大規模DDoS攻撃対処を想定した 高可用なネットワークアーキテクチャの提案

前田　浩明† 小島　久史† 相原　正夫†

† 日本電信電話株式会社 NTT ネットワーク基盤技術研究所

あらまし 近年、大規模な DDoS 攻撃が発生しており、ISP 等の広域ネットワーク (NW) において、攻撃通信を DDoS 対策装置へ転送して対処する際に、通信路やデータセンタの入口のネットワークが輻輳することで、DDoS 攻撃に対処しきれない可能性がある。一方で、SDN、NFV 等の仮想化技術により、サーバ等のコンピューティングリソースやネットワークリソースを柔軟に割り当てて利用できるようになっており、ネットワーク内に存在する余剰リソースを活用することで、大規模 DDoS 攻撃対処における問題を解決し、可用性を向上させられる可能性がある。本稿では、大規模な DDoS 攻撃に対処する場合において、従来の DDoS 攻撃対処に加えて、ネットワーク内に存在する余剰リソースを有効活用することで、通信サービスの可用性を向上させるネットワークアーキテクチャを提案した。また、提案アーキテクチャの実現に必要な技術を提案し、その有効性を示した。

キーワード DDoS 攻撃，可用性，仮想化，ネットワーク負荷分散，輻輳回避

A Proposal of High-Available Network Architecture against Large-Scale DDoS Attacks

Hiroaki MAEDA†, Hisashi KOJIMA†, and Masao AIHARA†

† NTT Network Technology Laboratories

Abstract ISPs cope with massive DDoS attacks by forwarding DDoS traffic to DDoS mitigation appliances. Considering the scale of recent DDoS attacks, DDoS traffic may congest network links and entry points of data center where DDoS mitigation appliances are located. The introduction of SDN/NFV technologies enables ISPs to flexibly allocate redundant network and computing resources in order to improve availability against massive DDoS attacks. In this paper, we propose a high-availability network architecture which can deal with massive DDoS attacks and improve service availability. We also clarify elemental technologies which constitute the architecture and propose the solutions. Finally, we evaluate the our proposed solutions and show the effectiveness.

Key words DDoS Attacks, Availability, Virtualization, Network Load Balancing, Congestion Avoidance

1. まえがき

ISP 等の広域ネットワークでは、ルータ等から収集したフロー情報等の解析により、特定の宛先に対する DDoS 攻撃の発生を検知した場合、ネットワークの入口で標的宛の全通信を破棄する（正常通信も破棄されるためサービスは停止）というブラックホールルーティングだけでなく、標的宛の通信を DDoS 対策装置に転送して詳細に検査することで、正常通信と攻撃通信を識別し、攻撃通信のみを遮断する（正常通信は通過させることでサービス停止を防ぐ）といった、高度な対処を行っている [1], [2]。一方で、近年、数 100Gbps クラスの大規模な DDoS 攻撃が発生しており [3]、攻撃通信を DDoS 対策装置まで転送する際に特定の経路やデータセンタ（DC）に通信が集中した場合、ネットワークが輻輳することで、標的のサービスだけでなく、ネットワークやデータセンタを共用する他の通信サービスも巻き添えでサービス不能になる恐れがある。また、DDoS 対策装置の性能やコ

スト観点で設置台数が限られることから、想定以上の大規模攻撃が発生した場合にも標的のサービスを守りきることはできない。深刻度は標的のサービスに依存するが、DNS サーバ等が標的となった場合は、インターネットの利用ができなくなる可能性もある [4]。

このような状況の中、SDN、NFV 等の仮想化技術により、サーバ等のコンピューティングリソースやネットワークリソースを柔軟に割り当てて利用できるようになっており、ネットワーク内に存在する余剰リソースを活用することで、前述の大規模 DDoS 攻撃対処における問題を解決し、可用性を向上できる可能性がある。

本稿では、大規模な DDoS 攻撃に対処する場合において、従来の DDoS 攻撃対処に加えて、ネットワーク内に存在する余剰リソースを有効活用することで、通信サービスの可用性を向上させるネットワークアーキテクチャを提案する。また、提案アーキテクチャの実現に必要な技術を提案し、その有効性を示す。

2 章では、本稿で対象とする DDoS 攻撃のパターンについて述べる。3 章では、提案するアーキテクチャの概要とアーキテクチャを構成する装置について述べ、アーキテクチャを実現する上での技術課題を述べる。4 章では、3 章で述べた技術課題のうち、DDoS 攻撃対処の際の利用経路と各経路への収容量算出アルゴリズムの検討について述べる。5 章では、3 章で述べた技術課題のうち、提案アーキテクチャに適したネットワーク経路制御方式の検討について述べる。6 章は、本稿のまとめと今後の課題である。

2. 対象とする DDoS 攻撃のパターン

検討に際して、攻撃の流量と、ネットワークに攻撃が流入するエッジノード（外部との接続点）数に着目して、DDoS 攻撃を表 1 のように分類し、考察を行った。

攻撃の流入するエッジノード数が多く、各エッジノードの流量が少ない場合（例：世界中のオープンリゾルバや Botnet を用いた DDoS 攻撃（DNSamp 攻撃等））には、DDoS 対策装置の設置されたデータセンタに近づくにつれて通信が集まり、ネットワークが輻輳することで、他サービスに影響を及ぼす恐れがある。一方で、余剰リソースの活用により、DDoS 攻撃通信を分散できれば、他サービスに影響を与えずに、DDoS 攻撃に対処できる可能性があるため、本稿では、この DDoS 攻撃のパターンを対象とした。

3. 提案アーキテクチャ

3.1 提案アーキテクチャのコンセプト

提案アーキテクチャのコンセプトを図 1 に示す。前提として、DDoS 対策装置やサーバは仮想化されており、（例えば、DDoS 対策装置の場合はライセンスで決められ

表 1 対象とする DDoS 攻撃のパターン

	1エッジノードにおける攻撃量大（各エッジノードの有するリンクの総収容量以上の場合）	1エッジノードにおける攻撃量小（各エッジノードの有するリンクの総収容量未満の場合）
攻撃の流入するエッジノード数多（攻撃の総量がDC付近のリンクの収容量以上の場合）	×（ブラックホールルーティングにより、攻撃パケットを遮断するor より上流のネットワークで対処する以外で対処不能）	○（適切な制御により、他サービスに影響を与えずに、対処できる可能性あり）
攻撃の流入するエッジノード数少（攻撃の総量がDC付近のリンクの収容量未満の場合）	×（同上）	有効だが考慮不要（ネットワーク帯域を逼迫せず、他サービスにも影響がないため制御不要）

