B-026

iSCSIリモートストレージアクセス時における暗号処理最適化手法の複数プロセスを使用した性能評価と考察

Performance Evaluation with Multi Processes of Encryption Processing Optimized in iSCSI Remote Storage Access

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

1. はじめに

インターネットなどで通信されるデータ量の急激な増大に伴い，ストレージ管理コストの削減が計算機システムの課題となっている．それらの問題に対応するため，現在ではストレージ群とサーバ群を高速なネットワークで接続し，ストレージ統合によって遠隔ストレージにある大容量データを容易に管理可能である SAN(Storage Area Network) が多くの企業で使用されている．

SAN の中でもファイバチャネル (Fibre Channel) 技術を用いる従来の FC-SAN に代わり，IP ネットワークを使用し，ストレージの導入および管理コストを軽減することができる IP-SAN が提案され，徐々に普及し始めている．

IP-SAN で使用される iSCSI(Internet SCSI) は，サーバなどの計算機と（Initiator）とストレージシステム（Target）間を TCP/IP プロトコルと Ethernet で接続するデータ通信プロトコルである．iSCSI を用いてストレージに接続する際には，インターネットを介するため安全に通信を行うことは重要である．そのため iSCSI では転送データの暗号化に，IP パケットに対して強固な暗号化と認証機能を提供する IPsec を使用することが可能である．しかし IPsec は下位の IP 層で処理するため，効率的な暗号化を行うことはできず，ストレージアクセスの通信性能が大幅に低下する．

そこで本稿では，iSCSI 層より上位層のミドルウェアで暗号処理最適化を行う手法に基づいたシステムを実装した．また，低遅延・高遅延環境において，最適化処理を想定した複数プロセスを起動し，実装したシステムのシーケンシャルリード性能を IPsec 使用時の性能と比較した．その結果，提案手法である暗号化処理最適化手法は高遅延環境において非常に有効であることがわかった．

2. 暗号処理最適化手法と実装

IPsec は IP パケットを暗号化するため，上位のソフトウェアを変更する必要がなく透過的に暗号化することができるが，一方で下位層に位置しているため，上位層から渡されたデータを逐次的に処理するのみであり，性能を向上するための機能を容易に追加することができない．しかし iSCSI より上位層で暗号化を行うミドルウェアを用いた場合は，下位の IP 層の実装に変更を加えることなく，アプリケーションや SCSI 層，TCP 層などにおける処理に柔軟に対応することができ，上位層のソフトウェアで様々な工夫をすることにより，アクセス性能向上を実現できると考えられる．

我々はこれまで，安全な iSCSI によるストレージアクセスにおいて性能を向上させる手法として，上位層で暗号化・復号化処理を行うミドルウェアを用い，暗号処理の最適化を行う手法を提案してきた [1][2][3].

iSCSI を用いて暗号化を行うシーケンシャルリードアクセスでは，まず iSCSI Read コマンドが Initiator から Target に発行され，Target で暗号化を行い，それらが Initiator に送信され，Initiator で復号化が行われ，データを受け取った後に Initiator が確認応答 (Ack) を返す．Initiator で復号化を行っている間，Target で暗号化を行っている間などで通信の待ち時間が発生する．よって，暗号化最適化手法では，この通信の待ち時間の間に次のデータの暗号化・復号化処理を行うことによって，CPU 処理の空き時間を有効に使用し，性能を向上させる．

本稿では，上位層で暗号化・復号化を行うシステムを構築した．Initiator 側においてはアプリケーションより下位に位置するミドルウェアとして実装した．Target 側においては暗号化・復号化を行うカーネルモジュールを実装し，SCSI 層より上位のミドルウェアを構築している．ミドルウェアとして暗号化・復号化機能を独立させることにより，簡単に性能を向上させる手法を適用し，機能を追加，改良することができる．また本稿のシステムでは，IPsec においてデフォルトで使用されている 3DES 暗号化アルゴリズムと同じ実装コードを使用している．

