社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

Mesh of Trees トポロジにおけるトレースバックメッセージ伝達効率に関する一考察

宮本　大輔† 　櫨山　寛章† 　門林　雄基†

† 奈良先端科学技術大学院大学 情報科学研究科
〒 630–0101 奈良県生駒市高山町 8916–5
E-mail: †{daisu-mi,hiroa-ha,youki-k}@is.naist.jp

あらまし　本論文では，現在のインターネットのトポロジとして知られる Mesh of Trees トポロジにおける，トレースバックにおける追跡メッセージの伝達効率に関する考察を行う．IP トレースバック方式の 1 つである InterTrack [1] は逆探知を行うために送受信する追跡メッセージの数が，トポロジの複雑であればあるほど増加する．そこで，Mesh of Trees トポロジにおいてメッシュを構成するコア AS，ツリーを構成するリーフ AS，及びその中間にあたる中規模 AS にそれぞれトレースバック装置を配備した場合を想定する．この想定に基づき，CAIDA の提供する AS 隣接データセットを用い，各 AS 群にトレースバック装置を配備した際における，追跡メッセージ数と追跡可能性について調査を行い，メッセージ伝達効率を観察する．さらに，追跡メッセージの伝達効率が高い配備シナリオについて考察を行う．

キーワード　トレースバック，InterTrack, Mesh of Trees, トポロジ

A Consideration for Effectiveness of Traceback Messages Forwarding in Mesh of Trees Topology

Daisuke MIYAMOTO†, Hiroaki HAZEYAMA†, and Youki KADOBAYASHI†

† Graduate School of Information Science, Nara Institute of Science and Technology, Takayama 8916–5, Ikoma, Nara, 630–0101 Japan
E-mail: †{daisu-mi,hiroa-ha,youki-k}@is.naist.jp

Abstract　In this paper, we explain the effectiveness of traceback messages forwarding in mesh of trees network topology. Within our proposed IP traceback system, named InterTrack [1], the number of the messages for discovering the attack source and/or constructing attack path would increase when the network topology is complicated. We focus on mesh of trees network topology and assume our system deployed in the core ASes which organize mesh network, the leaf ASes which organize tree network, and other ASes, respectively. Based on this asusmption, We investigate both the number of traceback messages forwarding and the traceability for observing the effectiveness of traceback messages forwarding. Finally, we consider the deployment scenario for achieving high effectiveness.

Key words　Traceback，InterTrack, Mesh of Trees, Topology

1. はじめに

DDoS 攻撃の規模と被害は年々増加傾向にある [2]．DDoS 攻撃では送信元 IP アドレスが偽装されたパケットを攻撃パケットとして使うことが多く，その送信元を突き止めることは容易ではなかった．IP トレースバック技術は，このような DDoS 攻撃の攻撃パスを発見し送信元を特定手法する技術の 1 つとして提案され，今日でも様々な方式が研究されている．

代表的なトレースバック方式としては，通過するパケットとルータ情報を記載した追跡用パケットを生成し送信先 IP アドレスへ向けて送信する逆探知パケット方式 [3]，ルータを通過する際パケットのヘッダ部にルータ情報をある確率で記入するパケットマーキング方式 [4]，ルータなどにおいて配送するパケットのハッシュ値を保存するダイジェスト方式 [5] などが挙げられる．とりわけ，ダイジェスト方式はその追跡精度とパケットのハッシュ値のみを保存するためプライバシー保護といったセ

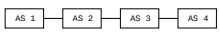


図 1　トポロジ A

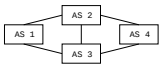


図 2　トポロジ B

キュリティ面の両方で実用化が期待されている．ダイジェスト方式では，各ルータの間でパケットのダイジェストを記録しているか否かを問い合わせることが求められる．このため，異なる組織間での問い合わせにおける効率面や運用面でのセキュリティ上の問題が指摘されている．

