔離やフィルタリングを行い，通信の規制を行うと，多数の端末の通信に弊害が出たり，被害を受ける端末の数が多くなるため望ましくない．

したがって，ネットワーク管理者はネットワーク機器だけでなく，管理対象のネットワークおよび通信下の端末も構成管理する必要がある．

本研究では，ネットワーク管理者支援のため，ネットワーク管理の中でも特に障害管理と構成管理において有用となるシステム **MATT**（MAC Address Tracing Trailer）を開発した．MATT は，組織内ネットワークにおいて MAC アドレスのトレースバックを行うシステムであり，端末特定に MAC アドレスを用いる．MAC アドレスは Layer-2 のアドレスを指すため，発信端末の物理的な位置情報を特定できる．さらに，ネットワーク機器との接続を指すパッチリストと連携し，端末が設置されている部屋名を表示できる．

端末を特定する必要が生じた場合，一般的に端末の情報として判明しているのは IP アドレスであるため，IP アドレスに対応する MAC アドレスを割り出す必要がある．これら 2 つのアドレスの対応情報は，ネットワーク機器から取得できる．ネットワーク機器からの情報取得方法として，機器に telnet 接続してコマンドを実行することにより情報を得る機能と，SNMP で情報を得る機能の 2 通りでシステムを構築した．

本論文では，まず第 2 章で関連研究と問題点を述べ，第 3 章では我々の構築した MATT の設計，第 4 章では考察を述べる．

2　関連研究と問題点

パケットの発信端末を探知する技術として，IP トレースバック [1] がある．IP トレースバックとは，一般に IP パケットの送信元アドレスが詐称されても，発信端末を特定できる技術の総称である．

IP トレースバックには様々な手法が提案されており，その手法の中でも注目度が高いのが Hash-Based IP トレースバック [2] である．この手法は，ネットワーク要所に通過パケットのログを収集する機器を設置し，収集した情報を元にトレースバックを実行し，製品の開発も行われている [3][4]．さらに，Hash-Based IP トレースバックを Layer-2 まで拡張し，MAC アドレスとネットワーク機器のポート情報を用いて，より詳細にトレースバックを行う手法も提案されている [5]．

Hash-Based IP トレースバック以外にも，多くの IP トレースバックの手法が存在しているが，広く普及し使われるまでには至っていない．これは，トレースバックの精度や，システムの導入コスト，運用コストの問題が主たる原因であると考えられる．Hash-Based IP トレースバックの場合，通過パケットのログを収集するのは，ネットワーク要所に設置された機器あるいは，ネットワーク機器自体である．どちらも，現存のネットワーク環境でトレースバックを行うのは不可能であり，機器の追加や機器の入れ替えが必要になる．

また，IP トレースバックは DoS 攻撃や DDoS 攻撃への対策として考えられた技術であるため，AS（Autonomous System）間のような大規模なネットワークでのトレースバックが対象になっている提案が多い．このため，IP トレースバッ

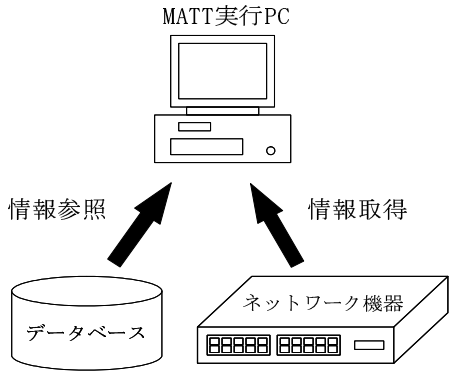

図 1: 基本動作

クを適用する目的は，組織内ネットワークにおける端末の特定とは異なると考えられる．

3　システムの構築

本章では，MATT の挙動，ネットワーク環境，ネットワーク機器からの情報取得方法について述べる．

3.1　MATT の基本動作

MATT には，ネットワーク機器に対して SNMP で問い合わせ，および telnet でログインできる環境と，パッチリスト等の情報が保存されたデータベースにアクセスできる環境が必要である．図 1 に，MATT の基本的な動作を示す．

ネットワーク機器から情報を得る際の通信は暗号化されておらず，他者にスニッフィングされる危険性がある．このため，ネットワーク機器との通信は管理 VLAN セグメント内で行い，外部に情報が漏洩しないようにした．

