DEWS2007 E7-3

iSCSI over VPN 環境における 複数経路アクセス適応制御手法の提案と評価

武田　裕子† 　小口　正人†

† お茶の水女子大学　〒 112–8610 東京都文京区大塚 2–1–1
E-mail: †yuko@ogl.is.ocha.ac.jp, ††oguchi@computer.org

あらまし　近年サーバにおけるストレージ接続に SAN が用いられることが多くなってきた．SAN を利用することによってサーバとストレージを高速ネットワークで接続することが可能となるが，現状では主にサーバサイト内のみでしか使用されていない．そこで VPN を利用して，IP-SAN の代表である iSCSI を広域ネットワークに適用する手法を考察していく．SAN は大きなデータを送信するため安定した通信環境が必要となるが，VPN では一般にオープンなインターネット環境を利用することが多いため，接続が不安定であったり帯域が保障されないという問題点が生じる．そこで本稿ではネットワークの性能と信頼性を高めるために複数経路を使用した実験を行った結果，複数経路を用いたほうが単一経路よりも高いスループットを得ることができた．さらに本稿では負荷を考慮した適応制御手法を検討する．

キーワード　iSCSI，VPN，マルチルーティング，スループット，負荷分散

A Proposal and Assessment of a Method to Control Multi-route Access for iSCSI over VPN Environment

Yuko TAKEDA† and Masato OGUCHI†

† Ochanomizu University　Ohtsuka 2–1–1, Bunkyo-ku, Tokyo, 112–8610 Japan
E-mail: †yuko@ogl.is.ocha.ac.jp, ††oguchi@computer.org

Abstract　SAN has come to be often used for the storage connection in the server in recent years. It is chiefly used only in the server site under the present situation though connecting the server with storage on a high-speed network becomes possible by using SAN. Thus, the technique for applying iSCSI which is the representative of IP-SAN to the wide area network is considered by using VPN. The problem is caused that the connection is unstable because open and unsecured Internet environment is often used generally in VPN, though SAN needs a communication environment steady to transmit big data. Therefore, we did the experiment that used multi-routes to improve the performance and the reliability of the network. As a result, it is higher to use multi-route than a single route. In addition, the adjustment control technique for considering the load is examined in this paper.

Key words　iSCSI, VPN, Multi-routing, throughput, load-distribution

1. はじめに

近年ブロードバンドインターネット技術が向上し，マルチメディアコンテンツなど大容量のデータが通信され，ストレージで管理されることが多くなってきた．組織や企業などが保持するデータ量が年々増加しており，その管理コストが問題となっている．そこで，SAN(Storage Area Network) が導入されるようになってきた．DAS(Direct Attached Storage) はサーバとストレージを直接接続するが，SAN はサーバとストレージを高速なネットワークで接続する．SAN は他のストレージソリューションに比べて高性能であり，異機種混在環境でのデータ共有が容易で，管理コストや管理負荷を大幅に削減することが可能となる．

現在 SAN の中で広く使用されているのは FC-SAN(Fibre Channel-SAN) で，これはサーバとストレージ間をファイバチャネルで接続する．高速アクセスが可能で対応製品が豊富になってきてはいるが，FC 用の機器が高価であること，FC 管理技術者が少ないこと，SAN 対応でないシステムも混在していること，および接続距離に制限があることなどの問題がある．そのため，Ethernet と TCP/IP を用いて構築する IP-SAN が

普及し始めている．IP-SAN は FC-SAN よりも安価で，接続性が高く，既存の IP ネットワークとシームレスな統合が可能となり，接続距離に制限がない．

IP-SAN の中で現在特に期待されているものは，2003 年 2 月に IETF によって承認された iSCSI である [1]．iSCSI とは，イニシエータと呼ばれるサーバとターゲットと呼ばれるストレージ間を Ethernet で接続し，TCP/IP パケット内の SCSI コマンドをカプセル化してストレージアクセスを行う技術のことである．

SAN を利用することによって，コンピュータとストレージを 1 対 1 や 1 対 N で接続するのではなく，N 対 N で接続することが可能となる．また，DAS などと比べ管理コストや管理負荷を大幅に削減することができる．しかし，現状においては SAN は主にサーバサイト内においてのみしか使用されていない．そこで本稿では，SAN をオープンなインターネット環境で広く利用できるようにするための手法を検討する．

具体的には VPN(Virtual Private Network) の仮想ネットワーク構築機能を利用して，ローカルな環境で使用される iSCSI を広域ネットワークに適用することを考える．その実現例を図 1 に示す．

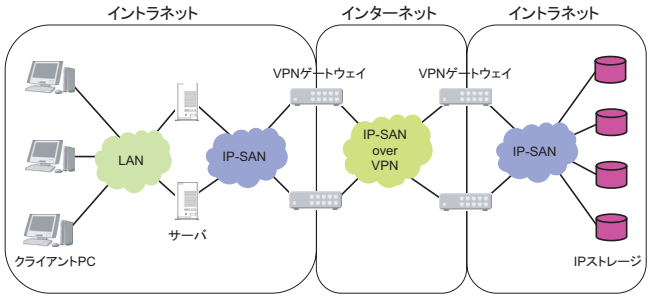

図 1　VPN 上の IP-SAN 利用の提案モデル

本稿では始めに基礎実験として低スループット VPN 環境において単一経路の iSCSI 環境を構築し，スループットの測定を行い直接接続時と比較を行った．また，複数経路アクセス実験として高スループット VPN 環境において複数経路の iSCSI 環境を構築し，スループットの測定を行い，複数経路と単一経路の比較を行った．そして複数経路環境において負荷影響の評価実験も行い，負荷に対する適応制御手法を提案する．

