2005－DBS－137（II）（59）
2005／7／14

RDB 分散問合せ処理へのサイト間アクセス制御の導入

品川 徳秀 †‡　　北川 博之 ‡,*
siena@kde.cs.tsukuba.ac.jp　　kitagawa@cs.tsukuba.ac.jp

† 科学技術振興機構 戦略的創造研究推進事業
‡ 筑波大学大学院システム情報工学研究科　〒 305–8573 茨城県つくば市天王台 1–1–1
* 筑波大学計算科学研究センター　〒 305–8577 茨城県つくば市天王台 1–1–1

概要　古典的な分散問合せ処理計画の導出手法では、全てのサイトの立場が同等である事が仮定されている。しかし、現実的には個人情報や社外秘情報など機密性の高いデータが含まれている事が一般的であり、従来手法では問合せ処理に参加可能なサイトが強く限定されてしまうという問題がある。一般に、これらの機密データにはアクセス制御が施され、利用権限のない第三者への漏洩から保護されている。このようなデータの公開範囲が非対称な環境においては、従来手法では問合せ処理計画を導出する事ができない。このため、アクセス制御を考慮した分散問合せ処理計画の導出手法の確立が必要である。本稿では、System R* をベースとし、アクセス制御を尊重した計画導出手法を提案する。

キーワード: RDB, セキュリティ, アクセス制御, 分散問合せ

Introduction of Access Contorol into Distributed Query Processing

Norihide Shinagawa†‡　　Hiroyuki Kitagawa‡,*
siena@kde.cs.tsukuba.ac.jp　　siena@kde.cs.tsukuba.ac.jp

† Core Research for Evolutional Science and Technology,
Japan Science and Technology Agency
‡ Graduate School of Systems and Information Engineering, University of Tsukuba
1–1–1 Tennodai, Tsukuba, Ibaraki, 305–8573 Japan
* Center for Computational Sciences, University of Tsukuba
1–1–1 Tennodai, Tsukuba, Ibaraki, 305–8573 Japan

Abstract　Typical query plan derivation algorithms in distributed relational database systems suppose that all the sites can access resources without discrimination each other. In actual databases, they tend to include sensitive data such as personal privacy information and secret infomation of organizations. Such data are usually protected from unauthorized accesses by access contorol mechanisms. In this case, visibility of data across sites are asymmetric, and typical algorithms do not work. We need a new scheme to derive distributed query plans considering restriction given by access contorol policies. This paper proposes such a query plan derivation algorithm based on System R*'s one.

Keywords: RDB, Security, Access control, Distributed query processing

1　はじめに

RDB 分散問合せ処理の計画導出手法には、System R* [1] や Distributed INGRESS [2]、SDD-1 [3] 等を始めとした様々なアルゴリズムが知られている [4]。これらに基づく従来の分散問合せ計画導出アルゴリズムでは、問合せ処理に参加するサイトは互いに同等な立場に位置付けられている。即ち、同じリレーションのデータを全てのサイトが一様に取得可能となっている。しかし、現実的には、個人情報や社外秘情報など機密性の高いデータが含まれている事が一般的である。このため、サイトが対等である事を要求する従来手法では、問合せ処理に参加できるサイトが非常に限られてしまうという問題

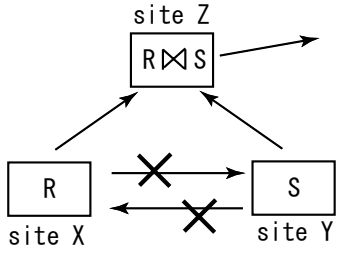

図 1: 第三者サイトでの結合処理

がある。

ビューによって機密性の高いデータを外部に漏らさないようにし、それらを参照する処理は情報源サイト内で行なうというアプローチも考えられるが、この場合には処理の多くが情報源サイトに集中してしまう。また、信頼関係にないサイト間では互いに結合属性を参照する事ができないが、両者と信頼関係にある第三者サイトではそれらを参照でき、結合処理をするといった処理方法の可能性も排除されてしまう (図 1)。

