L-028

エッジルータにおける DDoS 防御機能配備法に関する一検討

A study on edge-routers with DDoS Attack defense

吉田　順一‡　　片山　勝‡　　山田　博希‡

Junichi Yoshida　　Masaru Katayama　　Hiroki Yamada

１．はじめに

近年インターネットにおけるセキュリティ上の脅威として、ＤＤｏＳ（Distributed Denial of Service）攻撃が頻発しており、その対策が求められている。ＤＤｏＳ攻撃は、インターネット上に分散して設置された攻撃ノードから、攻撃ターゲットノード（サーバ）に対して大量のパケットを送ることによって、サーバ資源やネットワーク資源を消費させる攻撃である。なかでも、ネットワーク資源を消費させる攻撃は、ネットワーク全体に大きな影響を及ぼすものである。このため、キャリアやＩＳＰ（Internet Services Provider）においても、インターネットサービスを安定して提供するために積極的に対策をとる必要が増してきている。

ＤＤｏＳ攻撃に用いられるＩＰパケットの送信元アドレスは、攻撃元の特定を避けるために詐称されていることが多い。このため、ＩＰアドレス詐称に対する有効な対策の一つとして、イングレスフィルタ[1]がある。イングレスフィルタは、管理対象内部にないアドレスを送信アドレスに持つパケットが内部から出て行くときにフィルタを行う方法である。しかし、イングレスフィルタが全ＩＳＰで実装されていないと、他ＩＳＰの接続点からのトラヒックについて送信元アドレスの正当性を判断できない。また、イングレスフィルタは、攻撃パケットの送信アドレスがイングレスフィルタに設定されている範囲内であった場合はフィルタできない。さらに、攻撃者が踏み台を仕立てて攻撃を行った場合など、送信アドレスを詐称しないＤＤｏＳ攻撃の場合もフィルタできないといった問題がある。

このため、キャリアやＩＳＰにおけるＤＤｏＳ攻撃防御対策としてイングレスフィルタに加え、トレースバック[2]を行う方法が盛んに研究されている。トレースバック技術は、送信アドレスが詐称されたとしても、攻撃フローが通過した経路（流入経路）を特定し、攻撃ノード（攻撃元）を特定する方法である。トレースバックは、攻撃フローの流入経路であるルータの追跡に必要な情報を以降のルータに伝えることにより、ＩＳＰの境界を越えて攻撃ノードを特定することが可能となる。このため、複数のＩＳＰをまたがった遠いネットワークからの攻撃に対しても攻撃元に近いところで防御する方法として有効性が期待できる。

しかし、トレースバックは、複数のＩＳＰを越えて追跡を行う必要がある場合、攻撃元の特定には時間がかかるという問題がある。

この問題点の改善策の一つとして、マネージドされたＩＳＰ内部では、イングレスフィルタにより送信アドレスの正当性を保証できるため、ノード間連携により攻撃フローの流入点となっているエッジルータの特定をダイレクトに行うことが可能となる。このことから、ＩＳＰ内においては短時間でエッジノードでの帯域制限を行う方法として有効性が期待できる。

そこで、筆者らは、マネージドされたキャリアやＩＳＰ内におけるノード間連携を考慮したエッジルータにおけるＤＤｏＳ攻撃防御法（以下、３ステージ防御法と記す）を提案する。

３ステージ防御法とは、攻撃ターゲットノードの特定を行う１ st ステージと、エッジルータの入口で帯域制御を行う２ nd ステージと、攻撃フローの流入点となっているエッジルータでＤＤｏＳ攻撃パケットを特定しフィルタを行う３ rd ステージの３段階に分けてＤＤｏＳ攻撃防御を行う方法である。

本稿では、３ステージ防御法の実現の可能性を明らかにするために、ＩＳＰで必要とされるＤＤｏＳ防御機能の条件を明確化し、３ステージ防御法のアーキテクチャと連携動作について論じる。また、３ステージ防御法の特徴を考慮したエッジルータの実装法について論じる。さらに、シミュレーションにより評価を行う。

