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.

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

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，ストレージ接続にSANを用い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な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，オープンなインターネット環境を通してアクセスするための手法を考察していく．しかしVPN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．このためQoSのレベルが低いネットワーク環境を使用することになり，接続が不安定で帯域が保障されないという問題点が生じる．そこで本研究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，その制御を行う手法を検討する．

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 of a Method to Control Multi-route Access for IP-Storage using VPN

Yuko TAKEDA† and Masato OGUCHI†

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

Abstract　SAN has come to be often used for the storage connection in recent years. It is 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. Then, the technique to access it is considered by using VPN through the open Internet environment. However, VPN often uses the open Internet environment in general. Therefore, the network environment that QoS is low will be used, and the connection is problem from which the network bandwidth is not stably assured. Then, the technique for doing the control is examined by using two or more routes to improve the performance and the reliability of the network.

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

1. はじめに

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．SANは，サーバとストレージを直接接続するDAS(Direct Attached Storage) と異なり，サーバとストレージを高速なネットワークで接続する．DASと比べ，SANは管理コストや管理負荷を大幅に削減することができる．

SANの中で現在広く使われているのはFC-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．しかし，FC用の製品が高価であること，FC管理技術者が少ないことや，接続距離に制限があるなどの問題がある．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．FCよりも安価で，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の中で特に注目されているものが，2003年2月にIETFにより承認されたiSCSIである [1]．iSCSIとは，図1のようにサーバ (Initiator) とストレージ (Target) 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である．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．

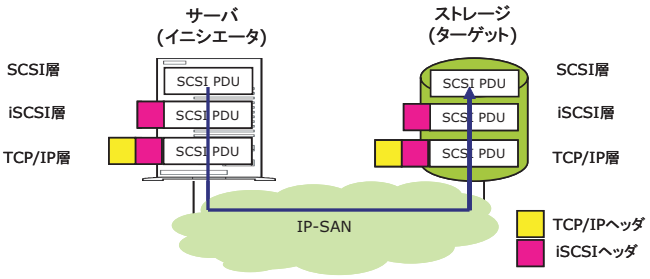

図 1　iSCSI

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 と比べ，高速なネットワークで接続できたり，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，現状では SAN はサーバサイト内においてのみしか使用されていない．そこで本研究では，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．はじめに基礎実験として単一経路で iSCSI 環境を構築，スループットの測定を行い，また，複数経路においても同様に iSCSI 環境を構築，スループットの測定を行い，単一経路の場合との比較をした．

2.　VPN 上の IP-SAN の実現例

これまで SAN は，一般にサーバサイト内のみにおいて用いられてきたが，本研究ではその制限を取り払い，ローカルな環境で利用されている iSCSI を広域ネットワークに適用することを検討する．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，オープンなインターネット環境を介してサーバサイト内の IP ストレージへリモートアクセスを実現し，その評価を行う．その実現例を図 2 に示す．

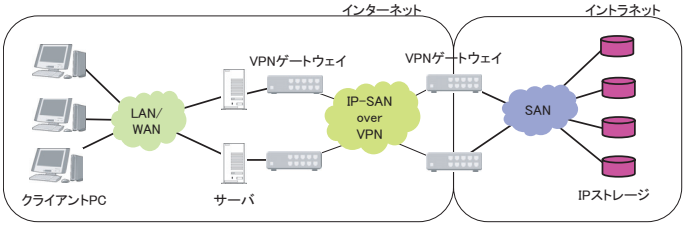

図 2　VPN 上の IP-SAN の実現例

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．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．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．

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．カプセル化により，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できるようになる．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．

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：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：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：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：IP パケットをカプセル化するプロトコル．
- SSL：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．

3.3.1　IPsec

VPN で現在もっとも普及しているプロトコルが IPsec(Security Architecture for Internet Protocol) である [2]．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 ルータで使う 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．

本研究では，IPsec の VPN ルータを用いて実験を行った．

3.3.2 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．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利用できるようになってきている．

4. 研究方針

VPN を利用することによって安く安全に通信を行うことが可能となるが，オープンなインターネット環境を使用するということは，接続が不安定であったり，帯域が保障されないといった問題点も生じる．そこで，本研究ではネットワークの信頼性を高めるために，複数経路を使用することを考える．

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，同じあて先のパケットを IP アドレスやポート番号を指定し異なる経路を通すことで，これは VPN ルータにもともと備わっていた機能を利用している．本研究では異なったポート番号を指定し複数経路を実現している．

