2008－HPC－118 (5)
2008／12／16

Tsukuba-GAMA: E-サイエンス基盤のためのユーザ管理システムの設計と実装

山本直孝† 田中良夫†
小島 功† 関口智嗣†

E-サイエンス基盤においては，公開鍵暗号（Public Key Infrastructure, PKI）と X.509 証明書及びその拡張である代理証明書（プロキシ証明書）を用いたグリッドセキュリティ基盤（Grid Security Infrastructure, GSI）が広く利用されている．プロキシ証明書を用いることで，シングルサインオンや権限移譲（delegation）が実現され，頑健かつ多機能なセキュリティ基盤が実現されている．一方で，GSI に基づく認証・認可を採用する場合，ユーザはユーザ証明書及び秘密鍵を管理しプロキシ証明書の作成をする必要があり敷居が高いものになっている．さらに，秘密鍵を正しく管理出来ないユーザが居た場合，システム全体の頑健性が失われてしまうことが危惧される．そこで，本研究ではアプリケーションやデータサービスの保護には GSI を用いた頑健なセキュリティ基盤を採用し，かつユーザには使い勝手の良いユーザインタフェースを提供するユーザ認証情報管理システムである Tsukuba-GAMA の設計と実装について報告する．また，実際の運用環境に適用することで本設計の妥当性を検証した．

Tsukuba-GAMA: Design and Implementation of User Management System for e-Science

Naotaka YAMAMOTO,† Yoshio TANAKA,† Isao KOJIMA† and Satoshi SEKIGUCHI†

The Grid Security Infrastructure (GSI), based on Public Key Infrastructure (PKI), X.509 certificate, and proxy certificate, is widly adopted in the e-Science infrastructure. However, there is a need for users to generate and manage a credential carefully. In order to reduce vulnerability risks due to mistakes by inexperienced users, Tsukuba-GAMA provides a flexible and easy to use interface for GSI. In this paper, firstly we describe design principles of the Tsukuba-GAMA which allows us to generate a credential on the portal server to access Grid-enabled services. Secondly, software architecture and its prototype implementations are described, where we take the Grid technology, especially, GSI and Virtual Organization (VO) concept. Tsukuba-GAMA allows the user to generate and retrieve a VOMS-enabled proxy certificate, in order to perform their application even if they does not have the Grid credential on their client.

1. はじめに

スーパーコンピュータ等を利用した科学技術上の問題を解く計算科学（第三の科学）が発展し幅広い分野における技術発展に貢献した．さらに近年，ネットワーク技術の進歩，普及にともない，高速ネットワークで接続された高性能計算機，データベースなどの様々なネットワーク上の資源を統括的に利用する科学技術研究手法である E-サイエンス（第四の科学）に関する研究が活発に行われている（UK e-Science[1]，EGEE[2]，the Open Science Grid[3]，the Cyber Science Infrastructure[4] など）．例えば，多様な地球観測データとシミュレーションを組み合わせる地球科学分野，バイオ情報データベースを用いて創薬を効率よく行うバイオ情報分野などにおいて E-サイエンスにより技術開発を大幅に加速することができると期待される分野は多岐にわたる．

本稿においては，地球科学分野における E-サイエンス基盤として研究開発を進めている地球観測グリッド[5](Global Earth Observation Grid, GEO Grid) を題材としてセキュリティ基盤としてのユーザ管理システムの設計及び実装，評価について述べるが，これらは地球科学分野固有のものではなく，多様かつ大量のデータや計算から必要なものを組み合わせて問題を解

† 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology

く，様々な応用分野に適用可能なE-サイエンスにおけるセキュリティーアーキテクチャの設計及び実装の指針となる．本稿の目的は，既存のアプリケーションコミュニティーに対してE-サイエンス基盤を適用する上で大きな問題となっているセキュリティ基盤の実現方法を明確に論じ，E-サイエンス基盤の研究開発を促進させ，E-サイエンスによって科学技術の飛躍的な発展を促すことである．

