# 事後評価報告書

１．研究課題名：日米サイエンスグリッドにおけるセキュリティ基盤の構築

２．研究代表者名：

２－１．日本側研究代表者：

田中良夫（(独）産業技術総合研究所グリッド研究センター主幹研究員）

２－２．米国側研究代表者：

Marty Humphrey（バージニア州立大学工学・応用科学校コンピューター科学部准教授）

総合評価：　良

３．研究交流実施内容及び成果：

本研究交流においては、複数の組織により構成されるグリッドのセキュリティ基盤の実現に必要な（１）複数の管理ドメインにより構成される仮想組織において適切にかつ容易にエンドエンティティの識別および認証を行なう PKI アーキテクチャの設計および評価、（２）複数の組織が相互に信頼できるセキュリティ基盤を実現するためにセキュリティポリシの整合性の確保、について研究活動を行なった。

（１）にあげた「PKI アーキテクチャの設計および評価」については、日米双方が協力して日米間でグリッドテストベッドを構築し、日本側が複数の管理ドメインにまたがる PKI アーキテクチャの実験・評価を行いながら研究を進め、新たな PKI アーキテクチャの開発を行った。日米グリッドテストベッド上に、複数の認証局が発行するユーザ証明書およびサーバ証明書を相互に信頼する仕組みを実現し、さまざまな点において検証および評価を行なった。評価結果に基づき、ユーザがグリッドを容易に利用する認証基盤を構築するために、(1)ユーザ各個人がそれぞれ認証局となり、自分が信頼する人間との間でクロス認証を行なうことにより信頼関係を構築し、ピアツーピア技術を用いて信頼関係を広げていく、(2)直接の信頼関係にあるユーザ同士のみがお互いの個人情報を知りえるが、通信時においてはすべてのユーザ間で匿名性を保つ（個人情報を保護する)、という 2 つの特徴を持つ新たな発想に基づく PKI システム（AUBReX: Authentication method Using Buddy-buddy relationship Represented by Cross certificate）を日本側が開発し、プロトコルレビューを行ってその頑健性を確認した。AUBReX は、グリッドが持つ堅牢性とピアツーピア技術が持つ簡便性を兼ね備えた新たなセキュリティ基盤を実現する、極めて新規性の高い PKI アーキテクチャである。

（２）にあげた「セキュリティポリシの整合性の確保」については、日米が協力してセキュリティポリシのすり合わせに関する議論を進め、産業技術総合研究所が運営する認証局（産総研認証局）の運用規程および運用マニュアルをベースに認証局の運用ガイドラインを作成し、米国側の認証局の運用規程と比較し、整合性がとれるよう調整を進めた。その結果として、産総研認証局が米国の大規模グリッド基盤である TeraGrid に「信頼できる認証局」として登録され、産総研認証局が発行した証明書を利用して、米国のスーパーコン

ピュータセンターが保持する計算資源へのアクセスが可能となった。産総研、東大、東工大、TeraGrid および南カリフォルニア大を接続した日米グリッドを構築し、その上にある合計 6 か所のスーパーコンピュータセンターのスーパーコンピュータを利用した大規模実証実験に成功した。複数の管理組織に跨る PKI アーキテクチャはすでにいくつも存在するが、ポリシーのすり合わせがうまくいかないために実運用に至るものは少ない。本研究でまったく異なる組織間でセキュリティポリシの整合性を確保し、相互信頼の枠組みを実用レベルで確立したことは貴重な先例となる。

日米で協力して実験を進めた結果をもとに新たな PKI アーキテクチャを開発し、また、セキュリティポリシの整合性を確保することにより、日米間での信頼性の確立に成功した。これらはいずれも日米が密に協力することなくしては実現が困難なものであり、当初の目標を達成する、高い成果をあげたと考える。

研究成果の今後期待される効果であるが、開発した AUBReX は、ピアツーピア技術とグリッド技術を相補的に利用した新規性の高い技術である。従来グリッドは組織単位で信頼関係を構築し、それに基づいた認証・認可を行ってきた。スーパーコンピュータのような組織が所有する大規模な計算資源の共有についてはこのモデルで問題ないが、このような環境を利用できる研究者はごくわずかである。その一方で、Folding@HOME や SETI@HOME のように、ピアツーピア技術を用いて世界中の PC を利用した大規模計算も広く普及しており、総演算性能は現在世界最速のスーパーコンピュータの性能を超える 1 ペタフロップス超を記録するなど、サイエンスアプリケーションの一つの基盤として定着しつつある。しかし、ピアツーピア技術をベースにした場合はセキュリティに問題があり、データの不正コピーや誤った計算結果の提示などの問題があった。AUBReX はピアツーピア技術が持つ簡易性とグリッド技術が持つ堅牢性を兼ね備えた新たな認証基盤として、そのような不正な行為に対する抑止力を持ち、グリッドおよびピアツーピア基盤におけるセキュリティシステムとして普及していくことが期待される。

日米間で行ったセキュリティポリシのすり合わせについては、日米に限らずに全世界的に標準的なセキュリティポリシを策定する活動が進められており、本研究の成果はその活動に対して重要なインプットとなる。また、今後は認証だけではなく認可に関する標準的なポリシーの策定も重要になり、それらについて研究を展開していきたいと考える。

## ４．事後評価結果

### ４－１．総合評価

総合コメント：

日米間の大規模科学技術計算のために定常的に利用可能なサイエンスグリッドの実現のため、複数の組織により構成されるグリッドのセキュリティ基盤の実現に必要なＰＫＩアーキテクチャーの設計及び評価、セキュリティポリシーの整合性の確保について、研究活動・交流を行ったが、電子メールやビデオ会議による交流が主であり、内容のある交流がなされたかに疑問が残る。人材育成についても成果はあがっていない。

### ４－２．研究交流の有効性

新しい知の創造に関しては、ユーザ各個人が各々認証局となって、自分が信頼する人間との間で、クロス認証を行うことにより信頼関係を構築し、ピアツーピア技術を用いて信頼関係を広げていくという新たな発想による新規性の高いＰＫＩシステム、AUBBeX を開発した。

両国の研究者は、本プロジェクト発足以前から、互いに国際会議や標準化会合で既知の関係にあり、本プロジェクトでの研究交流は、電子メール、ビデオ会議に加え、上記の国際会議の場を利用して行われた。このため、人材育成に関しては、成果を挙げたとは言い難い。

研究交流の今後に関して、グリッドは国際間に跨るインフラであり、本研究の成果であるセキュリティ・ポリシーの整合性が確保されたことにより、互いの資源利用などの面で、研究交流が持続的に発展するよう、努力されることを期待したい。

４－３．当初目標の達成度

研究交流実施体制は不十分であった。ワークショップは開催されていない。国際会議での講演もなされていない。