本研究では基礎実験として VPN ルータ 2 台を挟んだ単一経路の IP-SAN 接続 iSCSI システムを構築し，VPN 上の iSCSI の性能評価を行う．そして，基礎実験とは性能の異なる VPN ルータ 4 台を挟んだ複数経路の IP-SAN 接続 iSCSIS システムを構築し，評価を行う．

5. iSCSI の仕組み

5.1 iSCSI の特徴

SAN プロトコルは，図 3 のように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．iSCSI の場合，リモートブロックは TCP/IP パケットの中に SCSI コマンドをカプセル化することによってアクセスされる．また，ファイルシステムはクライアント上に存在する．

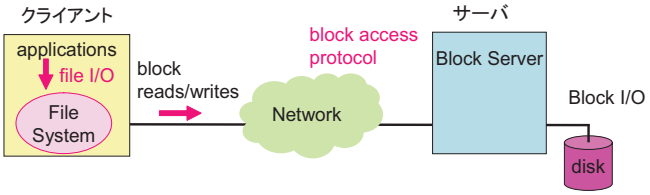

図 3 iSCSI

iSCSI の主な特徴は次のとおりである [3]．

- 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す．
- 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．
- 明示的な再伝送リクエストや，高度な誤り回復をサポートする．
- 直接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ある．また，データやメタデータの更新は非同期的に行われる．

5.2 iSCSI の複数コネクション

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．

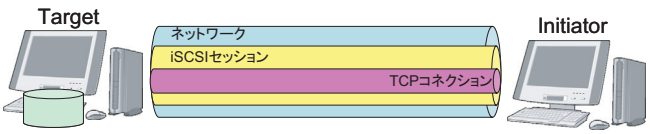

図 4 iSCSI の単一コネクション

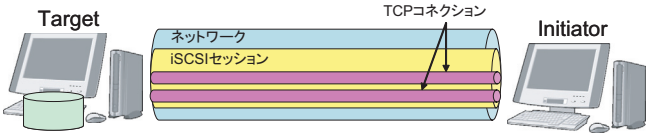

図 5 iSCSI の複数コネクション

図 4 では iSCSI セッション中に TCP コネクションは一本だが，図 5 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．

6. 基礎実験

6.1 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．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 [4]．図 6 に示すように，VPN ルータ 2 台を挟んだ iSCSI システムを構築して評価を行った．測定ツールには自作のベンチマークツールを用いて，raw デバイスに対して測定を行った．実験システムの概要は以下のとおりである．

- CPU: Intel Xeon 2.4GHz
- Main Memory: 512MB DDR SDRAM
- HDD：36GB SCSI HD
- NIC：Intel PRO/1000XT Gigabit Ethernet
- OS: Linux2.4.18-3
- iSCSI: UNH IOL reference implementation ver.3
- VPN ルータ: 富士通 Si-R180(IPsec 暗号化スループット: 100Mbps)

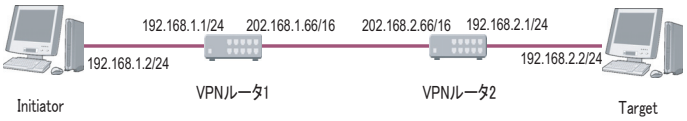

図 6　基礎実験環境

6.2 測定結果・考察

VPN ルータ 2 台を挟んだ iSCSI システムを構築し，評価を行った [6][7]．VPN 接続時と直接接続時の比較の結果を図 7 に示す．また図 8 は図 7 の VPN 接続時の結果をスケールを変えたものである．VPN ゲートウェイを挟むと，挟まないときよりかなりスループットが低下した．

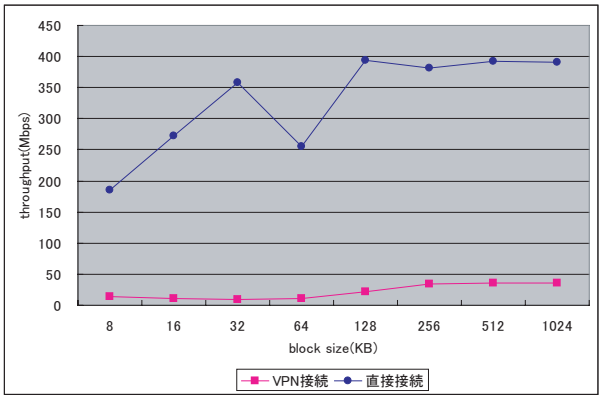

図 7　VPN 接続時と直接接続時の比較

また VPN をはさんだ場合には，スループットは 36Mbps 程度で飽和状態となっている．iSCSI は VPN をはさまない環境で，最大 400Mbps 程度出ており，実験機器の VPN は IPsec 暗号化スループット 100Mbps 程度である．両者の値とも実験機器やアクセスパターンなどにより値が大きく変動するものであり，両者のバランスを考慮した IP-SAN 環境の構築が重要といえる．また，各環境においては，スループットがブロックサイズに対応して変化するもので，適切なパラメータ設定が必要であるといえる．