次章ではE-サイエンスにおけるセキュリティ基盤に対する要件を示し，3章では設計方針，ソフトウェアアーキテクチャの設計を述べる．4章ではプロトタイプの実装方法及び予備評価結果を示し，5章では実装したプロトタイプを通じて得られた知見を述べ，最後にまとめと今後の課題を述べる．

2. セキュリティ基盤への要件

本章では，E-サイエンス基盤を既存のアプリケーションコミュニティーへ適用する上でのセキュリティ基盤，ユーザ認証情報管理システムに対する要件を述べる．

2.1 認証方式への要件

データやアプリケーションサービスは，その提供者のポリシーに応じて求められるセキュリティレベルが大きく異なる．たとえば，地球科学分野においては全くフリーにアクセス可能なものや無償ではあるもののユーザ登録が必要なもの（到達可能なメールアドレスがあればアカウントが自動的に発行される等），ユーザへ利用申請書などの提出を求め厳密に個人を認証するもの，有償のものなど種々さまざまである．

我々は，データやアプリケーションサービスの提供者のポリシーに応じてアクセスコントロールを柔軟かつスケーラブルに実現するため，仮想組織（Virtual Organization, VO）の概念を導入したGEO Gridにおけるセキュリティ基盤を実装した[6]．これにより，VO毎にアクセスの許可・不許可を設定することが可能となりサービス提供者はVO管理者を信頼することでユーザ管理が実現されユーザ数に対してスケーラブルなユーザ管理体系が実現されている．また，VOを実現する方法としてVOMS[7] (Virtual Organization Membership Service)を利用することでVOよりも細かい粒度のグループやロールを設定することが可能となっており，アクセスコントロールを柔軟に実現することが出来る．しかし，GEO Gridにおけるセキュリティ基盤[6]を含め，UK e-Science[1]，EGEE[2]など既存の実装ではユーザの認証レベルが単一のものに限定されており，資源提供者の求める保証レベルに応じてユーザ認証方式を切り替える等の機能が実現されていない．例えば，前述のメールアドレスのみでアクセスを許可しているようなデータサービスには冗長な認証となってしまう．すなわち，資源を保護するための保証レベルに応じてユーザ認証方式を切り替えるといった機能を持つセキュリティ基盤が必要である．

また，MyProxy[8]やGEO Gridにおいて，多くのユーザにとって慣れ親しんでいるユーザ名パスワードの組み合わせでグリッドにおける代理証明書（プロキシ証明書）を生成することが可能となっているが，ユーザにとってはサイトが増える都度，新たなパスワードを設定しなければならず，同じパスワードの再利用や，記憶しやすい簡単なパスワードが設定されることになりシステム全体としてのセキュリティーレベルを下げることになりかねない．すなわち，ユーザ認証機能を外部の集中サーバに移譲し，その認証情報に基づき証明書及びプロキシ証明書を生成するための仕組みが必要である．さらに，ユーザ証明書によるより頑健な認証方式を同時にサポートするためにもユーザ認証インタフェースを目的に応じて開発するためのフレームワークが必要でり，同時に保証レベルをサービスへ伝達するための仕組みも必要である．

2.2 アプリケーション開発からの要件

地球科学分野でのコンポーネントは，主に（1）メタデータの検索，（2）データの取得，転送，（3）アプリケーションの実行の3つの要素から成る．たとえば，これらの機能は（1）OGSA-DAI[9]による複数のデータベースを用いた検索，（2）GridFTPを用いたデータの第三者転送，（3）GridRPC[10]の参照実装であるNinf-G[11]や，NetSolve/GridSolve[12]を用いたアプリケーションのタスク並列化などを用いることで実現される．しかし，これらのミドルウェアを利用するにはミドルウェアのAPI等を用いたアプリケーションの修正が必要であり一般の研究者には敷居が高い．一方，地球科学分野においてはOGC[13] (Open Geospatial Consortium)が定めるREST型の非常に簡便なインタフェースによるデータの検索や取得，アプリケーションの実行が可能となっている．E-サイエンス基盤をこのような分野に普及させるには，導入のコストを下げる必要がありこれら既存のアプリケーションを修正することなくE-サイエンス基盤へ導入可能となる必要である．

