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. 2　169–179 (Aug. 2008)

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

田中良夫[†1]　山本直孝[†1]　関口智嗣[†1]

我々は地球観測衛星データやフィールドセンサデータ，シミュレーションプログラムなどのデータや計算などをグリッド技術により統合・連携させることにより，防災，環境，資源探索などの様々な応用分野に調査・実験環境を提供する地球観測グリッド（Global Earth Observation Grid，GEO Grid）の研究開発を進めている．本稿では，GEO Grid を実現するセキュリティ基盤の設計と実装について報告する．GEO Grid は，サービスとして抽象化されたデータや計算をアプリケーションコミュニティの要望に応じて組み合わせることにより仮想組織（VO）を構成し，それらの柔軟な連携・統合を可能とする設計となっている．また，ユーザ単位での認証と VO 単位での認可を組み合わせることにより，スケーラブルかつ容易なアクセス制御を実現する．実際の衛星データなどを提供するシステムの実装により，本設計の妥当性を検証した．

Design and Implementation of Security Infrastructure of the GEO Grid

Yoshio Tanaka,[†1] Naotaka Yamamoto[†1]
and Satoshi Sekiguchi[†1]

The authors have been leading the “GEO (Global Earth Observation) Grid” project since 2005 which is primarily aiming at providing an E-Science infrastructure for worldwide Earth Sciences community. In the community there are wide varieties of existing data sets including satellite imagery, geological data, and ground sensed data that each data owner insists own licensing policy. Based on a concept of a Virtual Organization (VO), the GEO Grid is designed to integrate all the relevant data virtually, enabled by Grid technology, and is accessible as a set of services. In this paper firstly we describe design principles of the GEO Grid Security infrastructure that are determined based on accommodating users requirements for publishing, managing, and using data. Secondly, software architecture and its implementations are specified where we take the Grid computing and Web service technologies as the core components that comply with standard set of technologies and protocols.

1. はじめに

近年，地球温暖化などの環境問題，地震や洪水などの災害予測・対策，および天然資源探索などの地球観測に関する問題が重要になっている．GEO（Global Earth Observation）Grid [1] は，グリッド技術[2] を用い，地球観測衛星データなどの大規模アーカイブおよびその高度処理を行い，分散環境下の各種観測データや地理情報システムデータと統融合した処理・解析を，ユーザが手軽に扱えることを目指したシステムかつコンセプトであり，地球観測情報のインフラとして期待されている．GEO Grid は，地球観測に関わる多種多様なデータや計算を研究コミュニティや事業者が安全・安心に利用できる環境の提供を目指している．産総研の有する地質情報と衛星情報との情報融合を進め，さらに広く地球観測情報との融合化を図り，また，国際連携を積極的に推進し，特にアジアにおける高度利用を重点的に展開する計画である．この際に国際的な標準動向に配慮し情報システムとデータの国際的な相互利用性を確保することを目指している．

GEO Grid はアプリケーション，コンテンツ，および情報基盤により構成されるが，本稿においては情報基盤のセキュリティアーキテクチャの設計と実装について報告する．GEO Grid は，サービスとして抽象化されたデータや計算を研究コミュニティの要望に応じて組み合わせることにより仮想組織（VO）[3] を構成し，それらの柔軟な連携・統合を可能とする設計となっている．また，ユーザ単位での認証と VO 単位での認可を組み合わせることにより，スケーラブルかつ容易なアクセス制御を実現する．本稿においては，情報基盤への要求に基づいて設計方針を示し，その実装方法および実システムの構築を通じて得られた知見，検証結果を述べる．

近年，ネットワーク技術の進歩およびネットワーク基盤の普及にともない，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，大規模記憶装置，実験装置などの様々な資源を統括的に利用し，科学技術における新発見や融合研究領域などの新たな研究分野の創出を促進する科学技術研究手法である e サイエンスに関する研究がさかんに行われている．GEO Grid は e サイエンスの一例であるが，ほかにもたんぱく質データベースなどバイオ情報データベースを用いて創薬を効率良く行うといったバイオ情報分野，大量の医療画像

†1 独立行政法人産業技術総合研究所
National Institute of Advanced Industrial Science and Technology

データベースを活用してがん診断を支援するシステムや医療データベースを利用して治療に役立てる次世代医療診断システムなどを開発する医療産業分野など，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．

e サイエンスの情報基盤のセキュリティは，応用コミュニティの利用シナリオ，ユーザベース，新たな情報基盤を用いることに対する理解度や積極性，データや計算機などの資源の配備・所有状況やその公開ポリシ，アクセス制御に必要とされる粒度，複数のコミュニティによるデータ共有の有無など，様々な要素を考慮して設計・実装する必要がある．関連研究については 7 章で詳しく述べるが，e サイエンスに関する研究はさかんに行われており，情報基盤の構築を支援するセキュリティ関連のソフトウェアやツールとしても，グリッドのセキュリティ技術である Grid Security Infrastructure（GSI）[4]，仮想組織の管理を行う Virtual Organization Membership Service（VOMS）[5]，Credential Service システムである MyProxy [6]，ユーザアカウントおよび証明書を管理する GAMA [7]，ユーザに簡便なインタフェースを提供するポータルである GridSphere [8] など多々開発されている．しかし，GEO Grid のセキュリティに対する要件については 2 章で詳しく述べるが，GEO Grid が求める複数のセキュリティ要件に対し，それらを個別に満たすシステムは存在するが，すべてを満たすシステムおよび実装例はない．

本稿の目的は，e サイエンスにおける VO の考え方やアカウント管理，認証・認可の実現方法を明確に論じ，e サイエンス基盤の研究開発に指針を与えることにある．また，既存のソフトウェア，ツールなどを有効に活用することにより，少ない開発コストで GEO Grid が求める複数のセキュリティ要件をすべて満たすシステムが実装されることを示す．本稿においては，GEO Grid を題材としてセキュリティアーキテクチャの設計および実装について述べるが，これらは GEO Grid 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アーキテクチャの設計および実装の指針となる．次章では，GEO Grid アプリケーションから情報基盤のセキュリティに対する要件を示す．3 章では設計方針，利用モデルおよびソフトウェアアーキテクチャの設計を述べる．4 章では実装方法および各ソフトウェアコンポーネントの予備評価結果を示し，5 章と 6 章では実際の衛星データを用いた実装を通じて得られた知見を述べ，関連研究に続いて最後にまとめと今後の課題を述べる．