我々の先行研究 [1] では，各組織を Autonomous System (AS) 単位で集約して，AS 境界ルータ（ASBR）を通過するパケットのみをダイジェスト方式で記録し，AS 間でパケットの通過記録の問い合わせを行う相互接続アーキテクチャ “InterTrack” を提案した．InterTrack は，文献 [6] のような AS マップを用いた反復的な問い合わせ手法とは異なり，eBGP の AS の隣接関係だけを用いて再帰的に問い合わせを行う特徴を持つ．このため，InterTrack では隣接関係にある AS 全てに通過記録の問い合わせメッセージ（追跡メッセージ）が伝達される反面，追跡メッセージ数の増加によってネットワークが過負荷になる可能性を持つ．

本論文では，追跡メッセージ数が AS 間の隣接関係に依存している点に着目する．InterTrack における最も簡単な追跡メッセージ送受信アルゴリズムは Flood 型メッセージ転送方式 [7] である．Flood 型メッセージ転送方式では，追跡メッセージを受け取った AS は，追跡メッセージを送信してきた AS を除く全ての隣接 AS に対して追跡メッセージを中継する．例えば図 1 に示すような直線的なトポロジの場合，追跡メッセージ数は AS1 から AS2 へ，AS2 から AS3 へ，AS3 から AS4 へと計 3 個の追跡メッセージが発生する．同様に，図 2 に示すようなトポロジの場合 AS1 から AS2 と AS3 へ，AS2 から AS3 と AS4 へ，AS3 も同様に AS2 と AS4 へと計 5 個の追跡メッセージが発生する．このように，追跡メッセージ数はトポロジが複雑であればあるほど増加すると考えられる．

現在のインターネットのトポロジは，Mesh of Trees 型トポロジであると考えられている．Mesh of Trees 型のトポロジとは，任意の AS がそれぞれ無秩序に他の AS とピアリングしているのではなく，Tier 1 等と称される世界規模の広域ネットワークを所有する AS 同士がメッシュ状に接続し，これらの AS を頂点として他の AS がツリー状にぶらさがっているトポロジである．

これらをふまえ，本論文ではトレースバック装置を複数の AS に配備した場合におけるメッセージ伝達効率の考察を行う．本論文での考察は，トレースバック装置を 1〜50 台，それぞれメッシュを構成する AS，ツリーを構成する AS，その中間となる中規模 AS に配置した場合におけるメッセージ数を，追跡メッセージを送受信する装置の隣接関係の数で近似する．さらに，この隣接関係の数と，トレースバックが網羅できる範囲を AS 数，AS 間のリンク数を，日本国内に配備した場合について考察する．

