IP-SAN を利用したセキュアなストレージアクセスにおける性能向上手法の提案と検討

A Proposal of Performance Improvement in Secure Storage Access using IP-SAN

神坂 紀久子 † 山口 実靖 ‡ 小口 正人 †
Kikuko Kamisaka Saneyasu Yamaguchi Masato Oguchi

1. はじめに

近年，ストレージシステムに格納するデータ量が急増している．それに伴い，ストレージの運用や管理のコストも増加しており，データ管理の効率化とコスト削減のため，SAN(Storage Area Network) に対する関心が高まってきている．

SAN ではサーバごとに管理されていたストレージを高速なネットワークで接続し，ストレージ統合と集中管理を可能にする．現在では，FC(Fibre Channel) とよばれる専用ネットワークを用いた FC-SAN が一般的に普及している．しかし，FC-SAN は導入や管理のコストが高く，専門知識を持った管理者が少ないことなどから，最近では IP ネットワークを用いてストレージアクセスを行う IP-SAN が登場してきた．

IP-SAN の実現技術として，iSCSI プロトコルが 2003 年に IETF に承認され，有力視されている．iSCSI では，イニシエータとよばれるサーバとターゲットとよばれるストレージの間で，SCSI プロトコルを TCP/IP プロトコルにカプセル化し，通常の SCSI アクセスと同様の操作で遠隔ストレージへのアクセスを可能にするものである．しかし，TCP/IP は高速な通信インフラを想定して設計されたプロトコルではないため，一般に大容量のデータを送受信する iSCSI でストレージアクセスを行う際には，TCP のプロトコル処理がサーバの負荷を増大させる．また，iSCSI ネットワークでセキュアな通信を行うためには IPsec というセキュリティ技術を用いることが可能であるが，暗号化処理による CPU 負荷や性能低下の問題が生じている．これらの性能面における問題に対して，iSCSI TOE や HBA によりハードウェアに処理を任せることもできるが，P. Sarkar らにより，CPU 負荷を軽減させることはできるものの，総合的な性能ではソフトウェア実装の方が性能の方が高くなるという結果が得られている [1]．

そこで本稿では，IP-SAN を利用した安全なストレージアクセスに伴う性能低下に関する問題点の解決手法を提案し，試作システムを用いた評価を行う．

2. IP-SAN における IPsec の適用と問題点

iSCSI では，IP 層で透過的に認証と暗号化を行う IPsec が一般的に広く利用されている．

そこで，iSCSI ネットワークにおいて IPsec を利用したシーケンシャルリードアクセスの評価実験を行った [2]．その結果，スループットが大幅に低下し，CPU 負荷が非常に高くなることがわかった．その性能低下の詳細を知るため，iSCSI 使用時における TCP/IP 層のパケット転送の振る舞いを解析した [3]．解析結果として，IPsec 層において各パケットごと 3DES で暗号化をしてから転送する処理が性能に大きな影響を与えていることがわかった．

IPsec では暗号化アルゴリズムとして 3DES(Triple Data Encryption Standard) が広く使われている．しかし，3DES の暗号化処理は計算量が非常に多く，著しい性能低下をまねく．基本的にセキュリティとパフォーマンスはトレードオフの関係にあるため，IP-SAN においても，暗号化などのセキュアな通信を行いながら可能な限り性能を落とさないように工夫する必要がある．

3. 上位層における暗号化方式の提案

IPsec を用いて通信を行う際，IPsec は上位層の処理を知ることができないため，効率的な暗号化処理を行うことは困難である．たとえば，IP-SAN を利用したストレージアクセスでは，大規模なデータをシーケンシャルにアクセスすることが多いが，その場合，IPsec 層はただ上位層から渡された小さなパケットを順次暗号化するだけである．上位層の処理内容を把握して，データを大きなブロックに分割して暗号化を行ったり，1 つのブロックを送信し，ACK を待っている間に次のブロックの暗号化を行うような処理を行うことによって，効率的なデータ転送が可能であるはずだが，IPsec を用いてそれを実現することは難しい．

