

全国共同利用環境へのグリッドミドルウェアの適用

坂根 栄作[†] 東田 学[†] 岡村 真吾[†] 寺西 裕一[†] 秋山 豊和[†]

馬場 健一[†] 下條 真司[†]

[†] 大阪大学サイバーメディアセンター 〒567-0047 大阪府茨木市美穂ヶ丘 5-1

E-mail: †{sakane,manabu,okamura,teranisi,akiyama,baba,shimojo}@cmc.osaka-u.ac.jp

あらまし 大阪大学サイバーメディアセンターでは、全国共同利用施設である大規模計算機システムにNAREGI グリッドミドルウェアを導入し、グリッド技術を利用できるようにする一方で、グリッド技術を用いない従来の運用形態も維持し、それらを両立する。本稿では、既存のシステムにグリッドミドルウェアを適用する上での問題点を述べ、課金、認証、証明書発行、ユーザ管理、計算資源管理等における適用手法を示す。

キーワード グリッドミドルウェア

An application of grid middleware to a nationwide joint-use environment for computing

Eisaku SAKANE[†], Manabu HIGASHIDA[†], Shingo OKAMURA[†], Yuuichi TERANISHI[†],

Toyokazu AKIYAMA[†], Ken-ichi BABA[†], and Shinji SHIMOJO[†]

[†] Cybermedia Center, Osaka University 5-1 Mihogaoka, Ibaraki, Osaka, 567-0047 Japan

E-mail: †{sakane,manabu,okamura,teranisi,akiyama,baba,shimojo}@cmc.osaka-u.ac.jp

Abstract In the Cybermedia Center, Osaka University, we introduce the NAREGI grid middleware to our latest large-scale computing system for nationwide joint-use, and make grid computing technology available on them. At the same time, we keep the past operation style to compatible with the grid computing technology. In this paper, we mention the acquiring problems on accounting, authentication, issuing certificate, user management and resource management through the introduction process of the grid middleware to our system, and discuss solutions for them.

Key words grid middleware

1. はじめに

近年、大規模かつ高性能な計算機システムへの需要は、一組織あるいは一機関で賄いきれないほどの物量にまで拡大している。複数組織・機関を跨る計算資源の共有化を実現し、より大規模な計算環境を提供する技術としてグリッドコンピューティングが注目を集めている。グリッドコンピューティングは、大雑把に言えば、実際の計算資源が何処にあるかをユーザが意識することなくその資源を利用できるようにする技術であり、その実現には、複数の計算資源が連携し仮想化される必要がある。このように計算資源を共有する利点は、大規模な計算能力を有するシステムの提供にとどまらず、複数の組織に跨る研究開発プロジェクトにおけるデータ共有のための基盤を提供し、ひいては組織そのものの仮想化を促す。学界に依らず、産業界の様々な分野にグリッドコンピューティング技術の応用が期待

されている。

大阪大学サイバーメディアセンター(CMC)では、国立情報学研究所(NII)が推進するCSI(Cyber Science Infrastructure)構想の一環として、国立情報学研究所グリッド研究開発拠点[1]において研究開発が行なわれているNAREGIグリッドミドルウェアによるグリッド実験環境を構築し、その実証評価実験としてe-Science研究分野への支援活動を行なった。

CMCは、全国共同利用施設としてベクトル型スーパーコンピュータを始めとする大規模計算機システムを全国の大学研究者に提供している。上述の情勢を踏まえ、全国共同利用施設という観点から考えれば、保有する計算資源のグリッドコンピューティング技術による共有化は積極的に推進されなければならない。CMCでは、平成18年度にスーパーコンピュータシステムおよび汎用コンピュータシステムの調達を行ない、新システムの導入にあわせてグリッドコンピューティング環境の構