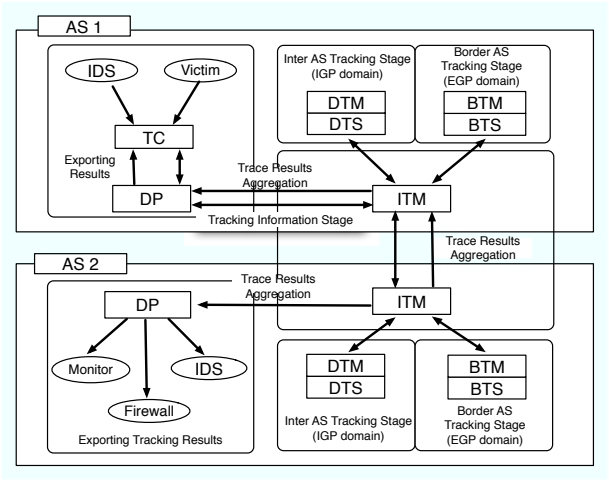


図 3　InterTrack 追跡手順

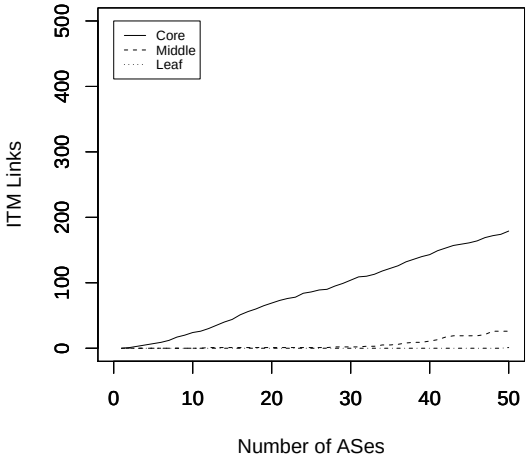


図 4　IP-TB 配備 AS 数と ITM 隣接リンク数

以下，2. 節にて関連研究について説明を行う．3. 節では追跡メッセージの伝達効率について初期調査を行い，4. 節において考察を行う．最後に結論を 5. 節に述べる．

2. 関 連 研 究

この節では，後の議論を正確にするため，InterTrack におけるメッセージ伝搬について説明する．

我々の提案した IntarTrack [1] は，AS 間を横断したダイジェスト方式の IP トレースバックを行うためのアーキテクチャである．このアーキテクチャでは主要なコンポーネントして ITM(Inter-domain Traceback Manager)，DP(Decision Point)，TC(Traceback Client)，DTM(Domain Traceback Manager)，BTM(Border Traceback Manager)，を定義している．

InterTrack におけるメッセージ伝搬について図 3 に示す．IP トレースバック (IP-TB) が行われるにあたり，攻撃を受けている被害者や IDS などの攻撃検知システムは TC に問い合わせを行うべきパケットのダイジェストを作成するよう依頼する．

TC の作成するダイジェストは直接 ITM に転送されるのではなく，一端 DP に集約される．DP は　ITM が過負荷にならないように TC からの追跡メッセージのとりまとめを行い，信頼できない TC からの追跡メッセージを排除する役割を担う．ITM は DP から追跡メッセージを受け取り，問題のパケットの流入 AS を BTM に問い合わせ，かつ発信源が自分か否かを DTM に問い合わせる．BTM や DTM は具体的には ITM と追跡メッセージの送受信する役割を担い，問題のパケットの具体的な状況については BTS や DTS 等のシステムと連携するモデルとなっている．攻撃が流入してきたことが分かった場合，ITM は隣接 ITM に対して追跡メッセージを送信し，隣接 ITM でも同様の追跡作業を再帰的に行う．

3. 追跡メッセージ伝達効率

本論文では 2. 節で述べた IP-TB を行う装置を，複数の AS に配備した場合におけるメッセージ伝達効率について考察を行う．本論文でのメッセージ伝達方式は Flood 型メッセージ方式を想定し，メッセージ伝達効率を ITM の隣接関係，すなわち追跡メッセージが送受信されるリンクの数によって近似する．また，ITM は AS の隣接関係に従って配備されることを想定する．AS 間の隣接関係の再現には CAIDA [8] が観測した AS 間の隣接関係データセットを用いた．CAIDA は隣接関係データセットを定期的に配布しており，本論文で用いたのは 2008 年 8 月 18 日のデータセットである．なお，本データセット内には日本国内 AS に隣接している AS のリンク数は 1,332 リンクであり，日本国内 AS 及びその隣接 AS の数は 649 であった．

次に，Mesh of Trees トポロジにおけるメッシュを構成する AS（コア AS）と，ツリーを構成する AS（リーフ AS）の分類について考える．本論文では，文献 [9] に示される AS ランクを基に，高い順からコア AS，低い順からリーフ AS として取り扱う．また，その中間に位置づける中規模 AS としては，少なくとも他の AS 1 つに対しトランジット AS として機能している AS から AS ランク値が低い順に選んだ．

