ASN.1 データベースのための ASN.1 処理系の実装と評価

4M－7　小野 智弘　西山 智　堀内 浩規　小花 貞夫
国際電信電話株式会社

1. はじめに

OSI ディレクトリにおける DIB(Directory Information Base) や OSI 管理における MIB(Management Information Base) 等の OSI の応用では、抽象構文記法 1(ASN.1)[1][2]で定義されたデータ型を持つ情報 (以下、ASN.1 データと呼ぶ) をデータベースに格納する。これらのデータベースは運用中に動的に ASN.1 定義を追加、変更する必要があるものが多い。筆者らはこれを可能とする ASN.1 データベースを提案し、開発を行なっている[3][4]。本稿では、ASN.1 データベースにおいて ASN.1 定義を動的に変更可能とする ASN.1 処理系の実装と、その評価結果を述べる。

2. ASN.1 処理系の概要

筆者らの提案した ASN.1 データベース[3] (以下、ASN.1 データベースと呼ぶ) は、(1) 任意の ASN.1 定義をスキーマとして ASN.1 データを格納し、(2) データベース運用中に動的にスキーマの変更を可能とし、また、(3) 高速化のために、データを通信路上の転送構文と同じ符号化バイト列で格納するという特徴を持つ。図 1に示すように、ASN.1 データベースは、ASN.1 データの符号化／復号処理と ASN.1 定義の追加、変更を行なう「ASN.1 処理系」、ならびに、それを利用して DB の検索、更新処理を行なう「DB 処理系」から構成される。

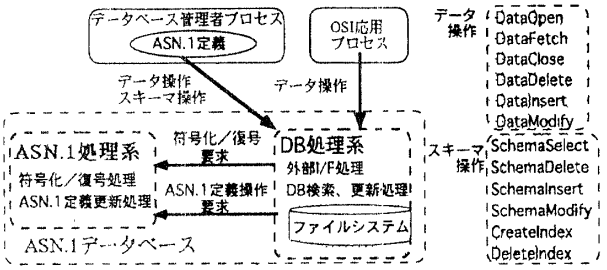

図 1: ASN.1 データベースの概念図

ASN.1 処理系では、以下の方式の採用により、符号化／復号処理の高速化を図っている[5]。

コンパイラとインタプリタの併用　ASN.1 定義を、データベース操作におけるプロトコルヘッダ等の運用中に動的に変更されない部分と、格納するデータ等の変更され得る部分に分けて定義した。前者はコンパイラの生成する符号化／復号関数を用い、後者はインタプリタが実行中に動的に符号化／復号する。

部分符号化／復号　符号化列中の、処理に使用する部分のみを部分的に復号し、また、一部に符号化列を含むデータを符号化する。

一意識別符号化　ASN.1 データベースでは、インデックスを利用して検索の高速化を図る際に、インデックス値と条件値とを符号化列で比較する。その際に、符号化列が一意に定まる DER[2]に変換する処理を行なう。

3. ASN.1 処理系の実装

3.1 ASN.1 処理系のソフトウエア構成

図 2に示すように、ASN.1 処理系をコンパイラ部とインタプリタ部から構成した。コンパイラ部はあらかじめ ASN.1 定義の静的定義部に対応する「符号化/復号関数」と、符号化／復号時に利用する「ASN.1 定義の内部表現」を生成する。インタプリタ部は「ASN.1 定義処理部」と「データ処理部」から構成されるライブラリで、1)DB 処理系からの ASN.1 定義操作要求に対して、ASN.1 定義処理部が構文解析を行ない、「ASN.1 定義の内部表現」に対して追加、変更を行う。また、2)DB 処理系からの符号化／復号要求に対して、データ処理部が「符号化/復号関数」と「ASN.1 定義の内部表現」を用いてデータを符号化/復号する。

