7N-7

IP-SAN における暗号処理最適化ミドルウェアの構築

神坂 紀久子 † 山口 実靖 ‡ 小口 正人 †

† お茶の水女子大学 ‡ 東京大学生産技術研究所

1 はじめに

計算機で管理されるデータ量の急激な増大に伴い，ストレージシステムとサーバ機を TCP/IP ネットワークで接続してストレージを統合する IP-SAN (IP-Storage Area Network) が提案され，徐々に普及し始めている．IP-SAN の登場で，専用のハードウェアを使用し，接続距離に限界がある FC-SAN と比較して，ストレージ管理コストの大幅な削減と大規模広域 SAN を実現することが可能になった．

IP-SAN で使用される iSCSI (Internet SCSI) プロトコルを用いてストレージに接続する際には，オープンなインターネットを介する可能性があるため安全に通信を行うことが重要である．そのため iSCSI では転送データの暗号化に IPsec を使用することが可能であるが，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ができない．

そこで本稿では，IPsec の代わりに暗号化を効率的に行う暗号処理最適化ミドルウェアシステムを構築した．また高遅延環境において，構築したシステムのシーケンシャルライト性能を評価した結果，IPsec 使用時と比較して，高遅延環境において高い性能を示し，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ミドルウェアの構築

IPsec は下位層 (IP 層) に位置しており，上位層において細分化されたデータセグメントに対して，下位層で逐次的に暗号化処理するのみであるため，上位層の処理内容を把握した上で効率的な暗号化を行うことが困難である．そのため，性能を向上するための機能は下位層の改良が必要になり，容易に追加することができない．この問題に対応するために，我々は IP 層より上位層で暗号化を行う手法を提案した [1]．この手法により，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 層などにおける上位層の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．

また，その上位層に適用する性能向上手法として暗号処理最適化手法を提案した [1]．この手法について図 1 を用いて説明する．上位層で暗号化する際のシーケンシャルライトアクセスでは，イニシエータのミドルウェアでデータの暗号化を行い，SCSI Write コマンドがイニシエータからターゲットへ転送される．暗号化されたデータはネットワーク上で転送され，ターゲットは復号したデータをディスクに書き込んだ後にレスポンスを送信する．その際，相手側がデータの暗号化

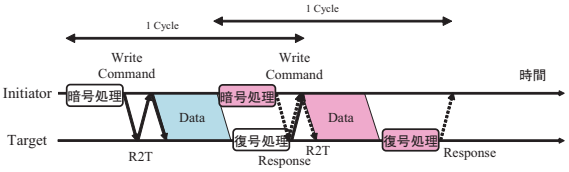

図 1: 暗号処理最適化手法

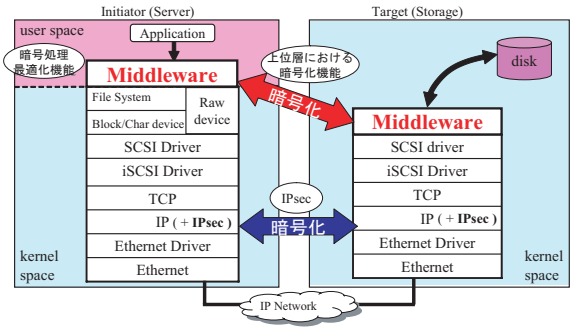

図 2: 暗号処理最適化ミドルウェアの実装

を行っている間，あるいは SCSI コマンドなどを転送している間などに通信の待ち時間が発生する．これに対して暗号処理最適化手法では，そのような通信の待ち時間を利用して次のデータを先読みし，暗号化の先処理を連続的に行う．それにより，CPU 処理の空き時間を有効に使用することができ，暗号化通信の性能を向上させる．

本稿では，IP-SAN において安全で効率的に通信を行うために，上位層における暗号化手法と暗号処理最適化手法をミドルウェアとして実装した (図 2)．

3 性能評価

効率的に暗号化を行う暗号処理最適化ミドルウェアの性能を評価するため，構築したシステムを用いて，IP-SAN において raw デバイスを使用した iSCSI シーケンシャルライトアクセスを行い，IPsec を用いた iSCSI アクセスの場合の性能と比較した．

3.1 実験環境

本稿では，IP-SAN が非常災害対策などために比較的遠距離で設計されることを想定するため，イニシエータとターゲット間に人工的な遅延装置として FreeBSD Dummynet を設置し，擬似的な高遅延環境において提案システムの性能を評価している．実験に用いたシステム環境を表 1 に示す．片道遅延時間を 1ms から 64ms まで変化させた高遅延環境において，本稿で実装したシステムと IPsec のスループットを比較している．

3.2 スループットと CPU 使用率測定結果の考察

高遅延環境において，iSCSI シーケンシャルライトアクセスで暗号化を行った場合の性能を測定した．また本実験のスループットと CPU 使用率の測定結果では，暗号処理最適化においていくつのデータブロック

Implementation of Middleware Optimized for Encryption Processing on IP-SAN
† Kikuko Kamisaka, Masato Oguchi
‡ Saneyasu Yamaguchi
Ochanomizu University (†)
Institute of Industrial Science, The University of Tokyo (‡)

表 1: 性能評価実験環境

OS	initiator : Linux 2.4.18-3 target : Linux 2.4.18-3 Dummynet : Free BSD 4.9 - RELEASE
CPU	Intel Xeon 2.4GHz
Main Memory	512MB DDR SDRAM
HDD	36GB SCSI HD
NIC NIC	Intel PRO/1000XT Server Adapter Intel PRO/1000MT Server Adapter
iSCSI	UNH-iSCSI Initiator and Target for Linux ver. 1. 5. 3
IPsec	FreeS/WAN ver. 2.01