日本国内の AS に対し，1〜50 のコア AS，中規模 AS 及びリーフ AS に IP-TB 装置を配備した時の ITM 隣接リンク数を図 2. に示す．x 軸は AS 数，y 軸は ITM 隣接関係のリンク数である．また，この場合の ITM 隣接構造のトポロジを図 5(a), 5(b), 5(c) に示す．50 AS に IP-TB 装置を配備する場合，コア AS 上位 50 組織に配置すると ITM 隣接リンクは 179 リンクになるのに対し，リーフ AS 下位 50 組織に配置した場合の隣接リンクは 1 であった．これは，下位 50 AS 群において隣接関係にある AS が 2 AS のみであり，トレースバックの目的である攻撃パスを発見可能な隣接リンクが 1 つだけとなる事を示す．

IP-TB 装置を配備した場合の追跡可能性について図 6(a), 6(b) に示す．図 6(a) は，x 軸が IP-TB 配備 AS 数，y 軸が AS 単位での追跡可能性，すなわち追跡可能性のある AS 数が日本国内のトポロジにおいて占める割合（パーセント表示）である．追跡可能性については文献 [9] で与えられる定義，すなわち IPTB を配備した AS (Strict AS) の数と，IP-TB 装置を配備していないが，隣接 AS に IP-TB が装置が導入されている AS が存在する AS (Loose AS) の数の和の AS トポロジ内での占める割合を用いた．また，図 6(a) は x 軸が IP-TB 配備 AS 数，y 軸が AS 間隣接リンク数単位での追跡可能性である．これらのグラフから，IP-TB を配備する AS を増やすことにより，追跡可能性は高まることが考える．

このように，配備する AS を増やした時，ITM 隣接リンク数が増えることにより追跡メッセージの総数が増えるが，追跡可能性も向上するため IP-TB の性能が上昇すると考えられる．視点を切り替えると，メッセージの伝達効率は，ITM 隣接リンク数の増加によって低下し，追跡可能性の向上によって上昇するのではないかと考えられる．ここで，単一追跡メッセージあたりの伝達効率 E を，IP-TB 配備 AS 数 n，AS 単位での追跡可能性 T_{as}，AS リンク単位での追跡可能性 T_{asl} を用いて 1 式で定義する．

$$E_{as} = T_{as}/n, \qquad E_{asl} = T_{asl}/n \tag{1}$$

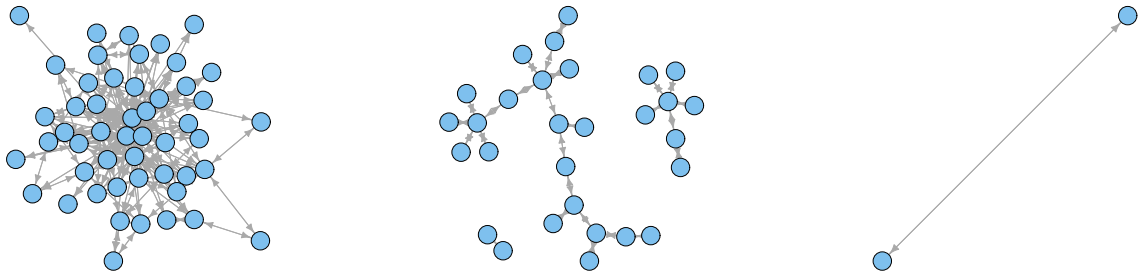
E の値が高い状態にあるときは，ITM 隣接リンク数が少なく，従って伝搬される追跡メッセージ数も少なく，それにも関わらず追跡可能性が高い状態である．翻って E の値が低い状態にあるときは ITM 隣接リンク数が多いために追跡メッセージ数も多く，追跡可能性がそれに反して高まらない状態にあることを示す．

単一追跡メッセージあたりの伝達効率を図 7(a), 7(b) に示す．x 軸は IP-TB 配備 AS 数，y 軸はそれぞれ伝達効率 E_{as}, E_{asl} を示す．コア AS，中規模 AS については配備 AS 数が少ない時にメッセージ伝達効率が高くなるが，配備 AS 数が多くなるについれて効率が低下する傾向が観測された．また，中規模 AS に関しては 27 AS をピークに導入する頃まで配送効率が上昇する傾向が観測された．なお，リーフ AS に関しては ITM 接続リンク数が図 2. の通り少ないため，グラフとして表示されていない．