そこで，IP-SAN を用いてセキュアなストレージアクセスを行う際に IPsec の代わりに IPsec 層より上位層において暗号化を行う方式を提案する．IP-SAN で，IPsec を用いた場合のアクセス方式と，IPsec を使わずに上位層で暗号化を行う場合の実現方式をそれぞれ図 1，2 に示す．IPsec を利用した方式 (図 1) では，データの暗号化，復号化を IPsec 層において行う．上位層から IPsec 層にデータが送られるまでに，データが小さいブロックに分割され，その後暗号化処理が行われる．一方，提案手法を用いた場合 (図 2) は，ターゲットのディスクに格納されているデータが読み出されて，SCSI 層と同位の暗号化/復号化層において暗号化が行われ，SCSI Driver に送られる．暗号化されたデータは，IP 層を通り，ファイルシステムから読み出された後に復号化が行われ，アプリケーションに渡される．まとまったブロックを上位層で暗号化するため，ヘッダ処理をともなう暗号化処理を細分化された各パケットごとに行うよりも効率的であると考えられる．

4. 提案方式の性能評価実験

本稿では，提案手法を実装した際の性能を予測するために，IPsec を用いる方式と上位層で暗号化する方式それぞれを，iSCSI を利用せずに単純なソケット通信を行った場合と iSCSI ネットワークでリモートストレージアクセスを行った場合それぞれにつきモデル化して評価する．
提案手法の上位層における暗号化には OpenSSL の crypto ライブラリを用い，3DES の暗号化を行った．これは IPsec で用いられているものと同じ暗号化ア

† お茶の水女子大学
Ochanomizu University
‡ 東京大学生産技術研究所
Institute of Industrial Science, The University of Tokyo

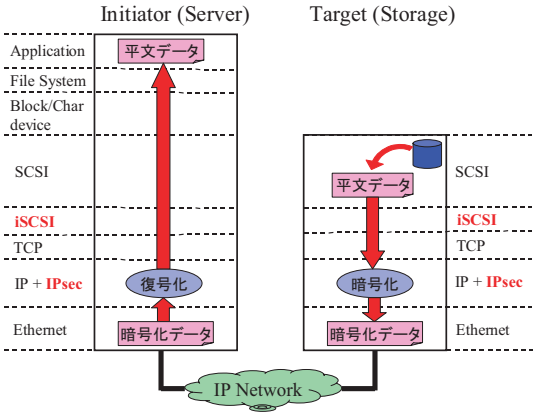

図 1: IPsec を用いて暗号化するストレージアクセス方式

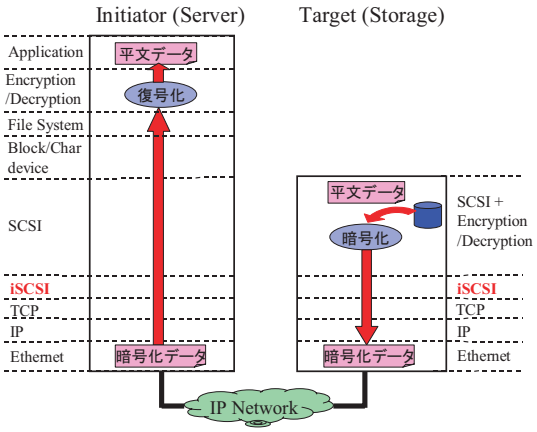

図 2: 上位層において暗号化するストレージアクセス方式 (提案手法)

ルゴリズムである．また，微小パケットに対する Nagle アルゴリズム起動による性能低下を防止するため，TCP_NO_DELAY オプションを用いた [3]．実験に用いた計算機とソフトウェアの詳細を表 1，2 に示す．

4.1 iSCSI を用いない単純なソケット通信によるシーケンシャルリードアクセスの実験

まず，iSCSI を用いずに単純なソケット通信を行う実験では，どちらの方式においても，ターゲット側に相当するホストのディスクからデータを読み出しソケットを通じて送信し，イニシエータ側に相当するホストがこれを受信する．その際，IPsec を用いる方式では，上位層であるアプリケーションはデータの送受信だけを行い，下位層として IPsec を起動して，IPsec 層において暗号化を用いて，復号化を行う．上位層で暗号化する方式では，下位層は通常の TCP/IP であるが，ターゲット側では，上位層 (アプリケーション) がディスクからデータを読み出した後に暗号化してから送信し，イニシエータ側も，上位層でデータを受け取ってから復号化を行う．本実験は，図 1，2 において SCSI 層と iSCSI 層を除いたシステム環境における比較実験に相当する．