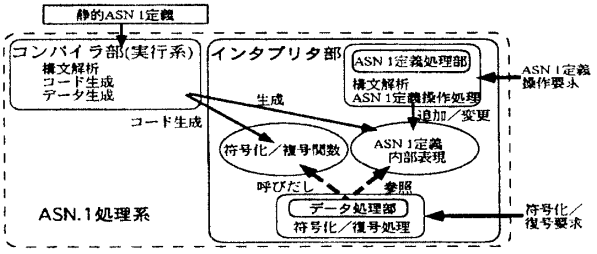

図 2: ASN.1 処理系のソフトウエア構成

また、符号化／復号関数として以下の関数を持つ。

符号化　(1) 一部に符号化列を含むデータの符号化、(2) データ全体の符号化、(3) BER 符号化列の DER 化

復号　(4) 符号化列の該当部分の切出し、(5) 符号化列の該当部分の復号、(6) 符号化列全体の復号、(7) 符号化列の構文検査

各関数の引数には、「符号化／復号対象の型」、「符号化／復号範囲」等を指定する。

3.2 ASN.1 処理系の利用

ASN.1 データベース内部における ASN.1 処理系の利用状況を、ここでは、DataOpen 操作 (条件に合致した

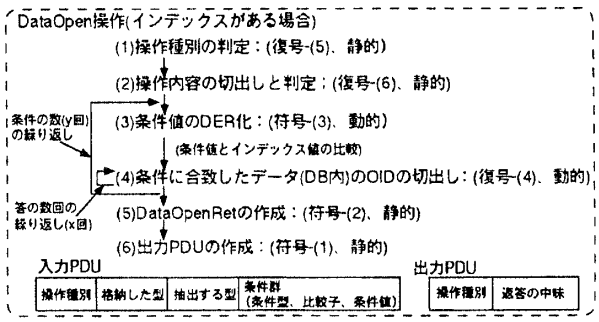

図 3: DataOpen 操作の流れ

Implementation and Evaluation of ASN.1 Translator for ASN.1 Database
Chihiro ONO, Satoshi NISHIYAMA, Hiroki HORIUCHI and Sadao OBANA, KDD

データの OID を取得する操作) を例として図 3に示す。符号化／復号関数の呼ばれる回数 (W) の合計は以下のようになる。

W = 4+(x+1)y　　..式 (1)(x、y は図 3 参照)

4. ASN.1 処理系の評価と考察

ASN.1 処理系の性能について、基本性能を 4.1 に示し、2 節で述べた方式の効果を 4.2〜4.3 に示し、データ操作における性能を 4.5 に示した。結果はそれぞれ 1000 回の平均を示す。

4.1 データ量とタグ数に応じた速度の変化

ASN.1 処理系の基本性能を調べるために、データ量 (0〜1Kbyte) と ASN.1 のタグの数 (20、40 個) をパラメータとして所要時間の変化を測定した (図 4)。所要時間 (Tmsec) は符号化／復号共に、データ量 (xKbyte) とタグ数 (y 個) に比例し、復号では、T = 0.5x + 0.055y + 0.01 と近似できる。例えば、タグが 40 個からなる 1KByte のデータの復号時間は、約 2.8msec となる。

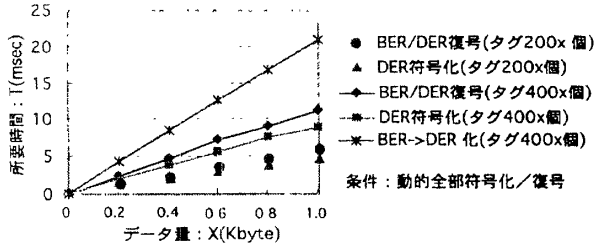

図 4: データ量とタグ数に応じた速度の変化

4.2 コンパイラとインタプリタの併用の効果

5 段の入れ子構造からなる 550byte のデータを用いて、全符号化列中の静的定義の割合 (静的符号化／復号率) に応じた所要時間の変化を測定した (図 5)。動的定義と静的定義の差が、符号化では 45 %、復号では 30 %であった。