本稿は以下の構成から成っている．第 2 章で iSCSI の説明，第 3 章で VPN の説明，第 4 章で基礎実験の概要と結果の考察，第 5 章で複数経路アクセス実験の概要と結果の考察，第 6 章で負荷に対する適応制御の提案をし，第 7 章でまとめと今後の課題を述べる．

2.　iSCSI の仕組み

2.1　iSCSI のコンセプト

SCSI は，HDD やテープドライブ，スキャナなどといった周辺装置との入出力に使用されるインタフェースで，パラレルバスを介したブロックデータの送受信を基本とする．また，SCSI はクライアントサーバ型モデルであり，SCSI コマンドを発行し，処理を要求する「イニシエータ」と，その処理を行い，レスポンスを返す「ターゲット」によって構成されている．

iSCSI のコンセプトは，SCSI コマンドやレスポンスを TCP パケットにカプセル化することによって，従来のパラレルバスを元にした SCSI トランスポートを，IP ネットワークによるトランスポートに置き換えることである．これにより，IP-SAN の構築が可能となる．図 2 に示すように iSCSI 対応サーバが IP ネットワークを経由して iSCSI 対応ストレージと通信を行う．サーバには iSCSI 対応機器が組み込まれる．

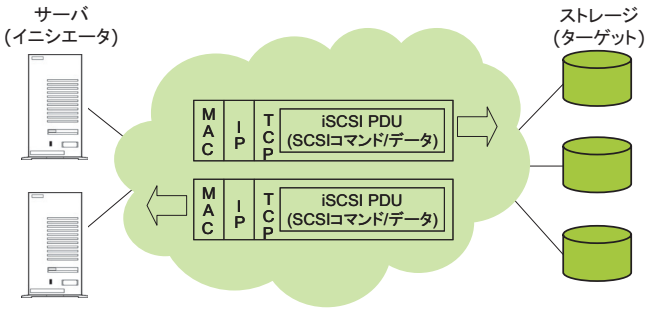

図 2　iSCSI のコンセプト

2.2　iSCSI 階層モデル

iSCSI の階層モデルを図 3 に示す [2]．iSCSI 層は，SCSI 層と TCP/IP 層との間に位置する．

SCSI 層からの SCSI コマンドやレスポンス，データを受け，それを iSCSI PDU にカプセル化処理して，トランスポート層として TCP/IP が提供する TCP コネクションを介して送信を行う．TCP/IP ヘッダが付加されるとカプセル化された SCSI コマンドは IP パケットと同様に扱われ，IP アドレスに基づいて宛先にルーティングされる．

また，宛先の装置が TCP コネクションを介して iSCSI PDU を受信すると，各階層でヘッダを取り去り SCSI コマンドやレスポンス，データを抜き出して，最終的に元の SCSI コマンドに戻しそれを SCSI 層に通知する．このコマンドは送信元と宛先が直接接続されているのと同様に処理される．このように iSCSI は，SCSI over iSCSI over TCP/IP over Ethernet という複雑な階層構造となっている．

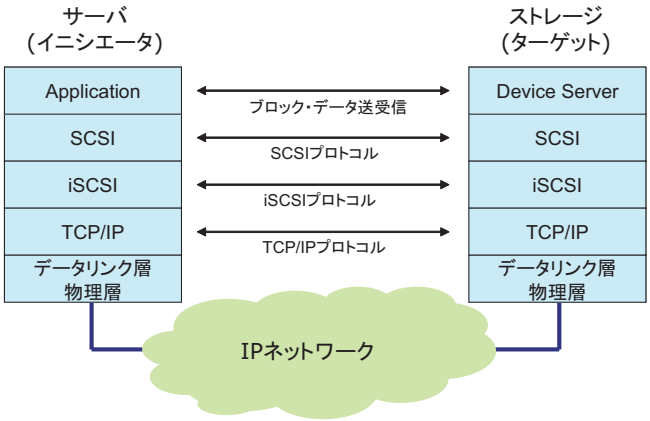

図 3　iSCSI の階層モデル

2.3 iSCSI の特徴

iSCSI は SCSI コマンドを直接やり取りするため，データベースなどを利用しても問題はない．しかしファイルシステムを装置内で管理していないため，iSCSI 装置自身にはファイル共用の機能がない．SAN プロトコルは，ディスクブロック単位でリモートデータにアクセスする．また，ファイルシステムはクライアント上に存在する．

iSCSI は異なる通信ストリームを識別するためにクライアントとサーバ間のセッションの概念を用いる．多数のコネクションによるセッションへの多重送信を許しており，暗号化と高度なデータ完全性と認証のプロトコルをサポートする．また明示的な再伝送リクエストや，高度な誤り回復もサポートしている．しかし iSCSI は，単一のクライアントマシン上で動いているアプリケーションがサーバ上のリモートデータを共有することが可能であるが，直接にクライアントマシン間のデータ共有をするには適していない．ファイルシステムのキャッシュは，クライアントにあるのでデータやメタデータはキャッシュからとりだすことが可能で，データやメタデータの更新は非同期的に行われる．