表 1: 実験環境：使用計算機

OS	initiator:Linux 2.4.18-3 target:Linux 2.4.18-3
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)

表 2: 実験環境：使用実装

iSCSI	UNH-iSCSI Initiator and Target for Linux ver.1.5.3
IPsec	FreeS/WAN ver. 2.01

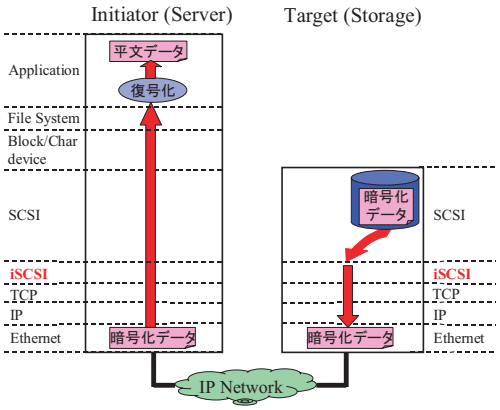

図 3: 提案手法を模擬した iSCSI ストレージアクセス

4.2 iSCSI ネットワークにおけるリモートストレージアクセスによる実験

iSCSI ネットワークでイニシエータからターゲットの RAW デバイスに対してシーケンシャルリードアクセスを行い，提案手法の試作システムによる実験を行った．IPsec を用いた場合は，通常の iSCSI シーケンシャルリードアクセスを行う．一方，提案手法を模擬した試作システムにおいては，crypto ライブラリを使用して 3DES 暗号化を行ったデータをあらかじめディスクに格納しておく．シーケンシャルリードアクセスを行う際には，その暗号化されたデータをディスクから読み出し，上位層であるアプリケーションで復号化を行う．この実験を図 3 に示す．提案手法を模擬した実験は，あらかじめ暗号化されたデータを読み出すため，IPsec を用いる場合との比較は完全に公平ではない．これは提案手法の実装が完成し，暗号化処理時間を通信処理の待ち時間に隠蔽することが可能になった場合等における理想的なケースをモデル化したものと考えることができる．

4.3 実験結果と考察

ソケット通信を行った場合の各方式のスループットと CPU 使用率を測定した結果を図 4，5 に示す．また，iSCSI ネットワークを利用した場合の各方式の実験結果を図 6，7 に示す．