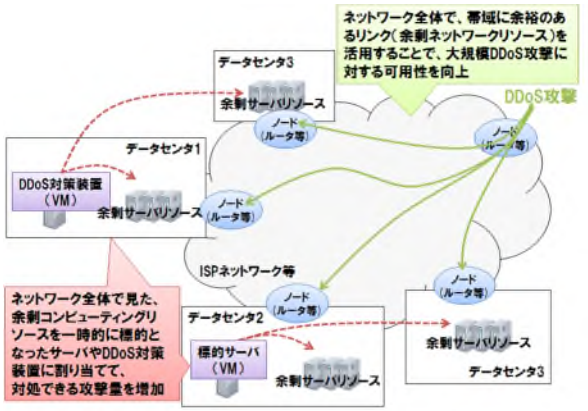

図 1 提案アーキテクチャのコンセプト

たリソースの範囲内で）柔軟にリソースを増減可能とする。提案アーキテクチャでは、ISP 等の広域ネットワーク内に存在する複数のデータセンタにおける、予備系の物理サーバのリソース（余剰コンピューティングリソース）を DDoS 対策装置や標的サーバに一時的に割り当て、対処可能な DDoS 攻撃量を増加させることで、サービスの可用性を向上させる。また、コアネットワークにおいて、攻撃発生時点で利用率の低いリンクの帯域（余剰ネットワークリソース）を活用して DDoS 攻撃通信を DDoS 対策装置まで転送したり、複数のデータセンタに通信を振り分けて、特定の経路・データセンタへの通信集中によるネットワーク輻輳を回避することで、サービスの可用性を向上させる。

3.2 提案アーキテクチャの構成と各装置の機能

提案アーキテクチャを構成する装置と各装置の機能を図 2 に示す。オーケストレータは、コアネットワークとデータセンタを横断したネットワーク全体でのリソース（ネットワークリソース、コンピューティングリソース）を管理する。また、ルータやスイッチ等のネットワーク機器から収集したトラヒック情報や負荷情報に基づき、攻撃の発生やネットワークの輻輳を検知し、それらに対処するためのシナリオを生成する。生成したシナリオは、コアネットワークにおいて、ルータ等を動的に制御するコアネットワークコントローラと各データセンタにおいて、仮想マシン（DDoS 対策装置、標的サーバ）の複製

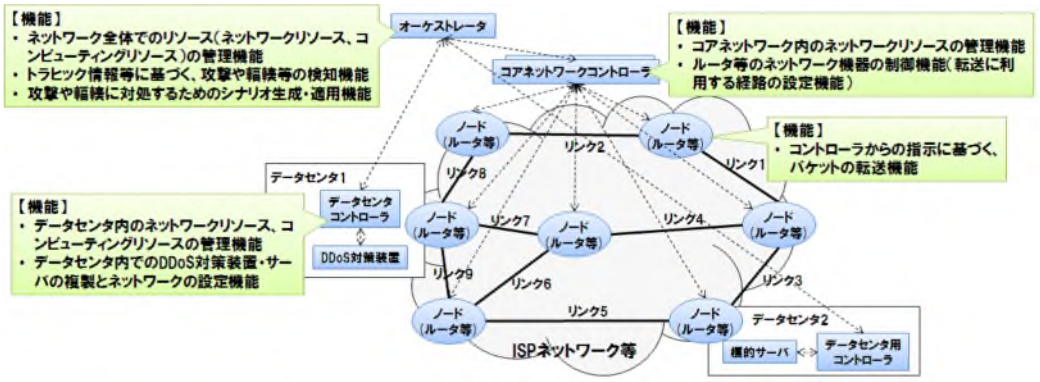

図 2　提案アーキテクチャの構成と各装置の機能

やネットワークの設定を行うデータセンタコントローラを介して実行される。

3.3　DDoS 攻撃に対する可用性を向上させるための対処シナリオ

オーケストレータで生成する対処シナリオとして、本稿では、ISP 等で実用化されている DDoS 攻撃対処（i）に加えて、DDoS 攻撃に対する可用性を向上させるための対処（ii, iii, iv）を提案する。なお、各シナリオを実現するための機能は、第 3.2 節で述べた各装置の機能を組み合わせて実現される。

i. DDoS 攻撃の検知と対処

特定のサーバに対する DDoS 攻撃の発生を検知した場合に、攻撃通信を DDoS 対策装置に転送して対処することを目的としたシナリオであり、次の機能により実現される。

(i-a) DDoS 攻撃検知機能

ルータやスイッチ等のネットワーク機器から定期的に収集したトラヒック情報やフロー情報を解析することで、特定のサーバに対する DDoS 攻撃の発生を検知する。

(i-b) 標的サーバ宛通信をエッジノードから DDoS 対策装置に転送する機能

コアネットワークコントローラの指示に従い、攻撃の流入するエッジノード等において、標的となったサーバ宛の通信のみを DDoS 対策装置まで転送する。

ii. コアネットワークにおける転送路の輻輳の検知と対処

攻撃通信を DDoS 対策装置まで転送する際の転送経路上で輻輳が発生した場合に、帯域に空きのあるリンクを活用して通信を分散させることで輻輳を回避することを目的としたシナリオであり、次の機能により実現される。

(ii-a) ネットワーク輻輳検知機能

ネットワークの各リンクの帯域使用率に基づき、輻輳（または閾値を設定して、輻輳の予兆）を検知する。

(ii-b) 輻輳回避に利用する経路と各経路に収容する通信量の算出機能

標的サーバ宛の通信の転送に利用する新たな経路および元の経路との間での通信の分散量を算出する。

(ii-c) 算出した経路に標的サーバ宛通信を分散させる機能

コアネットワークコントローラを介して通知された経路（ii-b で算出した経路）に、通知された割合で標的サーバ宛の通信を分散させる。

iii. データセンタ入口ノードにおける輻輳の検知と対処

特定のデータセンタ内で、DDoS 対策装置のリソースを増加させる際に、データセンタ入口ノードの帯域にこれ以上余裕がない場合に、コンピューティングリソースとネットワーク帯域に空きのある他のデータセンタに DDoS 対策装置を複製して、エッジノード等から広域ネットワークワイドで通信を分散させることで、特定のデータセンタへの通信集中による輻輳を回避することを目的としたシナリオであり、次の機能により実現される。

(iii-a) データセンタの入口ノードの輻輳検知機能

DDoS 対策装置の設置されたデータセンタの入口ノードの負荷を監視することで輻輳の予兆を検知する。

(iii-b) DDoS 対策装置の複製機能

データセンタコントローラを介して、DDoS 対策装置を他のデータセンタに複製する。

(iii-c) 標的サーバ宛通信をエッジノードから複数のデータセンタに存在する DDoS 対策装置に分散させる機能

コアネットワークコントローラを介して、エッジノード等を制御し、ネットワークワイドで標的サーバ宛通信を複数データセンタの DDoS 対策装置に分散させる。

iv. DDoS 対策装置による対処の限界の判断と対処

DDoS 対策装置の性能やコスト観点で設置数が限られることから、利用可能な DDoS 対策装置の範囲内では攻撃に対処しきれない場合に、標的のサーバ自体を複製して通信を分散させることで、サービスの可用性を向上させることを目的としたシナリオであり、次の機能により実現される。