既存のアプリケーションは，iSCSI を意識することなく従来どおりローカルストレージにアクセスするのと同じ手順でターゲットストレージのデータを読み書きできる．ディスクへの読み書きは，FC-SAN と同じブロック I/O であり，NAS のようなファイル・システムはストレージ側に必要としない．現在は FC-SAN のインフラ・スピードとあまり変わりはないが，今後のイーサネットの伝送スピードが 10 倍速で向上すると考えると，そのメリットは計り知れない．ネットワーク管理の面からも，ストレージ機器をほかの通信機器と同じように同一インフラ網上で統合管理が可能である．

3. VPN

3.1 VPN の概要

専用網は，通信事業者の専用線サービスを利用するもので，その企業専用の閉じたネットワークである．銀行のオンラインシステムなど，機密性や回線の安定性が重要な場合に利用される．しかし回線を占有して利用するため，コストが高くなってしまう．

専用網の対義語は「公衆網」で，一般に開放されたネットワークのことをいう．例としてインターネットや一般の電話回線などが例としてあげられる．公衆網はオープンな環境を利用するため，コストが安く済む．

VPN は，インターネットや通信事業者が持つ公衆ネットワークを使って，拠点間を仮想的に閉じたネットワークで接続する技術である．図 4 のようにインターネット上にトンネルのような専用網をつくり，通信を行う．専用網には機密性や回線の安定性に優れるというメリットがある一方で，高価になってしまうというデメリットがある．そこで安価であるという公衆網のメリットを活かしつつ，機密性の低さを別の方法で補えば，「実質的な専用網」を実現できる，という考え方が VPN の基本的な発想である．

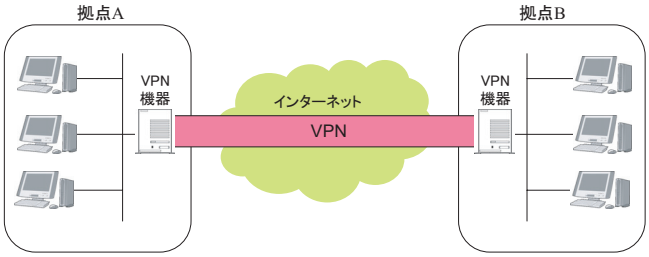

図 4　VPN の概要

3.2 VPN を支える技術

VPN を支える基本技術として，カプセル化，暗号化，ユーザ認証の 3 つが挙げられる．

カプセル化とはトンネリングを実現する方法で，元のパケットを別のパケットで包み込むことである．カプセル化することによって，LAN 内でしかやり取りできないプライベート IP アドレスのパケットをインターネット経由で送信することが可能となる．トンネリングとは，インターネット上にあたかもトンネルのように仮想的な専用線を作ることである．この回線上を送信されるパケットは公衆網を送信される他のパケットと同じように宛先に届くが，宛先としてプライベート IP アドレスを指定できる．

ただし，カプセル化だけではデータを盗聴できてしまうので，実際には暗号化も必要である．また，VPN の利用をユーザごとに認めるユーザ認証も必要となる．

また，LAN 内のパケットをカプセル化してインターネット側に送信したり，インターネット側からパケットを取り出す機器を VPN ゲートウェイという．VPN ゲートウェイは，VPN によってネットワーク同士を接続する一種のルータである．

3.3 VPN で使用されるプロトコル

VPN では，用途や通信事業者のサービスを使う場合と自前で構築する場合などで，使用するプロトコルが異なってくる．代表的なプロトコルを以下に挙げる．

- MPLS(Multi Protocol Label Switching)：第 2 層と第 3 層のヘッダの間にラベルと呼ばれる情報を付加することでパケットを転送する．
- PPTP(Point to Point Tunneling Protocol)：マイクロソフトやルーセント・テクノロジーなどが開発した VPN プロトコルで，ダイヤルアップ接続で使われる PPP でトンネルを実現する．
- L2TP(Layer 2 Tunneling Protocol)：マイクロソフトの PPTP と，シスコシステムズが開発した L2F を組み合わせたプロトコル．
- IPsec(Security Architecture for Internet Protocol)：IP パケットをカプセル化するプロトコル．
- SSL(Secure Socket Layer)：Web ブラウザとサーバ間のセキュリティ向上を目的に開発されたプロトコルで，この SSL の暗号化や認証の仕組みを使ってリモートアクセス VPN を実現する．

VPN で現在もっとも普及しているプロトコルが IPsec である [4]．IPsec は，本来 IPv6 用のセキュリティ機能として考案された技術の集合である．VPN ルータで使用する IPsec は，IPv4 のオプションとして改良し，IP パケットのカプセル化機能を加えたものである．IPsec は第 3 層におけるカプセル化になるので，IP 以外のプロトコルには対応できない．