2. 情報基盤のセキュリティに対する要件

図 1 に GEO Grid アプリケーションの例として，火山噴火時の溶岩流の流れを予測し，

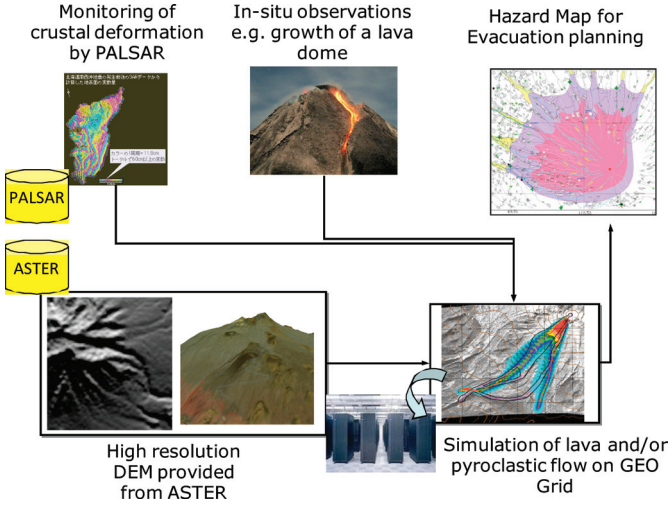

図 1　ハザードマップ作成システム
Fig. 1　Hazard map generator.

ハザードマップを作成するシステムを示す．本システムにおいては，異なる特徴を持つ 2 つの衛星観測データを用いて求められる火山一帯の地殻変動および標高モデルに加え，現地で観測される溶岩ドームの形状，成長過程などのデータを入力として火砕流のシミュレーションを行い，ハザードマップを作成する．本システムは GEO Grid アプリケーションの一例にすぎないが典型的なシナリオによるものであり，この例から以下に示すような情報基盤のセキュリティに対する要件を洗い出すことができる．また，これらの要件は GEO Grid アプリケーションから抽出したものであるが，他分野のアプリケーションにおいても同様な要件が存在しうることは容易に推察できる．

(1)　複数の組織にまたがる資源への透過的なアクセスの実現
GEO Grid は，衛星データベース，GIS データベース，フィールドセンサデータベース，シミュレーションプログラムなど，異なる組織により提供される多様なデータベースやアプリケーションの中から応用コミュニティの要求に応じて必要なものを選択，組み合わせて利用環境を構築し，ユーザに提供する．それぞれの組織は独立したセキュリティドメインであり，提供される資源へのアクセスに際しては個別に認証・認可によるアクセス制御を行う必要があるが，ユーザの利便性を向上させるため，複

数の組織にまたがる資源に対してあたかも単一のセキュリティドメインであるような透過的なアクセスを実現する認証・認可機構を実現する必要がある．

(2)　データ提供ポリシの尊重

データには利用に制限がかからないフリーなものも存在するが，一般的にはデータ所有者はデータアクセスの許可範囲や提供可能なデータ書式の制限など，利用許諾権とその条件を設定・変更する権限を有し，データ提供者の公開ポリシに応じた柔軟なアクセス制御を実現する必要がある．データだけではなく，シミュレーションプログラムなどの計算（処理）に対しても同様なアクセス制御を実現する必要がある．

(3)　多様なアクセスパターンによるデータや計算の統合の支援

たとえば検索結果として得られた複数のデータをシミュレーションの入力とし，得られたシミュレーション結果を第三者が提供するストレージに蓄えていくというような，クライアント・サーバ型にとどまらない多様なアクセスパターンによってデータや計算を統合する機能を支援するセキュリティ機構を実現する必要がある．

(4)　簡便性

ユーザ，データ提供者，プロジェクト管理者など，すべての参加者に対して「簡単に使える」インタフェースやツールを提供する必要がある．たとえば，ユーザに対しては特別なソフトウェアをインストールすることなく，ユーザ名とパスワードによる慣れ親しんだ認証によって利用可能な環境を提供し，データ提供者に対しては，ユーザ数が数千〜数万人規模になる場合も想定し，管理コストがユーザ数に比例しない（スケーラブルな）アクセス制御機構を提供する必要がある．

3. 設　　計

前章において述べた要件に基づき，本章では GEO Grid 情報基盤の設計思想，利用モデルおよびセキュリティアーキテクチャの設計を述べる．

3.1 設計方針

我々は，複数の組織により構成される仮想的な組織（Virtual Organization，VO）の概念を GEO Grid 情報基盤の設計に導入する（**図 2**）．GEO Grid 情報基盤においては，様々なデータや計算が標準的なプロトコルおよびインタフェースを通じて利用可能な「サービス」として提供され，研究コミュニティはその要求に応じて必要なデータや計算を統合することにより，VO を構成する．たとえば図 2 において，防災 VO（VO for Disasters）は Building and Energy Management System（BEMS）サービスおよび衛星データ処理サービスにより構成され，地質 VO（VO for Geology）は BEMS サービス，ASTER データサービスおよび衛星データ処理サービスにより構成される．このように，世の中の多様なデータサービスや計算サービスの中で研究コミュニティが必要とするサービスが組み合わされ，仮想的な 1 つの情報基盤として構成される研究環境が VO である．

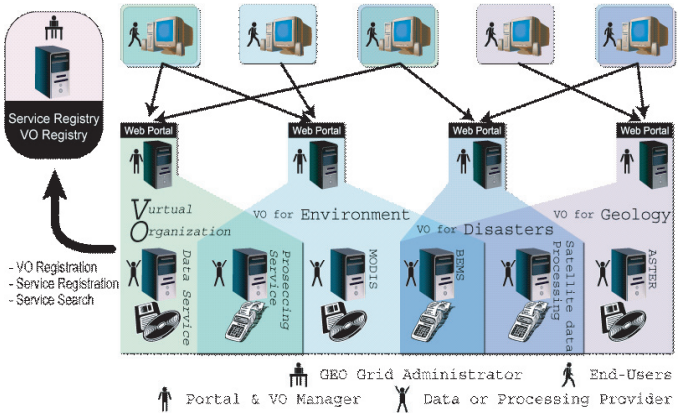

図 2　VO による GEO Grid 情報基盤
Fig. 2　Concept of VO.

