グリッドコンピューティングのセキュリティ機構とその改良の試み

余　小溪　(指導教員：金子　晃)

1　はじめに

グリッドコンピューティング (Grid Computing) とはネットワーク上の機器，情報を結合することによって，仮想的な計算機環境をネットワーク上に構成することである．この技術は分散計算，可視化，ディレクトリサービス，認証など実証計算機科学における近年の技術革新の集大成であるともいえる．応用分野として，高エネルギー研究，宇宙科学研究，デバイス技術，バイオテクノロジー研究，ナノテクノロジー研究などが考えられる．これらの研究を行う研究部門に対するこれまでのサイバー・アタックが顕著であったことから，グリッド技術がこれらの研究部門で広く用いられることになったとき，グリッドの個々の基盤技術を精密に分析し，研究基盤を成すグリッドへのサイバー・アタックが最も効率的な攻撃手段となりうることが予想される．従って，セキュリティはグリッドデザインにとって基本となるであろう．

GloBus Toolkit はグリッドソフトウェアの開発を進める団体である GloBus によって開発された，グリッドコンピューティングを構成するためのミドルウェアであり，事実上の標準になりつつある．GloBus Toolkit はグリッドコンピューティング間で行われる通信のための認証，承認と機密性のメカニズムを提供する．セキュリティ機能がなければ，グリッド間で行われているデータ通信の完全性と信頼性は危険に陥る恐れがあるので，適切にグリッド環境を安全にするため，さまざまの有効なツールとテクノロジーを用いることが必要となる．

本研究では，GloBus が配布した最新版ソフトウェア GloBus Toolkit 4.0 の GSI(グリッドセキュリティ基盤) によって提供されたテクノロジーとさまざまなコンポーネントを調べてみた．そして，その利点と欠点について考察し，改良を図る．

2　GSI(グリッドセキュリティ基盤)

2.1　GSI の基本機能

GloBus の GSI(グリッドセキュリティ基盤) と PKI(公開鍵基盤) はテクニカル・フレームワーク (プロトコル，サービス，標準を含む) を提供し，グリッドコンピューティングの五つのセキュリティ機能をサポートする:

1. **ユーザ認証** ユーザの正当性を検証する．
2. **データの機密性** 秘密情報を第三者に漏らさない．
3. **データの完全性** 不正な手段によってデータは改竄また破壊されていないことを保証する．
4. **否認防止** 事後に送信事実 (受信事実) を否認することを防ぐ．
5. **鍵管理** 暗号に使われる鍵を安全に生成，配布，認証及び管理する．

2.2　電子証明書と認証局

Globus のセキュリティアーキテクチャの大部分は X.509 の電子証明書 (Digital certificates) に基づくセキュリティアーキテクチャから派生したものである．Globus では X.509 の電子証明書を用いたホストの認証とユーザの認証を行っている．それぞれの計算機に対して DN(Distinguished Name) と呼ばれる識別子を付与し，それぞれの DN に対して電子証明書を発行する．電子証明書は利用者の計算機において一旦生成され，これを CA(認証局，Certificate Authority) において CA の秘密鍵で署名することによって正式なものとなる．CA は秘密鍵と公開鍵の組をもっており，CA ユーザの公開鍵をふくむ情報を CA の電子証明書として広く全てのホストから参照可能とすることで，どのホストにおいてもユーザの認証が可能となる．ユーザからアクセス権限を求められたときに，ホストは自らが持つ CA の公開鍵を用いてユーザの電子証明書を確認することができる．GloBus Toolkit 4.0 には simpleCA が含まれており，CA の機能と，公開鍵の証明書に対しての承認と廃棄，CA にユーザの情報を転送するという RA(Registrant Authority) の機能を両方とも持っている．

DN はグローバルに一意な識別子であるので，これに付帯する電子証明書を用いることでグローバルなユーザやホストの認証を行うことができる．DN は実際にユーザプログラムを実行するうえで個々の計算機のユーザ ID にマッピングされるため，GloBus Toolkit では個々のユーザの DN からユーザ ID への変換情報を一つのファイルに納める方式をとっている．変換情報を納めたファイルは grid-mapfile と名付けられ，これにシステム管理者が利用権限ごとに許可するユーザを書き込むことで個々のホストにおけるアクセス制限が実現される．

GloBus Toolkit 4.0 の実装では公開鍵を使い，グリッド間のファイル転送を暗号化し，同じ鍵を使って OpenSSL セションの ID を復号することによってデータ通信の内容の機密保持を実現する．CA の証明書の署名によって，ノード間のメッセージ交換におけるなりすまし攻撃を防ぐことができる．

2.3　グリッドへのアクセス

2.3.1　GSI の構築

GSI コンポーネントを用いてグリッド環境を構築するため，まず，公開鍵暗号のためのキーセットを生成する． 次，CA から自分の証明書と CA の公開鍵のコピーを要求する．以下の手続きと図 1 は GSI 通信を構築するためのステップを説明する．

1. グリッドホストは GSI をセットアップした認証局の公開鍵をコピーする．
2. 自分の秘密鍵と自分の証明書の署名要求を生成する．
3. 安全な方法で CA に自分の証明書の署名要求を送る．
4. CA はその証明書に署名しグリッドホストに送り返す．

