従量課金のバックアップ用トランジット回線で過大な課金を避けるためのトラフィック制御の手法

菊池 豊[1] 栢分 正人[2] 本間 誠治[3] 井上 望美[3] 柴田 祐輔[4]

概要：災害や障害の対策としてマルチホーム、すなわち複数のトランジット先を持つことで冗長性を確保する手法がある。そのような複数のトランジット経路に対して、課金や品質により主従関係をもたせる場合がある。この場合、従たるバックアップ側の経路側に対しては、コストを抑えたいという要求とともに、主たる経路に障害があった際に全てのトラフィックを流すだけの容量をバックアップトランジットにも求めたいという要求もある。
一方で、インターネットトランジットの課金は、上流/下流の関係にある ISP や大きな法人ユーザに対しては、トラフィックの上限を定めた固定課金か、95 パーセンタイル法に基づく従量課金が行われる。どちらの課金スタイルであってもバックアップトランジットに対する要求を満たせない。
そこでここでは、バックアップに用いるような短い時間においては、主たるトランジット同様の伝送容量を提供し、なおかつ課金が固定であるような手法を提案する。

A Traffic Engineering Method to Avoid Unreasonable Charge for Backup Transit Links

KIKUCHI Yutaka[1] KAYAWAKE Masato[2] HON'MA Seiji[3] INOUE Nozomi[3]
SHIBATA Yusuke[4]

1. 背景

インターネットを含む ICT 環境は生活にも業務にも不可欠になっており、特に近年、南海大地震等の災害に対する堅牢性の確保が重要になっている。各組織では事業継続計画 (BCP) の整備が進み、災害時の対応の準備がなされている。また著者らは、地域 IX を用いた高知学術ネットを構成することで、高知県内において ICT 環境を堅牢にする活動を行っている [1][2]。

高知学術ネットは、各組織がキャンパス間接続やインターネット接続を行う際に、第 2 層（Ethernet 層）や第 3 層（IP 層）の接続構造が冗長になるようなネットワーク構成を作ることを目的としている（図 1）。これにより、一部の障害や事故に対する堅牢性を上げることが出来ており、地域 IX の有効性に関する一つの証左となっている。

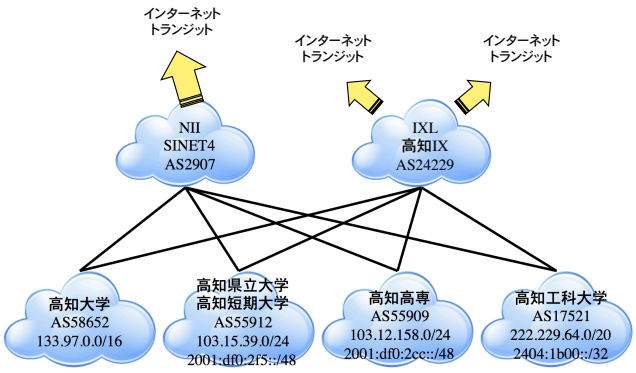

図 1 高知学術情報ネットワークの L3 構造

2. 課題

しかしながら、現状では災害と呼ばれるクラスの障害が発生したような状況には対応できない。それは以下の理由

1 高知工科大学, Kochi University of Technology
2 フォーサイトウェーブ, Foresight Wave Inc.
3 新潟通信サービス, Niigata Tsuushin Service Corp.
4 愛媛 CATV, Ehime CATV Inc.

による。

(1) 高知市中心部が被災すると県外との通信が不通となる可能性がある

(2) 地域内で IP データグラムが交換できても DNS が機能しなくなる可能性がある

(3) バックアップトランジット側の費用が過大になる可能性がある

(4) 検討個所が広範囲でかつ複雑な依存関係を持つため全体を把握できない可能性がある

(5) 設計した耐障害性や策定した計画が災害時に適切に適用できるかを平時には十分に確認できない可能性がある

このうち (3) については、バックアップ側のトランジットの伝送速度を固定で確保しておくと平時から費用がかかり、従量課金にしておくと主トランジット回線の障害が長引いた場合に課金が過大になるという問題がある。

例えば、高知工科大学では BGP を制御することで、ほとんどのトラフィックが通常は SINET4 を経由し、SINET4 に障害があった際にはバックアップである商用トランジット側を使うような経路制御を実施している（図 2)。