一般に，ユーザは 1 つ以上の VO に所属し，サービスへのアクセスに際しては，VO に基づく認可を基本とする．VO において，各ユーザがそれぞれどういったグループに所属するか，あるいはどういった権限，役割を持つかは VO 内で管理するが，サービスへのアクセス制御において，VO 単位で行うか，VO におけるユーザの権限・役割を確認して行うか，あるいは VO の情報は用いずにユーザごとに行うかは，サービス提供者のポリシに応じて決定される．たとえば，特定の VO に所属するユーザであればすべてのユーザに対して同様なアクセス許可を与える，同じ VO に所属するユーザであっても，VO 内で所属するグループによってアクセス制御を切り替える，あるいは所属する VO によらず，ユーザごとにアクセス制御を指定する，といった，サービス提供者のポリシに応じた柔軟かつユーザ数に対してスケーラブルなアクセス制御と管理が実現される．また，VO の概念の導入により多様なデータと計算を統合し，研究環境構築を支援する．

3.2 利用モデル

図 2 に示すとおり，GEO Grid 情報基盤においては，サービス提供者，VO 管理者，エン

ドユーザ，および GEO Grid 管理者の 4 つの役割が存在する．サービス提供者はデータや計算の所有者であり，エンドユーザに対してそれらをサービスとして提供する．VO 管理者はコミュニティやプロジェクトの管理者と考えればよく，VO の構築，VO に所属するユーザの管理，ユーザ向けポータルの構築を行う．GEO Grid 管理者は利用可能なサービスが登録されているレジストリの管理およびそれへのアクセス制御を行う．エンドユーザは基本的には 1 つ以上の VO に所属し，実際にサービスを利用することにより研究・調査を行う．

サービス提供者は提供するサービスの情報を GEO Grid 管理者が運用するレジストリに登録する．VO 管理者はどのようなデータ，計算が利用可能であるかレジストリを通して検索し，利用を希望するサービスがあればサービス提供者と個別に交渉する．サービス提供者は VO へのサービスの提供を許可する場合はその VO に対するアクセスを許可するべくシステムの設定を変更する．前述のようにアクセス制御はサービス提供者のポリシに応じて VO 単位，ユーザ単位，あるいはフリーアクセスなどに設定可能である．

3.3　セキュリティアーキテクチャ

GEO Grid 情報基盤のセキュリティは，Grid Security Infrastructure（GSI）および VO レベルの認可機構を基本とする．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．認証を受けたユーザは，通常サービス提供者側で UNIX アカウントにマップされ，UNIX アカウントの権限でアクセス制御が実現される．しかし，この方法ではすべてのユーザのエントリをサービス提供者側で管理しなければならず，サービス提供者に対する管理コストが高くなってしまうことや，ユーザ数に対してもスケーラブルでないといった問題がある．そのため，VO レベルの認可機構を導入し，VO 単位での認可，VO においてユーザが所属するグループや与えられた権限に応じた認可などにより，サービス提供者の負担を軽減し，ユーザ数に対してスケーラブルかつ柔軟なアクセス制御を実現する．

また，ユーザは，VO が提供するポータル上でログインし，VO が提供するアプリケーションを実行することになるが，サービスへのアクセスに際しては，GSI による認証および VO レベルの認可が行われることになる．GSI は X.509 証明書を用いた認証を行うため，一般にユーザはユーザ証明書の取得および秘密鍵の管理を行う必要がある．しかし，そのためには特別なソフトウェアのインストールや証明書を取得するための手続きが必要となる．また，セキュリティに詳しくないユーザに秘密鍵の管理をさせることは，かえってセキュリティの脆弱性を高めるという意見もある．これらの問題を考慮し，基本的にはユーザ証明書および秘密鍵の管理およびプロキシ証明書の作成はユーザに任せずにアカウント管理サーバ（Account Server）において行い，VO が提供するポータルへのアクセスに際してはログイン名とパスワードによる認証を行う．また，VO におけるユーザの属性管理は VO サーバが担当する．

このように，GEO Grid におけるセキュリティコンポーネントとしては以下の 3 つが存在する．

- ポータルごとに管理される，そのポータルへのアクセスが許可されるユーザのログインアカウント情報．
- 各 VO により立ち上げられ，その VO に属するユーザ情報を管理する VO サーバ．
- VO とは独立に存在し，ユーザのアカウント情報（ログイン名，ユーザ証明書，秘密鍵など）を管理するアカウント管理サーバ．

GEO Grid においては，以下のような理由によりこれら 3 つの関係は多対多とした．

- アカウント情報はユーザの実体を表す情報であり，アカウント管理サーバと VO およびポータルは独立と考えるのが自然である．また，たとえば VO ごとにアカウント情報を管理するとなると，あるユーザが複数の VO に所属する場合，それぞれにおいてアカウント作成が必要になり，ユーザの負担が増えるという問題もある．ポータルごとにアカウントを管理する場合も同様．
- VO ごとにポータルを提供することになるが，VO とポータルの関係も 1 対 1 とはならない．これは，あるポータル上でログインしたユーザが，複数の VO 属性を持ってサービスにアクセスしたい場合があるという要求を実現するためである．たとえば，ASTER という衛星データへのアクセスは，ASTER VO に所属するユーザのみが許可され，MODIS という衛星データへのアクセスは MODIS VO に所属するユーザのみが許可されている場合，これらの両方の衛星データにアクセスするアプリケーションを実行する際には，ユーザは ASTER VO の権限と MODIS VO の権限の両方を持っている必要がある．

したがって，ユーザはまずアカウント管理サーバ上でアカウントおよびユーザ証明書の作成などを行い，その後 VO 管理者がアカウント管理サーバから情報を参照し，VO サーバにユーザを登録して権限を付与したり，ポータルのアカウントを作成したりするというモデルになる．**図 3** は，以下のような構成を図示したものである．

- Account Server-1 と Account Server-2 の 2 つのアカウント管理サーバが存在する．
- VO Server-X は Account Server-1 の，VO Server-Z は Account Server-2 の，VO Server-Y は両方のアカウント情報を参照して VO メンバの登録，権限付与を行う．

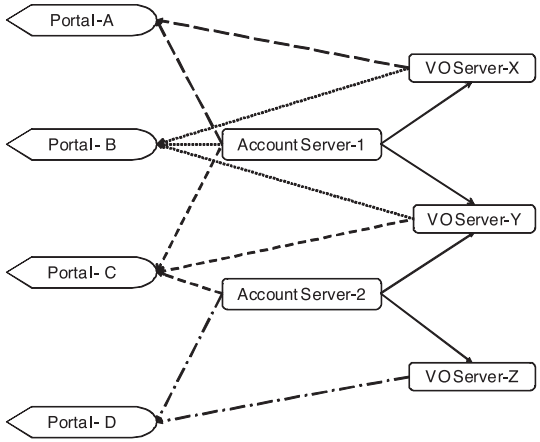

図 3　GEO Grid セキュリティにおける 3 つのコンポーネントの関係
Fig. 3　Three components of GEO Grid Security: portal, account server and VO server.