4. 考　　察

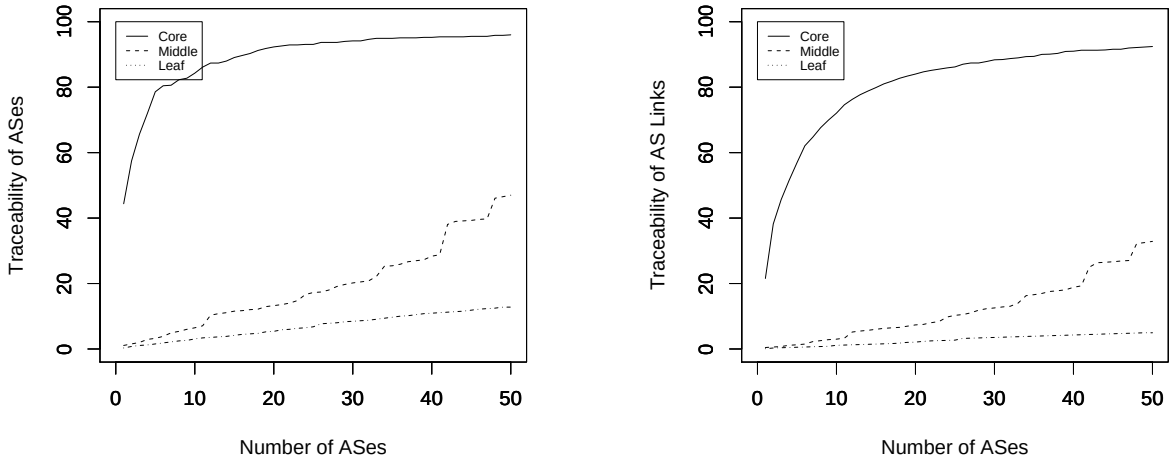
コア AS への IP-TB 装置の配備に関しては，配備した AS が少ない場合でも図 6(a), 6(b) に示した通り追跡可能性が高められる反面，配備した AS を増やし続けても可能性がさほど高まらない．反対に ITM 隣接リンク数は図 2. に示す通り AS 数に比例して増加している．このため，IP-TB を配備する AS を増やせば増やすほどメッセージ配送効率が下がると考えられる．反対に，中規模 AS は配備した AS 数が少ない場合は追跡可能性が高まらず，ある程度の AS 数になると追跡可能性が上昇する．ITM 隣接リンク数は低く，メッセージ配送効率は AS 数が比較的多い時にピークを迎えている．

そこで，コア AS のみに，または中規模 AS のみに IP-TB 装置を配備するのではなく，その両方に配備を行った場合におけるメッセージ伝達効率について考察する．文献 [9] では 20 のコア AS に IP-TB 装置が導入されてる場合に 90% 以上の追跡可能性があると考察されており，本論文ではコア AS から $1, 2, 3 \cdots 19$ 個の AS を，中規模 AS から $19, 18, 17 \cdots 1$ 個の