(iv-a) DDoS 対策装置による対処の限界の判断機能

DDoS 対策装置で利用可能なリソース量と DDoS 攻撃量を比較することで、利用可能な DDoS 対策装置の範囲内では対処しきれない攻撃量であることを判断する。

(iv-b) 標的サーバの複製機能

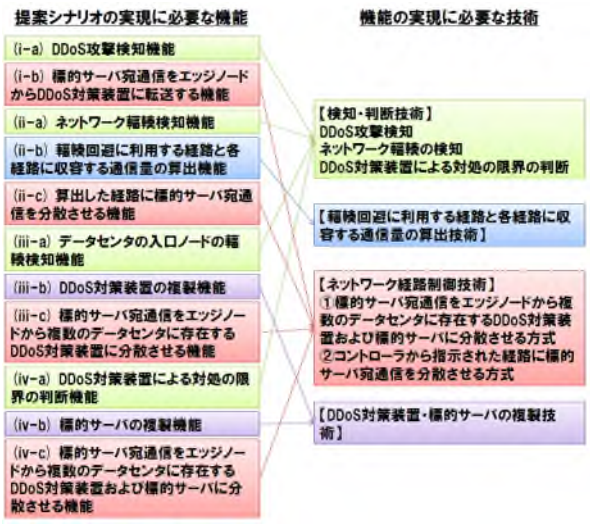

図 3　提案シナリオを実現する機能と機能の実現に必要な技術

データセンタコントローラを介して、標的のサーバ自体を複数のデータセンタに複製する。

(iv-c) 標的サーバ宛通信をエッジノードから複数のデータセンタに存在する DDoS 対策装置および標的サーバに分散させる機能

コアネットワークコントローラを介して、エッジノード等を制御し、DDoS 対策装置だけでなく、標的サーバ（オリジナル・複製したもの）にも通信を分散させる。

なお、本稿では、他の通信サービスに影響を与えないように、標的のサーバ宛の通信のみを、攻撃の検知を契機に制御することを想定しており、非攻撃発生時や他の通信サービスのパケットは、任意のルーティングプロトコルで転送される。

3.4　提案アーキテクチャの実現に必要な技術と課題

第 3.3 節のシナリオ (i～iv) を実現する機能と機能の実現に必要な技術を図 3 に示す。

検知・判断技術に関して、DDoS 攻撃の検知は、例えば、SAMURAI [1], [2] が利用可能である。SAMURAI では、NetFlow [5] や sFlow [6] 等を用いて、ルータ等から収集したフロー情報を分析することで、特定の宛先 IP アドレスに対する DDoS 攻撃の発生を検知する。また、コアネットワークやデータセンタ入口ノードの輻輳検知も同様に、NetFlow や sFlow 等のフロー情報の分析により実現可能である。さらに、DDoS 対策装置による対処の限界の判断は、例えば、オーケストレータ等のネットワーク全体を管理する装置において、DDoS 対策装置で利用可能なリソース量の上限と観測した攻撃量を比較することで実現可能と想定される。

輻輳回避に利用する経路と各経路に収容する通信量の算出技術に関して、DDoS 攻撃の場合、攻撃の発生する時間帯や攻撃の流入地点、攻撃の規模等の予測が困難なため、利用する経路と各経路へ収容する通信量を事前に設定しておくことは難しく、攻撃の発生後に、攻撃の流入地点や攻撃量、ネットワークの各リンクにおける利用可能帯域を考慮して、転送に利用する経路や各経路へ収容する通信量を迅速に算出する必要がある。線形計画法を用いた既存方式 [7]～[9] では、ネットワーク全体で最適な経路・収容量の組み合わせを求めるため、今回対象の大規模なネットワークや第 2 章で述べた多数のエッジノードから攻撃が流入する DDoS 攻撃の場合には、迅速な求解ができない可能性があり、迅速性を重視したアルゴリズムを検討する必要がある。（⇒第 4 章）

ネットワーク経路制御技術に関して、次の 2 つの動作を実現できる必要がある（図 4）。

① 標的サーバ宛通信をエッジノードから複数のデータセンタに存在する DDoS 対策装置および標的サーバに分散させる（i-b, iii-c, iv-c より抽出）

② コアネットワークコントローラから通知された複数の経路に標的サーバ宛通信を分散させる（ii-c より抽出）

①に関して、標的サーバ宛通信をエッジノードから DDoS 対策装置まで転送するための技術としては、BGP 経路広告により標的サーバ宛通信の転送先を一時的に DDoS 対策装置宛に変更する方式 [10] が存在するが、標的サーバ宛通信を複数の宛先（DDoS 対策装置や標的サーバ）に分散させる制御を実現できないため、提案アーキテクチャにそのまま適用することはできない。他の方式としては、OpenFlow を用いてフローテーブルを変更することで標的サーバ宛通信を DDoS 対策装置に転送する方式 [11] が存在し、パケットの 5tuple を用いることで、フロー単位で任意のデータセンタの任意の装置に通信を分散できるが、エッジノードから目的のデータセンタまでの経路上の全てのノードのフローテーブルを変更する必要があるため、ISP のような大規模なネットワークに適用する場合、スケーラビリティの課題がある。以上より、①の動作を大規模なネットワークで迅速に実現可能なネットワーク経路制御方式を検討する必要がある。（⇒第 5 章）

②に関して、Segment Routing(SR) [12], [13] や OpenFlow 等を用いて標的サーバ宛通信の転送に利用する経路を変更することで実現可能と想定される。このため、いくつかの方式の中から、迅速性やスケーラビリティの観点で、本稿で想定している輻輳回避の実現に適した方式を検討する必要がある。（⇒第 5 章）

DDoS 対策装置・標的サーバの複製技術に関して、DDoS 対策装置やサーバが仮想化されている場合、仮想マシンのスナップショットやデータを別のデータセンタの物理サーバに転送して仮想マシンを複製する技術は実用化されており、それらの技術で実現可能と想定される。

以上を踏まえ、第 4 章では、DDoS 攻撃通信の転送に利用する経路と各経路に収容する通信量を攻撃発生後に

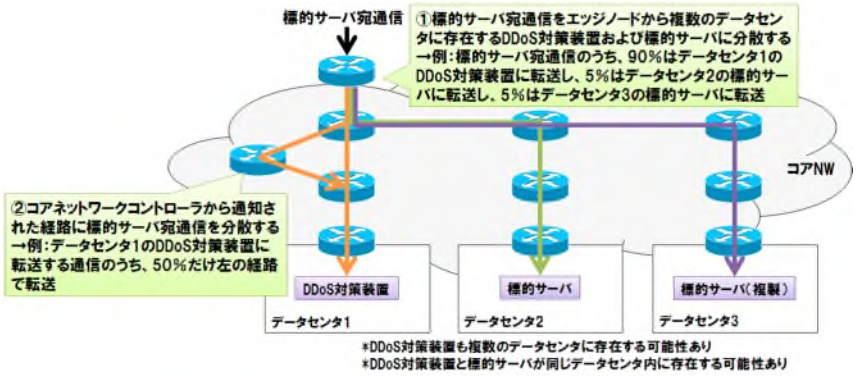

図 4　提案アーキテクチャの実現に必要なネットワーク経路制御方式の動作

図 5　DDoS 攻撃対処の際の利用経路と各経路への収容量を算出する問題の定義

迅速に算出するためのアルゴリズムを提案する。また、第 5 章では、①や②の動作を実現するネットワーク経路制御方式を提案する。

4. DDoS 攻撃対処の際の利用経路と各経路への収容量算出アルゴリズム

4.1　問題の定義

検討に先立ち、利用経路と各経路への収容量の算出に関する問題を、図 5 のように定義した。ここでは、あるリンクで輻輳を検知した際に、利用経路算出アルゴリズムを用いて輻輳回避のための経路を生成し（問題 i）、その結果を各経路への収容量算出アルゴリズムの入力とすることで各経路に収容する通信量を決定する（問題 ii）。

