6W-8

MO-SRV における Grid 計算サービスのための分散認証機構に関する考察

甲斐啓文† 伊東栄典†† 大庭淳一†† 青柳睦††
† 九州大学大学院システム情報科学府 †† 九州大学情報基盤センター

1 はじめに

遠隔地に分散した計算資源を、シームレスに利用するグリッド計算 (Grid computing) グの研究が進んでいる [1, 2, 4]。

グリッド環境においてセキュリティを考える場合、グリッドの特殊性、すなわち計算はネットワーク上の複数の組織から提供される複数の資源にまたがって行われ、その構成は動的に変化するという特徴を考慮する必要がある。そのため、グリッド環境では、1. データの盗聴・改ざん・サーバへのアタック等への対処、2. 各組織のセキュリティポリシを変更しないこと、3. シングル・サインオン機能の実現などが考えられる。本論文では、これらの機能を実現する認証機構に関する考察を行う。ただしこの認証機構は、我々が開発しているグリッド計算サービス「MO-SRV」に特化し、特に上記の 2. を意識したものである。

2 MO-SRV

MO-SRV とは、著者の一人である青柳、大庭らにより開発された、分子軌道計算のためのグリッド計算サービスを行なうサーバソフトウェアである。現在、九州大学情報基盤センターでは、ジョブ投入が可能な MO-SRV を公開している [3]。MO-SRV の機能を以下に示す。

1. MO Calcuation
   非経験的（第一原理）電子状態計算を行う。Gaussian,HONDO,PSCF の計算が可能。
2. Visualization
   計算結果を可視化する。
3. Search MO Database
   過去に共同研究者が実行したジョブの計算結果を格納する簡易データベース。計算結果及び計算入力データの検索・再利用が可能。

MO-SRV では、キューイングシステムを用いて計算をバッチ実行することができる。また、Globus Toolkit[1] を使って他計算機に計算ジョブを投入することも可能である。

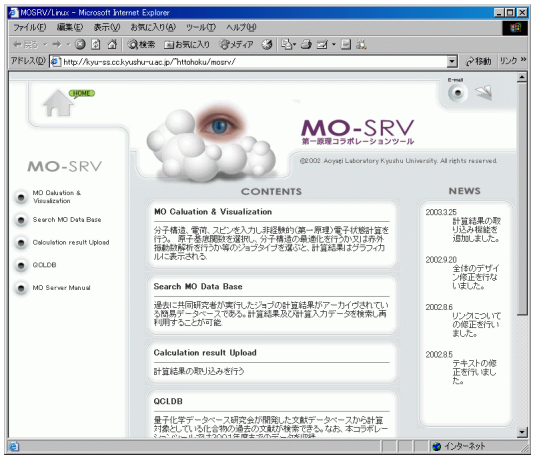

図 1: MO-SRV

3 分散認証機構

MO-SRV で多数のジョブを処理する場合、ジョブを複数の計算機に分散させることが考えられるが、この場合のクライアント・サーバの認証・認可をどう行うかが問題になる。

3.1 GSI

現在広く使われているグリッド計算ミドルウェアとして Globus Toolkit がある [1, 4]。Globus Toolkit では、PKI[5] に基づいた Grid Security Infrastructure(GSI) と呼ばれるセキュリティ機能によって、グリッド環境における認証・認可を実現している。GSI では、認証に認証局 (CA) から発行される X.509 証明書を用いる。

一方、認可は Globus Toolkit サーバ上の grid-mapfile というマッピングファイルによって実現されている。grid-mapfile は、各サーバマシン上でそれぞれ独立に管理されたテキストファイルで、クライアントから送られてきたユーザー証明書の subject (=DN; Distinguished Name) と、サーバマシン上のローカルユーザーとを関連付

A Study of distributed authentification mechanism for MO-SRV grid computing sytem

ける。これによってクライアントから依頼されたジョブはユーザー証明書の DN に応じたユーザー権限で実行される。

しかしながら、grid-mapfile のようなローカルファイルによる認可の仕組みは、グリッド環境を構成する計算機数が多くなるにつれ問題が起こる。grid-mapfile は各計算機で独立に管理されているため、計算機数が多くなると管理に大きなコストがかかることになる。