3. 設　　計

本章では，前章で述べた要件を実現するためのユーザ管理システムであるTsukuba-GAMAの設計方針，セキュリティアーキテクチャについて述べる．我々は，GEO Gridにおけるセキュリティ基盤[6]で導入した仮想組織（Virtual Organization, VO）の概念をユーザ管理システムの一部として採用し，それを拡張する．

3.1 セキュリティアーキテクチャ

Tsukuba-GAMAはウェブポータルを用いてポータルのバックエンドにあるVOで束ねられたサービス群を利用するためのユーザ認証情報管理機構を提供す

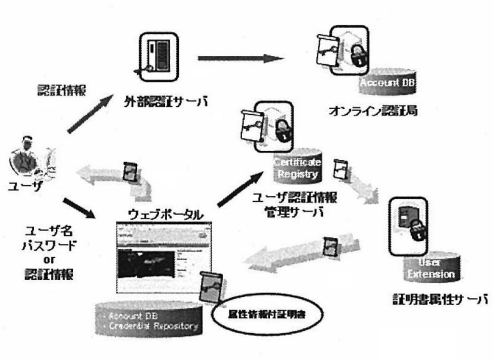

図 1 Tsukuba-GAMA アーキテクチャ
Fig. 1 Tsukuba-GAMA design architecture

る．Tsukuba-GAMA におけるユーザ認証情報管理システムは（1）ユーザ認証情報管理サーバ，（2）証明書属性サーバ，（3）外部認証サーバ，および（4）オンライン認証局で構成され（図 1），様々な認証レベルの認証方式に基づき属性情報が付与された証明書をウェブポータルサーバ上に作成する．ユーザ認証情報管理サーバは，それぞれのユーザ認証方式の結果を受けユーザ証明書の管理やプロキシ証明書の生成，管理を行う．また，生成された証明書に応じて証明書属性を付与するため，証明書属性サーバに接続し，属性情報付証明書を要求する．作成された属性情報付証明書をウェブポータルサーバへ移譲し保存する．

外部認証サーバを用いて認証を行う場合は，ユーザ認証情報管理サーバはユーザ証明書等のユーザ認証情報を持ち得ないため，認証結果を受けてオンライン認証局を用いて動的にユーザ証明書を作成し保存する．認証方式の違いを吸収し，ウェブポータルサーバ上に属性情報付証明書を生成することで，ユーザはポータルサーバを介してバックエンドにあるデータやアプリケーションサービスを利用することが可能となる．

また，ポータルサーバを介せずユーザ独自のアプリケーションを実装可能するため，ウェブポータルサーバを通じて属性情報付証明書をユーザ端末へ転送可能とする．こうすることで，ユーザはダウンロードした証明書を用いてバックエンドのサービスへ直接アクセスすることが出来る．

4. プロトタイプ実装

前章で述べた設計に基づき，我々は E-サイエンス基盤におけるユーザ管理システムである Tsukuba-GAMA のプロトタイプを実装する．ここでは，GSI[14] (Grid Security Infrastracture) および VOMS[7] を用いる．GSI は公開鍵暗号と X.509 証明書を用いたグリッドにおける標準的な認証基盤であり，プロキシ証明書を用いてシングルサインオンと権限委譲を実現する．Tsukuba-GAMA においては，VOMS 属性付きのプロキシ証明書（VOMS プロキシ証明書）をポータルサーバ上に作成することで認証を完了する．また，ユーザ認証情報管理サーバには，GAMA[15] (Grid Account Management Architecture) サーバをそのまま利用し，オンライン認証局は，MyProxy CA サーバにより実現した．ユーザ認証インタフェースについては，図 2 に示すように 3 種類のユーザ認証方式に付いてユーザインタフェースの実装を行った．

4.1 証明書保存機能

ウェブポータル上に VOMS 属性の付いたプロキシ証明書を保存するため，Crecential ポートレットを実装した．ここでは，GridSphere のユーザ名をキーにしてプロキシ証明書の保存，取得が出来るよう実装した．また，ユーザが直接サービスへアクセスするため，Credential ポートレット（図 2 左下）において，必要に応じて PKCS#12 形式の VOMS プロキシ証明書をウェブブラウザへダウンロードする機能を実装した．