4.2　アルゴリズムの要件

第 4.1 節で述べた問題 i、ii を実現するアルゴリズムには、以下の要件が求められる。

要件 1：高速に結果を算出できること

DDoS 攻撃の場合、攻撃の発生する時間帯や攻撃の流入地点、攻撃の規模等の予測が困難である。このため、攻撃の流入するエッジノードから、DDoS 対策装置までの経路における輻輳を回避するためには、攻撃の発生後に、攻撃の流入地点や攻撃量、ネットワークの各リンクにおける利用可能帯域を考慮して、利用する経路や各経路に収容する通信量を迅速に算出できなければならない。また、攻撃者が攻撃パターンを変化させた場合に、再計算が必要なことからも迅速性が重視される。

要件 2：大規模なネットワークに適用できること

ISP 等の大規模なネットワークでの利用を想定しているため、ノード数やリンク数が数千以上の規模の場合にも、利用経路と各経路へ収容する通信量を迅速に算出できる必要がある。

4.3　既存方式を利用した場合の課題

第 4.2 節で述べた要件を満たす方式を検討するに当たり、まず、既存方式の適用可否を考察する。

ルータ、スイッチ等の通信機器をノード（ノード集合：V）、機器間をつなぐケーブルをリンク（リンク集合：E）とし、ネットワークをノードとリンクの集合で構成されるグラフ $G = (V, E)$ で表現した場合に、リンクの利用可能帯域やネットワークのトポロジ情報、各ノードペア（今回は、攻撃が流入するエッジノードと DDoS 対策装置の設置されたデータセンタの入口ノード間）の通信需要（今回は、標的サーバ宛の通信量）等を入力として与え、特定のリンクに対するトラヒック集中を回避するように、利用する経路と各経路へ収容する通信量を決定する問題は、ネットワークフローの割り当て問題として次のようにモデル化でき、線形計画法のアルゴリズム（単体法等）を用いて解くことが可能である [7]〜[9]。

$$\text{目的関数：} F \rightarrow min \tag{1}$$

$$\text{制約条件 1：} \sum_{r \in R_k} x_r = d_k \ (for\ k \in K) \tag{2}$$

$$\text{制約条件 2：} \sum_{r \in R} a_{lr} \cdot x_r - u_l \cdot F \leqq 0 \ (for\ l \in E) \tag{3}$$

(1) 式は、特定のリンクに対するトラヒック集中を避けるため、全てのリンクのリンク容量使用率の中で最大の値を表す F を最小化する目的関数である。また、(2) 式は、需要収容制約を表し、(3) 式は、リンク容量使用率制約を表す。

なお、パラメータと変数はそれぞれ以下である。

・パラメータ ･･･ 需要が与えられるノードペアの集合：K, 通信を収容する経路の集合：R, ノードペア k を結ぶ経路の集合：R_k, ノードペア k に対する通信需要：d_k, リンク l の容量：u_l, 経路 r の経由リンク：a_{lr} (= 1 ならば経路 r はリンク l を経由する)

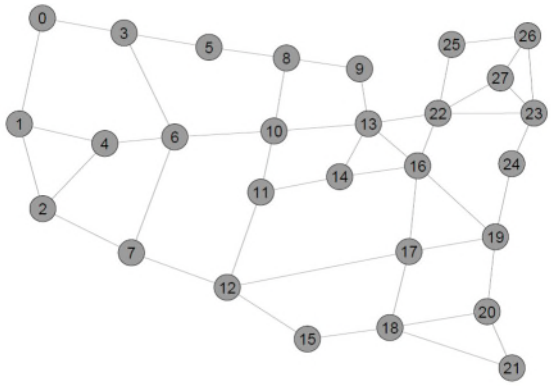

図 6　評価に用いたネットワークのトポロジ 1

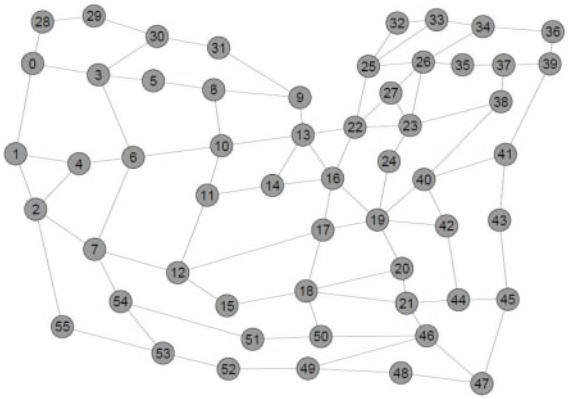

図 7　評価に用いたネットワークのトポロジ 2

・変数（全て非負）… 経路 r に収容する通信需要：x_r, 最大リンク容量使用率：F

本モデルでは、各ノードペアの通信需要を収容するための候補経路を予め用意しておく必要があり、候補経路が膨大になる大規模なネットワークに適用するのは難しい。これに対して、文献 [9] では、最初は、各ノードペア間で 1 つの経路を用意して与えられた需要の収容可否を線形計画問題を解くことで判定し、需要が収容しきれない場合は、各ノードペア間で新たな経路を生成して再度収容可否を判定するといったように、候補経路を逐次生成しながら線形計画問題を解くことで、問題規模を抑える方式（列生成法）が説明されている。

本方式では、通信需要が与えられるノードペア数を $v \in V$ とすると、需要の収容可否を判定するための線形計画問題の計算量は、単体法の場合、約 $O(vE)$、候補経路生成のための計算量は、ダイクストラ法の場合、約 $O(ElogE)$、幅優先探索の場合、約 $O(vE)$ である。全体の計算量は、各計算量を加算したもの（例えば、$O(vE)+O(vE)$）になり、通信需要が与えられるノードペア数やネットワークの総ノード数、総リンク数が増加するに従い、計算時間が増加するという課題がある。

このため、ISP 等の大規模なネットワークの場合や第 2 章で述べた DDoS 攻撃のように攻撃が多数のエッジノードから流入する場合には計算量が増加するため、候補経路の探索と各経路に収容する通信量の算出が迅速にできず、要件を満たせない可能性がある。