IPsec には 2 つのモードがある．トランスポートモードは IP のデータ部分を認証したり暗号化することでセキュリティを向上させる．トンネルモードは元のパケットの送信元と宛先アドレスも含めて，IP パケット全体を暗号化する．VPN ルータで使用するのはトンネルモードである．

また，ヘッダも 2 種類用意されている．AH は，パケットが改ざんされたり，なりすましによって送信元が詐称されていないかを認証する機能が備わっており，ESP は，認証に加えてパケットの暗号化機能も備わっている．IPsec では，こうしたヘッダ形式やモードを組み合わせて，合計 4 パターンの通信方式が選択できる．本稿では，IPsec の VPN ルータを用いて実験を行った．

3.4 VPN の現状

VPN で使用されるプロトコルは上で挙げたようにいくつか種類があるが，現状としては，PPTP は Windows に標準で搭載されており，簡単なセットアップを行うだけで VPN を構築することができる．IPsec は現在もっとも普及しているプロトコルで，LAN と LAN を接続する LAN 間接続 VPN に向いている．IPsec を利用するにはクライアントに特別なソフトウェアが必要となるが，安価ですむ．また SSL は，ブラウザのみからのアクセスとなり，IPsec と比べ高価である．

このように最近では VPN ゲートウェイ等の性能が向上し，価格も安くなり手軽に VPN を利用することが可能になってきている．

4. 基礎実験

4.1 実験環境

インターネット環境における IP-SAN の利用モデルを評価するため，実験システムを構築して性能評価を行った [5][6]．図 5 に示すように，低スループットの VPN ルータ 2 台を用いて VPN 上に単一経路の iSCSI システムを構築して性能評価を行った．iSCSI にはニューハンプシャー大学 InterOperability Lab が提供するドライバを用いた [7]．VPN ルータには富士通の Si-R180 を用いており，この VPN ルータの IPsec 暗号化スループットは暗号化アルゴリズムに 3DES を用いた場合，100Mbps である [8]．測定ツールには自作のベンチマークツールを用いており，raw デバイスに対してシーケンシャルリードアクセスをし，測定を行った．実験システムの概要は以下のとおりである．

- Initiator，Target
  - OS: Linux2.4.18-3
  - CPU: Intel Xeon 2.4GHz
  - Main Memory: 512MB DDR SDRAM
  - HDD：36GB SCSI HD
  - NIC：Intel PRO/1000XT Server Adapter on PCI-X(64bit，100MHz)
  - iSCSI: UNH IOL reference implementation ver.3 on iSCSI Draft 18
- VPN ルータ: 富士通 Si-R180(3DES 使用時 IPsec 暗号化スループット:100Mbps)
- 測定ツール: 自作のベンチマークツール

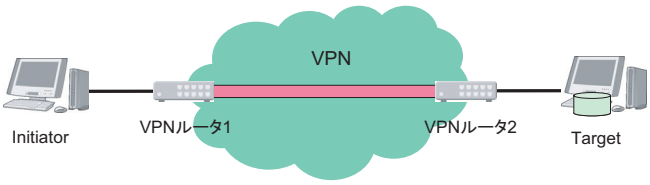

図 5　基礎実験実験環境

4.2 測定結果と考察

低スループットの VPN ルータ 2 台をはさんだ単一経路の iSCSI システムを構築し，性能評価を行った．VPN 接続時と VPN ルータをはさまない直接接続時のスループットの測定結果を図 6 に示す．また図 7 は図 6 に示す VPN 接続時の測定結果をスケールを拡大したものである．VPN ルータをはさんだ場合には，はさまない場合と比べかなりスループットが低下している．

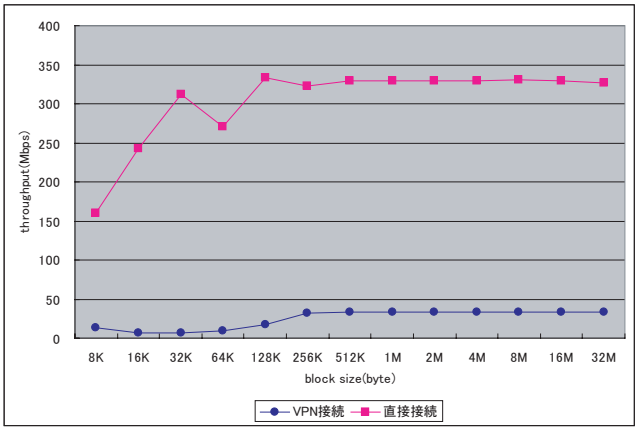

図 6　VPN 接続時と直接接続時の比較

直接接続時には，スループットは最大 330Mbps 程度出ているが，VPN 接続時には 33Mbps 程度で飽和状態となっている．実験機器の VPN ルータは 3DES 使用時の IPsec 暗号化スループットが 100Mbps 程度である．本実験環境においては，VPN ルータの性能と両端の端末でのプロトコル処理がボトルネックとなっていると考えられるが，これらの結果から VPN ルータの性能がボトルネックとなりスループットを大幅に低下させていると考えられる．

また直接接続時にはブロックサイズが 128Kbyte まで，VPN 接続時も 256Kbyte まではスループットが増加し続けている．このようにブロックサイズが変化するとスループットも変化しており，適切なパラメータ設定が必要であるといえる．