3.2　MATT 処理の流れ

MATT は，管理 VLAN に接続した PC が，データベースに保存された情報と，ネットワーク機器から得た情報を処理することでトレースバックを実現する．MATT システムにおける処理の流れを以下に示す（図 2 参照）．

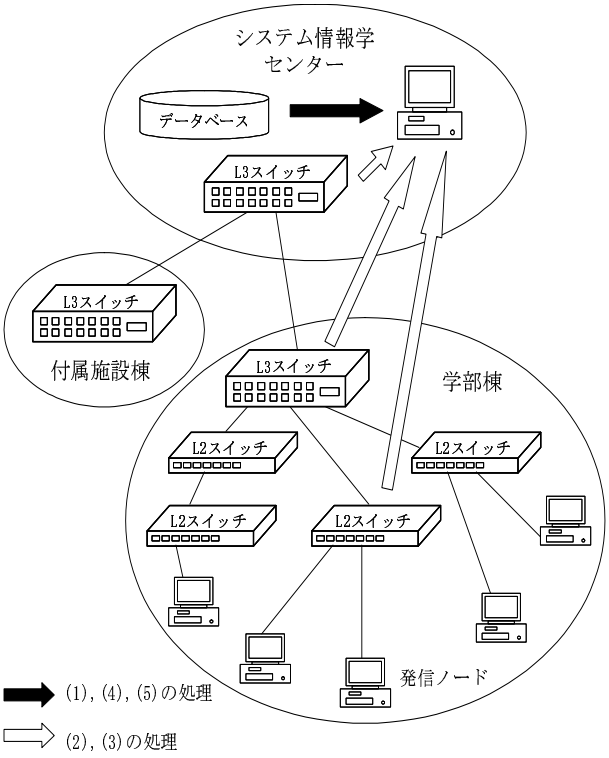

図 2: 処理の流れ

(1) トレースバックする対象端末の IP アドレスをルーティングする機器を特定する．
(2) ルーティングする機器で，対象の IP アドレスから MAC アドレスを特定する．
(3) MAC アドレスの流入ポートを割り出す．
(4) 上記ポート接続先の情報をデータベースより取得する．
(5) ポートの接続先がスイッチであれば (3) へ戻り，接続先が部屋に到達するまで処理を実行する．接続先が部屋であれば情報を表示して，処理を終了する．

3.3　ネットワーク環境

本システムは和歌山大学（以下，本学という）の学内ネットワークにおいて構築しており，本学のネットワーク環境に依存している部分がある．本節では，本学におけるネットワーク環境の特徴を述べる．

ネットワークの基幹となる機器は，Cisco 製の Catalyst スイッチであり，主に同スイッチの

Layer-3 モジュールを用いてルーティングしている．以下に本学の基幹ネットワークに設置された機器を示す．これら Layer-3 および Layer-2 スイッチは，MAC アドレスをトレースバックする際に情報を得る対象の機器である．

- Catalyst 6509, 6506, 4006
- Catalyst 3524, 2950, 2940

上記のスイッチには，各スイッチに一意なホスト名（以下，スイッチ名という）が割り振られており，スイッチの各ポートの配線情報を記したパッチリストが存在する．

本学のネットワークは，VLAN を用いたネットワークを構築している．これらネットワークの基幹となっている Catalyst スイッチのみが所属している管理 VLAN セグメントが存在し，管理 VLAN セグメントは外部から侵入されることのないセキュアなネットワークになっている．

3.4 データベース

MATT には，ネットワーク機器から取得する情報以外に，パッチリストやスイッチの IP アドレスの情報等が必要である．本節では，これらの前もって必要となる情報について述べる．

IP アドレス
: スイッチ名と，管理 VLAN セグメント上で割り当てられた IP アドレスの対応情報である．各スイッチに管理 VLAN 上から telnet 接続する場合や，SNMP の Agent に問いかける場合に使用する．

各ポートの接続先情報（パッチリスト）
: スイッチ名と，そのスイッチが持つ各ポートの接続先情報である．トレースバック中に MAC アドレスの流入ポートが特定された際，その接続先のスイッチや部屋名を特定する場合に使用する．

ルーティングアドレス空間
: ルーティングをしているスイッチ名と，このスイッチがルーティングしているアドレス空間の情報である．トレースバック対象の IP アドレスをルーティングしているスイッチ名を特定する場合等に使用する．