- Potral-A と Potral-B は Account Server-1 の，Potral-D は Account Server-2 の，Potral-C は両方のアカウント情報を参照してポータルアカウントを作成する．
- Potral-A は VO Server-X の，Portal-C は VO Server-Y の，Portal-D は VO Server-Z の，Portal-B は VO Server-X と VO Server-Y の VO 情報を参照し，属性を設定可能である．

本章で述べたセキュリティアーキテクチャは，GSI および VO レベルでの認可機構を基本とすることにより，複数の組織にまたがる資源への透過的なアクセスを実現するとともに，データ提供者に対し，ユーザ数に対してスケーラブルな管理コストで，データ提供ポリシを尊重した柔軟なアクセス制御を実現する仕組みを提供する．GSI が持つ権限移譲は多様なアクセスパターンによるデータや計算の統合を支援する．また，アカウント管理サーバとポータルを組み合わせ，ユーザに対して証明書や秘密鍵の管理を隠蔽することにより，簡便なインタフェースを提供する．

4. 実　　装

前章で述べた設計方針に基づき，我々はグリッド技術を用いて GEO Grid 情報基盤を実装する．実装コストの削減および他システムとの相互利用性を高めるため，我々は既存のツール，ソフトウェアを有効に利用して実装を進めている．本章では GEO Grid 情報基盤の実装について述べる．

4.1　VO サーバ

我々は VO サーバとして VOMS（VO Membership Service）を用いて VO レベルでの認可を実現する．VOMS は VO に所属するメンバを管理し，メンバの登録，グループの作成，ユーザに対する役割の付加などを行う．また，ユーザからの要求に応じて，ユーザのプロキシ証明書にユーザの VO における属性情報（所属する VO 名，グループ名，与えられている役割など）を埋め込んだ VOMS プロキシ証明書を発行する．サービス提供者側では，ポリシに応じた様々なアクセス制御が実現できる．たとえば，ある VO に属するすべてのユーザを単一のアカウントにマップすることにより，VO に所属するユーザ数にかかわらず，VO 単位でのアクセス制御を容易に実現できる．あるいは，ユーザの所属するグループや役割に応じたより柔軟なアクセス制御も実現できるが，この場合も LCAS および LCMAPS[9] などを用いることにより，各ユーザに対して個別のアカウントを作成する必要がない（LCMAPS の詳細は 5 章で述べる）．また，VO 属性は参照せずにユーザの認証情報のみを用いたアクセス制御や，フリーなサービスに対しては認証・認可を行わずにアクセスを許可することも可能である．

4.2　アカウント管理サーバとポータル

我々はサーバ側でユーザのアカウントおよび証明書を管理する仕組みを GAMA（Grid Account Management Architecture）を用いて実現する．GAMA はユーザに対してアカウントの作成依頼やログインなどの機能を，アカウント管理者に対してユーザ管理のための機能を，portlet として提供するソフトウェアである．ユーザのアカウントは GAMA サーバによって管理され，GAMA サーバはユーザに証明書を発行するための認証局の機能も備えている．

また，ユーザに対するポータルとして GridSphere を用いる．GridSphere は JSR168 に基づいた portlet を用いてポータルを構築するためのフレームワークであり，GAMA サーバからプロキシ証明書を作成するための認証モジュールと，ポータル管理者用の portlet が提供されている．

オリジナルの GAMA 認証モジュールは GAMA サーバからプロキシ証明書を取得するのみであり，VOMS とのインタフェースは提供されていないため，我々は GAMA サーバからプロキシ証明書を取得した後に，VOMS サーバに問い合わせて VOMS プロキシ証明書を作成するように GAMA 認証モジュールを修正した．また，ログインの際にはデフォルトの設定で VOMS Proxy 証明書が生成されるが，ログイン後に VO や属性を明示的に指定

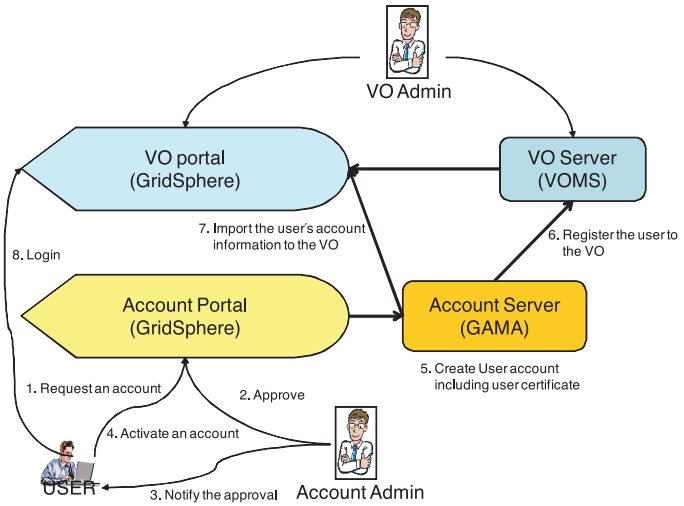

図 4　アカウント作成のフロー
Fig. 4　Procedure of the account creation.

して VOMS Proxy を再生成するインタフェースおよび機能も開発した．**図 4** に，GAMA と VOMS を用いたアカウント作成，VO への登録およびポータルアカウントの作成シナリオを示す．

(1)　ユーザはアカウント作成ポータル上でアカウント申請を行う．
(2)　アカウント管理者は申請を審査し，審査基準に従って受理/不受理を決定する．
(3)　申請が受理された場合はユーザにアカウントを作成するための Web ページの URL がメールで送られる．
(4)　ユーザは通知された Web ページ上でアカウントの作成を行う．Web ページへのアクセスは，アカウント申請の際に設定した PIN 番号により守られる．アカウント作成の際に，ユーザ名とパスワードを入力する．以後，このユーザ名とパスワードによりポータル上でログイン可能となるほか，このパスワードはユーザ証明書作成に際し，秘密鍵の暗号化にも用いられる．
(5)　GAMA サーバはユーザアカウントおよび秘密鍵とユーザ証明書を作成し，保持する．
(6)　アカウントが作成されたら，ユーザは VO 管理者にポータルアカウントの作成および VOMS サーバへの登録，権限付与を申請する．
(7)　VO 管理者はポータルアカウントを作成する．具体的にはアカウント管理サーバの情報をインポートすることにより，ポータルアカウントを作成する．また，VOMS サーバへの登録申請を審査し，ポリシに応じてユーザのグループへの登録および役割付与などを行う．
(8)　アカウントが作成後，ユーザはユーザ名とパスワードでシステムにログインする．その際に GAMA 認証モジュールがプロキシ証明書の作成と，それを用いた VOMS プロキシ証明書の作成を自動的に行い，認証に利用する．