3. 低遅延・高遅延環境における暗号化処理最適化手法の性能評価実験

提案手法である暗号化処理最適化手法を評価するため，構築したシステムを用いて，Target の raw デバイスに対する iSCSI シーケンシャルリードアクセス時の性能を評価し，IPsec を用いた場合の性能と比較した．

本実験では，アプリケーションにおいて複数プロセスを起動することにより，CPU 処理の空き時間の間に連続的にデータの暗号化を行って，暗号化処理最適化手法を模擬した性能を評価している．また IP-SAN において，非常災害対策のために比較的遠距離で使用されることを想定し，高遅延環境において提案システムの性能を評価した．

3.1 実験環境

実験に用いたシステム環境を表 1，2，3 に示す．

低遅延環境における実験では，Initiator と Target を Gigabit Ethernet スイッチで 1 対 1 接続した単純な構成になっている．高遅延環境における実験では，図 1 に示すように，iSCSI Initiator と Target を Gigabit Ethernet で接続して TCP/IP 接続を確立し，Initiator と Target の間に人工的な遅延装置として FreeBSD Dummynet を設置した．片道遅延時間は 1ms，2ms，4ms，8ms と設定し測定した．

Initiator と Target の OS には Linux を用いた．また iSCSI の実装には，ニューハンプシャー大学 InterOperability Lab[4] が提供しているオープンソースの実装 (UNH-iSCSI) を用い，IPsec の実装には，Linux におい

† 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

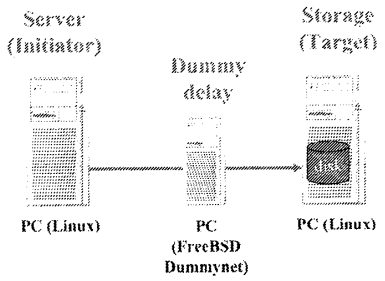

図 1: 高遅延環境における実験環境

表 1: 性能評価実験環境 1：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

表 2: 性能評価実験環境 2：使用計算機

Dummynet OS	Free BSD 4.9 - RELEASE
CPU	Intel Xeon 2.4GHz
Main Memory	512MB DDR SDRAM
NIC	Intel PRO/1000MT Server Adapter

表 3: 性能評価実験環境：使用実装

iSCSI	UNH-iSCSI Initiator and Target for Linux ver. 1. 5. 3
IPsec	FreeS/WAN ver. 2.01

表 4: IPsec に対するスループットの平均向上比率 (片道遅延時間 0ms〜8ms)

	IPsec	1pro	2pro	3pro	4pro
0ms	1.000	0.752	1.323	1.465	1.512
1ms	1.000	0.719	1.379	1.825	2.082
2ms	1.000	0.772	1.510	2.093	2.522
4ms	1.000	0.804	1.607	2.382	3.013
8ms	1.000	0.894	1.803	2.692	3.537

て広く利用されているオープンソースの FreeS/WAN[5] を用いた．IPsec の設定に，ホスト間の通信を暗号化するトランスポートモードおよび ESP プロトコルを使用している．

3.2 スループット測定結果と考察

低遅延環境 (片道遅延時間 0ms) において，本稿のシステムを用いて複数プロセスを起動して測定した際のスループットと IPsec を使用した際のスループットを図 2 に示す．また，高遅延環境 (片道遅延時間 8ms) における