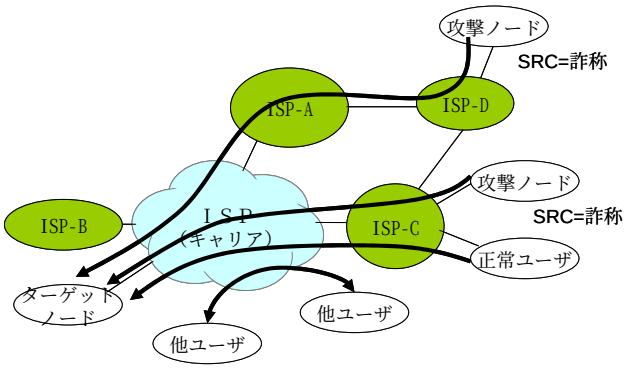

図１　ＤＤｏＳ攻撃モデル

２．前提条件

2.1 ＤＤｏＳ攻撃モデル

本稿が前提とするＤＤｏＳ攻撃モデルを図１に示す。ＤＤｏＳ攻撃に用いられるＩＰパケットの送信元アドレスは、攻撃元の特定を避けるためにランダムなアドレスで詐称されている。また、ＤＤｏＳ攻撃は、複数のマシンからターゲットに対して一斉に攻撃を行う。これにより、ネットワーク資源が消費され、攻撃ターゲットノードだけではなく他のトラヒックに対しても影響がある。

2.2 キャリアやＩＳＰでの防御に必要な機能

2.1 で述べたＤＤｏＳ攻撃モデルに対してキャリアやＩＳＰにおけるＤＤｏＳ攻撃防御対策に必要な機能を以下に示す。

（１）ターゲットノードの防御

（２）他のトラヒックへの影響の回避

（３）ターゲットノード宛のトラヒックの帯域制限などを行うことで、間接的にターゲット間で通信を行っている

‡（社）電子情報通信学会, IEICE

正常ユーザトラヒックまでも影響を与えてしまうことの回避

3．ノード間連携

3.1 ノード間連携の概要

ノード間連携とは、攻撃を検知するエッジルータとＤＤｏＳ攻撃の帯域制限するエッジルータがお互いに連携することで、ＤＤｏＳ防御対策を実現する方法であり、連携により通知する情報は、攻撃ターゲットノードを識別する情報（宛先アドレス）である。

図２に示すように、ＩＳＰ内のエッジルータがそれぞれ連携動作し、ターゲットノードに最も近いエッジルータでＤＤｏＳ攻撃を検知した場合、攻撃フローの流入点となっているエッジルータに攻撃ターゲットノードを識別する情報を通知し、そこで帯域制限を行う。

ＩＳＰと接続しているエッジルータでは、ターゲットノード宛のアドレスで帯域制限を行い、ユーザを直収するエッジルータでは、ターゲットノード宛のアドレスに対して帯域制限を行い、その後、攻撃フローを特定してフィルタを行う。

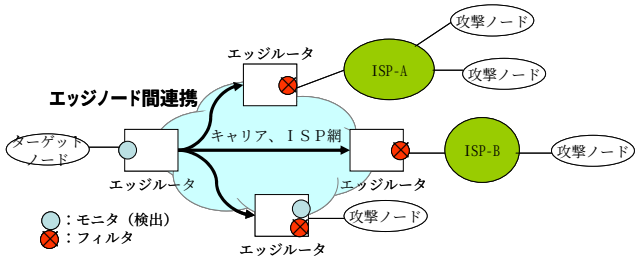

図２　エッジノード間連携

3.2 課題

前提とするＤＤｏＳ攻撃モデルは、攻撃ノードに近づくにつれて相対的にトラヒック量が減るため、エッジルータにおいて必ずしも最適な帯域を設定できない可能性がある。よって、ターゲットノード宛のトラヒックについて帯域制限を行いすぎることで、間接的にターゲット間で通信を行っている正常ユーザトラヒックまでも影響を与えてしまう可能性がある。

4．エッジルータにおける３ステージ DDoS 防御法の概要

4.1　提案アーキテクチャ

３ステージ防御法は、攻撃ターゲットの特定を行う１ st ステージと仮防御の２ nd ステージ、攻撃フローの特定および防御を行う３ rd ステージの３つに分離し、１ st ステージと２ nd ステージ間はノード内連携（ｉ）、２ nd ステージと３ rd ステージ間はノード間連携（ii）で行うアーキテクチャとなっている。

１ st ステージは、ターゲット宛の全てのパケットが通過する Egress 側でトラヒックをモニタし、フラッド型攻撃パケットフローを識別する。２ nd ステージは、識別した攻撃被疑パケットに対して、全経路の Ingress 側ラインカードで帯域制御を行い、ルータのスイッチ、アクセス網の帯域資源の消費を防ぐ。また、３ rd ステージは、（ii）ノード間連携により通知を受けたターゲット宛のフローに対して帯域制限を行い、ＩＳＰ内のネットワーク帯域の消費を防ぐ。その後、攻撃被疑フローに対して攻撃フローの特定を行い、攻撃者の直近でフィルタする。