以上から、機密性の高いデータを含む RDB での分散問合せの計画導出は、従来手法では不十分であるといえる。

一般に、機密データの保護はアクセス制御機構によって行なわれる。データへのアクセス時に、ユーザの権限に応じてその可否が判定される。これにより、強い信頼関係にあるユーザへは許可された機密データを提供でき、信用できないユーザには限定されたデータのみを提供する事が可能である。

非分散環境においては、Oracle DBMS では、情報源サイトにおけるユーザの権限に基づいて自動的にアクセス制御を行ない、問合せを書き換える事で、アクセスが許可されないデータを除外した部分解を生成する問合せを実行する FGAC (fine-grained access control) 機構が提供されている [6]。また、Agrawal らの論文 [7] では、ユーザ権限に応じて動的に生成されるビューを通じて問合せを処理するという方法が述べられている。他の DBMS においても、類似した何らかのアクセス制御機構を持っている事がある。

一方、分散問合せにおいては、複数のサイトが問合せの中間処理に参加する。それらの中間処理サイトが持つ権限に応じて処理結果を最大化しつつ、全体としてアクセス制御に違反しないような計画を導出する事が望ましい。例えば、ユーザによる参照が許されていないデータを、もし許されていれば中間のサイトでは利用して問合せ処理を行ない、中間結果を移送する際にそのデータを除去するような計画である。このためには、情報源サイトで問合せユーザの権限に応じたアクセス制御を直接行なうよりも、図 1 に示したように中間サイトではそのサイトの権限で部分問合せを行ない、更に移送先に応じたアクセス制御を行なう必要がある。

アクセス制御機構を前提とすると、データの公開範囲が非対称になり、全てのサイトに同等の権限を仮定する従来手法では、問合せ処理計画を導出できない。本研究では、サイト間でのデータ移送にアクセス制御が行なわれる分散環境を想定し、そこにおける問合せ計画の導出を目的とする。あるサイトに異なる権限を持つ複数のアクターがいる場合については、単純化して異なるサイトとみなすものとする。導出される計画は、与えられたユーザ問合せに対して正しい結果を生成できるだけでなく、移送経路上で機密データの漏洩が起きないようなものでなければならない。

本稿では、S-J-R 形式 (Selection-Join-Projection form) の問合せに限定して、完全な結果を生成する問合せ計画の導出について考察する。現時点では、部分解を生成する問合せ計画の導出については言及しないものとする。提案アルゴリズムは、System R* の問合せ処理計画導出アルゴリズムと同様に、ボトムアップアプローチで計画を導出する。これにより、同等な部分問合せ計画の検討を削減し、組合せ爆発を抑制する事ができる。

以下では、2 節で System R/R* での問合せ処理計画導出アルゴリズムについて概略を述べる。3 節で、分散問合せにアクセス制御を導入する。4 節で、アクセス制御を考慮した分散問合せ処理計画導出ア

ルゴリズムを説明し、5 節に幾つかの例を示す。後に、7 節にまとめと今後の課題を述べる。

2 System R*

分散 DBMS である System R* では、System R [5] の問合せ処理計画導出アルゴリズムを分散問合せ処理に発展させたものを使用する。このアルゴリズムでは、線形結合木の問合せ処理計画のうち、コストが最小と見積もられるものをボトムアップに構築する。一般に問合せ処理の演算コストは結合処理に大きく影響されるため、結合順序を最適化する事でコストの少ない問合せ処理計画を導出する。また、線形結合木に限定するのは、検討される部分問合せの結合木の数が爆発するのを避けるためである。

トップダウンで問合せ計画を行なうアプローチでは、同一の部分問合せを処理する計画が重複して出現する。その組合せは爆発的に多くなるという問題がある。System R および System R* では、ボトムアップに問合せ計画を構築する事で、同一の部分問合せを検討する可能性を避けている。

System R* の問合せ計画導出アルゴリズムの概要を説明する。まず、単一のリレーションの最小コストのアクセス方法を決定する。これは、そのリレーションにローカルな選択演算の適用が含まれ、索引の利用などが検討される。