4.2 ユーザインタフェース

ユーザインタフェースの構築にあたっては，JSR168 に基づいたポートレットを用いてウェブポータルを構築するためのフレームワークである GridSphere[16] を用いた．GridSphere はポータルに対する認証モジュールを開発するためのインタフェースが提供されており，Tsukuba-GAMA のように異なるユーザ認証インタフェースを提供する際に，開発コストを大幅に軽減することが出来る．また，証明書管理ポートレット（Credential ポートレット）を同時に実装したことで，アプリケーションポートレットの開発に際しても，証明書を証明書管理ポートレットから Java API を用いて取り出すことが可能なため，OGSA-DAI[9] や GRAM[17] といったグリッド環境におけるサービスに容易にアクセスすることが可能となる．

Tsukuba-GAMA のプロトタイプでは 3 種類のユーザインタフェース：1）GAMA[15] と同様ユーザ名パスワードのペアから VOMS プロキシ証明書を作成するためのインタフェース，2）ユーザが複数のポータルサイトへアクセスする上で，ユーザ情報を一元管理し，共通のユーザ名パスワードのペアでログインできるようにするための仕組みである OpenID[18] を元にしたプロキシ証明書作成インタフェース，3）ユーザ証明書及び秘密鍵を自己管理出来るユーザ向けにユーザ証明書からプロキシ証明書を移譲することにより生成するインタフェースを実装した．

4.2.1 ユーザ名パスワード認証

ユーザ名パスワードによるユーザ認証インタフェースは，GAMA[15] が提供する GridSphere における認証モジュールに VOMS サーバへの問い合わせを追加し，VOMS プロキシ証明書を作成している（文献 6)）．この際，GAMA サーバは修正することなく用いてお

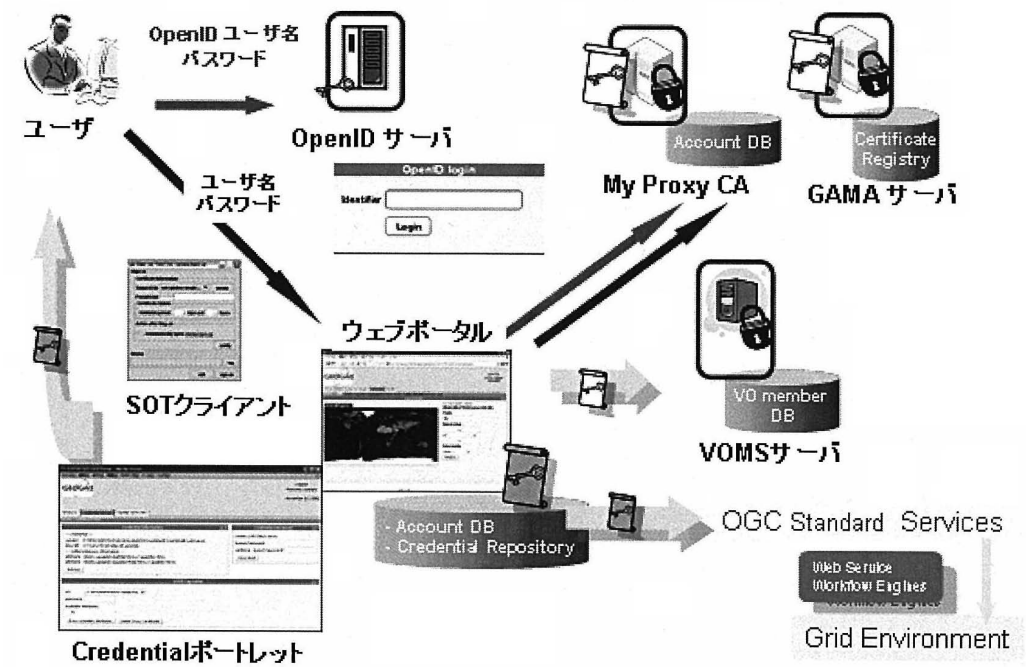

図 2 Tsukuba-GAMA プロトタイプ実装の概要
Fig. 2 Tsukuba-GAMA prototype implementation

り，ユーザ証明書は GAMA サーバにパスワード付きで保存されている．ユーザが入力したユーザ名とパスワードをポータルサーバから GAMA サーバへ転送し，秘密鍵のパスワードに合致した場合にプロキシ証明書の作成が成功する．この成功をもって，ポータルシステムへのログインを実現している．Tsukuba-GAMA では，作成されたプロキシ証明書に VOMS 属性を追加するために VOMS サーバに VOMS プロキシ証明書を要求し，作成された VOMS プロキシ証明書を Credential ポートレットへ保存する．