4.3　サービス側のアクセス制御

GEO Grid 情報基盤においては，計算やデータなどのリソースはすべて標準的なプロトコルを用いて利用可能な「サービス」として提供される．我々は Globus Toolkit Version 4（GT4）[10] を用いてリソースをサービスとして構築する手段を提供する．計算リソースをサービスとして構築する方法としては，Apache Axis 上での Java Service として実装する方法や，汎用のジョブ管理サービスである GRAM を介して計算リソースを呼び出す方法があるが，現状では GRAM を用いて計算サービスを提供している．データリソースについては，OGSA-DAI を用いてサービスとして提供する．また，衛星データや地図情報の検索結果については，Web Map Service（WMS），Web Feature Service（WFS），および Web Catalogue Service（WCS）など，Open Geospatial Consortium（OGC）[11] によって規定されている Web サービスによって提供されるのが一般的である．そのため，サービス提供者側において，WS GRAM，OGSA-DAI [12]，および Apache などのウェブサーバ，およびファイル転送などのサービスが，VOMS プロキシによるアクセス制御を実現する必要がある．我々は WS GRAM，Pre-WS GRAM，GridFTP，Apache のいずれも VOMS を用いたアクセス制御機能を実現していることを確認した．Apache については，GridSite ツール[13] の 1 つとして提供されている mod_gridsite モジュールを採用した．OGSA-DAI については，現在開発中であり，ベータ版が評価用に提供されている Version 3.0 において，VOMS を用いたアクセス制御が実現されている．

4.4　各ソフトウェアコンポーネントの検証

GEO Grid 情報基盤の設計および実装の妥当性を検証するため，我々は GEO Grid 情報基盤で用いる主要ソフトウェアコンポーネントである GAMA，VOMS，OGSA-DAI，GT4，GridFTP および Apache with mod_gridsite の配備および検証を行った．我々が開発した GAMA における VOMS インタフェース拡張を組み込むことにより，GAMA と VOMS を用いたユーザアカウント管理および VOMS プロキシの生成が期待どおり実現できることを

確認した．また，GT4 WS GRAM，GT4 Pre-WS GRAM，GridFTP，OGSA-DAI および Apache with mod_gridsite のいずれにおいても，VOMS プロキシに埋め込まれた属性情報を用いたアクセス制御が実現できることを確認した．

5. 実システムの構築

我々は提案アーキテクチャに基づき，衛星データのひとつである ASTER（Advanced Spaceborne Thermal Emission and Reflection Radiometer）[14] データを主要コンテンツとしたシステムを実装した（**図 5**）．

本システムは，ASTER データ（Level 0 データ）を保存，提供する GEO Grid クラスタおよび GRAM や GridFTP サーバを介して GEO Grid クラスタへのアクセスを提供する gateway サーバ，ASTER データのメタデータやカタログを提供するサーバ，画像データを WMS として提供する Map Server，WFS，WCS などの高次データを提供する GIS サーバ，アカウント管理を行う GAMA サーバおよび VOMS サーバにより構成される．本システムにおいては，現在環境 VO，防災 VO，情報 VO の 3 つの VO が存在し，それぞれにおいて実際のユーザが利用する実運用を開始している．ASTER は NASA が打ち上げている Terra という衛星に搭載されたセンサであるが，実際には 2 台のセンサが備えられており，それらの観測結果をもとに地上の標高モデルを求めることができる．ASTER データは Terra の打ち上げ後 ERSDAC（Earth Remote Sensing Data Analysis Center）が管理するテープライブラリに保管され，有償データとしてユーザに提供されてきたが，昨年来産総研にもデータが提供され，産総研においては，ASTER データはテープライブラリではなくクラスタファイルシステムに保存されている．利用するクラスタ（GEO Grid クラスタ）は Giga-bit Ethernet で接続される 36 台の dual Xeon ノードにより構成され，全体で 264 TB の容量を備える．クラスタファイルシステムとしては Gfarm v1.4 [15] を用いている．現時点で約 140 TB の全 ASTER データが格納され，日々NASA から約 70〜100 GB のデータが転送され，GEO Grid クラスタに保存されている．メタデータの管理には PostgreSQL に対して GIS の拡張を行っている PostGIS を用い，メタデータは OGSA-DAI によりデータサービスとして提供される．また，データ処理には Giga-bit Ethernet で結合された 256 ノードの dual Xeon により構成される F32 クラスタを用いている．GEO Grid クラスタと F32 クラスタは 10 Giga-bit Ethernet で接続されている．

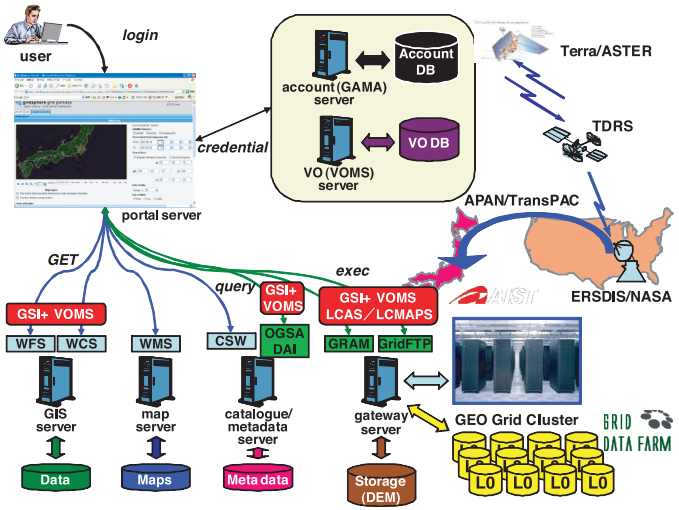

図 5　GEO Grid システムの構成
Fig. 5　Current configuration of the GEO Grid System.

本稿では，情報 VO の提供するアプリケーションである，産総研の ASTER データおよび MODIS（Moderate Resolution Imaging Spectroradiometer）[16] データと，台湾の NSPO が保持する Formsat2 のデータを同時に検索する Database 連携アプリケーション「DB 連携アプリケーション」を例に，システムの動作およびそこにおけるセキュリティコンポーネントの振舞いを述べる．

まず初めにユーザは，4.1.2 項で述べたようにアカウントを作成し，BIG VO の VOMS サーバへの登録およびポータルアカウントの作成を申請する．VO 管理者によりこれらの作業が終わった時点で，ユーザはポータルからログインできる．ログインすると，ポータルサーバ上にユーザの VOMS プロキシ証明書が自動的に生成される．DB 連携アプリケーションにおいては，ユーザは GUI 上で地域や時期，検索対象のデータベースを指定してデータを検索する（**図 6** 左上）．アプリケーションは指定されたデータのメタデータサーバを OGSA-DAI クライアントとして検索する．この際，GSI による認証および VOMS によるアクセス制御が行われる（図 6 中央）．検索結果は Database における画像の ID として返され，それをもとにサムネイル画像を生成し，ポータル上に表示する（図 6 右上）．