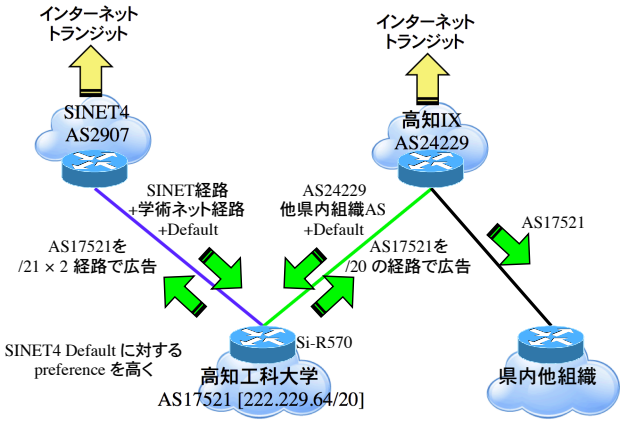

図 2 高知工科大学の BGP 制御

SINET4 の障害が長引いた場合に、この商用側のトランジットの課金が過大にならず、なおかつ障害が短い期間である場合にはバースト的に大きなトラフィックが発生してもバックアップ側がそれを許容するようにしたい。この相反する 2 つの要求を同時にどう満足させるかが課題である。

3. 目的と手法

そこで本研究では、平時および障害時のどちらでも妥当な範囲に経費を押さえることの出来る冗長構成を提供する技術を実現することを目的とする。

これを、BGP マルチホームによるトランジットの冗長化を行い、トラフィックを片側に寄せてそちらを主トランジットとする。その上で、バックアップとなる副トランジットは、トラフィックが長期に渡り増大しそうな場合にトラフィックを抑制するような機構を導入する、という手法で実現する。

トラフィックの抑制については、95 パーセンタイル課金方式を前提に、バックアップ用トランジットトラフィックが 95 パーセンタイルが、事前に設定してある流量を超えそうな場合に、トラフィックを自動で絞るような方式を検討した。

4. トラフィック制御の手段

トランジットの接続関係が図 3 のようであるとする。この赤で囲った ISP 間に対して、トランジットルータに対する制御用のサーバを設置し、両者の間では以下の通信がなされるものとする（図 4)。

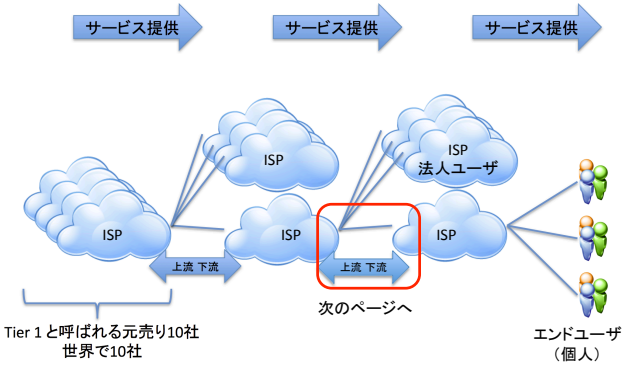

図 3 トランジット接続の構造

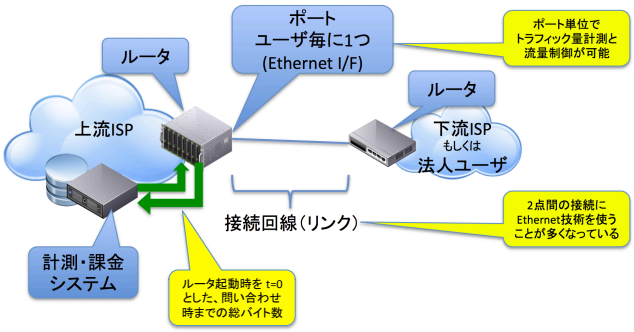

図 4 制御システムの構成

- ルータはインタフェース毎のトラフィックを計量することができ、それをサーバに SNMP 等で定期的に知らせることができる
- サーバはトラフィックのデータベースと制御用のアルゴリズムを持ち、サーバに対して特定のインタフェースの通過可能トラフィックの上限を設定できる

この構成を前提として以下のアルゴリズムにより制御を行う。以下でトラフィック計測を行う単位となる時間をスロットと呼ぶ。スロットは、通常は 5 分間で、この時間に流れる総トラフィック (bps) をスロットの時間である 300 秒で除した値 (bps/s) がトラフィックとして記録される。

- サーバは月の頭に、以下を行う
  - ルータに対してトラフィックの制約を解除するコマンドを送る
  - 月全体のスロットで 95%になるスロットの個数を計算する
    小の月（30 日間）の場合、全体で 8640 スロットあり、95%に相当するのは 8208 スロットである。
- サーバは、スロット単位で、ルータより SNMP により、対象となるインタフェースのトラフィックを得る
- トラフィックがコミット値を超えたかどうかを判定し、月頭よりコミットを超えたスロット数を計算する。これが予め月頭に計算しておいた 95%のスロット数と比較して
  - 越えると判断した場合は、ルータに対してトラフィックを制約するコマンドを送る
  - 越えないと判断した場合は、なにもしない