4 分散認証機構の提案

Globus Toolkit の GSI の機能を拡張して、ユーザー証明書の DN とローカルユーザーとのマッピング情報を一元管理することを考える。以下で複数の組織に跨った認可の管理ついてその実装方法を述べる。

4.1 複数の組織に跨る認可の管理

異なる組織間で認可機構を一元化するためには、組織を跨る認証が可能であることが前提となる。これは、組織間での CA の一元化、または複数の CA 間で連携により実現される。このような前提の下では、複数の組織に属するユーザー間で DN が重複しない。次に、組織内の計算機のマッピング情報を一元的に管理するマッピングサーバを用意する。マッピングサーバを利用することで、grid-mapfile のような認可のためのローカルファイルを利用せずに済む。

例として異なる組織 A,B における認可の一元管理機構について考察する。概念図 2 に示す。

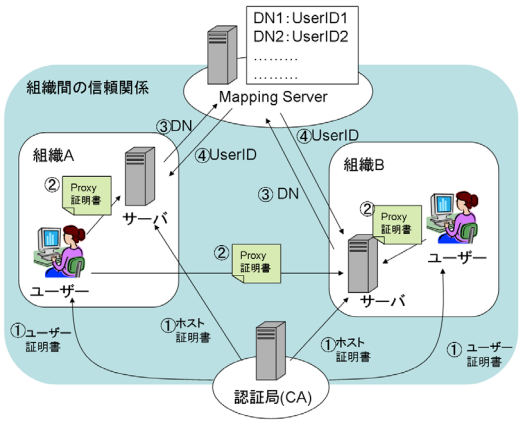

図 2: 組織 A,B における認可の一元管理

図 2 では CA を共有することで、組織 A,B に属するユーザー間で DN の重複が起こらない。つまり、組織 A,B 内では、すべてのユーザーが固有の DN を持つことになり、マッピングサーバによるマッピング情報の一元管理が可能になる。

新規にユーザーを追加する手順は次のようになる。ユーザーはまず、CA からユーザー証明書の発行を受けると、証明書の DN を提示することで、マッピングサーバの管理者にマッピングサーバへの登録を依頼する。マッピングサーバの管理者は、マッピングサーバに新規エントリとして、DN とローカルユーザーとのマッピング情報を追加する。それと平行して、組織内の計算機の管理者に新規にユーザーを追加してもらう。ただしこの機構においては、ある DN には 1 つのローカルユーザーが対応しているだけなので、ユーザーが複数の計算機を利用したい場合、それらの計算機にはすべて同じローカルユーザーが追加されなくてはならない。

次に実際の認証・認可の流れを示す。ユーザーはユーザー証明書からプロキシ証明書を生成し、それを利用したいサーバに送る。サーバ側では、認証の処理とともにプロキシ証明書からユーザーの DN を読み込み、DN をマッピングサーバに送ることで DN に対応するローカルユーザーアカウントを得る。これによって、クライアントから依頼されたジョブをサーバのユーザー権限で実行することが可能になる。

5 おわりに

本稿では、MO-SRV におけるグリッド計算サービスのための分散認証機構に関して考察を行った。今後は、本稿で提案した認証機構を実際の MO-SRV に実装していく予定である。

参考文献

[1] “the globus alliance”, http://www.globus.org/.

[2] “NAREGI:National Research Grid Initiative”, http://www.naregi.org/.

[3] “MO-SRV”: http://kyu-ss.cc.kyushu-u.ac.jp/~httohoku/mosrv/

[4] 日本アイ・ビー・エムシステム・エンジニアリング株式会社：“グリッド・コンピューティングとは何か”, ソフトバンクパブリッシング, 2004.

[5] Andrew Nash, William Duane, Celia Joseph, Derek Brink 著, RSA セキュリティ株式会社監修 : “e セキュリティの実装と管理 PKI”, 翔泳社, 2004.