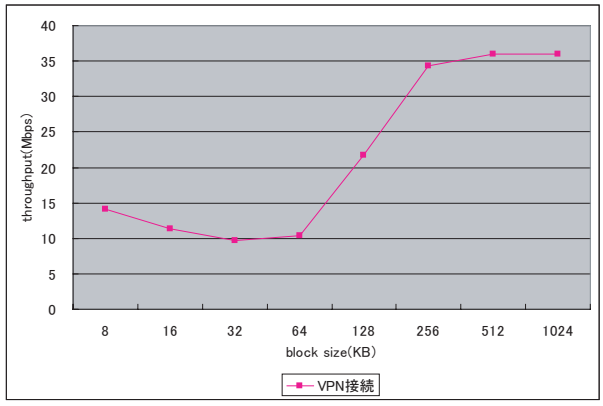

図 8　VPN 接続時の iSCSI アクセススループット

7. 複数経路アクセス提案モデル

7.1 実験環境

図 9 に示すような複数経路での VPN 上の iSCSI 環境を構築し，単一経路と複数経路でスループットを測定した．また，異なるポート番号を用いることによって複数のコネクションを生成し，単一経路単一コネクション，単一経路複数コネクション，複数経路複数コネクションの 3 つの条件でそれぞれスループットの測定を行い，基礎実験と比較を行った．

マシンは基礎実験と同じマシンを用いており，ルータは富士通 Si-R570 を用いた．基礎実験で用いた Si-R180 は 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 IPsec 暗号化スループットが 500Mbps となっている．

- NIC：Intel PRO/1000XT Gigabit Ethernet,
  Intel PRO/1000MT Gigabit Ethernet
- VPN ルータ: 富士通 Si-R570(IPsec 暗号化スループット: 500Mbps)
- その他は基礎実験と同じ

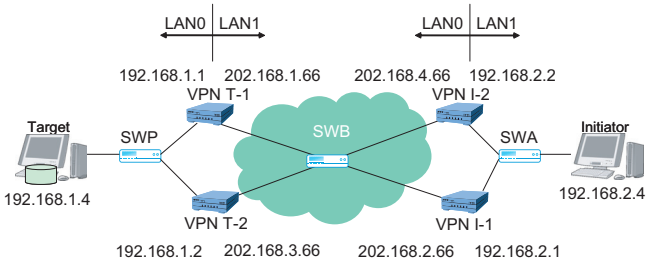

図 9　複数経路実験環境

なお，イニシエータからターゲットへの送信は図 10 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は図 11 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．