築を計画した。これにより他センターの計算資源の連携が容易になり、接続形態の変更などにも柔軟に対応できるようになる。

グリッドコンピューティングを実現するミドルウェアとしては、NAREGI グリッドミドルウェアを採用し、特に今回導入した新システム群においては、平成 19 年 5 月にリリース予定のバージョン β2 を導入するための開発を進めている。NAREGI グリッドミドルウェアのユーザインターフェイスはウェブベースである。ユーザにとって親しみやすいものであると考えられる一方で、従来のキャラクタベースのインターフェイスに慣れたユーザに対して、必ずしも開発効率の向上を約束するものではない。新たなインターフェイスへの一方的な移行を強いることなく、従来のインターフェイスとの両立という過程を経て、グリッドコンピューティング環境の普及を目指さなくてはならない。

本稿では、CMC における従来の運用形態を維持しつつ、NAREGI グリッドミドルウェアを導入し運用していくために、基本的な運用ポリシー、それに反する問題点を述べ、それらを解決する手法ならびにグリッドコンピューティング環境構築に際する固有の問題について報告する。

2. NAREGI グリッドミドルウェア

NAREGI グリッドミドルウェア (以下、単に NAREGI と呼ぶ) は、国立情報学研究所グリッド研究開発拠点において研究開発されているグリッドミドルウェアであり、以下の特長を持つ；

- プラットフォームは Globus Toolkit 4-WSRF [2]
- OGF OGS-EMS ベースの資源管理機構
- VO 機能の一部サポート
- OGF-ACS 標準の WS-Application/Deploy 機能
- データグリッド機能
- NAREGI-WFML による複雑な連成アプリケーションの簡便記述

- GridMPI の完成 / GridRPC の Globus 4 対応
- 他のグリッド基盤と互換性の高いセキュリティ機構

ここでは、後の議論に必要となるものを主に列挙した。

NAREGI の資源管理機構は、Super Scheduler (SS)、Information Service (IS)、GridVM (Grid Virtual Machine) サーバが担う。

SS は利用可能な資源を自動的に探索、予約を行ない、ジョブを実行する。IS は各計算資源の情報を管理する。GridVM サーバは計算資源を仮想化し SS からのジョブ実行要求に応答し、ローカルスケジューラに引き渡す。

グリッド環境においては、VO (Virtual Organization) が重要である。この機能によってユーザおよび計算資源の組織単位での管理が可能となり、全国に点在する研究者および施設からなる研究コミュニティをグリッド環境上に仮想的に組織することができる。NAREGI においては、VOMS (Virtual Organization Membership Service) サーバによって実現される。

ユーザから見れば、NAREGI はウェブサービスとして提供される。アプリケーションの登録および計算資源への展開、一連のジョブを記述するワークフローの作成および実行は、NAREGI

ポータルから行なわれる。

NAREGI における認証は、X.509 証明書に基づく公開鍵認証基盤 (PKI) を用いて行なう。NAREGI では、認証局を構築するためのソフトウェアである NAREGI-CA が提供されている。NAREGI β2 では、ユーザの鍵ペアおよび証明書を UMS (User Management Server) に集中管理することで、ユーザの利用端末を限定しない環境を提供している。UMS に格納された自身の鍵ペアおよび証明書をを用いてさらに鍵ペアおよび証明書 (プロキシ証明書) を発行し MyProxy サーバに格納する。この鍵ペアおよびプロキシ証明書はグリッド環境における認証および権限委譲に用いられる。

3. CMC の大規模計算機システム

CMC では、平成 19 年 1 月に行なったスーパーコンピュータ・システムの更新において、NEC 製のベクトル型スーパーコンピュータ SX-8R を 20 ノードを導入するとともに、インテル社製 Dual-Core Xeon プロセッサを 2 基ずつ搭載する PC クラスタ (SUSE Linux, kernel-2.6) を 128 ノードを導入した。前者の総演算処理能力は 5.3TFLOPS、総メモリ容量は 3TB であり、後者の総演算処理能力は 6.1TFLOPS、総メモリ容量は 2TB である。ベクトル型スーパーコンピュータと PC クラスタによる連成シミュレーションを容易にするため、総容量 250TB のストレージを FibreChannel による SAN で共有している。これらの計算資源は平成 20 年 8 月に中間増強を行なう。