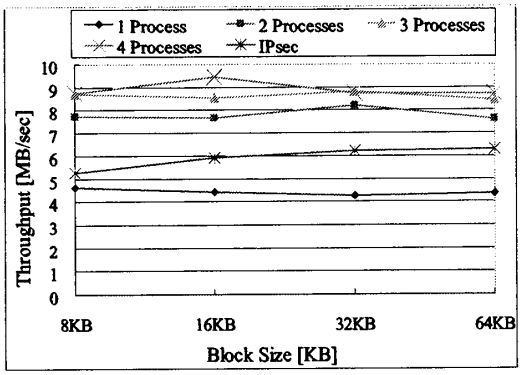

図 2: 低遅延 (片道遅延時間 0ms) におけるスループット

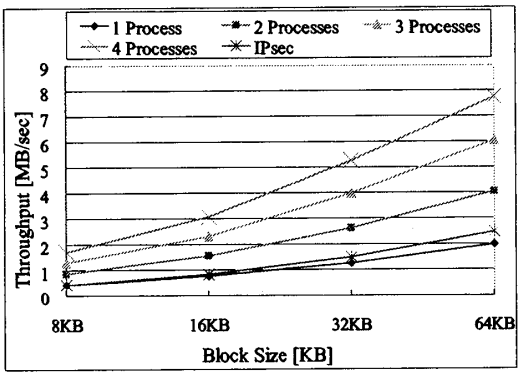

図 3: 高遅延 (片道遅延時間 8ms) におけるスループット

スループットを図 3 に示す．表 4 は，IPsec を 1 とした場合のプロセス数によるスループット向上比率を全ブロックサイズで平均したものである．

同表より，片道遅延時間 0ms である低遅延環境において 1 プロセスを起動した場合，提案システムは IPsec よりスループットが低く，0.75 倍にとどまっている．しかし，2，3，4 プロセスを起動した場合には IPsec よりも 1.3 倍から 1.5 倍程度性能が向上することがわかった．

高遅延環境においては，ブロックサイズを増加させるとスループットも向上するという結果が得られた．これは 1 つのデータセグメントを送信するのにかかる時間が長くなるためであると考えられる．また片道遅延時間を 1ms，2ms，4ms，8ms と増加させると，提案システムの性能向上比率も増加し，最終的に片道遅延時間が 8ms の場合には，2 プロセスで 1.8 倍，3 プロセスで 2.6 倍，4 プロセスで 3.5 倍の性能向上を確認できた．

低遅延環境においては，通信時間はデータセグメントの暗号化/復号化時間と比較して相対的に短い．そのため，提案手法における暗号化の先処理による最適化はプロセス数を増加させてもそれほどの効果は見られない．しかし，高遅延環境においては，通信時間はデータセグメントの暗号化/復号化時間と比較して相対的に長くなる．そのため，通信の待ち時間，つまり CPU 処理の空き時間が長くなることにより，1 つの暗号化サイクルが終了しないうちに，連続的に次のデータセグメントを暗号化する暗号

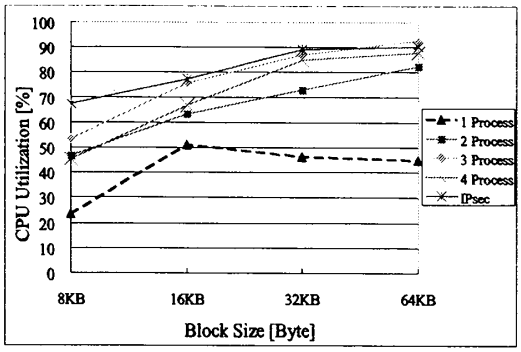

図 4: 低遅延 (片道遅延時間 0ms) における CPU 使用率 (Target)

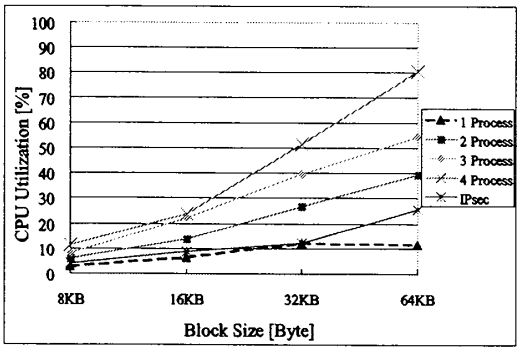

図 5: 高遅延 (片道遅延時間 8ms) における CPU 使用率 (Target)