4.4　提 案 方 式

第 4.3 節で述べた既存方式の課題を解決するために、ネットワークの大きさに依存しない方式を提案する。提案方式では、輻輳を検知したリンクの両端のノードのみを対象に輻輳回避処理を行うことで、問題の規模を縮小し、利用経路と各経路に収容する通信量を高速に算出可能となる。具体的なアルゴリズムを以下に示す。

問題 i. 輻輳を回避するための経路の探索

標的サーバ宛の通信を DDoS 対策装置の設置されたデータセンタに任意の経路で転送中に、あるリンクの輻輳を検知した場合、元々のネットワークトポロジからそのリンクを除いたネットワークトポロジを対象に、そのリンクの両端のノード間を接続可能な新たな経路を探索する。例えば、ノード i とノード j を結ぶ リンク (i,j) が輻輳と検知されたとすると、リンク (i,j) の両端のノードである、ノード i とノード j を対象に、リンク (i,j) を利用しない新たな経路を探索する。なお、経路探索アルゴリズムとして、本稿では、ノード i とノード j のそれぞれから幅優先探索を行い、共通するノードに到達するまでの経路を組み合わせることでノード i とノード j 間の経路を生成する双方向幅優先探索を用いた。

問題 ii. 各経路に収容する通信量の算出

i において、ノード i →ノード k →ノード j という経路が生成されたとする。元の経路に含まれるリンク（リンク (i,j)）と、新たな経路に含まれるリンク（リンク (i,k), リンク (k,j)）の中から、経路毎に利用可能帯域が最小のリンクを抽出し、抽出したリンクの利用可能帯域の和に対する各経路の最小の利用可能帯域の割合を算出する。ノード i に標的サーバ宛の通信が到達した場合、算出した割合に従い、各経路に通信を分散することで輻輳回避を行う。例えば、元の経路では、リンク (i,j)、新たな経路では、リンク (k,j) が利用可能帯域が最小のリンクとすると、標的サーバ宛通信を

$$\frac{\text{リンク } (i,j) \text{ の利用可能帯域}}{(\text{リンク } (i,j) \text{ の利用可能帯域} + \text{リンク } (k,j) \text{ の利用可能帯域})}$$

の割合で、元の経路に分散し、

$$\frac{\text{リンク } (k,j) \text{ の利用可能帯域}}{(\text{リンク } (i,j) \text{ の利用可能帯域} + \text{リンク } (k,j) \text{ の利用可能帯域})}$$

の割合で、新たな経路に分散する。

4.5　提案方式の評価

4.5.1　評 価 概 要

第 4.4 節で述べた提案方式の有効性を評価するために、文献 [14], [15] で用いられている、米国の通信ネットワークのトポロジ（図 6）と図 6 をベースにノード数とリンク数を 2 倍に拡張したトポロジ（図 7）を対象に、表 2 の条件の下、シミュレーション評価を行った。

ここでは、DDoS 対策装置の設置されたデータセンタの入口ノードをノード 1 とし、時間経過とともに、ノー

表 2　シミュレーション条件

対象とするネットワークのトポロジ	【トポロジ1】 U.S. Long-Distance Network ノード数：28、リンク数45
	【トポロジ2】 トポロジ1を元に、ノード数・リンク数を2倍に拡張したもの ノード数：56、リンク数90
DDoS対策装置の設置されるデータセンタノード	ノード1
攻撃発生時点での各リンクの利用可能帯域	10Gbps
シミュレーション時間	600sec
DDoS攻撃の通信量	【攻撃パターン1】1回の生起あたり、3Gbps
	【攻撃パターン2】1回の生起あたり、1.5Gbps
DDoS攻撃の発生するノード数の最大値	【攻撃パターン1】10か所
	【攻撃パターン2】20か所
DDoS攻撃の発生頻度	約10sec毎にデータセンタノード以外のノードをランダムに選択して攻撃発生
DDoS攻撃の持続時間	600sec
シミュレーション試行回数	1000回

表 3　トポロジと攻撃パターンの組み合わせ

①	トポロジ1＋攻撃パターン1
②	トポロジ2＋攻撃パターン1 （ノード数、リンク数：2倍）
③	トポロジ2＋攻撃パターン2 （ノード数、リンク数、攻撃の発生するノード数：2倍）

ド 1 を除く、最大 10 個のランダムなノードから DDoS 攻撃が流入してくる場合に、それらの通信をノード 1 まで転送する状況を想定した。各ノードからノード 1 までの最短経路をデフォルトルートとして予め設定し、DDoS 攻撃が発生した際には、まず、デフォルトルートで転送を行う。その後、任意のリンクで輻輳が発生した場合、提案方式または従来方式による輻輳回避処理を実施し、A. 輻輳回避にかかった時間と B. シミュレーション終了までの間にデータセンタの入口ノードまで転送できた DDoS 攻撃量を比較評価した。また、A. 輻輳回避にかかった時間は、ネットワークのノード数、リンク数、DDoS 攻撃の発生するノード数が変化した場合の各方式への影響を評価するため、表 3 に示す 3 パターンについて評価した。

なお、比較のための従来方式として、第 4.3 節で述べた、候補経路を逐次生成しながら線形計画問題を解く方式を用いた。また、従来方式において、輻輳回避のための経路探索アルゴリズムは提案方式と同様の双方向幅優先探索を、線形計画問題を解くためのアルゴリズムは単体法をそれぞれ用いた。

4.5.2　評 価 結 果

図 8 に、A. 輻輳回避にかかった時間の比較評価結果（トポロジ 1、攻撃パターン 1 の場合）を示す。ここでは、ネットワーク内の複数リンクで同時に輻輳が発生した場合には、全てのリンクの輻輳が回避されるまでの時間を計測した。図 8 より、提案方式は、問題の規模を輻輳リンク周辺のノードのみに縮小できることで、従来方式と比較して、経路探索時間と各経路に収容する通信量