続いて、$k-1$ 個のリレーションを結合する部分問合せの処理計画を元に、これらを拡大して k 個のリレーションを結合する部分問合せの処理計画を構築していく。その際、結合属性がなく、直積を行なわなければならない組合せを除外する。これは明らかに高コストな問合せ処理計画を導出してしまうためである。結合処理は、各辺のデータを保持するいずれかのサイト、もしくはそれら以外の第三者サイトのどこで行なうかに応じて選択可能なアルゴリズムが検討される。

各計画のコストは、ディスク I/O コスト、結合アルゴリズムに応じた演算コスト、サイト間のデータ移送コストなどを因子としたコスト見積り関数で計測される。同一の部分問合せの複数の処理計画のうち、コスト最小のものが採用される。これによって、部分問合せ処理計画の重複を避け、組合せ数の爆発を抑えている。

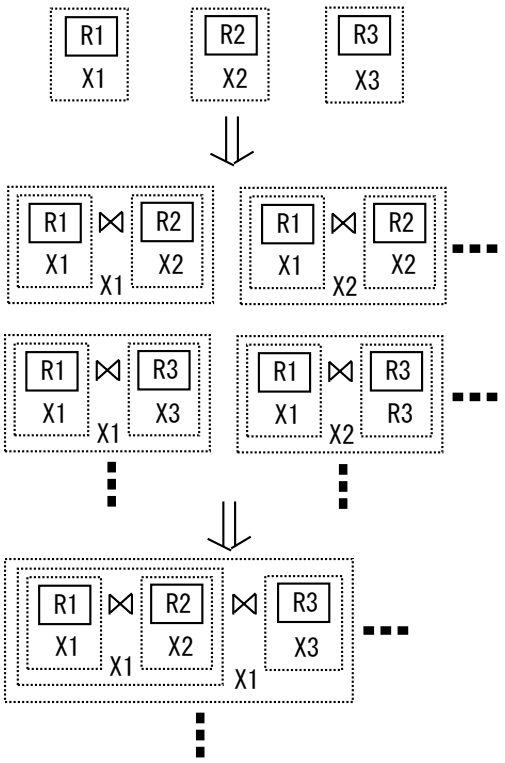

図 2: System R* での問合せ処理計画導出過程

これを、拡大していく事で与えられた問合せの最小コストの計画が導出される。得られた問合せ処理計画をサイト毎に分割し、各サイトに処理を指示する。

3 サイト間アクセス制御の導入

本稿では次の環境での分散問合せ処理を検討する。

ユーザサイト X_0 で与えられた問合せ Q 中において参照されるリレーション群を $R = \{R_i | i = 1, \cdots, n\}$、問合せの処理に参加可能なサイト群を $X = \{X_i | i = 1, \cdots, m\}$ とする。このうち、特に R_i を提供するサイトを $site(R_i)$ $(\in X)$ と表記す

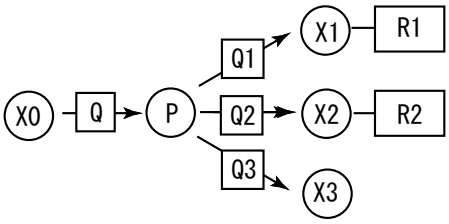

図 3: 問合せ処理実行方法

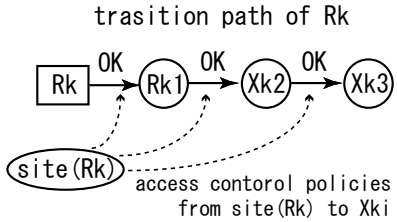

図 4: 安全な問合せ処理計画 (一部)

る。一般には、X にはデータベースを持たず、問合せ処理能力のみを提供するようなサイトも含まれうる。

これらに対して、サイト間のアクセス制御ポリシーを考える。アクセス制御の方式としては、行および列レベルでアクセスを制限する低水準アクセス制御を想定する [6], [7]。即ち、アクセス制御ポリシーは、選択および射影演算で表現可能な制限である。ここでは、セルレベルのアクセス制御は考慮しない。