3.5 telnet による情報取得

3.3 節で述べたネットワーク環境において，telnet によって情報取得を行う手法を，実行コマンドと共に述べる．

まず，ルーティングをするスイッチで“ show arp ”を実行し，トレースバック対象の IP アドレスに対応する MAC アドレスを取得する．MAC アドレスを取得した後は，特定した MAC アドレスが流入しているポートを調べ，ポートの接続先を調べる作業を繰り返す．MAC アドレスが流入しているポートを調べるコマンドは“ show cam dynamic ”と，“ show mac-macaddress-table ”である．コマンドが 2 種類ある理由は，Native IOS と Hybrid IOS 因る．

上記した 3 つのコマンドでトレースバックに必要な情報を表示できる．他にもスイッチ上でモジュールの移動，特権モードへの移行を行うために“ show module ”と“ session ”，“ enable ”のコマンドを使用する．

本節で述べたコマンドを実行して得た情報と，3.4 節で述べたデータベースに保存された情報により，IP アドレスを元にして MAC アドレスのトレースバックが可能である．

これらの処理を実現するにあたり，CPAN に登録されたモジュール“ Net::Telnet::Cisco ”を利用した．

3.6 SNMP による情報取得

3.3 節で述べたネットワーク環境において，SNMP によって情報取得を行う手法を，オブジェクト名，オブジェクト ID（以下，OID という）とともに，手順を追って述べる．

(1) atPhysAddress
OID：.1.3.6.1.2.1.3.1.1.2
ルーティングしている機器に対して atPhysAddress のクエリを実行すると，返された OID の下 4 つの ID が IP アドレスになっており，トレースバック対象の IP アドレスに対応する MAC アドレスが取得できる．

(2) atIfIndex
OID：.1.3.6.1.2.1.3.1.1.1

atIfIndex のクエリを実行すると，返された OID の下４つの ID が IP アドレスになっており，IP アドレスに対応するインタフェース番号が得られる．

(3) ifDescr
OID：.1.3.6.1.2.1.2.2.1.2
ifDescr のクエリを実行し，返された OID の下１つの ID が (2) で得られたインタフェース番号と対応するものより，トレースバック対象アドレスの所属する VLAN 番号が取得できる．

ここまでの処理は，ルーティングしている機器やモジュールに割り当てた IP アドレスに対してクエリを実行する必要がある．以降の処理は，Layer-2 の機器やモジュールに割り当てた IP アドレスに問い合わせる必要があり，クエリを実行する際には，コミュニティ名の後部に“ @ ”と，(3) で得られた VLAN 番号を記す必要がある．

(4) dot1dTpFdbAddress
OID：.1.3.6.1.2.1.17.4.3.1.1
dot1dTpFdbAddress のクエリを実行すると，機器の持つ MAC アドレステーブルが取得できる．

(5) dot1dTpFdbPort
OID：.1.3.6.1.2.1.17.4.3.1.2
dot1dTpFdbPort のクエリを実行し，返された OID の下６つの ID が (4) で返された ID の下６つと対応した値が，所属する VLAN のブリッジ番号となっている．

(6) dot1dBasePortIfIndex
OID：.1.3.6.1.2.1.17.1.4.1.2
dot1dBasePortIfIndex のクエリを実行すると，下１つの ID が (5) で得られた ID と対応しており，対応するブリッジポートのオブジェクト値が得られる．

(7) ifName
OID：.1.3.6.1.2.1.31.1.1.1.1
ifName のクエリを実行すると，下１つの ID が (6) で得られた ID と対応しており，対応するインタフェース名が得られる．

(1)〜(7) の処理を行った場合に，SNMP エージェントから得られる情報のうち，トレースバックに必要となる部分の例を図 3 に示す．例では，トレースバック対象の IP アドレスを“ 192.168.1.1 ”とし，MAC アドレスを“ Hex: AA AA AA AA AA AA ”とする．