ユーザは，サムネイル画像を見ながら求める画像が見つかったら，そのデータに対する数値地形モデルを求め，取得するという操作を行う．ただし，現時点では Formsat2 については有料データが公開されていないため，これらの操作は ASTER データに対してのみとなっ

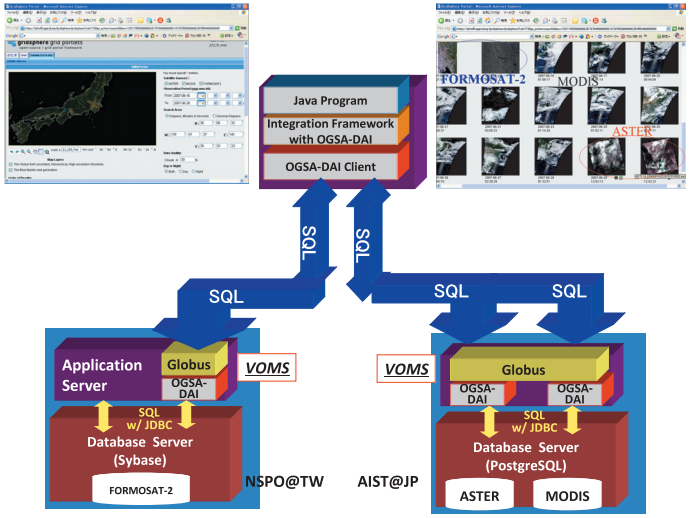

図 6　DB 連携アプリケーション
Fig. 6　DB federation.

ている．数値地形モデルの取得は，WS GRAM を用いて F32 クラスタ上で Level 0 データから数値地形モデルを求めるソフトウェアを実行することにより行う．この際，GEO Grid クラスタ上の Level 0 データは GridFTP により F32 クラスタに直接転送され，ユーザのクライアントマシンに中間データを転送する必要はない．

この WS GRAM および GridFTP の実行の際にも，GSI による認証および VOMS 属性による認可が行われ，ソフトウェアの実行権限のないユーザやデータへのアクセス権限のないユーザは実行できないようになっている．また，WS GRAM および GridFTP のいずれも，ローカルアカウントへのマッピングには LCMAPS を用いている．ユーザのアカウントを個別に作成するのではなく，プールアカウントを作成しておくと，LCMAPS がユーザの証明書に記載されているサブジェクト名や VOMS 属性（VO 名，所属グループ，権限など）に基づいて，自動的に一意にプールアカウントにマップする．初めてアクセスしてきたユーザの場合は未使用のプールアカウントにマップし，過去にアクセスしたユーザの場合はその際に割り当てられたアカウントにマップする．LCMAPS の利用により，サービス提供者はユーザごとのアカウントを作成しなくても，プールアカウントを（たとえばまとめて 1,000 個とか）作成しておくことにより，ユーザ単位のアクセス制御を実現することができ，容易かつスケーラブルなアクセス制御が実現される．

このように，「データの検索」「数値地形モデルへの変換」および「結果の転送」のそれぞれが個別のサービスとして実装され，それらが GSI および VOMS による認証認可をベースに連携することにより上位のサービスとして提供される．

なお，このほかにも ASTER データとフリーなセンサデータを連携させるアプリケーションや，検索結果を WFS で返すアプリケーションなどを通じ，提案したセキュリティアーキテクチャがアプリケーションおよびサービス提供者の要求に応じた適切なアクセス制御を実現することが確認された．

6. 考　　察

ここでは，今回のシステム構築および実運用を通じて得られた知見，考察を述べる．

各ソフトウェアコンポーネントの予備評価および ASTER Grid システムの開発・テストを通じ，我々は GEO Grid 情報基盤の設計および実装の妥当性を検証することができた．GAMA と VOMS を用いたセキュリティフレームワークにより，ユーザに対しては簡便なインタフェースを提供し，サービス提供者に対してはポリシに応じた柔軟なアクセス制御が実現可能であることが確認された．また，VOMS を用いた VO レベルでのアクセス制御により，ユーザ数に対してスケーラブルなセキュリティ機構が実現される．GAMA，VOMS，OGSA-DAI，Globus Toolkit など，既存のソフトウェアおよびツール群を利用することにより，少ない開発コストで実システムを構築することができた．アプリケーション用 portlet 以外に，情報基盤側で行った開発は VOMS と GAMA のインタフェースを GridSphere に組み込む部分のみであった．

ユーザ証明書および秘密鍵を集中管理サーバで管理するという方法については，「秘密鍵はユーザが秘密にしておく鍵」という PKI のコンセプトにそぐわないという指摘はある．しかし，3.3 節で述べたように，PKI に理解の浅いユーザに管理させるよりは，きちんとした方法で集中管理したほうがかえって安全であるということと，ユーザの手間を軽減するという理由により，今回のようなアーキテクチャとした．鍵生成の方法および管理方法は，証明書の保証レベルに影響を与えるものであるが，このようなアーキテクチャにおける証明書の保証レベルをきちんと定めることにより，世の中に広く受け入れられるアーキテクチャになると考える．この点について，我々は Open Grid Forum [17] や International Grid Trust Federation [18] において，「Portal-based Credential Services」の認証プロファイルおよび保証レベルを策定する活動を進めている．

また，ユーザ証明書を自分で管理・保持するユーザのために，クライアントマシン上のユーザ証明書から，delegation の機能を用いてポータルサーバ上に VOMS Proxy 証明書を生成する Java モジュールを実装し，システムに組み込んでいる．これにより，既存の保証レベルの高い証明書の利用を求める場合に対応することができる．

本セキュリティアーキテクチャにおいては，VO とポータルの関係を多対多とした．つまり，1 つの VO が複数のポータルを立ち上げてもよいし，1 つのポータルが複数の VO 情報を参照することも可能である．後者については，1 つのポータルにおいては，あくまでも 1 つの VO 情報のみ参照可能とするという選択肢もあった．その場合，たとえば ASTER と MODIS の両方を参照したい場合には，その両方を参照可能な VO を作成することになり，最悪 VO の組合せの数だけ VO を作成する必要が生じてしまうため，今回のような設計とした．ただし，複数 VO の取扱いについては「どれが正しい」といった正解はなく，アプリケーションの要求に応じて適切な設計をするべきである．また，複数 VO を取り扱う場合，ユーザが複数 VO を指定した際に，どれがプライマリ VO であり，どういった順番で VO 情報が設定されるかという点に留意する必要がある．今回の実装では，ローカルアカウントのマップに LCMAPS を用いているが，LCMAPS は VO 情報の順番にセンシティブであり，たとえばユーザが ASTER + MODIS という順番で VO 属性を設定した場合と，MODIS + ASTER という順番で VO 属性を設定した場合とでは，異なるローカルアカウントにマップされてしまう．特にストレージ領域への書き込みなど，ファイルのオーナのみがアクセスを許可されるような場合には，同じローカルアカウントにマップされる必要があるため，ユーザはプライマリ VO，プライマリグループを意識して VO 属性を設定する必要がある．これについては，ユーザに対して注意を喚起するほかに，システム的な対処を検討する予定である．