4.2.2 OpenID ユーザ認証

OpenID ユーザは，図 1 の外部認証サーバに OpenID サーバを用いることで認証を実現する．しかし，パスワードをポータルサーバが知る術がないため，パスワードなしでユーザ証明書をオンデマンドに発行する必要がある．MyProxy CA サーバは管理者証明書に基づいてパスワード無しのユーザ証明書を発行する機能を持っているため，図 1 のオンライン認証局として利用することができる．本実装では，ポータルサーバー上にある管理者証明書（ホスト証明書）を用いて MyProxy CA サーバへ証明書発行要求を出している．ユーザのログインの流れを表 1 に示す．ユーザは，図 2 にある OpenID ユーザ名を入力する．ここには，パスワードを入力するフォームは存在しない．

表 1 OpenID ユーザのログインの流れ
Table 1 OpenID user login flow

	手順
1	OpenID ユーザ名の入力
	OpenID サイトへリダイレクト
2	OpenID サイトにおいてパスワード入力
	GridSphere ポータルへリダイレクト
3	MyProxy CA からユーザ証明書の発行
4	VOMS サーバへリクエスト
5	Credential Portlet へプロキシ証明書の保存

4.2.3 Credential ユーザ認証

証明書を自らの端末に持つユーザは，Grid PSE Builder[19] で提供される SOT (Sign-on Toolkit) クライアント（図 2 左中）を用いてポータルサーバに直接プロキシ証明書を作成する．VOMS プロキシ証明書は，ユーザ名パスワードユーザと同様にプロキシ証明書から作成され，Credential ポートレットに保存される．また，ブラウザへユーザ証明書を登録しておくことで，GridSphere の X.509 ユーザ証明書による双方向認証モジュールを用いてログインすることが出来る．GridSphere 認証モジュールにおいては，SSL 双方向認証により接続された後，ユーザ証明書情報に元づき，Credential ポートレットに VOMS プロキシ証明書が保存されているかを確認してログインを完了

表 2 Credential ユーザのログインの流れ
Table 2 Credential user login flow

	手順
0	ユーザ証明書の登録
1	JNLP を用いた SOT クライアントのダウンロード及び起動
2	証明書パスワード入力
	プロキシ証明書の作成
	VOMS プロキシ証明書の作成
3	GridSphere ポータルへアクセス
4	Credential Portlet へプロキシ証明書の保存

する．認証の流れを表 2 に示す．保証レベルとしては Tsukuba-GAMA において最上位に位置するユーザインタフェースである．ログイン時の手順を表 2 に示す．

4.3 アカウント作成

認証方式を問わず，アカウントの作成における申請方法及び承認方法は基本的に文献 6) と同様に実装した．OpenID ユーザについては，ユーザからの申請情報に基づいて，利用許可情報を GAMA サーバに登録する．その際，OpenID サーバに対して，認証に必要な情報を要求することが出来る．ログイン時には，GAMA サーバからユーザ認証情報を取得し，ポータルサーバが MyProxy CA サーバへユーザ証明書発行要求を出す．Credential ユーザについては，GridSphere の持つ X.509 ユーザ証明書による双方向認証で実現しているため，アカウント情報はウェブポータル上に保存される．

4.4 プロトタイプの検証

Tsukuba-GAMA の設計及びプロトタイプ実装の妥当性を検証するため，我々は GEO Grid で既に提供しているサービスへのアクセスが実現されるか検証を行った．我々が開発した Tsukuba-GAMA プロトタイプにおける 3 つのユーザ認証方式いずれにおいても，Credential ポートレットに保存された VOMS プロキシ証明書を用いて，OGSA-DAI を用いた衛星データ検索，GRAM を用いた衛星データ処理アプリケーションの実行が期待どおり実現できることを確認した．

