3R-4

IP ストレージリモートアクセスにおける VPN 利用手法の検討

武田 裕子　　小口 正人
お茶の水女子大学

1. はじめに

近年ではサーバにおけるストレージ接続に SAN(Storage Area Network) を用いることが多くなってきた．SAN とはサーバとストレージを接続するデータ通信ネットワークである．現在のところファイバチャネルを用いる FC-SAN が主流であるが，近年 iSCSI などを利用する IP-SAN も利用され始めてきている．SAN を利用することにより，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 で接続することができる．しかし，現状では SAN はサーバサイト内にのみで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．

2. 本研究の評価モデル

これまで SAN は，一般にサーバサイト内のみに存在した．本研究ではその制限を取り払い，ローカル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 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よりサーバサイト内の 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 [図 1].

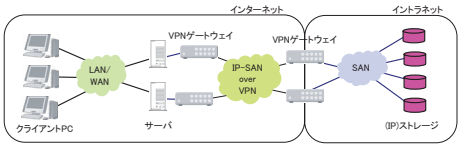

図 1: 評価モデルの概念図

3. VPN

3.1 VPN とは

VPN(Virtual Private Network) 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，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，というのが VPN の基本的な発想である．

A Study of a Method to Use VPN for IP-Storage Remote Access
Yuko Takeda, Masato Oguchi
Ochanomizu University

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．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．

3.3 IPsec

VPN で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 [1]．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 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 層での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 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機能が備わっている．一方 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．

4. iSCSI と NFS

4.1 iSCSI の特徴

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．iSCSI の場合は，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．SAN のアプローチでは、ファイルシステムはクライアント上に存在する．

iSCSI の主な特徴は次のとおりである．2 つの間の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

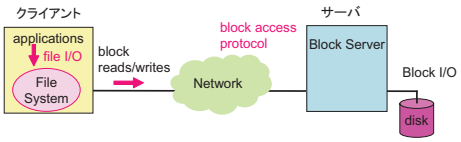

図 2: iSCSI

のセッションの概念を使う．多数のコネクションによるセッションへの多重送信をゆるす．暗号化（IPsec）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．

4.2 NFS の特徴

NFS(Network File System) は，ファイル単位でリモートデータにアクセスする [2]．クライアントは，RPC ベースのプロトコルを使用してサーバ上のメタデータやファイルにアクセスする．NFS ではファイルシステムは，サーバ上に存在する．

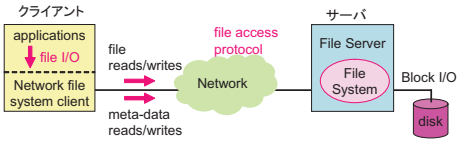

図 3: NFS

NFS には 2，3，4 のバージョンがある．

v2：クライアントとサーバは UDP，RPC を通って接続する．ステートレスで，NFS サーバはクライアントの状態を把握しておらず，結果，もしサーバがクラッシュしても情報を失うことがない．

v3：64 バイトまでのさまざまな長さのファイル処理を可能にし，最大の転送データサイズの制限を解消した．ファイル操作のオフセットを 64 ビットに拡張した．属性付きディレクトリの読み取りや非同期書き込みをサポートする．UDP に加えて，TCP を使用可能にする．

v4：一連のプロトコルを単一のプロトコルに統合し，多数の操作を単一の操作に統合した．前のバージョンと比べステートフルで，クライアントは，サーバとのステートフルなインタラクションが可能．クライアントが積極的にファイルデータをキャッシュすることが可能である．

4.3 iSCSI と NFS の比較

NFS は本質的に，多数のクライアントマシン間でファイルを共有することが可能であるため，データ共有に適している．

一方 iSCSI はブロックプロトコルなので，単一のクライアントがブロックサーバ上のそれぞれのボリュームをサポートする．結果，iSCSI は，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．

5. 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測定を行った [3]．図 4 に示すように，VPN ゲートウェイ 2 台を挟んだ iSCSI システムを構築して評価を行った．

・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 ゲートウェイ: 富士通 Si-R180(IPsec 暗号化スループット: 100Mbps)

図 4: 実験環境

6. 測定結果

iSCSI を VPN ゲートウェイをはさむときとはさまないときでスループットを測定した [図 5]．VPN ゲートウェイをはさむと，はさまないときよりかなりスループットが低下した．VPN をはさんだ場合にはブロックサイズが 256[KB] 以上では飽和し，スループットは 4.5[MB/sec] となっている．また，VPN をはさまなかった場合と同様，iSCSI のオーバーヘッドによりＶＰＮの暗号化スループットよりもかなり低下している．

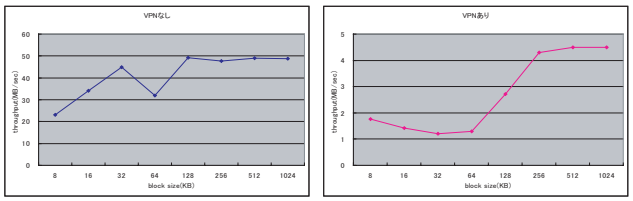

図 5: 測定結果

7. まとめと今後の課題

VPN ゲートウェイをはさんだときとはさまないときで iSCSI の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．今後は，iSCSI と NFS の性能を測定し，比較する．パフォーマンスの考察を行い，帯域や IPsec の設定を行う．アクセス認証等のセキュリティ手法を検討していく．

参考文献

[1] 小早川知昭：IPsec 徹底入門，翔泳社

[2] 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.

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