また以下のようなアルゴリズムでも制御が可能である。

- サーバは、月の頭にはトラフィックデータベースをクリアし、ルータに対してトラフィック抑制を行わないように設定を行う。
- サーバは、定期的に（通常は 5 分間隔で）ルータより SNMP により、対象となるインタフェースのトラフィックを得て、それをデータベースに蓄積しする。
- 月頭から次の計測タイミングまでの 95 パーセンタイルが従量課金のコミット値（すなわちこれを超えるトラフィックに対しては課金が増えるような値）を越える可能性があるかかどうかを判定する
  - 越える可能性があると判断した場合は、ルータに対してトラフィックを制約するコマンドを送る
  - 越える可能性がない判断した場合は、ルータに対してトラフィックの制約を解除するコマンドを送る

このようにすると、一旦トラフィックが抑制されるような状況になっても、しばらくコミット値より少ないトラフィック量の期間が続くと、再びバースト的なトラフィックが許されるようになる。これにより月全般でまんべんなくトラフィック抑制ができるようになる。

5. 実装と評価

アルゴリズムが想定通り機能するのかを確認するために、前者のアルゴリズムを実装した。ルータは Cisco2800 シリーズを対象とした。これは基本的な機能しか用いていないので上位機種でもほとんどそのままで実装できる。サーバには IBM の 1U サーバを用い、XenServer で仮想化した上で、linux 上に制御ソフトウェアを実装した。設定や状態監視は web 上で行える様に GUI を実装している（図 5）。実験室レベルで、通過トラフィックを変化させて、想定の機能が実現できることを確認した（図 6）。

図 5 評価用中の制御画面

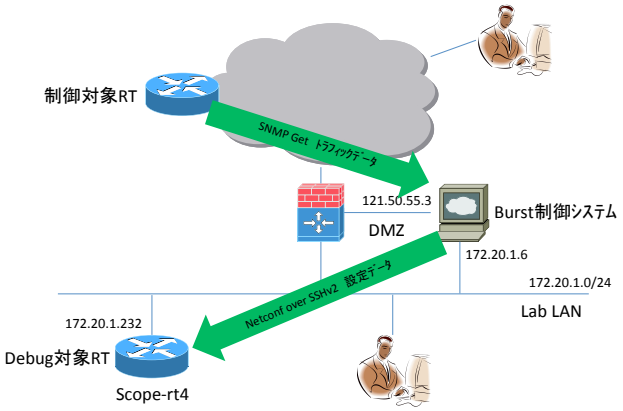

図 6 評価用ネットワーク

6. まとめと今後の課題

コミット値（すなわちこれをこれるトラフィックに対しては課金が増えるような値）以上の 95 パーセンタイルトラフィックは発生せず、従量課金でありながら実際の負担は毎月固定額となり、なおかつ瞬間的にはバーストトラフィックを通過させられるような機能を実現できた。これにより、トランジットの冗長化を希望する組織が、大きな負担なくバックアップトランジットを購入できるようになった。

今後は実際のネットワーク上、例えば高知学術ネットでの実証実験を準備している。これにより現実のトラフィックで期待通りに振る舞うのかどうかや、ネットワーク防災訓練等 [3][4] の実地のネットワーク演習において正しく動作するのかを検証したい。さらに、管理運用画面を現場の要望に応じて充実させる予定である。これにより、バーストトラフィックを通したいものの費用は固定にとどめたいというような法人向けビジネスへの利用を行いたい。

謝辞

本プロジェクトの一部は総務省 SCOPE で「災害時に事業継続性を発揮する情報通信インフラのための運用計画改善手法および冗長化技術の研究開発（受付番号: 132309010）」として支援を受けている。なお本方式は特許審査中である

ことを付記しておく [5]。

参考文献

[1] 菊池　豊：高知学術ネットワークの構築，第 1 回地域間インタークラウドワークショップ in 佐賀 (2012).

[2] 菊池　豊：高知における丈夫なネットワークの構築について (2013). 高知学術情報ネットワーク運用開始記念【災害に備える地域 ICT インフラ技術シンポジウム】.

[3] 菊池　豊：ネットワーク防災訓練 〜怖くて誰も出来なかった訓練の実現〜 (2014). 第 5 回地域防災情報シンポジウム @高知県立大学永国寺キャンパス.

[4] 菊池　豊ほか：地域 IX で恣意的な障害を発生させることによる耐障害性の検証 (2014). 第 4 回地域間インタークラウドワークショップ @おきでんふれあいホール.

[5] 菊池　豊：課金システムとプログラム (2011). 特願 2011-81015.