また，OGCProxy[20] ではユーザから直接サービスへアクセスすることは出来ずデータが全てのやりとりがポータルサーバを経由してしまうボトルネックがあったが，Credential ポートレットにおける PKCS#12 形式の VOMS プロキシ証明書ダウンロード機能により，ウェブブラウザから直接 Gridsite[21] で保護された OGC サービスへ期待どおり接続できることを確認した．これにより，OGC により定められている HTTP 上での REST 型アプリケーションプロトコルを変更することなく HTTPS を用いてアクセスするだけで，OpenLayers[22] 等を用いた既存の Web-GIS アプリケーションが変更無しに動作することが出来るのを確認した．

5. 考　　察

ユーザ証明書自動発行システムであるオンライン認証局として MyProxy CA を用いた．MyProxy CA における証明書発行時の認証は，クライアントの管理用 SSL 証明書が利用されており，プロトタイプ実装におけるポータルサーバと MyProxy CA が直接接続されている構成はセキュリティ上好ましくない．ポータルサーバのように，いわゆるインターネットにさらされる計算機からオンライン認証局は明確に切り離される必要があり，認証局はユーザ情報管理サーバでさらに保護されるべきである．また，ポータルシステムにおける認証局プロファイルは IGTF[23] で検討中である．

OpenID ユーザのケースにおいて，ユーザ認証情報管理サーバがオンライン認証局に対する証明書発行許可情報を持つ必要がある．プロトタイプ実装では，GAMA サーバに利用許可情報を記録し，その情報に元づきオンライン認証局に対して証明書生成要求を出している．

本稿で報告したプロトタイプ実装は，ユーザインタフェースとして JSR168 ポートレットに基づいたウェブポータルを構築するためのフレームワークである GridSphere を利用した．JSR168 ポートレットは，その可搬性から多くのウェブポータルサイトの構築に採用されている．一方，ユーザインタフェースを GridSphere に限定してしまうとウェブポータル構築の柔軟性が失われてしまう．この問題を回避するため，より一般的な方法でユーザインタフェースを提供する必要がある．MyProxy プロジェクトにおいても，Apache ウェブサーバの認証モジュールとして MyProxy モジュールを提供しており，CGI プログラムからポータルサーバ上に作成されたプロキシ証明書を参照できるようになっている．より一般的なユーザインタフェースとは何であるかは今後吟味する必要があるがウェブポータルを使う場合においては，認証もジュールによる実装が一般の利用に供することが出来ると考えられる．

Credential ユーザについて，Grid PSE Builder の一環で実装した SOT を用いたが，SOT は VOMS プロキシ証明書をサポートしていない．また，OpenID ユーザの認証モジュールにおいても GridSphere 認証モジュールが VOMS サーバへ VOMS プロキシ証明書を要求している．図 1 における証明書属性サーバのようにユーザ認証情報管理サーバが証明書属性サーバとの接続を中継する方がユーザ認証情報管理サーバのインタフェースが整理され，利便性が向上すると考えられる．これに対応して，SOT 及び OpenID 認証モジュールを修正する．

6. まとめと今後の課題

本稿では，E-サイエンスにおけるユーザ管理システムの設計とプロトタイプの実装について報告し，設計の妥当性を検証した．また，GEO Grid を題材として実際のデータへのアクセス，アプリケーションの実行について既存の仕様，プロトコルを変更無しに既存のアプリケーションを E-サイエンス基盤へと拡張するための手順を示した．今後さらに利用者の意見を採り入れつつより柔軟性の高いセキュリティ基盤を実現するためのソフトウェアとなるよう研究開発を進めていく予定である．

プロトタイプ実装によって得られた知見に基づき，ユーザ認証情報管理サーバのプロトコル及び，接続用 API の研究開発を進めていく予定である．

謝辞 本研究を遂行するにあたり常にアドバイス頂いた GEO Grid プロジェクトのメンバ諸氏に感謝致します．なお，本研究の一部は次世代ＩＴ基盤構築のための研究開発「研究コミュニティ形成のための資源連携技術に関する研究」の一環として行われたものである．