(a) コア AS　　(b) 中規模 AS　　(c) リーフ AS

図 5　IP-TB 配備 AS 数による ITM の隣接構造



(a) ITM 配備 AS 数と追跡可能性のある AS　　(b) ITM 配備 AS 数と追跡可能性のある AS 間リンク

図 6　ITM 配備 AS 数と追跡可能性

AS を抜き出し，配備する AS が 20 個となるようなトポロジを仮定する．

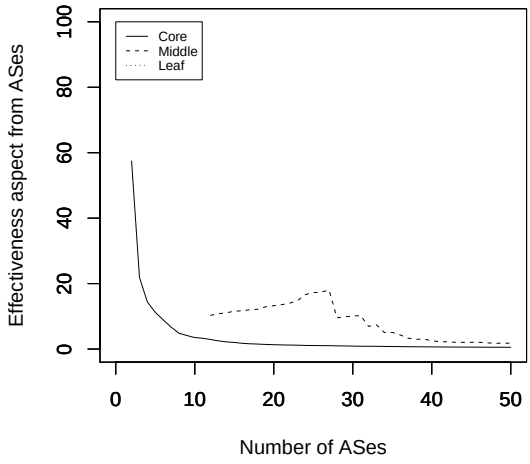
隣接 ITM リンク数を図 4. に示す．比較評価を行うため，コア AS と中規模 AS の混合 20AS 及びコア 20 AS の場合のグラフを表示している．x 軸はコア AS の数であり，混合 AS の場合は 20AS 中に占めるコア AS の数である．コア AS の ITM 隣接リンク数に加えて，中規模 AS の ITM 隣接リンク数が加わっているため，ITM 隣接リンク数は増加している．

追跡可能性 (T_{as}, T_{asl}) を図 9(a), 9(b) に示す．コア 5 AS のみの場合の追跡成功率 $(T_{as}, T_{asl} = 78.58, 56.91)$ に対し，中規模 15 AS を加えることにより追跡成功率は $(T_{as}, T_{asl} = 81.20, 63.21)$ に上昇することが確認された．ただし，IP-TB 装置がコア 15 AS に配備されている場合 $(T_{as}, T_{asl} = 89.06, 79.88)$，そこに中規模 AS を加えても $(T_{as}, T_{asl} = 89.68, 80.93)$ 効果は限定的である．

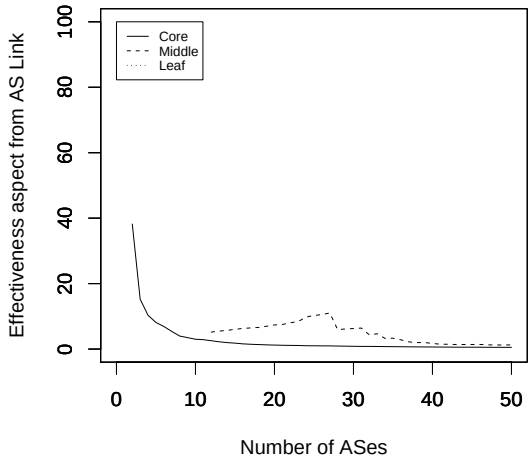
追跡メッセージの伝達効率 (E_{as}, E_{asl}) を図 10(a), 10(b) に示す．伝達効率に関しては，中規模 AS を加えることにより，コア AS のみの場合と比べて低下していることがわかる．これは，ITM 隣接リンク数の増加から比較からすると追跡可能性の増加は低調であるためと考えられる．従って，伝送効率の面から考えた場合，コア AS 以外の AS に IP-TB 装置を導入する利点は少ないと考えられる．

5. おわりに

本研究では，IP トレースバック (IP-TB) における追跡メッセージの伝達効率が，ネットワークトポロジの複雑さに依存している点に着目し，IP-TB 装置を配備した時のメッセージ伝達効率について初期調査を行った．現在のインターネットは Mesh of Trees トポロジーであり，Mesh を構成するコア AS，Tree を構成するリーフ AS 及びその中規模となる AS 群によっ