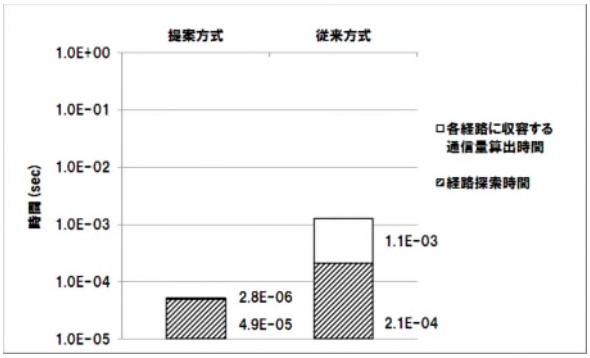

図 8　輻輳回避にかかった時間の比較評価（トポロジ 1、攻撃パターン 1 の場合）

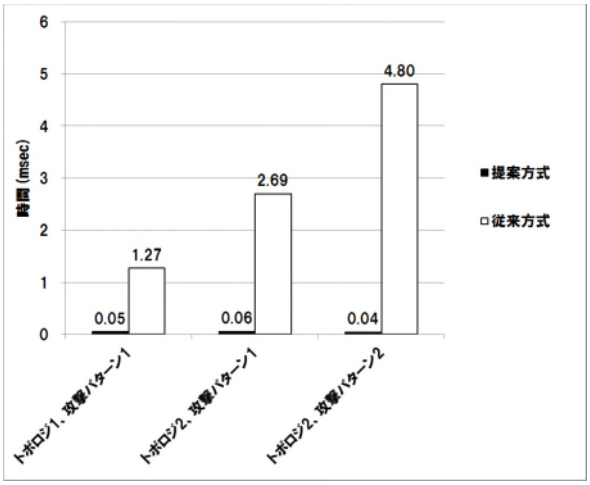

図 9　輻輳回避にかかった時間の比較評価 2

算出時間の両方を短縮可能である。また、経路探索と各経路に収容する通信量算出のトータルでは、従来方式の 10 分の 1 以下の時間まで短縮できている。

図 9 に、ネットワークのノード数、リンク数、DDoS 攻撃の発生するノード数を変化させた場合の A. 輻輳回避にかかった時間の比較評価結果を示す。図 9 より、従来方式は、リンク数や DDoS 攻撃の発生するノード数の増加に比例して計算時間が増加しており、リンク数と DDoS 攻撃の発生するノード数の両方を 2 倍にした、（トポロジ 2、攻撃パターン 2）の場合は、（トポロジ 1、攻撃パターン 1）の場合と比較して、計算時間が約 4 倍になっている。一方で、提案方式は、輻輳リンク周辺のノードのみに問題規模を縮小可能なため、ネットワークの規模や DDoS 攻撃の発生するノード数に依存せずに高速な算出ができている。このため、提案方式は、ISP 等の大規模なネットワークにおいて、多数のエッジノードから DDoS 攻撃が流入してくるような場合に特に優位だと考えられる。例えば、文献 [16] の Tier1 のネットワーク（ノード数 600 以上、リンク数 5000 以上）において、多数のノードから攻撃が流入してくる場合、従来方式では、結果の算出に約 10 秒かかるのに対して、提案方式

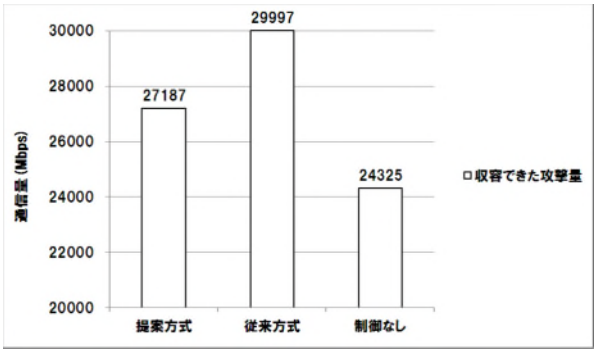

図 10　データセンタノードまで転送できた DDoS 攻撃量の比較評価（トポロジ 1、攻撃パターン 1 の場合）

では、1 ミリ秒未満に短縮できる可能性がある。

図 10 に、B. データセンタの入口ノードまで転送できた DDoS 攻撃量の比較評価結果（トポロジ 1、攻撃パターン 1 の場合）を示す。図 10 より、従来方式は、ネットワークに流入する通信需要（DDoS 攻撃量）の全体を見て、ネットワーク全体としての最適な経路と収容量を算出するため、発生した DDoS 攻撃量のほとんどをデータセンタノードまで転送可能である。一方で、提案方式は、輻輳回避の制御を実施しない場合と比べて、約 12% 多くの通信をデータセンタまで転送可能だが、従来方式と比較すると、約 10% 性能が劣る。これは、例えば、リンク (4, 1) の輻輳を回避する際に、ノード 4 →ノード 6 →ノード 3 →ノード 0 →ノード 1 のような経路が生成される可能性があり、ノード 6 →ノード 4 →ノード 6 →ノード 3 … のように特定ノード間を通信が往復することで、無駄に帯域が消費されることに起因している。これに対処する方法としては、例えば、(ノード 0, ノード 1, ノード 4, ノード 6, ノード 3) の局所的なトポロジを抽出し、そのトポロジに流入する攻撃量を局所的なトポロジ全体として最適に収容するような線形計画問題を解くことが考えられるが、具体的なアルゴリズム等は今後の課題である。

5. 提案アーキテクチャに適したネットワーク経路制御方式

5.1 ネットワーク経路制御方式の要件と既存技術の適用性

第 3.4 節で述べた①, ②の動作を実現するネットワーク経路制御方式は、以下の要件を満たすことが望ましい。

要件Ⓐ 迅速に適用可能なこと

要件Ⓑ スケーラビリティが高く大規模なネットワークにも適用可能なこと

また、①の動作（ネットワークワイドでの通信の分散）を実現する方式は、攻撃者が通信先のサーバを指定して攻撃できないように、次の要件を満たす必要がある。

要件Ⓒ ネットワーク側で通信をどの装置に分散するかを制御できること

①に関して、広域ネットワークワイドで通信を複数の宛先に分散させる技術としては、DNS ラウンドロビンが存在するが、キャッシュ等の仕組みにより、DNS の設定を変更してから、ネットワーク全体に設定が浸透するまでに時間がかかる場合があり、要件Ⓐを満たせない。また、クライアントの接続するサーバをネットワーク側から完全には制御できないため、攻撃者がサーバの IP アドレスを直接指定して攻撃してきた場合に対処できず、要件Ⓒを満たせない。このため、本稿では、IP レイヤで制御を行うことで、既存技術の課題を解決する方式を提案する。

5.2 エッジノードから DDoS 対策装置/標的サーバまでの通信の転送と分散（①）の実現案と評価

他サービスの通信に影響を与えず、標的サーバ宛通信のみを制御するため、ラベルにより正常パケットとの区別が可能なセグメントルーティング (SR) [12], [13] とオーバーレイのトンネリング方式に着目した案 a、案 b を提案する。

案 a : SR とトンネリングで実現 (図 11 左)

エッジノードにおいて、コアネットワークコントローラから通知された DDoS 対策装置のデータセンタ入口ノードを表す Segment ID をパケットに付与することで標的サーバ宛通信をデータセンタ入口ノードまで転送する。データセンタ入口ノードから DDoS 対策装置（の仮想スイッチ）までは、データセンタコントローラ経由で事前設定したトンネルを用いることで転送を実現する。

また、コアネットワークコントローラからの指示に従い、任意のデータセンタの入口ノードを表す Segment ID をパケットに付与することで、複数データセンタ間でのフロー単位等での通信の分散を実現する。データセンタ入口ノードから DDoS 対策装置または標的サーバ（オリジナル・複製したもの）までは、装置毎に異なるトンネルを設定することでデータセンタ入口ノードから各装置までの通信の分散を実現する。