我々はポータルシステムとして GridSphere を採用している．これは，GridSphere が広く利用されており，すでに GAMA とのインタフェースも提供され，若干の修正を加えるだけで利用可能であったことが主たる理由である．しかし，アプリケーションの実装に際しては JSR168 に対応したポートレットを個別に開発する必要がある．アプリケーションの実装技術としては，Java Script や Ajax などを用いたマッシュアップによるものが広く利用されるようになっているが，それらの実装方法では，GSI が用いるプロキシ証明書を取り扱う機能（たとえば Web ブラウザをクライアントとして用いる場合，証明書ストアにプロキシ証明書を登録する機能）の実装が必要である．これらについては今後の研究課題としている．

本稿で述べたセキュリティアーキテクチャは，単一アカウントへのマッピング，LCMAPS を用いたプールアカウントへの個別マッピング，および通常の GSI によるアカウントマッピング（各ユーザをプールアカウントではなく，既存のアカウントにマッピングする）など，複数のマッピング方法をサービス提供者のポリシに応じて採用することができる．たとえば計算サービスを提供する計算機にユーザが直接ログインしてシミュレーションコードの開発，実行をするようなレガシィな利用形態を実現する場合には，現状では通常の GSI によるアカウントマッピングを行う必要がある．しかし，VOMS および LCMAPS を用いたアカウントマッピングが可能な SSH が開発されれば，上記のようなレガシィな利用に対しても，LCMAPS によるプールアカウントへの自動マッピング機能を用いることができると考える．

7. 関 連 研 究

e サイエンスに関する研究は，英国における UK-eScience [19]，米国における Network Earthquake Engineering System [20]，Earthsystems Grid [21]，Open Science Grid [22]，欧州における Enabling Grid for E-Science in Europe（EGEE）[23] など，2000 年頃より活発に行われている．今回の実装に利用した VOMS も EGEE が開発したソフトウェアであり，EGEE の中の様々な研究グループが VOMS を用いた認可機構を導入している．ただし，EGEE においては，ユーザ証明書は各ユーザがクライアントマシン上で生成・管理することを求める，IGTF Classic Authentication Profile [24] にのっとった証明書の利用を前提として各国間での相互信頼を確保しており，集中管理サーバがユーザ証明書などを管理するモデルはない．いくつかのプロジェクトはポータルを提供しているが，これらのポータルは事前にコマンドラインから MyProxy のコマンドを実行し，MyProxy サーバにプロキシ証明書をストアしておくことを前提にしており，ユーザは証明書管理およびプロキシ証明書作成コマンドなどの環境が手元にあることが求められる．

その一方，Earthsystem Grid などの米国のプロジェクトでは，我々のアプローチのように集中管理サーバを用いてユーザ証明書などを管理するポータルの利用が主流となっている．アカウント管理サーバとしては，我々が用いた GAMA のほかに，アルゴンヌ国立研究所で開発している Portal-based User Registration Service（PURSE）[25] が用いられる．しかし，これらのプロジェクトでは，GEO Grid のように必要サービスを組み合わせて VO を構成し，VO 単位での認可を行うといったことはせず，GSI に基づく認証を行い，認可についてはユーザ単位で行うか，複数のユーザを単一のアカウントにマップしてしまうといったいくつかの方法に限られており，サービス提供者のポリシに応じた柔軟なアクセス制御は

実現されていない．複数のユーザを単一のアカウントにマップした場合，同時に複数のユーザがアクセスした場合にファイルの読み書きなどに競合が発生する可能性があるが，それについてはサンドボックス機能を用いた競合回避に関する研究などが行われている．GEO Grid においては，管理コストの削減を優先する場合は複数のユーザを単一のアカウントにマップし，ファイルアクセスの競合など，アカウントを共有することによる問題を回避する場合には LCMAPS を用いて異なるアカウントにマップするなど，サービス提供者の要望に応じた実装方法が選択可能である．また，LCMAPS を用いることにより，個別のアカウントにマップする場合でも管理コストは低く保たれる．

このように，各コミュニティの利用シナリオ，ユーザベースなどに応じてセキュリティアーキテクチャの設計および実装が異なっているが，本稿で述べた VO の考え方およびセキュリティアーキテクチャの設計と実装は，多様なデータの中から必要なものを組み合わせて研究環境を構築し，多数のユーザに提供するというシナリオに基づくものであり，この範疇に入る応用分野は多岐にわたると考える．

8. まとめと今後の課題

本稿では GEO Grid 情報基盤の設計と実装，および実システムの運用を通じて得られた知見について報告した．e サイエンスにおける VO の考え方やアカウント管理，認証・認可の実現方法を明確に論じた．GEO Grid 情報基盤においては，計算およびデータリソースはすべて標準的なプロトコルにより利用可能なサービスとして提供される．研究コミュニティは VO を構成し，必要なサービスを組み合わせて VO 内のユーザに提供する．VOMS 属性を用いた認可機構により，サービス提供者のポリシに応じた柔軟なアクセス制御および VO 単位での認可による，ユーザ数に対してスケーラブルなセキュリティ基盤が実現される．

今後さらに運用を通じてシステムのブラッシュアップおよび本システムを容易に配備，利用するためのツールキットの開発などを進めていく予定である．

謝辞　本研究は，GEO Grid プロジェクトにおいて応用分野の研究者と情報分野の研究者がシステム要件や解決方法などについて活発に意見交換を行いながら進められた．GEO Grid プロジェクトに参画する全研究者に感謝の意を表する．UK e-Science Centre の Neil Chue Hong 博士および OMII Europe の Valerio Venturi 博士には，OGSA-DAI についてご助言などをいただいた．産業技術総合研究所 Steven Lynden 博士には，OGSA-DQP について有益な議論をしていただいた．また，Dutch National Institute for Nuclear and High Energy Physics の David Groep 博士には，VOMS，LCAS/LCMAPS，Gridsite などについて様々なご助言をいただいた．ここに，感謝の意を表する．なお，本研究の一部は NEDO 国際共同研究助成事業「e インフラストラクチャ構築のための国際標準セキュリティポリシ策定事業」による．

