1D-2

大規模ログデータベースの実現

中村　隆顕　　山岸　義徳　　竹内　丈志　　郡　光則
三菱電機株式会社　情報技術総合研究所

1. はじめに

近年、情報セキュリティ分野を中心に、問題発生時の証拠保全などを目的として、ログを保存・分析する動きが進んでいる。ログはその形式が多様で、レコード長も様々である。また、ログは 100 テラバイトも蓄積される事例もあり、効率的に管理する必要がある。しかし、従来の関係データベース管理システム（RDBMS）は、ログのような特徴を持つデータを、必ずしも効率的に管理することができなかった。

本稿では、多様で大規模なログを効率的に管理するログ専用データベース管理システム「ログ DB」を提案する。ログ DB を実装し、評価した結果は[1]で報告する。

2. ログ

2.1. ログの特徴

ログ DB で扱うログの例を表 1に示す。表 1に示す通り、ログ DB で扱うログはその種類も形式も多様である。RDBMS の 1 個のテーブルで管理されるデータは、すべて同一のデータ構造を持つ。そこで形式が異なるログは、形式ごとに異なるテーブルで管理する必要があり、管理の負担の増加を招く。

ログは、データ長も可変長で、1 レコードは数バイトのものからメガバイト級以上と長大なものまで幅広く存在する。一方、RDBMS は、可変長で長大なデータの処理に必ずしも適した構造をもっていない。

RDBMS では、レコード単位の更新や、挿入・削除があるが、ログは基本的に時系列に従って追加されるだけであり、これらの機能を必要としない。ログには 1 日当たり 1 テラバイト以上も出力されるものもあり、蓄積し続けると数ヶ月で 100 テラバイトに達する。このように、ログの量は膨大なものであるが、前後の時間的に近いログ同士には依存関係があることが多く、データの冗長性が高いという特徴がある。

表 1　ログの種類

ログ	説明
サーバ	アクセス、エラーなどの履歴。
ｾｷｭﾘﾃｨ	PC の操作履歴。建物等の入退出履歴。
メール	メール本文や添付ファイル。
ﾈｯﾄﾜｰｸ	ネットワーク上のパケットデータ。

2.2. ログ管理の課題

形式の異なるログを、1 個の RDBMS のテーブルで管理するためには、事前にログの形式を統一する必要があり、未知の形式のログには対応できないという問題がある。また、その変換処理のために蓄積時に追加の処理が必要になる、また、RDBMS では、ログの量が増加すると処理速度が低下するという課題がある[2]。ログを索引型の全文検索エンジンで管理する場合も、索引の生成が必要なため、実際にログが検索可能になるまでに時間がかかってしまう。このように、一般の RDBMS や索引型の全文検索エンジンは、ログの効率的な管理には適していない。

また、ログはある一定期間追加され続けるものであるため、時間の経過と共に蓄積に必要なディスクの量も増大するという問題がある。そのために、ログ DB には、不要になったログを別の長期保存媒体に保存したり、削除したりする世代管理機能も必要となる。

3. ログ DB

3.1. 多様なログへの対応

ログ DB のデータベースを LogSet と呼ぶこととする。1 個の LogSet で多様なログに対応するためには、蓄積時に特定のデータ構造を仮定して処理することはできない。そこでログ DB では、入力されたログを加工せず、完全に復元可能な形式でディスクに蓄積する。これにより、蓄積時にログの形式に関する情報が不要になるため、任意の形式のログを蓄積することができる。ログはレコード単位の更新や挿入・削除が無いため、時系列順に単純に追加するだけである。

ログ DB では 1 個の LogSet に蓄積されたログの形式を、検索時に判別する。ログ DB は正規表現を含む検索条件によって、ログに含まれる文字列を照合することにより、その条件に適合し

The Architecture of the Large Scale Log Database.
Takaaki Nakamura, Yoshinori Yamagishi, Takeshi Takeuchi, Mitsunori Kori
Information Technology R&D Center, Mitsubishi Electric Corporation

たログを読み出すことができる。この時、特定のログの構造を意識した検索条件を指定することによって、複数種類のログの中から、その構造を持ったログだけを判別して読み出すことができる。検索時には、正規表現による照合の他に、ログを蓄積した時間の情報などを条件にして、読み出すログを絞り込むことができる。