案 b : トンネリングで実現 (図 11 右)

コアネットワークコントローラ、データセンタコントローラを介して、エッジノードと DDoS 対策装置の仮想スイッチ間でトンネルを設定し、トンネルを用いて標的サーバ宛通信を転送することで実現する。

また、DDoS 対策装置、標的サーバに対して、エッジノードから異なるトンネルを設定し、コアネットワークコントローラの指示に従い、フロー単位等で利用するトンネルを選択することで、複数のデータセンタに存在する任意の装置間での通信の分散を実現する。

2 案の比較評価を表 4 に示す。ここでは、迅速性（要件Ⓐ）とスケーラビリティ（要件Ⓑ）に関わる項目を評価した。攻撃が流入するエッジノード数を N、DDoS 対策

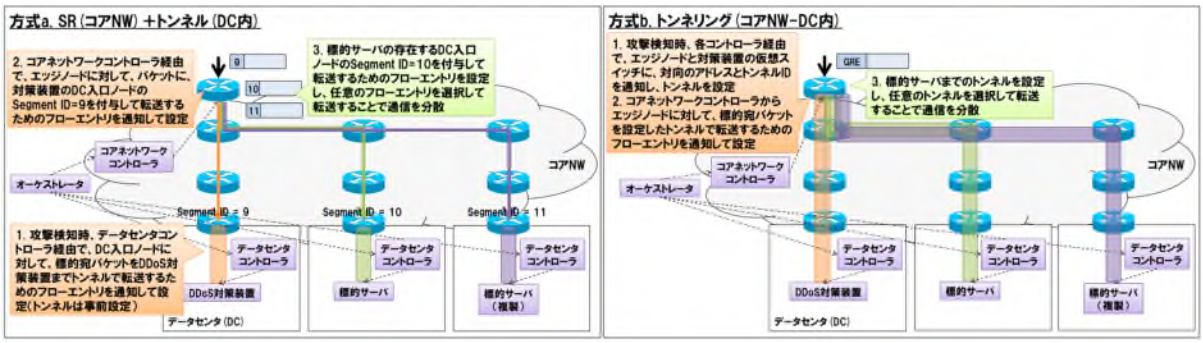

図 11　エッジノードから DDoS 対策装置/標的サーバまでの通信の転送・分散（①）の実現案

装置数を m、標的サーバ数を n とすると、案 a は、案 b と比較して、実現に 2 つの技術を併用する必要があるが、設定の必要なトンネル数を $N \times (m+n)$ 分から $(m+n)$ 分に抑えることができ、特に数百、数千といった多数のエッジノードから攻撃が流入する場合には、攻撃発生時に必要な処理を低減できる点で優れる。また、案 a は、DDoS 対策装置や標的サーバの仮想スイッチに設定するフローエントリ数が DC 入口ノードとの間でトンネルを用いて通信するために必要な 1 行だけで良いため、案 b と比較して、攻撃の流入するエッジノード数が増加した場合にも、各装置の仮想スイッチのフローエントリ数が増加せず、スケーラビリティの観点で優位である。一方で、案 a は、データセンタ入口ノードにもフローエントリを設定して制御する必要があるが、フローエントリの行数は、高々$(m+n)$ 分であり、影響は極小と考えられる。さらに、案 a は、同一データセンタ内で、DDoS 対策装置や標的サーバを複製して通信を分散させる場合には、エッジノードの制御が不要であり、データセンタ内に閉じた制御だけで実現できるという利点がある。

5.3　コアネットワークにおける輻輳回避（②）の実現案と評価

IP レイヤでの制御により、コアネットワークにおける高速な輻輳回避を実現する案 c、案 d を提案する。

案 c：SR で実現 (図 12 左)

コアネットワークコントローラからの指示に従い、輻輳回避に利用する経路を表す Segment ID をパケットに付与して転送することで、②を実現する。

案 d：フローエントリの変更で実現 (図 12 右)

コアネットワークコントローラからの指示に従い、輻輳回避に利用する経路上の任意のノードにおいてフローエントリを変更することで、②を実現する。

2 案の比較評価を表 5 に示す。案 c は、案 d と比較して、利用する経路のホップ数に比例して必要なラベル数が増加するため、パケットのオーバーヘッドが増加するが、制御が必要なノード数とコントローラの処理を常に 1 ノード分に抑えることができる点で優れる。なお、案 c の場合でも、元々のオーバーヘッドが小さい（ラベル

表 4　エッジノードから DDoS 対策装置/標的サーバまでの通信の転送・分散（①）の実現案の比較評価

		a. SR（コアNW）+トンネル（DC内）（U-PlaneがMPLSの場合で記載）	b. トンネリング（コアNW-DC内対策装置）
コントローラからノードへの通信回数 *1	エッジノード	攻撃の流入するエッジに対して、フローエントリの通知 →N回（同一DC内に複製する場合は不要）	攻撃の流入するエッジに対して、フローエントリの通知 →N回
		トンネルの設定は不要	攻撃の流入するエッジに対して、トンネル設定のための情報を通知 →N回
	DC入口ノード	装置の複製等をしたDC入口ノードに、フローエントリ通知 →1回	フローエントリの設定は不要
		装置の複製等をしたDC入口ノードに、トンネル設定のための情報を通知 →1回	トンネルの設定は不要
	対策装置・標的サーバの仮想スイッチ	複製された装置に、フローエントリの通知 →1回	エッジ数分のフローエントリの通知 →N回（まとめて通知可能）
		複製された装置に、DC入口ノードまでのトンネル設定のための情報の通知 →1回	エッジ数分のトンネル設定のための情報を通知 →N回（まとめて通知可能）
フローエントリの行数	エッジノード	（対策装置・標的サーバの存在するDC数）分 →m+n行	（対策装置＋標的サーバ数）分 →m+n行
	DC入口ノード	対象のDC内に存在する（対策装置＋標的サーバ数）分 →各DC入口ノードに1行ずつ	なし
	対策装置・標的サーバの仮想スイッチ	（DC入口ノード数）分 →1行	（攻撃の流入するエッジ数）分 →N行
設定の必要なトンネル数		（対策装置＋サーバ数）分必要 →m+n個	エッジ数×（対策装置＋サーバ数）分必要 →N×（m+n）個

- 攻撃が流入するエッジノード数N、DDoS対策装置数m、標的サーバ数n、DDoS対策装置や標的サーバが別々のデータセンタに存在する状況を想定
- Nは数10～数1000程度、mとnは最大10程度
- DC：データセンタ

*1：攻撃検知時と対策装置や標的サーバの複製時に実施

表 5　コアネットワークにおける輻輳回避（②）の実現案の比較評価

	c. SR（U-PlaneがMPLSの場合で記載）	d. フローエントリの変更
コントローラからノードへの通信回数	○ 上流側ノードに、フローエントリ通知 →1回の処理で1ノードのみ	△ 経路上のノードに、フローエントリ通知 →3ノード
コントローラで生成すべき情報量	○ 輻輳回避のためのフローエントリの生成 →1回の処理で1種類のみ	△ 輻輳回避のためのフローエントリの生成（経路上のノード毎に異なる） →3種類
制御のためのパケットのオーバーヘッド	○ 1ラベル毎に4byte増加 →8byte増加	○ なし

