4C-3

テキストストリーム並列処理方式の実現

中村　隆顕†　　山岸　義徳†　　菅野　幹人†

三菱電機株式会社　情報技術総合研究所†

1. はじめに

ログ、センサデータなどの時系列的に増加する大量の追記型データの高速処理を目的としてSISA 方式（Scalable Intelligent Storage Architecture）[1]と、SISA を適用した追記型ログデータベース[2][3]を開発した。

本稿では、追記型ログデータベースを元に、ログの入力に対し即時に検索し、検索結果を出力するテキストストリーム処理を実装し、評価した結果を報告する。

2. 背景

2.1. 追記型ログデータベース

追記型ログデータベース LDB[2][3]は、大量に発生する多様な形式とデータ長のログを一元管理するためのデータベース管理システムであり、以下の特徴を備える。

- ログを形式によらずそのまま蓄積保存
- 正規表現による高速検索[4]
- ログの圧縮保存によりストレージ容量を削減

LDB では、並列処理によりログを高速に検索することが可能である。（図 2-1）

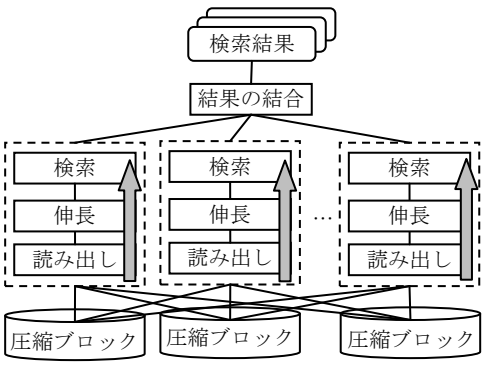

図 2-1 並列検索処理のデータの流れ

2.2. テキストストリームデータ

本稿では、ネットワーク上を流れる、サーバやネットワーク機器等のログ、Web コンテンツ、電子メール、センサデータなどのテキストデータをテキストストリームデータと呼ぶ。

それらは、以下の特徴を備えている。

- データの時系列的変化：データの形式や長さの傾向、発生頻度が必ずしも一定していない。
- 永続性：長時間・連続的にデータが発生する。
- 即時性：原則として即時的に処理することを要求される。また、処理の結果もストリームデータとなることもある。一方で、処理の遅延時間とのトレードオフで、厳密な処理結果が求められない場合もある。
- 順序依存性：処理の種類によっては、入力されたストリームデータと同じ順序で処理の結果を出力する必要がある。

本稿では、ストリームデータを順序・時間の情報を持ったレコードの列と見なす。例えば、ログの 1 件のイベントを 1 レコードとする。

3. テキストストリーム並列処理

3.1. 概要

異常の発生を即時に警告する等の目的のため、情報／物理セキュリティの分野を始めとして、ログデータの即時利用のニーズがある。そこで我々は、LDB を元に、多種多様なログデータの入力に対し、即時に並列に検索して、検索結果を出力するテキストストリーム並列処理基盤ソフトウェアを開発した。

3.2. 課題

ストリームデータの並列処理において、1 レコード単位でデータを各検索処理単位に振り分けた場合、処理単位が細分化され処理のスループットが向上しない課題がある。

3.3. 実現方式

上記の課題に対して、本方式では、データが入力されてから検索結果が出力されるまでに許容される遅延時間の範囲内で応答制約時間を設定する。入力されたデータは、その応答制約時間内で一度蓄積する。そして、蓄積したストリームデータをブロックとして、その時点で処理が割り当てられていない処理単位に転送する。各処理単位から出力された検索結果はレコードの入力順に結合して出力する。これにより、データの処理単位を大きくすることができ、処理のスループットを向上することができる。（図

Implementation of Parallel Processing Method of Text Stream Data.

†Takaaki Nakamura, Yoshinori Yamagishi, Mikihito Kanno Information Technology R&D Center, Mitsubishi Electric Corporation

5-1)

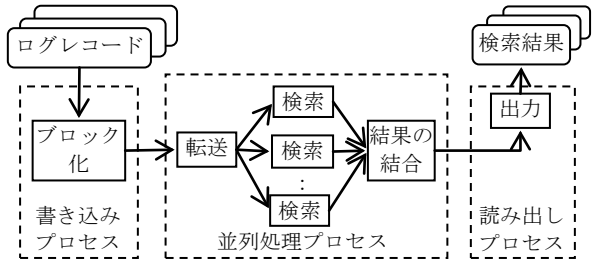

図 5-1　ストリーム並列処理のデータの流れ

4. 性能評価

4.1. 評価方針

様々な機器、ソフトウェアから生成されるログの内容を、正規表現キーワードによって検索し、条件にヒットしたログを出力する状況を想定して、下記の指標について性能評価を実施する（図 8-1）。