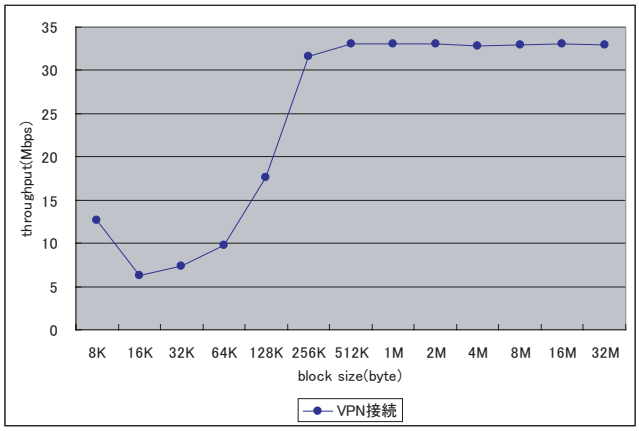

図 7　VPN 接続時の測定結果

5.　複数経路アクセス実験

5.1　複数経路ルーティング

もともとインターネットのルーティングには複数の経路が存在するが，実際にはあて先が同じパケットは同じ経路を通って相手に送られる．これに対し複数経路ルーティングとは，VPN ルータにもともと備わっていた機能を利用したもので，図 8 に示すように同じあて先のパケットを IP アドレス，ポート番号，上位プロトコル，TOS 値を指定し異なる経路を通すことである．この機能の本来の目的は VoIP と通常トラフィック，専用線と ISDN 回線などといった異なる通信を分離することである．本稿では異なったポート番号を指定することによって複数経路を実現している．

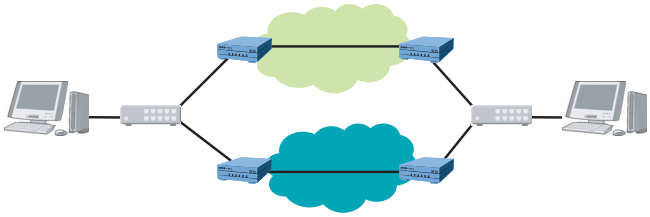

図 8　複数経路ルーティング

5.2　iSCSI の複数コネクション

iSCSI において，イニシエータとターゲット間の論理的な通信路は，iSCSI セッションと呼ばれる．iSCSI セッションは，1 つもしくは複数の TCP コネクションから構成される [9]．

iSCSI の複数コネクションとは単一の iSCSI アクセスを iSCSI ドライバが分割し複数の TCP コネクション上に載せることである．一つの iSCSI セッションの中に複数の TCP コネクションを確立することによって複数コネクションを実現する．図 9 では iSCSI セッション中に TCP コネクションは一本だが，図 10 のように複数の TCP コネクションを束ねることも可能となっている．本稿ではこの仕組みを利用して複数経路において複数コネクションを実現する．

また本実験で用いた UNH-iSCSI の複数コネクションにおいて，パケットはラウンドロビンで振り分けられている．ドライバの実装を修正することによってすべてのコネクションに公平にラウンドロビンで振り分けるのではなく，コネクションごとのスループットに応じてパケットの振り分け配分を変えることも可能である．そしてパケットを受け取ったターゲットでは，パケットを送出順に戻して処理を行っていく．

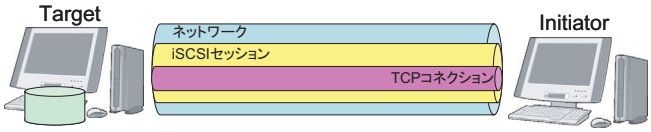

図 9　単一コネクション

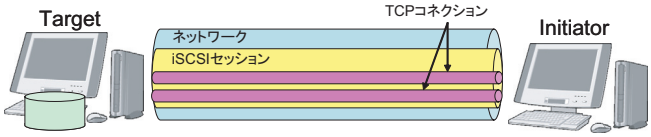

図 10　複数コネクション

この実装においては，複数のコネクションが同一経路を通ることを前提としてすべてのコネクションに公平にパケットの振り分けが行われている．しかしコネクションごとに経路が異なった場合，所要時間がコネクションごとに異なる形になるであろう．そのような場合には，ラウンドロビンのパケットの振り分けを比例配分するように変えれば，より高い性能をあげられる可能性があると考えられる．

なお iSCSI セッションの確立は，イニシエータがターゲットとの間で TCP コネクションを張り，認証とネゴシエーションすることにより行う．認証は，不正アクセスを防ぐためにターゲットによりイニシエータの認証を行うのみならず，なりすましなどを防ぐためにイニシエータによるターゲットの認証を行うことも可能である．認証方式にはいくつか挙げられるがどの認証方式により行うかは，イニシエータとターゲット間のネゴシエーションによって決めることができる．

5.3　実験環境

図 11 に示すように高スループットの VPN ルータ 4 台を用いて VPN 上に複数経路の iSCSI 環境を構築し，性能評価を行った [10]．VPN ルータの機能と iSCSI の性質を用いて複数経路，複数コネクションを生成し，単一経路単一コネクションと複数経路複数コネクションの条件でそれぞれスループットの測定を行い，基礎実験との比較を行った．