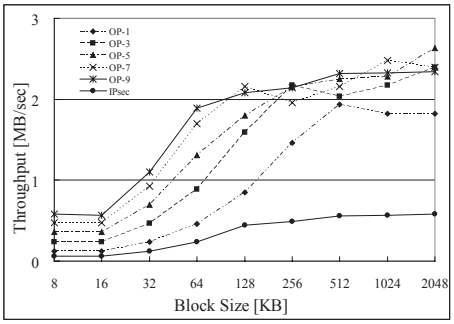

図 3: 高遅延 (片道遅延時間 64ms) におけるシーケンシャルライトアクセスのスループット

まで連続的に先処理するかという先処理の発行数を 1, 3, 5, 7, 9 まで変化させ，それらを “OP-1”，“OP-3”，“OP-5”，“OP-7”，“OP-9” として表している．図 3 は，片道遅延時間 64ms の場合のスループット測定結果であり，表 2 は，IPsec を 1 とした場合の提案システムの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．また表 3 は測定した全ブロックサイズの CPU 使用率の平均である．

図 3 より，ブロックサイズが大きい値の場合は，先処理発行数による性能向上への影響はあまりみられないが，暗号化の先処理をした提案システムは IPsec より大幅にスループットが高くなることがわかる．また，表 2 から，遅延時間が大きくなるにつれ，提案システムは IPsec よりも性能が向上することがわかる．この理由として，高遅延環境においては，通信時間の待ち時間が長くなるため，CPU 処理の空き時間が大きくなる．そのため，片道遅延時間を増加させるにつれ，1 つの暗号化サイクルが終了しないうちに次のデータセグメントを暗号化する暗号処理最適化手法の効果が高くなり，性能向上比率が大きくなったと考えられる．片道遅延時間が 64ms で，先処理発行数が 9 の場合には，提案システムは IPsec よりも 6.4 倍スループットが向上したことを確認できた．さらに，表 3 より，遅延時間を増加させると，全体的に CPU の負荷が小さくなっており，片道遅延時間が 64ms の場合には，最大でも 20%と低い値であるため，高遅延環境においては提案システムを用いる有効性が高いといえる．

3.3 スループットのモデル化による考察

提案手法の性能評価を行う際の指標として，片道遅延時間が 16ms の場合の iSCSI シーケンシャルライトアクセスのスループットをモデル化した．ここでは，通信の待ち時間に次のデータの暗号化処理をする最適化を行った後のスループットモデルを考える．提案システムで暗号化した場合の暗号化速度は 10.822MB/sec で

表 2: IPsec に対するスループットの向上比率

	IPsec	OP-1	OP-3	OP-5	OP-7	OP-9
1ms	1.000	0.973	1.366	1.450	1.460	1.418
2ms	1.000	1.076	1.726	1.995	2.038	1.978
4ms	1.000	1.338	2.205	2.787	3.198	3.240
8ms	1.000	1.393	2.598	3.471	4.114	4.560
16ms	1.000	1.856	3.314	4.310	5.105	5.764
32ms	1.000	2.098	3.938	4.479	5.198	6.009
64ms	1.000	2.509	3.921	4.926	5.770	6.403

表 3: 各遅延時間における CPU 使用率の平均 (%)

	IPsec	OP-1	OP-3	OP-5	OP-7	OP-9
1ms	57.035	64.538	83.432	85.812	87.811	86.121
2ms	47.347	55.082	77.497	85.618	87.197	86.019
4ms	39.735	48.074	69.666	78.648	83.716	84.800
8ms	22.490	37.255	59.226	68.581	75.301	79.198
16ms	12.989	30.838	48.126	55.630	60.172	64.790
32ms	7.150	20.685	32.579	31.099	33.280	36.872
64ms	3.577	12.140	16.066	17.616	18.642	19.959

表 4: スループット計算値とに最適化を行った提案システムの実測値（片道遅延時間 16ms）

Block Sizse	Calculated Value (MB/sec)	Actual Measurement (MB/sec)
8KB	0.234	0.361
16KB	0.448	0.429
32KB	0.830	0.865
64KB	1.446	1.558
128KB	2.298	2.560
256KB	3.258	3.691
512KB	4.118	4.807
1024KB	4.744	4.644
2048KB	5.135	4.270

あったため，図 1 より，先処理の発行数を 1 としてモデル化したスループットは以下の式で表される．

$$\text{スループット} = \frac{\text{ブロックサイズ}}{RTT + \frac{\text{ブロックサイズ}}{\text{下位層のスループット}} + \frac{\text{ブロックサイズ}}{\text{暗号化速度}}} \quad (1)$$

そこで，(1) 式により計算した値と，片道遅延時間 16ms において，先処理の発行数を 1 として最適化を行った場合の提案システムのスループット実測値を表 4 に示す．実測値はブロックサイズによってばらつきがあるが，スループットモデリングの計算値と実測値が近い値になっているため，このスループットのモデル式 (1) はほぼ正しいものであるといえる．よって，最適化処理をして暗号処理をオーバーラップする提案システムの性能をモデル式により確認することができた．これらより，本稿で実装した暗号処理最適化ミドルウェアが性能に関して非常に有効であることがわかった．

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，通信の待ち時間の間に次にデータの暗号化を先処理して性能を向上する暗号処理最適化ミドルウェアを構築した．また構築したシステムを用いて，高遅延環境においてシーケンシャルライトアクセスの性能を評価した結果，本稿のミドルウェアシステムが IPsec に比べ最大で 6.4 倍性能が向上し，高遅延環境において有効であることがわかった．

今後の課題として，提案システムの性能を総合的に評価する．

参考文献

[1] 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).