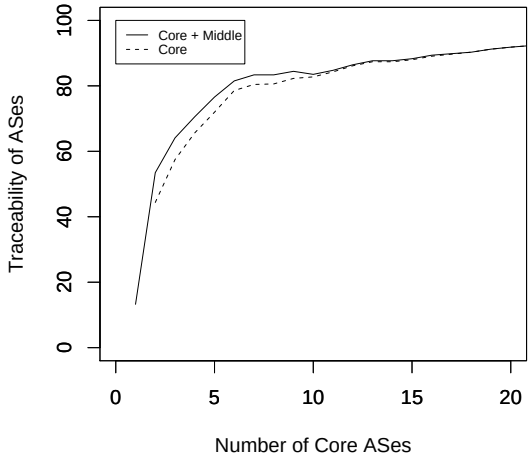


(a) 追跡可能 AS 数からみたメッセージ伝達効率

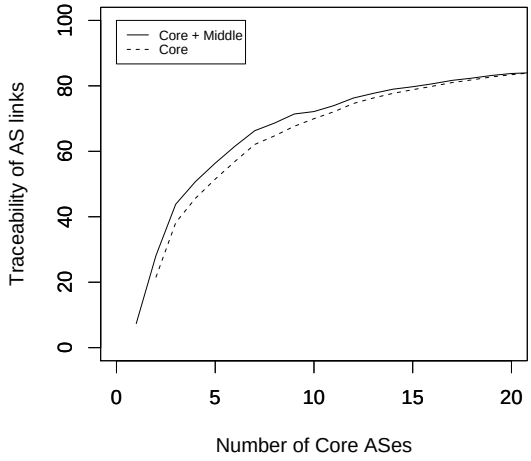


(b) 追跡可能 AS 間リンク数からみたメッセージ伝達効率

図 7　ITM 配備 AS 数とメッセージ伝達効率



(a) ITM 配備 AS 数と追跡可能性のある AS



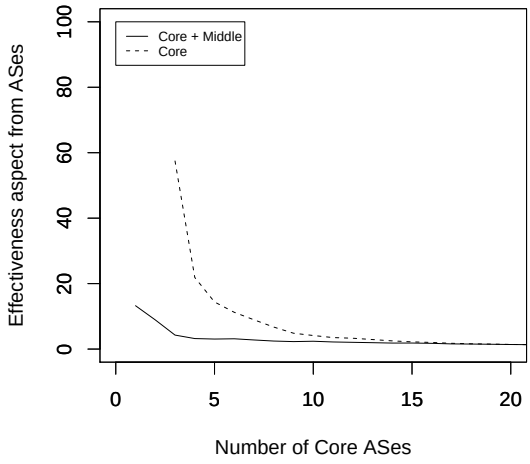
(b) ITM 配備 AS 数と追跡可能性のある AS 間リンク

図 9　ITM 配備 AS 数と追跡可能性

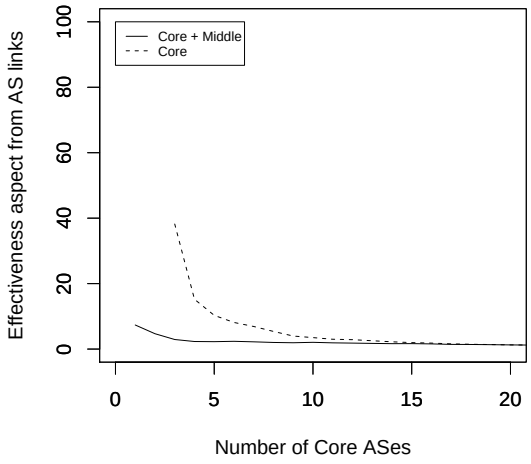
て分類できる．そこで，CAIDA の提供する AS 隣接データセットに対し，先行研究 [9] に示される AS ランク値を用いてコア AS，リーフ AS，及び中規模 AS のうちトランジット AS として機能している AS のうちランク値の高い中規模 AS をそれぞれ抽出した．また，各 AS 群に IP-TB 装置を配備した場合の伝達効率について考察を行った．

ITM の隣接リンク数が増えれば増えるほど，IP-TB の追跡メッセージの総数が増える．そこで本研究では，伝達効率を IP-TB 装置の先行研究 [9] に示される AS 単位の追跡可能性及び AS 間のリンク単位での追跡可能性を，IP-TB コンポーネントである ITM の隣接リンク数で除算した値と定義した．この上で，コア AS，中規模 AS 及びリーフ AS に配備していく 4 つの場合について，それぞれ ITM リンク数，追跡可能性，伝送効率を計測した．この結果，AS リンク数をコア AS の値をある程度増やしても伝送効率は低下する事象が確認された．また，中規模 AS を増加した場合，メッセージ伝達効率がピークとなる AS 数が，コア AS のみ，あるいは中規模 AS のみに配備したときと比較して多いことが観測された．