図 4 から，上位層で暗号化する方式の方が，IPsec を用

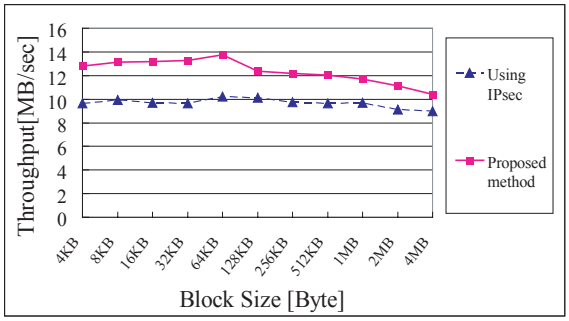

図 4: iSCSI を用いない単純なソケット通信に使った性能測定実験：スループット

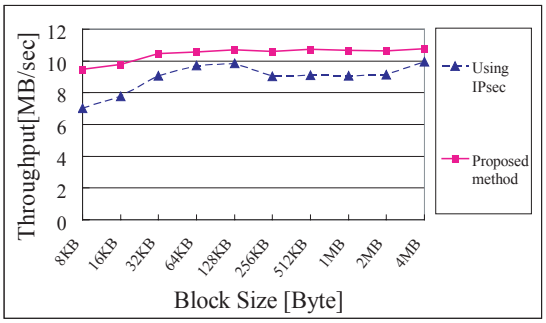

図 6: iSCSI を用いた試作システムによる性能測定実験結果：スループット

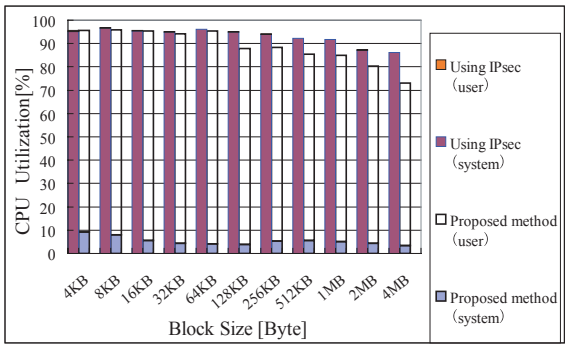

図 5: iSCSI を用いない単純なソケット通信を使った性能測定実験：CPU 使用率

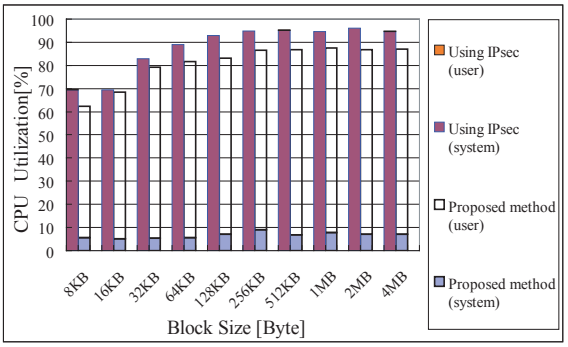

図 7: iSCSI を用いた試作システムによる性能測定実験：CPU 使用率

いた方式よりスループットが高く，ブロックサイズの平均で約 30% 向上していることがわかった．これは，上位層でブロックをまとめて暗号化した方が IPsec でパケットごとに暗号化するより効率が良かったためと考えられる．一方，図 6 は，理想的なケースをモデル化した場合における比較であるが，提案方式は IPsec を用いた方式に比べ，約 17% の性能向上がみられた．また実際には，IPsec と OpenSSL の暗号化コードは全く同じでは無いが，3DES の暗号化は負荷が大きく，暗号化の計算が実行のほとんどを占めるため，ほぼ公平な比較であると考えられる．

図 5，図 7 は，システムとユーザの内訳で全体の CPU 使用率をイニシエータ側で測定した結果である．比較的大きなブロックサイズでデータを転送した場合には，上位層で暗号化する方式の方が負荷が小さいことがわかる．また，IPsec の暗号化はカーネル空間における処理であり，一方上位層の暗号化処理はユーザ空間における処理である．一般にカーネル空間の実行の方がプロセスの優先度が高いため処理が速いが，それにもかかわらずこの場合はユーザ空間における実行の方が速くなった．優先度の高いカーネル空間で CPU 負荷の高い処理を大量に行うことは，ユーザ空間で動作するサービスの著しい性能低下や停止につながるため好ましくなく，これをユーザ空間の方へ移動させる上位層における暗号化方式は望ましい．

現状では，上位層における暗号化方式において，通信処理の ACK 待ちの間に次のブロックを暗号化するような処理は実現していないが，これを実現して暗号化処理を通信時間に隠蔽するなどを行えば，図 6 で示された理想的なケースに近い性能の向上が期待できる．

5. まとめと今後の課題

本稿では，IP-SAN を利用した安全なストレージアクセスを実現するために，IPsec の代わりにその上位層で暗号化する方式を提案した．また，簡易実装を用いた評価を行い，IPsec を用いる暗号化方式より，提案手法の方が有効性が高いことを確認した．今後の課題としては，提案手法の実装を完成させ，ACK を待っている間に次のデータの暗号化をする処理の実装を行うことが挙げられる．

謝辞

本研究は一部，文部科学省科学研究費特定領域研究課題番号 13224014 によるものである．

参考文献

[1] P. Sarkar, S. Uttamchandani, and K. Voruganti, “Storage over IP: When Does Hardware Support help?,” *Proc. FAST 2003, USENIX Conference on File and Storage Technologies*, pp. 231-244, Jan. 2002.

[2] 神坂 紀久子，山口 実靖，小口 正人: “IPsec を利用した iSCSI ネットワークにおけるシーケンシャルアクセスの考察”, 信学会全国大会，B-16-10, p.619, 2004 年 3 月.

[3] 神坂 紀久子，山口 実靖，小口 正人: “IPsec を利用した iSCSI ストレージアクセス時の TCP パケット転送の解析”, 情報処理学会研究報告, 2004-HPC-97, HOKKE2004, pp. 145–150. 2004 年 3 月.