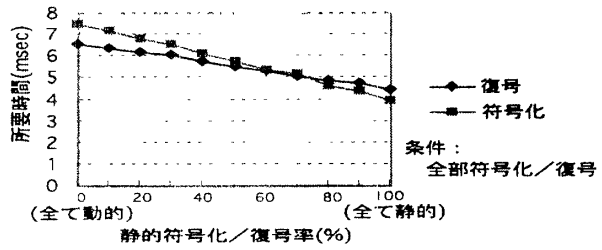

図 5: 静的定義の割合に応じた符号化 / 復号速度の変化

4.3 部分復号機能の効果

5 段の入れ子構造からなる 550byte のデータを用いて、全符号化列中の復号する割合 (部分復号率) に応じた所要時間の変化を測定した (図 6)。「部分復号指定」で全てを復号する場合は「全部復号指定」で復号した場合に比べて遅くなるが、部分復号率が約 95 %以下、つまり、ほとんどの場合に部分復号指定を用いた方が高速となる。

また、符号化列で格納しているデータから OID 等を必要に応じて切り出す場合等に使用する切出し処理は、切出し箇所の特定処理のみで済むため、図 6に示すように 1msec 以下で処理できる。

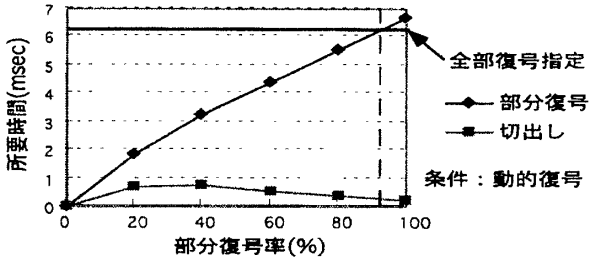

図 6: 全符号化列中の復号する割合に応じた速度の変化

4.4 DER 化の影響

DER 化処理では、符号化列を一旦復号してから再び DER 符号化をしているため、所要時間は同じデータ量のデータの符号化時間と復号時間を加算した時間を要する (図 4)。しかしながら、DER 化関数を使用する、DataInsert 操作のインデックス作成時のインデックス値、DataOpen、DataDelete、DataModify 各操作の条件比較時の条件値は、DER 関数を呼ぶ回数が少なく (3.2 節式 (1) では y 回)、さらに DER 化の対象 byte 数も短いため、インデックスの使用による効果に比べて、DER 化の処理時間は、ほぼ無視できる。

4.5 データ操作中の処理系の性能について

データ操作に対する性能として、DataOpen 操作を例にとり、2 節の方式を利用した場合と利用しない場合の所要時間を図 3、4、5、6を基に推定した。

DataOpen 操作では処理時間の大部分を切出し処理 (図 3(4)) に費やしており、この部分に「切出し関数」を利用した場合は 8msec、利用しない場合は 68.5msec (DB 内の 1 データが 1Kbyte の場合) と推定でき、60.5msec(88 %) の削減となる。また、図 3(1)(2)(5)(6) に静的符号化／復号を利用した場合は 7.46msec と推定でき、さらに 0.54msec(7 %) の削減となる。

また、4.2 節の結果より、格納するデータのうちで動的に定義が変更されない部分があれば、静的定義として扱うことで図 3(4) の部分の処理のさらなる高速化が可能となる。

5. おわりに

ASN.1 データベースにおいて ASN.1 定義を動的に変更可能とする ASN.1 処理系の実装と評価結果を述べた。ASN.1 処理系では、(1) コンパイラとインタプリタの併用、(2) 部分復号処理、(3) 一意識別符号化の各方式が高速化に有効である。最後に、日頃指導頂く KDD 研究所 村上所長に感謝致します。

参考文献

[1] "X680:Spec. of ASN.1",1992, ITU-T

[2] "X690:Spec. of Encoding Rules of ASN.1",1992,ITU-T

[3] 西山他,"ASN.1 データベースの実現方式に関する一考察", 第 49 回情処全大, 4W-11, 1994

[4] 西山他,"ASN.1 データベースのための高速な ASN.1 処理系の設計", 第 50 回情処全大, 2T-4, 1995

[5] 小野他,"ASN.1 データベースのための ASN.1 符号化／復号処理系の設計と実装",DPS 研究会資料 79-14, 1996