- スループット：テキストストリーム処理開始から終了まで（ストリーム処理時間）内に処理した単位時間あたりのデータ量。
- 平均遅延時間：1 レコードを処理系に入力してから出力を得るまでの平均時間

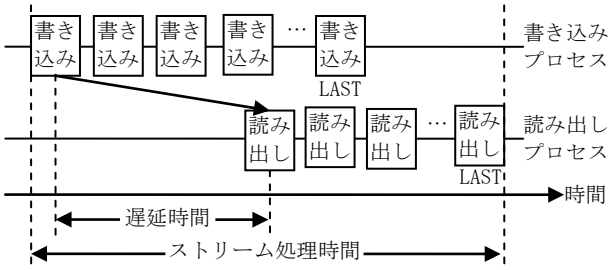

図 8-1　評価項目と測定方法

今回の評価では、データが一定のサイズ入力される毎にブロック化した。本方式では、ブロック化のタイミングを外部から明示的に指定することも可能である。

評価環境には表 4-1の PC サーバを使用した。

表 4-1　評価環境

OS	64bit Windows Server 2003 R2 Enterprise Edition
CPU	Xeon MP 3.0GHz×2（16 プロセッサ）FSB 800MHz
メモリ	16GB

評価には、物理セキュリティ装置が出力したログを想定したデータ「物理ログ」（平均レコード長 670 バイト）と、長大なテキストの入力を想定したデータ「10MB テキスト」（平均レコード長 9.8MB）を使用した。また、評価では、データ全件にヒットする検索条件を使用した。

5. 測定結果と考察

図 4-2にスループットの測定結果を示す。グラフ中の破線は、それぞれ原点と並列度 8 の点を結んだ線である。並列度 8 までは並列度に比例し、それ以降も並列度に従ってスループットが向上していることから、並列処理の効果を確認できた。

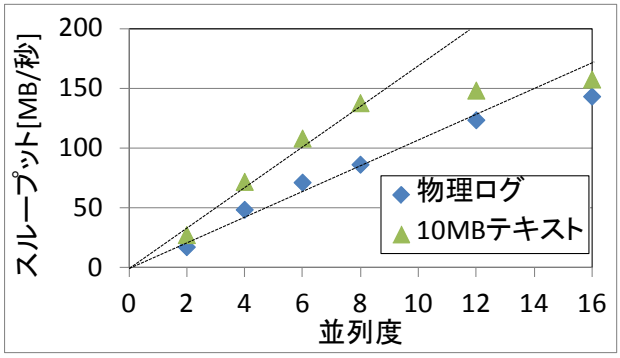

図 4-2　並列処理スループット

図 4-3に平均遅延時間の測定結果を示す。横軸は並列度の逆数とした。グラフ中の破線は、それぞれ原点と 0.5（並列度=2）の点を結んだ線である。平均遅延時間が並列度の逆数に概ね比例していることから、並列処理の効果を確認することができた。

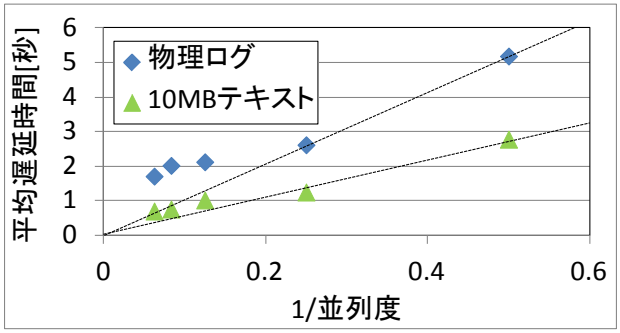

図 4-3　平均遅延時間

6. おわりに

SISA による追記型ログデータベースを元に、テキストストリーム並列処理機能を実装した。スループット、平均遅延時間に関して性能評価を実施し、本方式の有効性を確認した。

1. 参考文献

[1] 清水，他：スケーラブルインテリジェントストレージによる大規模並列全文検索の実現，第 64 回情報処理学会全国大会，4ZA-4，2002.
[2] 中村，他：大規模ログデータベースの実現，情報処理学会全国大会講演論文集 2006(3)，pp29-30，2006.
[3] 竹内，他：大規模ログデータベースの評価，情報処理学会全国大会講演論文集 2006(3)，pp27-28，2006.
[4] 中村，他：大規模正規表現の高速照合方式，情報処理学会全国大会講演論文集 2005(1)，pp235-236，2005.