イニシエータとターゲットのマシン 2 台は基礎実験と同じマシンを用いており，VPN ルータには富士通 Si-R570 を用いた．基礎実験で用いた Si-R180 は 3DES 使用時の IPsec 暗号化スループットが 100Mbps だったが，複数経路実験で用いる Si-R570 はこの暗号化スループットが 500Mbps となっている．実験システムの概要は以下のとおりである．

- Initiator，Target
  - OS: Linux2.4.18-3
  - CPU: Intel Xeon 2.4GHz
  - Main Memory: 512MB DDR SDRAM
  - HDD：36GB SCSI HD

- NIC：Intel PRO/1000XT Server Adapter on PCI-X(64bit，100MHz)
- iSCSI: UNH IOL reference implementation ver.3 on iSCSI Draft 18

• VPN ルータ: 富士通 Si-R570(3DES 使用時 IPsec 暗号化スループット:500Mbps)
• 測定ツール: 自作のベンチマークツール

なお，イニシエータからターゲットへの送信，write 時は図 12 のように VPN I-1 から VPN T-1 と VPN T-2 を通りターゲットへ到達し，ターゲットからイニシエータへの送信，read 時は図 13 のように VPN T-2 から VPN I-1 と VPN I-2 を通りイニシエータへ到達するものとする．

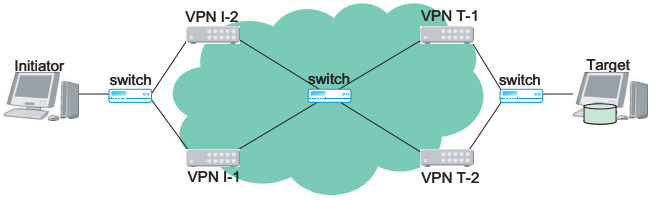

図 11　複数経路実験実験環境

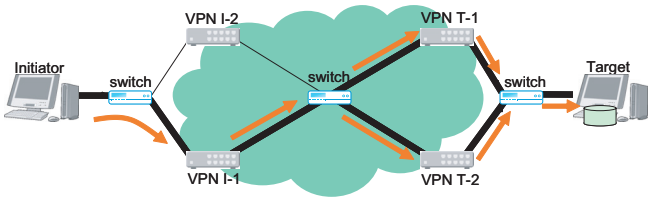

図 12　write 時の経路

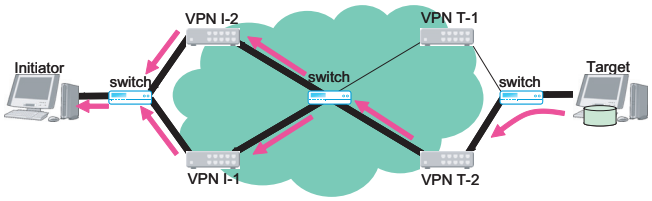

図 13　read 時の経路

5. 4　測定結果と考察

基礎実験とは性能の異なる高スループットの VPN ルータ 4 台を用いて複数経路の iSCSI over VPN 環境を構築し，単一経路単一コネクションと複数経路複数コネクションの条件でそれぞれスループットを測定し，基礎実験の結果と比較を行った．その結果を図 14 に示す．

単一経路単一コネクションは 165Mbps 程度で飽和状態となっている．基礎実験で用いた VPN ルータ Si-R180 は 33Mbps 程度で飽和状態となっていたので，Si-R180 と比較すると 5 倍程度になっており，VPN ルータの性能の差，100Mbps と 500Mbps と比例していることがわかる．

単一経路単一コネクションと複数経路複数コネクションを比較すると，ブロックサイズが 128Kbyte まではほぼ等しいスループットとなっており，これはブロックサイズが小さいためまだネットワークに余裕がある状態であると考えられる．しかしその後伸び方に差が出て，512Kbyte あたりでともに飽和状態となっている．

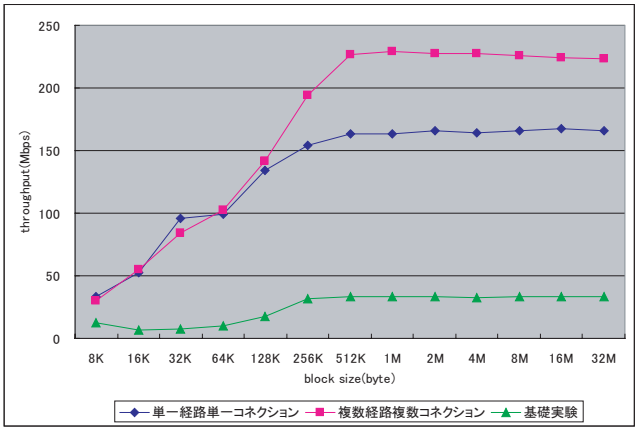

図 14　複数経路アクセス実験の実験結果

このとき複数経路複数コネクションのほうが高いスループットを得た．これは，本実験環境の中でスループットの性能限界であるボトルネックとなっている箇所は VPN を通るところであり，VPN ルータで暗号化の処理などを行うからであると考えられる．したがって複数経路にすると負荷が 2 つに分散されるので，スループットが高くなったと考えられる．しかし複数経路にしても VPN ルータをはさまない直接接続時の結果よりは低い値となっており，複数経路の実験環境においても基礎実験の環境と同様，VPN ルータがボトルネックとなっているといえる．