これに加えて、同年 3 月には、情報処理教育および CALL (Computer Assisted Language Learning) 用途を主目的とする PC ワークステーションを中心とする汎用コンピュータ・システムを導入し、教育用途の遊休時には約 500 ノードの PC クラスタとして全国共同利用システムの計算資源として活用できるシステム構築を行なった。総演算処理能力は 18.3TFLOPS、総メモリ容量は 1TB であり、全てのノードを TOE 機能を有する 10Gbps Ethernet NIC でクラスタリングしている。

CMC では、前スーパーコンピュータ・システム (平成 13 年から平成 18 年まで) の運用において、階層型グループ管理が可能なフェアシェア型スケジューラである NEC 社製 ERS (Extended Resource Scheduler) を採用し運用実績を重ねてきた。同時に、それに基づくフェアシェア型定額利用制度を導入し、特に大規模利用を行なうグループに対して従量制課金からの移行を促進した。従来の閑散期における投機的な先行利用を促す効果が顕著であり、かつ、長期的なグループ間の利用実績の公平性が保たれていることが統計情報からも実証されている。この実績を受けて、本システムからは小額利用においても従量制課金を廃した。さらに、ベクトル型スーパーコンピュータと PC クラスタを同一のフェアシェア・スケジューラの配下として、異機種混在環境においても出資比率に応じた利用実績の公平性が確保され、結果として連成シミュレーションを容易とするシステム構築を目指した。

このようなフェアシェア・スケジューラによるジョブ実行の優先制御は、ジョブの実行開始や終了時期が不確定となりうる潜在的な問題を有し、実際にユーザへの不利益を強いていた。

これを解消するため、フェアシェア・スケジューリングと同時にバックフィル型の事前ジョブ割当て機能を提供する NEC 社製 NQS II および JobManipulator オプションを導入し、中短期的なジョブの実行予約機能を導入することで解消を計った。この導入には、ジョブの予約機能を必須とするグリッドコンピューティング環境への資源提供も視野に入れている。

大規模計算機システムにおける認証システムは、Microsoft 社製 Active Directory サーバを中核とする Kerberos 認証システムを採用した。SPNEGO 方式 (IETF/RFC4559) によるクライアント側からのネゴシエーションによって、現時点で流通するほとんどすべてのクライアント OS と Web ブラウザの組合せにおいて各サーバへのシングル・サインオンを実現する。また、Kerberos 認証においては、認証に必要な情報管理と個々の認証作業そのものを KDC (Key Distribution Center) が集中して管理するが、KDC のセキュリティ・レベルを高めることによって認証情報の漏洩のリスクを抑えることが可能となる。

4. グリッドミドルウェアの適用手法

本節では、CMC における大規模計算機システムへの NAREGI の適用手法を述べる。前節までで説明したとおり、適用システムは以下の特徴をもつ；

- NQS II によるフェアシェア/バックフィル・スケジューリング
- Kerberos による認証システム

このシステムに NAREGI β2 を適用する上での問題点を洗い出し、それらの対応法を述べ、続いてグリッド環境構築固有の問題についての対応を議論する。

4.1 スケジューラ

前述のように、フェアシェアおよびバックフィル・スケジューリングを実現する NQS II は、ベクトル型スーパーコンピュータ SX-8R だけではなく PC クラスタ (GNU/Linux) にも導入され、利用面と運用管理面の両方において資源アーキテクチャに依らない統一的なインターフェイスを提供し、ユーザによる容易な連成シミュレーションを可能としている。