ユーザ問合せは、**問合せ計画サイト** P に対して発行される。問合せ計画サイトでは、アクセス制御に違反しない問合せ処理計画の導出と、各サイトへの部分問合せ処理の指示を行なう。ここで、問合せ計画サイトは、各サイトと**信頼関係**にあり、次を満たすものとする。

- サイトが提供するリレーションとそのスキーマ、設定されているアクセス制御ポリシーを知る事ができる
- いずれのアクセス制御ポリシーにも違反しない問合せ処理計画を生成しなければならない

一般に、問合せ Q の処理過程で、参照される R_i 中のデータは複数のサイト X_{i_j} $(j = 1, \cdots, k_i)$ を経由して移送される。Q のある問合せ処理計画が**安全であるとは**、全ての R_i について、X_{i_j} での部分問合せ結果が $X_{i_{j+1}}$ へ移送される際に、$site(R_i)$ で設定された X_{i_j} に対するアクセス制御ポリシーに違反しない事と定義する。安全でない問合せ計画では、緩いアクセス制御が設定された第三者サイトを経由する事で制限されるべきデータが移送されてしまうため、問合せ計画の候補から除外されなければならない。このため、候補となりうる問合せ計画は、System R* のそれと比較して限定される。

4 問合せ計画導出アルゴリズム

問合せ計画は、問合せ計画サイトにおいて導出される。本稿では、与えられた問合せと等価な結果を生成する安全な問合せ処理計画の導出について検討を行なう。

本節では、一般的な導出アルゴリズムを説明する。ボトムアップに部分問合せ処理計画を構築する。その過程でアクセス制御ポリシーが与える制約を考慮し、これに違反する部分問合せ処理計画は候補から除外する事で、一般に解候補が削減される。この制約が非常にきつい場合、完全な解を生成できる問合せ計画を導出できない事があるが、その場合は解無しとしてアルゴリズムは停止する。

以下では説明のため、$[\ Q'\ ]^S_{X_i}$ という表記を使用する。これは、$R' \subset R$ 上の問合せ Q' の処理結果がサイト $X_i \in X$ に保持されており、それをいずれの $X_j \in S \subset X$ へも安全に移送可能である、即ち、全ての $R_k \in R'$ について $site(R_k)$ での X_j への移送に対して適用されるアクセス制御に違反しない問合せ処理計画である。

4.1 単一リレーションの局所アクセス

各 R_i について、$site(R_i)$ でローカルに処理可能な選択、射影演算を適用する部分問合せについて、最善なアクセス方法を決定する。これは、単一リレーションに対する通常の問合せ最適化によって計画される。

4.2 問合せ処理計画の拡大

リレーション数 l 個の全ての $R' \subset R$ に対する部分問合せの処理計画が既知である時、それらを拡大してリレーション数 $l+1$ 個の全ての $R'' \subset R$ に対する部分問合せの計画を導出する。これは、各 R' に対する全ての部分問合せ Q' とそれに含まれない任意のリレーション $R_j \in R - R'$ について、以下の手順で $Q' \bowtie R_j$ の問合せ計画を導出する事で行なわれる。

4.2.1 可能な結合候補の探索

R_j は単一リレーションであるから必ず X_j に保持されている。どのアクセス制御ポリシーにも違反しない安全な移送先を S_{R_j} とする。$S' = S \cap S_{R_j}$ と置くと、この結合は $X_k \in S'$ でのみ安全に行なえる。この事から、各 X_k について次の導出が行なわれる。

$$[\ Q'\ ]^{S}_{X_i} \bowtie [\ R_j\ ]^{S_{R_j}}_{X_j} \rightarrow \left[\ [\ Q'\ ]^{S}_{X_i} \bowtie [\ R_j\ ]^{S_{R_j}}_{X_j}\ \right]^{S'}_{X_k}$$

この時の結合アルゴリズムは System R* と同様、結合処理を行なうサイトに応じて選択され、コスト計算に反映される。

4.2.2 射影によるデータの極小化

更に、手順 4.2.1 で導出された全ての部分問合せ処理計画について、結合が行なわれた事で適用可能となる射影演算を行なう。これにより、残りの部分問合せの継続に不要な属性を早期に除去してデータの移送コストを削減すると共に、アクセス制御ポリシーに抵触せずに安全に移送可能なサイト群が $S'' \supset S'$ に拡大される。

$$\Pi[\ Q' \bowtie R_j\ ]^{S'}_{X_k} \rightarrow \left[\ \Pi[\ Q' \bowtie R_j\ ]^{S'}_{X_k}\ \right]^{S''}_{X_k}$$