6.　ネットワーク負荷に対する適応制御

6. 1　ネットワーク負荷による影響の評価実験

次に複数経路の実験環境において，図 15 のようにネットワークの片方の経路に他のトラフィックを流し負荷をかけて，先ほどと同様に単一経路単一コネクションと複数経路複数コネクションの環境でスループットを測定し，それぞれ負荷のかかっていない場合との比較を行った．なおネットワークの負荷は，大きなファイルを scp コマンドで転送し続けるもので，約 130Mbps である．

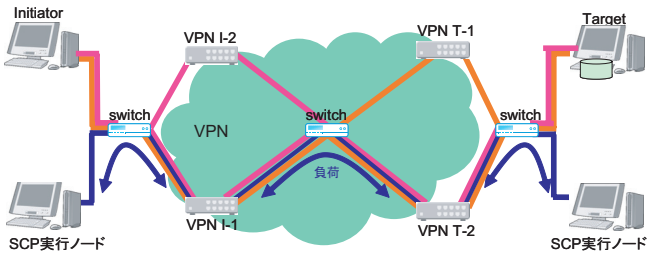

図 15　負荷評価実験

実行結果を図 16 に示す．負荷をかけると単一経路単一コネクションは 97Mbps 程度，複数経路複数コネクションは 136Mbps

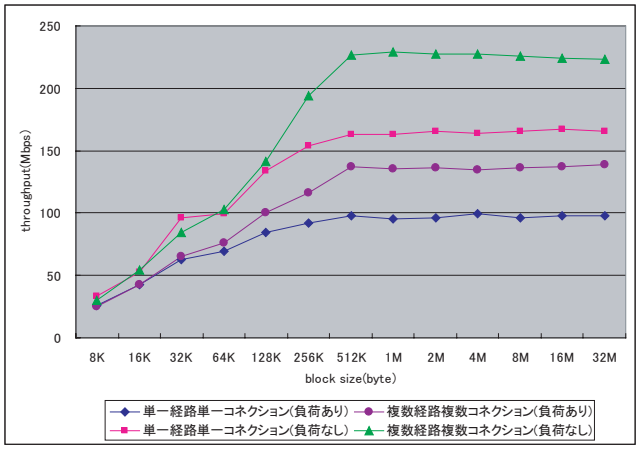

図 16　負荷評価実験の結果

程度で飽和状態となっている．複数経路アクセス実験より，負荷がない場合には単一経路単一コネクションは 165Mbps 程度，複数経路複数コネクションは 226Mbps 程度で飽和状態となっていたので，単一経路単一コネクションも複数経路複数コネクションも負荷をかけるとともに 6 割程度と同じ位の割合で低下していることがわかる．

これは UNH-iSCSI の複数コネクションにおいて，2 つのコネクションに対しパケットはラウンドロビンで振り分けられているので，iSCSI 層では，片方のコネクションへ送り出したパケットが処理されないと，もう片方のコネクションも次を送り出すことができずに待つことになってしまうと考えられる．

したがって，複数コネクションでパケットを送り出した場合に，たとえ片方のコネクションは空いていてパケットをどんどん送れる状態であっても，もう片方のコネクションが混んでいて遅いとそちらを待つことになり，性能は遅い方に引きずられて，結局混んでいる単一コネクションでパケットを送り出した場合と同程度に性能低下が起こってしまうということであると考えられる．

6.2　負荷に対する適応制御手法の提案

基礎実験より，VPN をはさむとはさまない場合に比べ大幅にスループットが低下することがわかった．一方，複数経路アクセス実験より，複数経路にすると単一経路よりスループットがあがることがわかった．しかしネットワーク負荷影響評価実験より，iSCSI の場合には複数コネクションにしても片方のコネクションが遅いとそちらに引きずられて単一コネクションと同様に全体の性能が落ちてしまうことがわかった．

また負荷のかかっている複数経路複数コネクションと負荷のかかっていない単一経路単一コネクションを比較すると，負荷のかかっていない単一経路単一コネクションのほうがスループットが高くなっている．特にブロックサイズが小さいところではその差が大きくなっている．これはブロックサイズが小さいところではネットワーク負荷の影響が大きく，一方ブロックサイズが大きいところでは負荷の影響よりも経路が 2 つになったことによって負荷が分散された影響のほうが大きいのであると考えられる．

そこで本稿では，複数経路で経路が混んでいる場合には，複数経路ではなく単一経路を利用するように切り替えることを提案する．すなわち，負荷が小さいときには複数経路を利用し，負荷が大きいときには負荷のかかっていない経路のみを通るように切り替えるようにする．具体的には図 17 に示すように VPN I-2 と VPN T-1 間に負荷がかかっている場合には VPN I-1 と VPN T-2 間のみを通るように切り替え，VPN I-2 と VPN T-2 間，VPN I-1 と VPN T-1 間は使用しないようにする．負荷のかかっていない経路のみを使用することによって負荷の影響がなくなり，性能が向上すると考えられる．