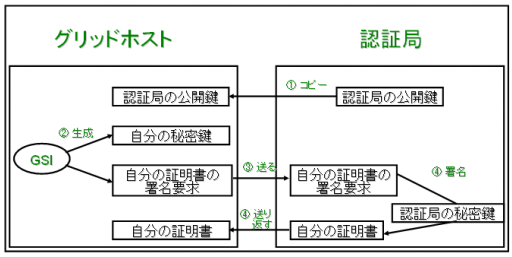

図 1: GSI の準備手続き

グリッドホストは署名したデジタル証明書を受領した後，CA の公開鍵，グリッドホストの秘密鍵，グリッドホストのデジタル証明書という 3 つの重要なファイルが必ず生成する．

2.3.2 GSI の認証と承認

グリッド間通信するとき，またはデータが本当の通信相手から来たかを確認したいとき，GSI の認証 (Authentication) 機能を用いる．図 2 のように，リモートグリッドを認証した後，リモートリソースへのアクセスを自分の代わりに行う権限を与える．この場合は，GSI の承認 (Authorization) 機能を使える．

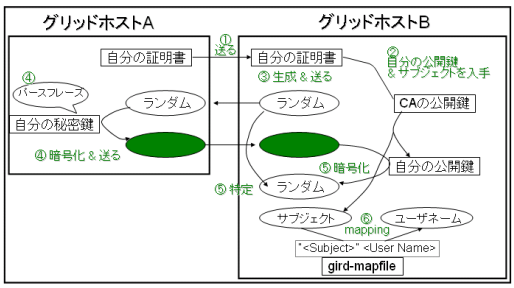

図 2: 認証の手続き

図 2 の 1〜5 は認証のための手続きであり，最後の 6 は承認のための手続きである．

2.3.3 GSI の委譲機能

セキュリティポリシーに従って，リモートグリッドマシンに仕事を配り，リモートグリッドマシンに子仕事を更に他のマシンに配らせるとき，GSI の委譲 (Delegation) 機能を使う．

自分がホスト A 側にいるとする．ホスト B 側で自分のプロキシを生成し，自分の承認を委譲する．このプロキシは自分のように働き，自分の代わりにホスト C にリクェストを提出する．プロキシを生成するため，ホスト A とホスト B の間に信頼できる通信がすでに構築されたことは前提とする．委譲リクェストを貰ったホスト B はプロキシ証明書を作成し，ホスト A に送る．ホスト A は自分の秘密鍵を使いプロキシ証明書に署名し，ホスト B にプロキシ証明書を送り返す．そして，ホスト A は自分の証明書もホスト B に送る．

ホストがリモートマシンにプロキシを作成するとき，プロキシの秘密鍵がリモートマシンにあるため，リモートマシンのスーパユーザはこのホストのプロキシの秘密鍵にアクセスことができ，このホストの名義でいろいろなことができるので，この委譲された信任状は攻撃に対して脆弱性がを持っている．これによるなりすましを防ぐため，プロキシの所有者がプロキシに制限ポリシーを課すことが推奨される．例えば，GloBus Toolkit のセキュリティ基盤のピラミッドの一つの GRAM(Grid Resource Allocation Manager) を用いる．

2.4 グリッドセキュリティ通信

GloBus Toolkit の基礎通信は電子証明書の相互認証と SSL/TLS(Secure Socket Layer/Transport Layer Security) に基づいている．

相互認証 グリッドの中で安全な通信を行えるように，OpenSSL パッケージは GloBus Toolkit の一部として実装されている．OpenSSL はグリッドクライアントとサーバの間に SSL/TSL を用いて暗号化されたトンネルを生成する．そして，鍵倉庫の代わりに，各グリッドリソースは電子証明書に基づいて互いに認証する．

SSL ハンドシェーク このハンドシェークは SSL セッティングの決定，公開鍵の交換，相互認証プロセスの基礎の交換に責任を持っている．

3 グリッド基盤のセキュリティ

様々な GSI ーネントと技術に加えて，グリッドを安全にするため他の基盤セキュリティコンポーネントがまだ存在する．

物理的なセキュリティ サーバが誰でも入れる部屋に設置されたら，どんな安全なアプリケーションがデザインされたり，複雑な暗号アルゴリズムが用いられたりしたとしても，サーバサービスは簡単に侵入されることができる．

オペレーティングシステムのセキュリティ サーバから必要がないプロセス，ユーザ，グループなどを除くなどの方法による．

グリッドとファイアウォール ファイアウォールによってコンピュータへのアクセスを制限．

侵入検知システム (Intrusion Detection System) グリッドコンピュータを更に安全にするため，IDS に投資することは賢明である．このシステムは暗号化されてない通信の分析に最適である．

4 潜在的なセキュリティリスク

公開鍵基盤の脆弱性

- なりすまし: 本人を装って証明書を入手.
- 秘密鍵の盗み: 有効な証明書を使った秘密鍵の無許可使用.
- ルート CA の秘密鍵の危殆化: CA の鍵を使って偽造証明書に署名させる，または秘密鍵を破る.
- 自動信用決定: 自動化された信用決定は自動詐欺にもなる.

グリッドサーバの脆弱性

グリッドに参加している全てのサーバやワークステーションは内部や外部のハッカーに対して潜在的な脆弱性を持っていることを常に考えなければならない．

5 まとめと今後の課題

GloBus Toolkit を実装し，セキュリティの評価をした．今後は，セキュリティ部分の改良を試み，特に，秘密分散計算の効率的な実装と融合させたい．

参考文献

[1] Introduction to Grid Computing with GloBus, Luis Ferreira et al., ibm.com/redbooks.

[2] 溝口文英雄，” グリッドコンピューティング”