4.2.3 コストに基づく候補の削減

次に、手順 4.2.2 で得られた部分問合せ処理計画のコストを見積もり、既知の同等な計画よりも低いコストである、もしくは同等な計画が存在しない場合には、これを新たな候補として採用し、以前の候補を除去する。同等な計画とは次を満たすものである。部分問合せ処理が行なわれる途中経路のサイトには依存せず、最終処理サイトでの状態のみで判定される。

- 論理的に同じ問合せである
- 最終処理サイトが同一である
- 安全な移送先が同一である

但し、同等でなくても、安全な移送先がより広く、コストが小さい場合には、その部分問合せ処理計画が新たな候補として採用される。

これを全ての X_k について繰り返し行なう事で、R'' に対する部分問合せの計画が導出される。

4.3 繰返し終了と問合せ処理の実行

手順 4.2 の部分問合せ処理計画の拡大を、与えられた問合せ Q を処理する問合せ処理計画になるまで繰り返す。但し、Q の問合せ処理計画の候補に対しては、ユーザサイト X_0 へも安全に移送可能である事を併せて確認しなければならない点に注意する。

問合せ計画サイト P は、図 3 に示した通り、得られた最小コストの問合せ計画を分割して、各サイト X_i に指示する。特に最終処理サイト X_j には、ユーザサイト X_0 への移送を併せて指示する[1]。

[1]直接の移送が許されない場合、P やその連携サイトなどのゲートウェイとなるサイトを経由する。

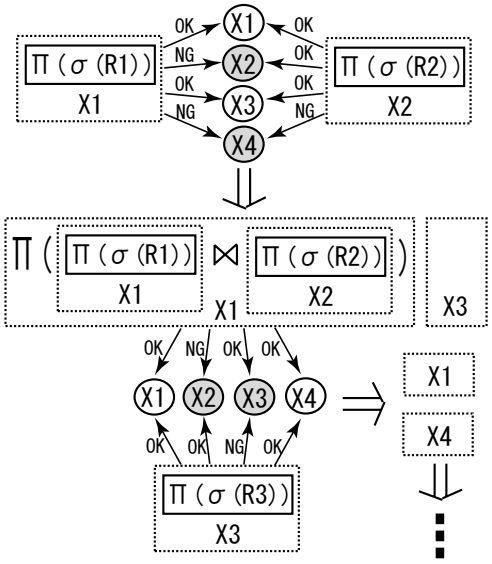

図 5: 問合せ計画候補の導出例

5 問合せ計画導出例

リレーション群 $R = \{R_1, R_2, R_3, R_4\}$ に対する S-J-P 形式の問合せ Q を考える。即ち、次の形式である。

$$Q = \Pi_1 \Pi_2 \cdots \Pi_p(\sigma_1(R_1) \bowtie \sigma_2(R_2) \bowtie \sigma_3(R_3) \bowtie \sigma_4(R_4))$$

また、問合せ処理に参加可能なサイトは $X = \{X_i = site(R_i) | i = 1, \cdots, 4\}$ のみとする。

4 節に示した提案アルゴリズムによる上記の問合せの処理計画導出過程を示すため、$k = 1, \cdots, 4$ 個のリレーション群に対する部分問合せ処理計画を導出する各ステップについて書き下す。特に例示した部分を図 5 に示す。

5.1 ステップ k=1

各 $R_i (i = 1, \cdots, 4)$ について処理を最大化し、サイト $site(R_i)$ にローカルな最小コストのアクセス方法を決定する。これは、選択演算 σ_i と明らかに不要な属性を除去する射影演算 Π'_i を適用するローカルな問合せ $Q(R_i) = \Pi'_i(\sigma_i(R_i))$ であり、その計画は $P_{X_i}(R_i) = [\ Q_i\ ]^{S_i}_{X_i}$ である。