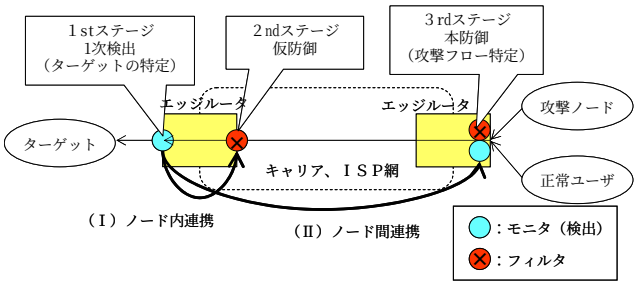

図３　３ステージ防御法

4.2　動作

提案法における動作について、一般的な閾値による検出、帯域制限手法に沿って述べる。

ＤＤｏＳ攻撃を検知すると、ノード内連携によりまず検知したエッジルータの全経路の Ingress 側ラインカードでターゲット宛のパケットを制限し始める。トラヒックがある閾値を越えた場合に攻撃とみなして検出を行い、あらかじめ定義された閾値まで帯域制御を行う。

２ nd ステージが仮防御を行うと同時に、ノード間連携により他エッジノードに検出情報の通知を行い攻撃フローの流入点となっているエッジルータでＤＤｏＳ攻撃のフィルタを期待する。ノード間連携により通知を受けたエッジルータは、ターゲット宛のトラヒックの帯域制限を行う。エッジルータが配下にユーザを収容する場合は、さらに攻撃被疑フローに対して攻撃フローの絞込みを行い、フィルタ或いは帯域制御を行う。

１ st ステージでの攻撃トラヒックの減少と、2nd ステージでの廃棄の状況とあわせて３ rd ステージでの帯域制限の状況を判断し、2nd ステージでの帯域制御を解除する。2nd ステージでの帯域制限解除と同時に、ノード間連携により他エッジノードに解除可能情報の通知を行う。解除可能通知を受けた 3rd ステージにおいて廃棄パケットを含めターゲット宛のトラヒック変化を監視しターゲット宛のトラヒックが閾値を下回ると、３ rd ステージのフィルタを解除する。

3rd ステージにおいてフィルタ設定後、タイムアウト以内に解除可能通知を受信しない場合は、フィルタ閾値をあらかじめ定義された設定に従って、自動的に下げる。

5.　評価

5.1　実装法

エッジルータは、経済化が要求されると共に、将来の変更にも柔軟に対応可能な機能拡張性への要求も増してきている。このため、各分析（１ st ステージ、３ rd ステージ）の特徴を考慮して効率的に実装する必要がある。１ st ステージは、常時監視を行う必要があり、扱うフロー数も多いためラインカード毎に分散して行うことが望ましい。３ rd ステージは、受動的分析（１ st ステージから要求があったときのみ実施される）により攻撃者のみフィルタを行い、正常ユーザを救済する。このため、フローカウンタだけでなくステート監視等の詳細分析を行う必要があり、実装性のよい構成が望まれる。そこで以降では３ rd ステージの構成について議論する。

以下に、アクセス網側ラインカード型、キャリア網側ラインカード型およびサービスカード型の３案を提案し、使用効率、制御性、機能変更追加の容易性の観点から評価を行

う。

（１）アクセス網側ラインカード型（図４-A 参照）

攻撃被疑パケットフローが全て通過するアクセス網側ラインカードで攻撃フローの特定を行なう。

（２）キャリア網側ラインカード型（図４-B 参照）

ステート監視（パケット双方向監視）のため攻撃被疑パケットフローが通過するキャリア網側ラインカードに全ての攻撃被疑パケットフローの応答も転送（コピー等）し攻撃フローの特定を行なう。

（３）サービスカード型（図４-C 参照）

双方向の攻撃被疑パケットフローをサービスカードに送り、攻撃フローの特定を行なう。

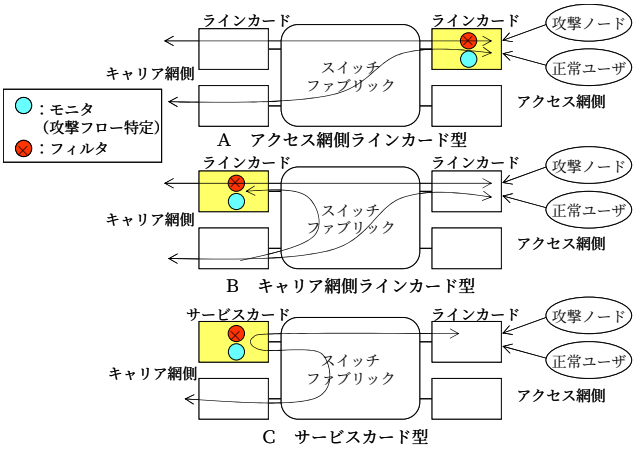

図４　３ rd ステージの実装法

5.2　比較評価

アクセス網側ラインカード型は、転送制御が不要である点で優れているが、機能変更追加の容易性、ハードウェアリソースの使用効率などの点でサービスカード型と比べて不利である。