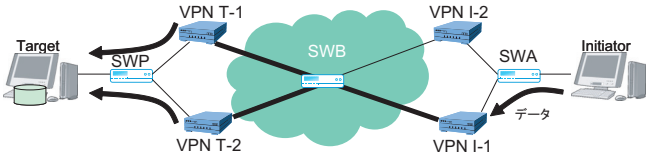

図 10　イニシエータからターゲットへの送信

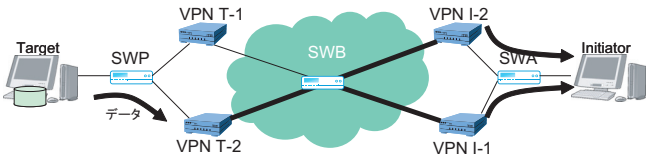

図 11　ターゲットからイニシエータへの送信

7.2　測定結果と考察

単一経路単一コネクション，単一経路複数コネクション，複数経路複数コネクションの環境を作り，それぞれでスループットを測定し，比較した．その結果を図 12 に示す．

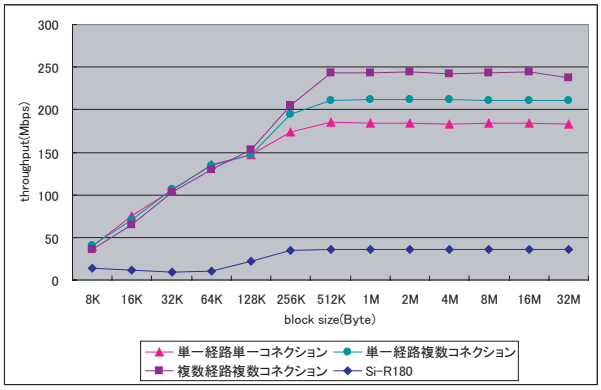

図 12　複数経路環境の iSCSI のアクセススループット

Si-R570 の単一経路単一コネクションでは 180Mbps 程度で飽和状態となっている．Si-R180 は 36Mbps 程度で飽和状態となっていたので，Si-R180 と比較すると約 5 倍になっており，ルータの性能の差，100Mbps と 500Mbps と比例していることがわかる．

単一経路で単一コネクションと複数コネクションを比較すると，複数経路のほうがよい結果となり，複数コネクションで単一経路と複数経路を比べると，複数経路のほうがよい結果になった．

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，そこで暗号化の処理などを行うからと考えられる．したがって複数経路にすると単一経路と違い負荷が 2 つに分散されるので，複数経路複数コネクションのほうが単一経路複数コネクションよりスループットが高かったと考えられる．

Si-R570 で測定した 3 パターンはブロックサイズが 128Kbyte まではすべてが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．しかしその後伸び方に差が出て，512Kbyte あたりですべて飽和状態となっている．

7.3　負荷の影響

次に，ネットワークに他のトラフィックを流し負荷をかけて，先ほどと同様に単数経路単一コネクション，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，それぞれ負荷をかけない場合と比較を行った．単一経路単一コネクションの実験結果を図 13 に，複数経路複数コネクションの実行結果を図 14 に示す．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とした．

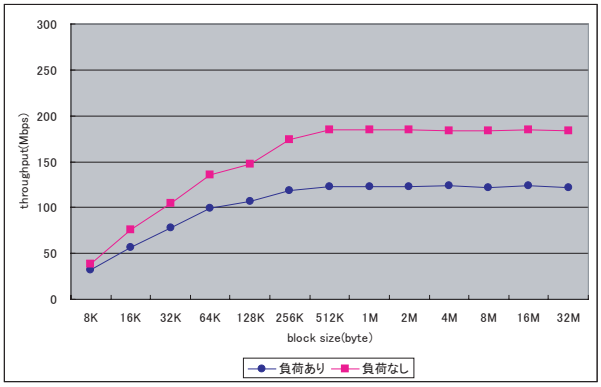

図 13　単一経路単一コネクションの実行結果

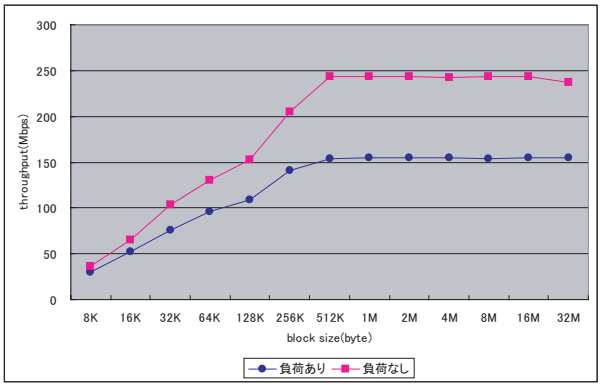

図 14　複数経路複数コネクションの実行結果

複数経路の場合も，単一経路の場合も，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．

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おり，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．

従って，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としても，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，ということだと考えられる．

8. まとめと今後の課題

基礎実験として単一経路の 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た．VPN ゲートウェイをはさむと，はさまないときと比べかなりスループットが低下した．しかしこれらは実験機器やアクセスパターンなどによって値が異なってくるもので，バランスを考慮する必要があるといえる．

また，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がもっとも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を分散させているからと考えられる．

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とほぼ同じ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待ち続けているからであると考えられる．

iSCSI で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全体の性能が落ちてしまうので，今後は負荷を分散するなどしてこれを制御する方法を考えていきたい．また，その制御をアプリケーションからは単一経路アクセスに見える仕組みをミドルウェアで実現することを考えていく．

文　　献

[1] iSCSI Specification, http://www.ietf.org/rfc/rfc3720.txt?number=3270/

[2] 小早川知昭：IPsec 徹底入門，翔泳社

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

[5] 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 8 回全国大会，2006 年 3 月

[6] 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，2006 年 3 月

[7] 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 ”DICOMO，2006 年 7 月