参 考 文 献

1) Hey, T. and Trefethen, A. E.: The UK e-Science Core Programme and the Grid, *Future Generation Computing Systems*, Vol. 18, pp. 1017–1031 (2002).
2) Gagliardi, F., Jones, B., Grey, F., Begin, M. and Heikkurien, M.: Building an infrastructure for scientific Grid computing: status and goals of the EGEE project, *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, Vol. 363, No. 1833, pp. 1729–1742 (2005).
3) Foster, I. *et al*: The Grid2003 Production Grid: Principles and Practices, *Proc. IEEE Int. Symposium on High Performance Distributed Computing* (2004).
4) Sakauchi, M. and Catlet, C.: Cyber Science in Japan, and Large Grid Deployments: Status and Outlook, *presented at the 17th Global Grid Forum, Tokyo, Japan* (2006).
5) Sekiguchi, S., Tanaka, Y., Kojima, I., Yamamoto, N., Yokoyama, S., Tanimura, Y., Nakamura, R., Iwao, K. and Tsuchida, S.: Design Principles and IT Overviews of the GEO Grid, *IEEE System of systems, in printing*, Vol. 2, No. 3, pp. 374–389 (2008).
6) 田中良夫, 山本直孝, 関口智嗣: 地球観測グリッドにおけるセキュリティ基盤の設計と実装, 情報処理学会論文誌　コンピューティングシステム, Vol. 1, No. 2, pp. 169–179 (2008).
7) Alfieri, R., Cecchini, R., Ciaschini, V., dell'Agnello, L., Frohner, A., Lorentey, K. and Spataro, F.: From gridmap-file to VOMS: manageing authorization in a Grid environment, *Future Generation Computer Systems*, Vol. 2, No. 4, pp. 549–558 (2005).
8) Novotny, J., Tuecke, S., and Welch, V.: An Online Credential Repository for the Grid: MyProxy, *Proceedings of the Tenth International Symposium on High Performance Distributed Computing (HPDC-10)*, IEEE Press, pp. 104–111 (2001).
9) OGSA-DAI: http://www.ogsadai.org.uk/.
10) Seymour, K., Nakada, H., Matsuoka, S., Dongarra, J., Lee, C. and Casanova, H.: Overview of GridRPC: A Remote Procedure Call API for Grid Computing, *Grid Computing - Grid 2002*, pp. 274–278 (2002).
11) Ninf-G: http://ninf.apgrid.org/.
12) NetSolve: http://icl.cs.utk.edu/netsolve/.
13) OGC: http://www.opengeospatial.org/.
14) Foster, I., Kesselman, C., Tsudik, G. and Tuecke, S.: *Proceedings 5th ACM Conference on Computer and Communications Security Conference*, pp. 83–92 (1998).
15) Bhatia, K., Chandra, S. and Mueller, K.: GAMA: Grid Account Management Architecture, *Proceedings of First IEEE International Conference on e-Science and Grid Computing* (Stockinger, H., Buyya, R. and Perrott, R.(eds.)), pp. 413–420 (2005).
16) GridSphere: http://www.gridsphere.org/.
17) Globus Alliance: http://www.globus.org/.
18) OpenID: http://www.openid.net/.
19) Hirano, M., Yamamoto, N., Takemiya, H., Tanaka, Y., Itoh, S. and Sekiguchi, S.: Grid PSE Builder: A Framework for Building Web-based Distributed PSE on Grid, *High Performance Computing and Grid in Asia Pacific Region, Seventh International Conference on (HPC Asia'04)*, pp. 34–41 (2004).
20) Yamamoto, N., Kojima, I., Tanaka, Y. and Sekiguchi, S.: VO-enabled Service Harmonization in the GEO Grid, *To appear in Proceedings of 4th IEEE International Conference on e-Science* (2008).
21) GridSite: http://www.gridsite.org/.
22) OpenLayers: http://www.openlayers.org/.
23) IGTF: http://www.igtf.net/.