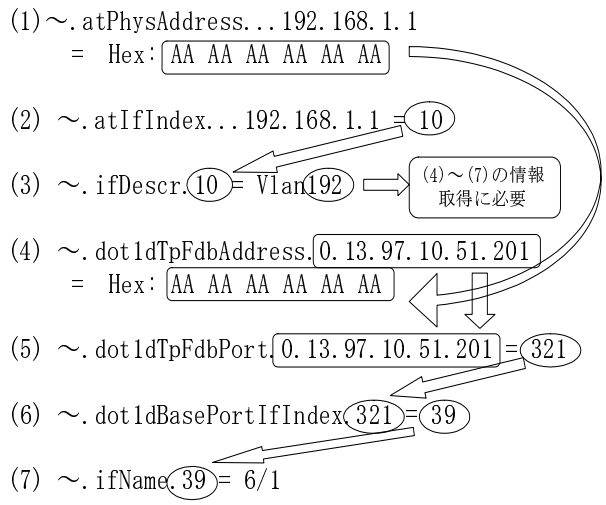

図 3: MIB 情報

本節で述べた手順で MIB 情報を参照と，3.4 節で述べたデータベースを参照することにより，IP アドレスを元にして MAC アドレスのトレースバックが可能である．

これらの処理を実現するにあたり，CPAN に登録されたモジュール“ Net::SNMP ”を利用した．

4 考察

4.1 評価

MATT を用いて MAC アドレスのトレースバックに成功したが，一部にトレースバック不可能なアドレスを確認した．これらは，NAT 環境や Proxy ARP を利用したネットワークを構築している場合である．どちらもネットワーク管理者が端末を特定するのは不可能であり，該当環境を構築した責任者に端末特定を依頼する必要がある．

さらに，本学のネットワークには，大学が設置した無線 LAN のアクセスポイントが多数存在する．全学における無線 LAN のルーティン

グは数台の Cisco2621 が行っており，現状では無線を利用した棟の特定に限定される．

今回，ネットワーク機器からの情報取得方法として２通りの手法を用いた．これは MATT が対応できるネットワーク機器を増やすことが目的であると同時に，MATT の使用用途の幅を広げるためである．telnet による情報取得は，ネットワーク機器のログインパスワードが必要になるが，MATT 実行と同時にネットワーク機器の設定も変更できる．SNMP による情報取得を用いた場合，MATT 実行可能な人間が，ネットワーク管理者だけでなく，サーバや他のシステム等の管理者も含まれる．これら両手法を使い分ければ，MATT の利便性を高められる．

4.2 今後の課題

MATT システムは，ネットワーク機器に残されている ARP 情報や，MAC アドレスのキャッシュを得ることでトレースバックを実現している．トレースバック可能な時間は，ネットワーク機器の MAC アドレスのエージング時間に依存してしまう．したがって，通信が終了し，一定時間が経過してしまうとトレースバック不可能となる．この問題の解決策として考えられる方法は，各ネットワーク機器の ARP 情報と，MAC アドレスのキャッシュ情報を収集・保存することである．これらの保存した情報と，パッチリストの情報を組み合わせることで，過去の通信に用いられた MAC アドレスのトレースバックが可能になる．

さらに，MATT システムは，実験環境である本学のネットワーク環境に依存している部分がある．SNMP によって情報を取得する場合は問題ないが，telnet によって情報収集する場合は，ネットワークベンダによって機器上での実行コマンドが異なるため，3.2 節で述べたネットワーク機器以外の製品が含まれる場合には，現在の MATT ではトレースバック不可能である．したがって，telnet による情報収集を様々なベンダーに対応させるには多くの機器で実験し，MATT の拡張をする必要がある．

5 おわりに

本研究では，現存のネットワーク上の機器構成を変更することなく MAC アドレスのトレースバックを目的とし，システムを構築した．すべての端末を特定するまでには至らなかったが，今回構築した MATT は有用であると考える．今後は，トレースバック可能な機器を増やしていくと共に，ARP 情報や MAC アドレスのエージング時間外でもトレースバック可能になるようシステムを拡張する．同時に，ネットワーク管理者以外の利用を検討し，システムの有用性を高めていく予定である．

参考文献

[1] 門林雄基, 大江将史:“ IP トレースバック技術 ”, 情報処理学会学会誌, Vol.42, No.12, pp.1175-1180 (2001).

[2] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, “Hash-Based IP Traceback,” Proceedings of ACM SIGCOMM 2001, pp.3-14, (2001).

[3] PAFFI^{TM}, 横河電機株式会社, http://www.paffi.net/

[4] 元来くん，NTT データ　サイバー・ソリューションズ.

[5] Hiroaki Hazeyama, Masafumi Oe and Youki Kadobayashi: “An Layer-2 Extension to Hash-based IP Traceback,” IEICE Transactions on Information and Systems, Vol. E86-D, No. 11, pp. 2325–2333 (2003).