5.2 ステップ k=2

全ての $Q(R_i)$ と、R_i 以外の全ての R_j の組合せの結合を検討する。例として、R_1 と R_2 の場合を示す。$k = 1$ の導出結果に基づき、$P_{X_1}(R_1) \bowtie P_{X_2}(R_2)$ を考えれば良い。ここでは、$S_1 = \{X_1, X_3\}$, $S_2 = \{X_1, X_2, X_3\}$ であったとすると、結合処理が可能なサイトは X_1 と X_3 であり、X_2, X_4 での結合処理は候補から除外できるため、得られる候補は、

$$P_{X_i}(R_1, R_2) = [\ P_{X_1}(R_1) \bowtie P_{X_2}(R_2)\ ]^{X_1, X_3}_{X_i}\ (i = 1, 3)$$

である。但し、それぞれのサイトでの最小コストとなる結合アルゴリズムが選択されるため、一般には結合の物理演算は互いに異なる。また、これらは最終処理サイトが異なっているため、同等な部分問合せとはみなされない。共に異なる部分問合せ処理計画として採用される。

更に、この結合に必要だった属性のうち、以降の問合せ処理に不要なものを除去する。X_1 における属性の除去により、X_4 への移送も安全になるとすると、最終的に導出される計画は

$$P'_{X_1}(R_1, R_2) = [\ \Pi(P_{X_1}(R_1, R_2))\ ]^{X_1, X_3, X_4}_{X_1}$$

$$= \Big[\ \Pi([\ P_{X_1}(R_1) \bowtie P_{X_2}(R_2)\ ]^{X_1, X_3}_{X_i})\ \Big]^{X_1, X_3, X_4}_{X_1}$$

である。

他の組合せの結合についても、それぞれのアクセス制御ポリシーの下で同様に導出される。

5.3 ステップ k=3

$k = 2$ の部分問合せ処理計画の全てについて、未結合のリレーション R_i の結合が検討される。前ステップと同様に導出が行なわれる。

R_1, R_2, R_3 の組合せの結合を例とする。このステップでは、全ステップで導出された部分問合せ処理計画に基づいて、次の 3 通りの順序の結合が検討される。

- $P'_{X_i}(R_1, R_2) \bowtie P_{X_3}(R_3)$
  (前ステップより $i = 1, 3$)

- $P'_{X_i}(R_1, R_3) \bowtie P_{X_2}(R_2)$
  (X_i は R_1 と R_3 の結合可能な任意のサイト)

- $P'_{X_i}(R_2, R_3) \bowtie P_{X_1}(R_1)$
  (X_i は R_2 と R_3 の結合可能な任意のサイト)

それぞれについて異なるサイトで処理を行なう複数の候補が導出される。例えば、始めの $P'_{X_i}(R_1, R_2) \bowtie P_{X_3}(R_3)$ について、$i = 1$ の場合は左辺が X_1, X_3, X_4 へ安全に送出可能である。仮に右辺が X_1, X_2, X_4 へ安全に送出可能であるとすると、この結合は $X_1, {}_4$ のいずれかで処理可能であり、これらの各サイトで結合を行なう部分問合せ処理計画がそれぞれ候補となる。

上記は全て、論理的には同じ問合せである。ステップ 4.2.3 に言及したように、得られた候補群に同等なものが複数存在する場合、コストが最小のものが部分計画として採用される。また、同等でなくても最終処理サイトが同一であれば、安全な移送先が広く、コストが低いものが採用される。

5.4 ステップ k=4

更に、$k = 3$ の部分問合せ処理計画を核として、同様に拡大を行なう。これで導出される計画が与えられた問合せの計画の候補となる。

ここで、最終処理サイトがユーザサイト X_0 でないものについては更に X_0 へ移送する必要がある。ここでは $X = \{site(R_i)|i = 1, \cdots, 4\}$ としたから、全ての候補について X_0 に安全に移送可能であるかが確認される。X_0 に移送可能である計画のみを候補とし、見積もられたコストに X_0 への移送コストを合わせて、コスト比較を行なう。これらのうち、最小コストの候補が、最終的な問合せ処理計画として採用される。