*輻輳回避に利用する経路のホップ数が3の場合

1 つにつき、4byte）ため、大量のパケットに対処する際にも影響は極小だと考えられる。

5.4　想定するシナリオ全体での評価

第 5.2 節、第 5.3 節より、想定するネットワーク経路制御を大規模なネットワークにおいて迅速に実現するた

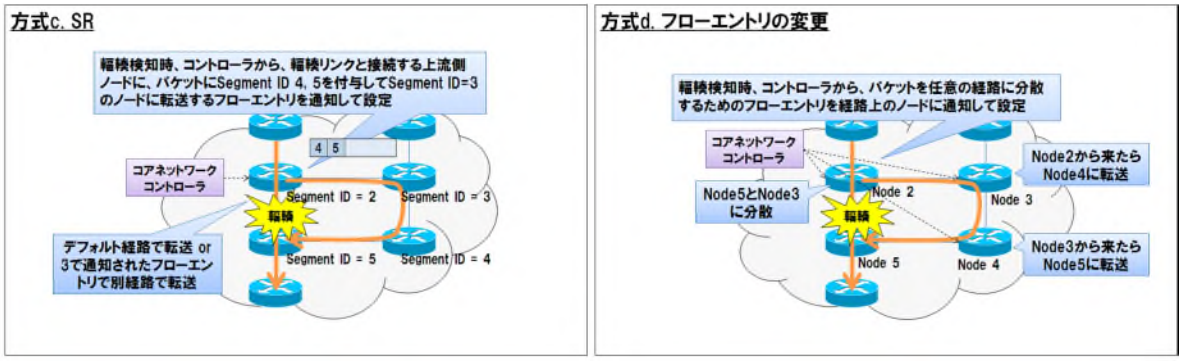

図 12　コアネットワークにおける輻輳回避（②）の実現案

めには、コアネットワークにおける DDoS 対策装置/標的サーバへの通信の転送・分散および輻輳回避の制御を SR、データセンタ内の転送をトンネリングで行う方式が望ましい。

6. まとめと今後の課題

本稿では、大規模な DDoS 攻撃に対処する場合において、ネットワーク内に存在する余剰リソースを有効活用することで、通信サービスの可用性を向上させるネットワークアーキテクチャを提案した。DDoS 対策装置に攻撃通信を転送する際に、特定の経路に通信が集中することで発生する輻輳を余剰ネットワークリソースを活用して、迅速に回避するための技術として、第 4 章では、転送経路と各経路に収容する通信量を高速に算出するためのアルゴリズムを提案した。輻輳したリンクの周辺ノードのみで輻輳回避処理を行う提案方式により、大規模なネットワークや多地点から攻撃が流入する DDoS 攻撃の場合でも、1msec 以内で結果を算出できるため、攻撃検知時や攻撃の変化に追従して、迅速に輻輳回避を実施でき、輻輳によるサービス停止時間を短縮できる。また、転送路の輻輳回避を行わない場合と比べて、約 12% 多くの攻撃通信を DDoS 対策装置まで転送して処理可能になるが、ネットワーク全体で最適経路を算出する従来方式と比較すると、約 10% 程度性能が劣るため、性能向上が課題である。また、余剰ネットワークリソースやコンピューティングリソースを活用して可用性を向上させる技術として、第 5 章では、第 4 章で検討した転送路の局所的な輻輳回避やネットワークワイドでの通信の分散を実現するネットワーク経路制御方式を提案し、他方式との比較により、コアネットワークにおける DDoS 対策装置/標的サーバへの通信の転送・分散と輻輳回避の制御を SR、データセンタ内の転送をトンネリングで実現することで、想定するネットワーク経路制御を大規模なネットワークにおいても高速に実現できることを示した。

今後は、実機による提案アーキテクチャの動作の評価や複数の ISP で連携して大規模 DDoS 攻撃に対処するためのネットワークアーキテクチャを検討予定である。

文　献

[1] 水口 孝則他, “トラフィック解析システム SAMURAI とサービス展開, ” NTT 技術ジャーナル, 2008 年 7 月.

[2] 倉上 弘他, “異常トラフィック検出・分析システム, ” NTT 技術ジャーナル, 2008 年 7 月.

[3] Akamai, “2015 年第 2 四半期「インターネットの現状」セキュリティレポート, ” 2015 年 8 月.

[4] ITmedia, “過去最大級の DDoS 攻撃が発生、世界のネットインフラに影響, ” 2013 年 3 月.

[5] B. Claise (Editor), ”Cisco Systems NetFlow Services Export Version 9,” IETF RFC3954, Oct. 2004.

[6] P. Phaal et al., “InMon Corporation’s sFlow: A Method for Monitoring Traffic in Switched and Routed Networks, ” IETF RFC3176, Sept. 2001.

[7] D. P. Bertsekas, “Network Optimization: Continuous and Discrete Models. Athena Scientific, ” 1998.

[8] M. Pioro and D. Medhi, “Routing, Flow, and Capacity Design in Communication and Computer Networks, ” Morgan Kaufmann, 2004.

[9] 岸 洋司, “ネットワーク性能の解析評価技術の実際, ” 信学会ソサイエティ大会 チュートリアル講演 BT-2 , 2006.

[10] Imperva, “Infrastructure DDoS Protection,” https://www.incapsula.com/infrastructure-ddos-protection-services.html.

[11] Yuzawa, “OpenFlow 1.0 Actual Use-Case: RTBH of DDoS Traffic While Keeping the Target Online,”http://packetpushers.net/openflow-1-0-actual-use-case-rtbh-ofddos-traffic-while-keeping-the-target-online, 2013.

[12] C. Filsfils, S. Previdi (Editor), “Segment Routing Architecture,” Internet-Draft, https://tools.ietf.org/id/draft-filsfils-spring-segment-routing-04.txt, 2015.

[13] C. Filsfils, S. Previdi (Editor), “Segment Routing with MPLS data plane,” Internet-Draft, https://www.ietf.org/id/draft-ietf-spring-segment-routing-mpls-01.txt, 2015.

[14] W. D. Grover, “The self healing network: A fast distributed restoration technique for networks using digital cross connect machines, ” in Proc. IEEE GLOBECOM ’87, pp. 1090–1095, 1987.

[15] Yijun Xiong and Lorne Mason, “Restoration Strategies and Spare Capacity Requirements in Self-Healing ATM Networks, ”IEEE/ACM Transactions on networking, vol. 7, pp. 98–110, 1997.

[16] シン ルー他, “残存次数の相互情報量にもとづくトポロジー構造の多様性が設備増設量に与える影響の評価, ” 信学会技術研究報告 (NS2012-157), pp. 93–98, January 2013.