3.2. 高速蓄積・高速検索の実現

3.1に示したログ DB の構成では、検索時にログの形式を判別するため、特に検索処理の負荷が大きく、検索速度の低下が予想される。ログ DB は、SISA[3]のディスク I/O 技術・並列処理技術、sDFA[4]の文字列照合技術により、大規模なログの高速な蓄積と検索を実現している。

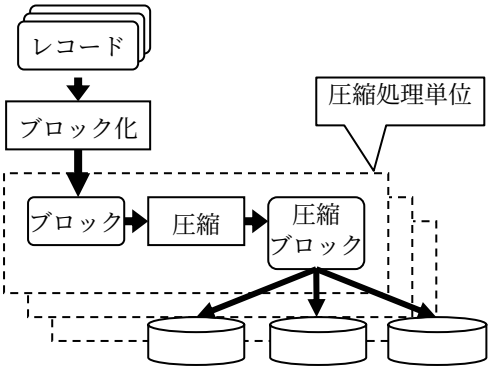

図 1　登録時データフロー

図 1はログ DB のデータフローである。ログ DB の書き込み時には、ログの複数のレコードからなる、あるまとまったサイズのブロックとする。次にそのブロック単位でログを圧縮し、圧縮ブロックの形式でディスクに格納する。

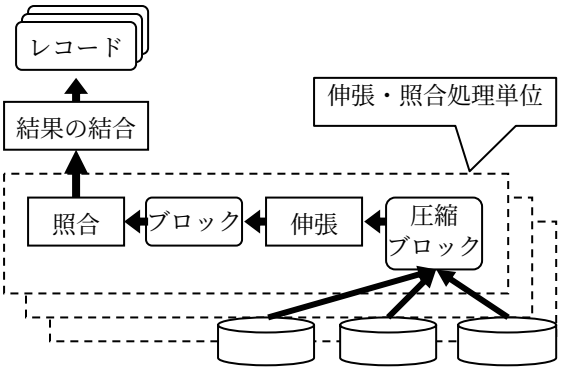

図 2　検索時データフロー

図 2はログ DB の検索時のデータフローである。検索時にも、ディスクに格納されている圧縮ブロックを最小単位として、格納された順番でディスクから読み出し、メモリ上に伸張して照合処理を実行する。

ログ DB は、サーバ上における複数のスレッドによる並列処理や、複数のサーバによる並列処理によりログの蓄積・検索を高速化する。ログの蓄積では、ブロックの圧縮から圧縮ブロックのディスクへの格納までを圧縮処理単位として並列に処理する（図 1）。ログの検索では、圧縮ブロックの読み出しからログの照合までを伸張・照合処理単位として並列に処理する（図 2）。処理の並列度を変更することにより、ログの寮の変化にも対応することが可能である。

また、ログの蓄積時に 1 つの LogSet を時系列に従って複数の領域に区切ることができる。検索時には、検索条件に対応する領域に限定して伸張・照合処理の対象とすることで、高速な検索が可能である。

3.3. ディスクの利用効率の向上

ログ DB では、ログを圧縮することにより、ログを蓄積するために必要なディスクの量を削減することができる。ログ DB では、その圧縮に LZ77 方式[5]に基づいた圧縮方式を利用している。LZ77 方式は、ログのようなデータに有効な方式であり、時間的に近いログを複数まとめて圧縮することにより、高い圧縮率を得ることができる。

また、ログ DB の区切られた領域を単位にして不要なログの削除や、バックアップ／リストアする、ログの世代管理が可能である。

4. まとめ

大規模かつ任意の形式のログを高速に蓄積・検索することが可能で、ディスクの利用効率も高いログ専用データベース管理システムを提案した。これにより、従来の RDBMS では困難であった、多様なログの効率的な管理を可能にした。

参考文献

[1] 竹内 他，大規模ログデータベースの評価，第 68 回情報処理学会全国大会，1D-1，2006.
[2] A. Sah, A New Architecture for Managing Enterprise Log Data. Proc. of LISA 2002, 121-132, 2002.
[3] 郡 他，検索機能を備えたストレージシステムによる大規模並列全文検索，信学技報，Vol.102, No.276, 41-46, 2002.
[4] 中村 他，大規模正規表現の高速照合方式，第 67 回情報処理学会全国大会 講演論文集 (3)235-236, 2005.
[5] J. Ziv 他，A Universal Algorithm for Sequential Data Compression, IEEE Trans. on Inform. Theory, IT-23(3)337-349, 1977.