6 考察

提案アルゴリズムは、既に述べたように System R* と同様の手順で問合せ処理計画を導出する。本質的な差異は、導出過程においてアクセス制御ポリシーによる制約を考慮している事である。

このため、解の探索空間の大きさは System R* のそれと同じである。結合の組合せ数は、全空間では $O(n!)$ であるが、導出過程で直積を避ける事、論理的に同じ問合せ処理計画が複数ある時に最小コストのものだけを候補として採用する事により、実質的には $O(2^n)$ で抑えられる [4]。更に、各結合木について結合処理サイトを割り当てる事から、これを考慮に入れた探索空間の大きさは $O(2^n \cdot m^n)$ である。

提案手法では、論理的に同じ問合せである問合せ処理計画でも、アクセス制御ポリシーによる制約に起因して同等とみなせない場合がある。これは、中間的に導出される部分問合せ計画の数が増加する事を意味する。一方で、アクセス制御ポリシーに違反するデータの移送は導出過程で除去される。これは、中間的に導出される部分問合せ計画の数を削減する事を意味する。この増減は、設定されたアクセス制御ポリシーに依存して決まるため、一概にはどの程度の影響を持つのかはケースバイケースである。様々なパターンについてシミュレーションを行なう事で、その性質を明らかにして行く必要がある。

また、提案手法では、部分問合せの処理計画の候補を検討する際、データ移送を安全に行なえるサイトを判定するなどのコストがあるため、System R* のアルゴリズムと比べると一つの候補を検討するために若干多くの処理時間を要する。

7 まとめ

古典的な分散問合せ処理計画導出手法では、全てのサイト間で権限が対等である事が前提となっている。しかし、現実的には、機密データを保護するためにはアクセス制御が施されており、このような環境では従来手法では計画を導出する事ができない。本研究では、サイト間のデータ移送に関してアクセス制御が施されている環境での安全かつ低コストな分散問合せ処理を実現する事にある。特に本稿では、完全な問合せ結果を生成する問合せ処理計画を導出する手法を提案した。今後、計画導出アルゴリ

ズムの改善や、部分解を生成するような問合せ処理計画の導出手法の検討、実験を通じた特性評価などを行なって行く予定である。

[謝辞]

本研究の一部は、CREST「自律連合型基盤システムの構築」、科学研究費補助金特定領域研究 (2)(#16016205)、基盤研究 (B)(#15300027) による。

参考文献

[1] P. G. Selinger, M. E. Adiba, Access Path Selection in Distributed Database Management Systems, Proc. 1st International Conference on Data Bases, pp. 204-215, Aberdeen, Scotland, 1980.

[2] R. Epstein, M. Stonebraker, E. Wong, Distributed Query Processing in a Relational Data Base System, Proc. 1978 ACM SIGMOD International Conference, pp. 169–180, Austin, Texas, May, 1978.

[3] P. A. Bernstein, N. Goodman, E. Wong , C. L. Reeve, J. B. Rothnie, Jr., Query Processing in a System for Distributed Databases (SDD-1), ACM TODS, Vol. 6, No. 4, pp. 602–625, Dec. 1981

[4] M. T. Özsu, P. Balduriez, Principles of Distributed Database Systems Second Edition, Prentice Hall, ISBN 0-13-659707-6, 1999.

[5] P. G. Selinger, M. M. Astrahan, D. D. Chamberlin, R. A. Lorie, T. G. Price, Access Path Selection in a Relational Database Management System, Proc. 1979 ACM SIGMOD International Conference, pp. 23–34, Boston, Massachusetts, May, 1979.

[6] T. Kyte, Fine-grained Access Control, Technical Report, Oracle, 1999.

[7] R. Agrawal, P. Bird, T. Grandison, J. Kiernan, S. Logan, W. Rjaibi. Extending Relational Database Systems to Automatically Enforce Privacy Policies, Proc. 21st International Conference on Data Engineering (ICDE 2005), pp. 1013–1022, Tokyo, Japan, Apr, 2005.