この観測結果に基づき，コア AS と中規模 AS の混合 AS に配備するシナリオが有効ではないかと推測し，考察を行った．



(a) 追跡可能 AS 数からみたメッセージ伝達効率



(b) 追跡可能 AS 間リンク数からみたメッセージ伝達効率

図 10　ITM 配備 AS 数とメッセージ伝達効率

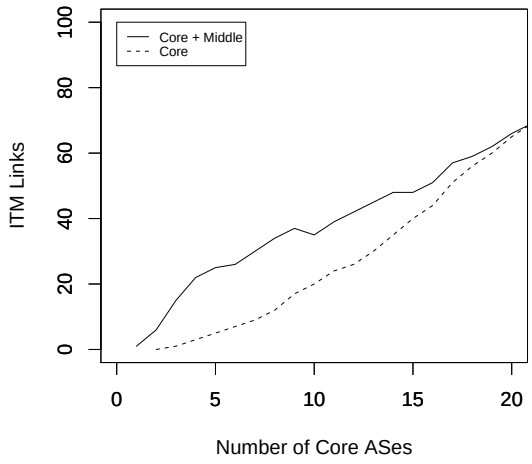


図 8　IP-TB 配備 AS 数と ITM 隣接リンク数

本考察では 20 AS に IP-TB 装置を導入する場合，コア 5AS と中規模 15AS に導入する場合，中規模 AS に配備することによる追跡可能性の向上が確認された．しかし，コア 15AS と 中規模 5AS に導入する場合，中規模 AS に配備したことによる追跡可能性の向上は微少であった．また，メッセージ伝送効率はコア AS のみの場合と比べて低下することが分かった．従って，IP-TB 機材の配備は小数上位のコア AS に対してのみ行う方が効率的であると考え，中規模 AS に配備する効果は乏しいと考えた．

謝　　辞

本研究は，独立行政法人情報通信研究機構の平成 17 年度からの委託研究「インターネットにおけるトレースバック技術に関する研究開発」の一部である．

文　　献

[1] H. Hazeyama, Y. Kadobayashi, D. Miyamoto, and M. Oe, “An autonomous architecture for inter-domain traceback across the borders of network operation,” Proceedings of 11th IEEE Symposium on Computers and Communications (ISCC ’06), pp.378–385, Jun 2006.

[2] D. McPherson, C. Labovitz and M. Hollyman, “WorldWide ISP Security Report Volume III.” Arbor Networks Technical Report, Sep. 2007.

[3] S. Bellovin, M. Leech, and T. Taylor, “ICMP traceback message,” IETF, Internet Draft, draft-ietf-itrace-04.txt, Feb. 2003.

[4] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” Proceedings of ACM SIGCOMM’00, pp.295–306, Aug. 2000.

[5] A.C. Snoeren, C. Partridge, L.A. Sanches, C.E. Jones, F. Tchakountio, S.T. Kent, and W.T. Stayer, “Hash-based IP traceback,” Proceedings of the 2001 conference on applications, technologies, architectures, and protocols for computer communications, pp.3–14, ACM Press, Aug. 2001.

[6] C. Gong, T. Le, T. Korkmaz, and K. Sarac, “Single packet ip traceback in as-level partial deployment scenario,” Proceedings of IEEE GLOBECOM 2005, Nov. 2005.

[7] H. Hazeyama, Y. Matsumoto, and Y. Kadobayashi, “Message Forwarding Strategies for Inter-AS Packet Traceback Network,” Proceedings of JWIS’07, Aug 2007.

[8] CAIDA, “Introduction to Relationship-based AS Ranking.” available at: http://www.caida.org/research/topology/rank_as/.

[9] 櫨山寛章, 若狭賢, 門林雄基, “実証実験に向けた IP トレースバックシステム導入シナリオに関する一考察,” 電子情報通信学会技術研究報告, IA2008-14, pp.25–30, July 2008.