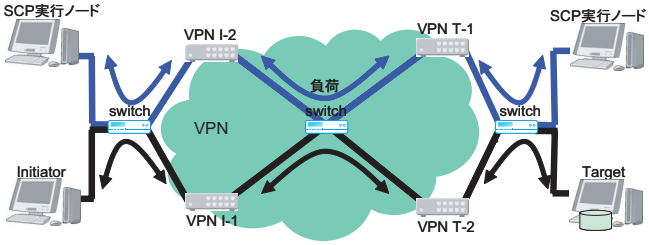

図 17　提案手法 (負荷存在時の通信経路)

6.3　実験結果

ネットワーク負荷の影響評価実験と同様に，複数経路の iSCSI over VPN 環境で図 17 のように VPN I-2 と VPN T-1 間に負荷をかけて，iSCSI は VPN I-1 と VPN T-2 間のみを通るように設定してスループットを測定し，比較を行った．その結果を図 18 に示す．

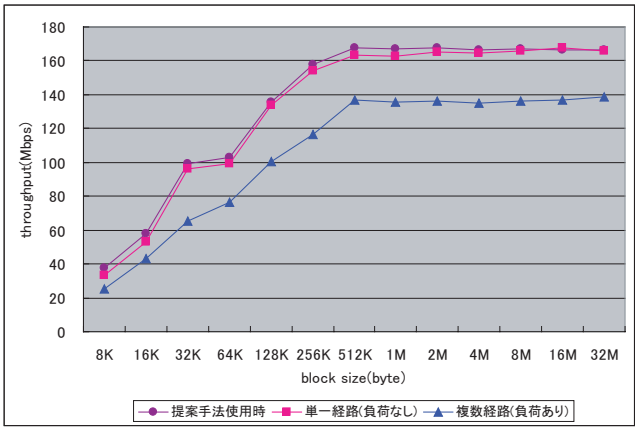

図 18　測定結果

提案手法と負荷のかかっていない単一経路単一コネクションのスループットの値がほぼ等しくなった．また負荷がかかっている複数経路複数コネクションより高いスループットを得ることができた．このことより負荷がかかっている場合には，複数経路を利用するよりも単一経路に切り替える提案手法のほうが性能がよくなると考えられる．

さらに負荷により異なるスループットに合わせて，各コネクションに対して配分するパケットの振り分けを変化させるように実装を変えることができれば，より性能の高いアクセスを実現する適応制御を行うことも可能である．

7. まとめと今後の課題

基礎実験として低スループット環境において単一経路の iSCSI over VPN 環境を構築し，VPN ルータをはさんだ場合とはさまない場合でスループットを測定し，比較を行った．VPN ルータをはさむと，はさまないときと比べかなりスループットが低下した．これは VPN ルータの性能がボトルネックとなっていると考えられる．

また，複数経路アクセス実験として高スループット環境において複数経路の iSCSI over VPN 環境も構築し，スループットを測定した．経路の数だけでなくコネクションの数も単一，複数と変化させスループットの比較を行った．複数経路複数コネクションの場合のほうが高いスループットを得ることができた．これは VPN を通るときの暗号化処理などの負荷が分散されたからであると考えられる．

しかし，負荷をかけると複数経路複数コネクションの場合も単一経路単一コネクションの場合もほぼ同程度スループットが落ちた．これは 2 つのコネクションのうち，空いているほうも混んでいるほうに影響されて通信の待ち時間が長くなるからであると考えられる．

そこで負荷に対する適応制御手法を提案した．また評価実験より負荷がかかっている場合には複数経路を利用せず，単一経路に切り替えることによって性能向上が期待できることが実証できた．

今後は提案手法を実装し，評価を行っていく予定である．

文　　献

[1] iSCSI Specification, http://www.ietf.org/rfc/rfc3720.txt?number3270/

[2] 喜連川優：ストレージネットワーキング，オーム社

[3] Peter Radkov, Li Yin, Pawan Goyal, Prasenjit Sarkar and Prashant Shenoy “ Performance Comparison of NFS and iSCSI for IP-Networked Storage, ”In Proc. FAST 2004, USENIX Conference on File and Storage Technologies, Mar 2004.

[4] 小早川知昭：IPsec 徹底入門，翔泳社

[5] 武田裕子，小口正人：“ IP ストレージリモートアクセスにおける VPN 利用に関する一検討，”情報処理学会第 68 回全国大会，pp.611-612，2006 年 3 月

[6] 武田裕子，小口正人：“ IP ストレージの VPN を介したリモートアクセス性能評価，”DICOMO2006，pp.713-716，2006 年 7 月

[7] InterOperability Lab in the University of New Hampshire, http://www.iol.unh.edu/consortiums/iscsi/.

[8] IP アクセスルータ GeoStream Si-R シリーズ, http://fenics.fujitsu.com/products/sir/.

[9] 藤原啓成，若宮直紀，志賀賢太：“ 広域 IP 網を介した iSCSI 通信におけるプロトコルチューニングの一検討，”情報処理学会第 68 回全国大会，pp.155-156，2006 年 3 月

[10] 武田裕子，小口正人：“ VPN を利用した IP ストレージへの複数経路アクセス制御手法の提案，”電子情報通信学会コンピュータシステム研究会，CPSY2006-39，pp.7-12，2006 年 12 月