参 考 文 献

1) 田中良夫，小島　功，山本直孝，横山昌平，谷村勇輔，関口智嗣：GEO Grid：地球観測グリッドの設計と実装，情報処理学会 HPC 研究会研究報告，Vol.2007, No.88, pp.37–42 (2007).
2) Foster, I. and Kesselman, C. (Eds.): *The Grid: Blueprint for a New Computing Infrastructure*, 2nd edition, Morgan Kaufmann Publishers (2004).
3) Foster, I., Kesselman, C., Nick, J.M. and Tuecke, S.: *The physiology of the Grid*, Wiley (2003).
4) Sundaram, B.: Introducing GT4 Security, IBM developerWorks (2005).
5) Alfieri, R., Cecchini, R., Ciaschini, V., Spataro, F., dell'Agnello, L., Frohner, A. and Lőrentey, K.: From grid-mapfile to VOMS: managing authorization in a Grid environments, *Future Generation Computer Systems*, Vol.21, No.4, pp.549–558 (2005).
6) Novotny, J., Tuecke, S. and Welch, V.: An Online Credential Repository for the Grid: MyProxy, *10th International Symposium on High Performance Distributed Computing*, pp.104–111 (2001).
7) Bhatia, K., Chandra, S. and Mueller, K.: GAMA: Grid Account Management Architecture, *IEEE International Conference on e-Science and Grid Computing*, pp.413–420 (2005).
8) Novotny, J., Russell, M. and Wehrens, O.: GridSphere: An advanced portal framework, *30th Euromicro Conference*, pp.412–419 (2004).
9) Cornwall, L., Jensen, J., Kelsey, D.P., Frohner, A., Kouril, D., Bonnassieux, F., Nicoud, S., Lorentey, K., Hahkala, J., Silander, M., Cecchini, R., Ciaschini, V., dell'Agnello, L., Spataro, F., O'Callaghan, D., Mulmo, O., Volpato, G.L., Groep, D.L., Steenbakkers, M. and McNab, A.: Authentication and Authorization Mechanisms for Multi-Domain Grid Environments, *Journal of Grid Computing*, Vol.2, No.4, pp.301–311 (2004).
10) Foster, I.: Globus Toolkit Version 4: Software for Service-Oriented Systems, *IFIP International Conference on Network and Parallel Computing*, Vol.3779, LNCS, pp.2–13 (2006).
11) Open Geospatial Consortium. http://www.opengeospatial.org/
12) Antonioletti, M., Atkinson, M., Baxter, R., Borley, A., Hong, N.C., Collins, B., Hardman, N., Hume, A., Knox, A., Jackson, M., Krause, A., Laws, S., Magowan,

J., Paton, N., Pearson, D., Sugden, T., Watson, P. and Westhead, M.: The Design and Implementation of Grid Database Services in OGSA-DAI, *Concurrency and Computation: Practice and Experience*, Vol.17, Issue 2-4, pp.357–376 (2005).
13) McNab, A.: The GridSite Web/Grid security system, *Software: Practice and Experience*, Vol.35, Issue 9, pp.827–834 (2005).
14) Yamaguchi, Y., Kahle, B.A., Pniel, M., Tsu, H. and Kawakami, T.: Overview of Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER), *IEEE Trans. Geoscience and Remote Sensing*, Vol.36, No.4, pp.1062–1071 (1998).
15) Tatebe, O., Morita, Y., Matsuoka, S., Soda, N. and Sekiguchi, S.: Grid Datafarm Architecture for Petascale Data Intensive Computing, *International Symposium on Cluster Computing and the Grid*, pp.102–110 (2002).
16) Justice, C., Vermote, E., Townshend, J.R.G., Defries, R., Roy, D.P., Hall, D.K., Salomonson, V.V., Privette, J., Riggs, G., Strahler, A., Lucht, W., Myneni, R., Knyazihhin, Y., Running, S., Nemani, R., Wan, Z., Huete, A., van Leeuwen, W. and Wolfe, R.: The Moderate Resolution Imaging Spectroradiometer (MODIS): Land remote sensing for global change research, *IEEE Trans. Geoscience and Remote Sensing*, Vol.36, No.4, pp.1228–1249 (1998).
17) Open Grid Forum. http://www.ogf.org/
18) International Grid Trust Federation. http://www.igtf.net/
19) UK e-Science. http://www.rcuk.ac.uk/escience/default.htm
20) NEES Cyberinfrastructure Center. http://it.nees.org/
21) Earth System Grid. http://www.earthsystemgrid.org/
22) Open Science Grid. http://www.opensciencegrid.org/
23) Enabling Grids for E-sciencE. http://public.eu-egee.org/
24) European Grid Policy Management Authority. http://www.eugridpma.org/
25) Portal-based User Registration Service. http://www.globus.org/grid_software/security/purse.php

(平成 20 年 1 月 29 日受付)
(平成 20 年 5 月 5 日採録)

田中　良夫（正会員）

昭和 40 年生．平成 7 年慶應義塾大学大学院理工学研究科後期博士課程単位取得退学．平成 8 年技術研究組合新情報処理開発機構入所．平成 12 年通産省電子技術総合研究所入所．平成 13 年 4 月より独立行政法人産業技術総合研究所．現在同所情報技術研究部門主幹研究員．博士（工学）．グリッドにおけるプログラミングミドルウェアおよびグリッドセキュリティに関する研究に従事．IC 1999，HPCS 2005，SACSIS 2006 最優秀論文賞，2006 年度情報処理学会論文賞．ACM 会員．

山本　直孝

昭和 49 年生．平成 11 年東京理科大学大学院理学研究科物理学専攻修了．同年東京理科大学理学部第二部物理学科助手．平成 14 年 10 月独立行政法人産業技術総合研究所グリッド研究センター特別研究員．平成 16 年 7 月同所入所．平成 20 年より同所情報技術研究部門研究員．博士（理学）．グリッドにおけるミドルウェア，アプリケーションへの応用に関する研究に従事．

関口　智嗣（正会員）

昭和 34 年生．昭和 57 年東京大学理学部情報科学科卒業．昭和 59 年筑波大学大学院理工学研究科修了．同年電子技術総合研究所入所．情報アーキテクチャ部主任研究官．以来，データ駆動型スーパコンピュータ SIGMA-1 の開発等の研究に従事．平成 13 年独立行政法人産業技術総合研究所に改組．平成 14 年 1 月より同所グリッド研究センターセンター長．平成 20 年 4 月より同所情報技術研究部門長．並列数値アルゴリズム，計算機性能評価技術，グリッドコンピューティングに興味を持つ．市村賞受賞．日本応用数理学会，ソフトウェア科学会，SIAM，IEEE 各会員．