表 5: 片道遅延 0ms, 8ms における複数プロセスを起動した場合の CPU 使用率の平均 (%)(Target)

	IPsec	1pro	2pro	3pro	4pro
0ms	81.148	41.408	66.428	77.306	71.375
1ms	43.777	29.066	54.386	73.014	71.792
2ms	33.593	22.429	43.092	59.738	67.348
4ms	18.768	14.305	30.803	42.707	56.577
8ms	12.899	8.351	21.642	31.228	41.915

処理最適化手法の効果が高くなるため，性能向上比率が大きくなったと考えられる．

3.3 CPU 使用率測定結果と考察

図 4，5 は，低遅延環境 (片道遅延時間 0ms) と高遅延環境 (片道遅延時間 8ms) において，本稿のシステムを用いて複数プロセスを起動し測定した際の CPU 使用率と IPsec を使用した際の CPU 使用率である．本実験では Linux の iostat コマンドを用い，提案手法において Target 側で CPU 使用率を測定した．表 5 は測定した全ブロックサイズの CPU 使用率の平均である．

低遅延環境において，IPsec を用いた際の CPU 使用率は提案システムの複数プロセスを起動した場合よりも高い値となった．表 5 より，提案システムが最大で 77% であるのに対し，IPsec を使用した場合は 81% に達している．

高遅延環境においては，IPsec を使用した際の CPU 使用率は提案システムの 2 プロセスを起動した際の CPU 使用率より低い値を示した．また図 5 より，ブロックサイズが増加するとともに CPU 使用率も増加し，ブロックサイズ 64KB の場合には 4 プロセスにおいて CPU 使用率が約 80% に達していることがわかる．一方，片道遅延時間を増加させると提案システムの CPU 使用率は減少する．

低遅延環境では提案システムで複数プロセスを起動した場合には，CPU 使用率は IPsec よりも低くなるが，全体的に高い CPU 使用率となった．しかし高遅延環境においては，CPU 使用率は IPsec よりも高くなるが CPU においてはまだ余裕がある．これは通信時間が長いために CPU 処理の空き時間が長くなり，その間に次のデータの暗号化を進める余裕が大きくなるためと考えられる．

4. まとめと今後の課題

本稿では，iSCSI ストレージアクセスを行う際，CPU の空き時間に連続的にデータを暗号化して性能を向上する暗号処理最適化手法を適用するために，上位層で暗号化するミドルウェアを構築した．また暗号処理最適化手法を模擬するために複数プロセスを起動させ，低遅延環境，高遅延環境において iSCSI シーケンシャルリードアクセスを行った場合のシステム性能を評価した．さらに，IPsec を使用した場合の iSCSI シーケンシャルリードアクセス性能と比較したところ，提案手法が有効であり，高遅延環境においては性能向上が大きくなることがわかった．

今後の課題としては，構築した提案システムにおいてアプリケーションレベルのベンチマークを使用した総合的な性能評価を行う．

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] 神坂紀久子, 山口実靖, 小口正人: 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, 第 3 回 情報技術レターズ (FIT 2004), Vol. 3, No. LD-003, pp. 59–61 (2004).

[2] Kamisaka, K., Yamaguchi, S. and Oguchi, M.: Performance improvement of an iSCSI-based secure storage access, *the 16th IASTED International Conference on Pararellel and Distributed Computing and Systems (PDCS 2004)* (Gonzalez, T.(ed.)), IASTED, pp. 522–527 (2004).

[3] 神坂紀久子, 山口実靖, 小口正人: iSCSI ストレージアクセスにおける暗号化処理の最適化を考慮したシステムの提案と性能評価, 先進的計算基盤システムシンポジウム (SACSIS 2005), pp. 435–442 (2005).

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

[5] FreeS/WAN Project, http://www.freeswan.org/.