キャリア網側ラインカード型は、アクセス網側ラインカード型と比べてハードウェアリソースの使用効率の点で優れているが、キャリア網側ラインカード数Nだけ転送先があり転送制御が複雑である。

サービスカード型では、サービスカードへの転送制御が必要となるが、上記２つのラインカード配備法と比べ、ハードウェアリソースをより有効に利用でき、高性能、高スループット化に向いている。表１に各実装法の評価を示す。

表１．各方式の評価

	使用効率	制御性	機能変更追加の容易性
A　アクセス網側ランカード型	×	○ 転送制御不要	× 全ラインカードの変更
B　キャリア網側ラインカード型	△ トラヒック多重による効果	× 転送先がN	× 全ラインカードの変更
C　サービスカード型	○ 集約による効果	△ 転送先が固定	○ サービスカードのみの変更

5.3　閾値設定に関する検討

ノード間連携により、３ rd ステージに最適な帯域制限を行うことが重要となる。帯域制限は、短時間で攻撃を収束させるためにノード間連携による通知回数を少なくする必要がある。また、帯域制限を行うことで正常ユーザのトラヒックまで影響を及ぼすことを考慮して段階的に帯域制限を強くする必要がある。そこで、効率よく帯域制限値を設定する方法として、二分探索について検討を実施した。

設定する閾値のチューニングには二分探索を適用する。3rd ステージにおいてフィルタ設定後、タイムアウト以内に解除可能通知を受信しない場合ごとに、現在の閾値と最大閾値の中央値を選択する。この方法をタイムアウト以内に解除可能通知を受信しない場合ごとに繰り返す。

閾値のチューニングを行なう場合に、閾値設定の効率性がどの程度であるか、シミュレーションした結果を図５に示す。図５は、閾値チューニングを行った回数を横軸に、帯域制限値を縦軸に計算したものである。

図５から、閾値初期値に関係なく３回の交換で８０%以上の帯域制限を設定できることが分かった。さらに、帯域制限が強くなるほど刻み幅が細かくなり、帯域制限を行いすぎることの抑止に有効性が期待できる。

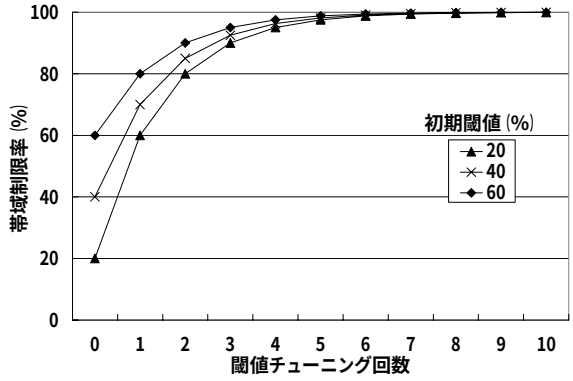

図５　閾値チューニング効率

6．おわりに

キャリアやＩＳＰのエッジルータにおけるＤＤｏＳ防御法に関する検討を行い、３ステージ防御法により、ターゲットの防御、他のトラヒックへの影響の回避が可能となる方法を提案した。また、３ステージ防御法の特徴を考慮したエッジルータにおける実装方式について述べ、３ rd ステージはサービスカード方式が効率性と機能拡張性や経済化を両立させた実装が可能であることを示した。さらに、帯域制限値をチューニングする方法として二分探索を適用することにより、効率よく帯域制限を行うことが可能であることを示した。

他のＤＤｏＳ攻撃への対応

本提案では、ＤＤｏＳ攻撃の中でもフラッド型攻撃に対しての防御法の検討を行った。しかし、実際には、ＤＤｏＳ攻撃の一つにすぎず、他のＤＤｏＳ攻撃に対し防御法の検討を行う必要があると思われる。

参考文献

[１]D.Senie. Network Ingress Filtering :Defeating Denial of Service Attacks which employ IP Source Address Spoofing,5 2000. RFC2827

[２] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Practical Network Support for IP Traceback," Proc. ACM/SIGCOMM, pp. 295--306, August 2000.