NAREGI β2 においては、標準的に対応するローカルスケジューラが数種類に限定されており、SX-8R の OS である SUPER-UX 上で動作する NQS II には対応するが、Linux (kernel-2.6) 版の NQS II には対応していない。CMC が運用する PC クラスタにおいて、NAREGI β2 が対応するローカルスケジューラによる運用を NAREGI ミドルウェア導入の必須要件としてしまうと、次のような問題に直面する。

まず、CMC の運用においては、従来型の利用に対する利便の提供を最優先課題としており、同一のローカルスケジューラによるベクトル型スーパーコンピュータと PC クラスタの連成シミュレーションを必須条件とすれば、PC クラスタのスケジューラを NQS II から変更することは極めて難しい。

この場合は、NAREGI ミドルウェアを運用するノードを特定し、それぞれのスケジューラが管理するノード資源を分割ことによって問題を解消することが一般的である。しかし、このような静的な資源分割は、資源の効率的な利用を阻害する主要

因となり得ると同時に、さらに NAREGI 利用のための専用課金制度の整備を要求する。ローカルスケジューラを従来運用方式に則ったものに統一すれば、NAREGI ミドルウェア運用における課金を従来型運用システムに委譲できることになる。また、NAREGI を利用しないユーザだけでなく、NAREGI を利用するユーザの間でも不公平を生じない課金制度の確立は難しい。NAREGI 占有環境のユーザ数と非 NAREGI 環境のユーザ数は同じではないことが予想されるため、効率よくユーザのジョブを処理するためにはどの割合で資源を分割すべきかも見積もることも難しい。

これらの問題を解決するためには、Linux 版の NQS II を NAREGI の資源管理機構に組み込めるスケジューラとして対応させるのが自然である。CMC では、NQS II の Linux 版を GridVM に対応させるべく改良を行ない、同時に計算資源の情報を IS に提供するクライアントの開発を行なっている。

4.2 認 証

CMC が採用した Kerberos 認証と NAREGI の認証システムの連携は、標準的には対応されていない。

NAREGI β2 で提供されるポータルでの運用では、NAREGI へのアクセス方法を既存のシステムから独立させる必要が生じる。これは、基本的にユーザに対して Kerberos のチケット入手用と NAREGI ポータルへのアクセス用の複数のユーザ ID とパスワードの管理を強いることになる。ユーザはどちらか一方の利用形態に固定されるとは考え難く、状況に応じて利用形態に選択肢を残すことが望ましい。しかし、同じ計算資源を利用するにも関わらず、利用形態の違いから生じる複数の ID 管理は好ましいものではない。一方で、NAREGI ポータルによる一元化も、従来ユーザに移行に伴う労力を要求することになり、また、NAREGI β2 のポータルが提供する機能だけでは従来のコマンドラインインターフェイスでの作業と同等のことができないことから、現実的には採用し難い。

更に、NAREGI β2 環境へのログインには

- UMS へのログイン (ユーザ ID とパスワード)
- プロキシ証明書発行 (パスフレーズ)
- プロキシ証明書とペアとなる秘密鍵の活性化 (パスフレーズ)

を必要とする。一度プロキシ証明書を発行すれば、それが有効な間は最初の 2 つのプロセスを省略できるが、これら一連のプロセスはユーザの利便性を損なっていると言わざるを得ない。

これらの問題を解決する 1 つの方法は、Kerberos クレデンシャルによる NAREGI ポータルへのシングル・サインオン対応とユーザ証明書およびプロキシ証明書の自動発行機能を追加することである。CMC では、APGrid に準拠した CP/CPS を尊重しつつ、NAREGI ポータルを通した UMS のログインを Kerberos チケットで行なえるように改良を行なった。ユーザ証明書自動発行機能およびプロキシ証明書によるグリッド環境へのサインオンは次小節でユーザ管理とともに述べる。

4.3 ユーザ管理

本小節以降は、NAREGI 環境を構築する上で固有の問題を取り扱う。

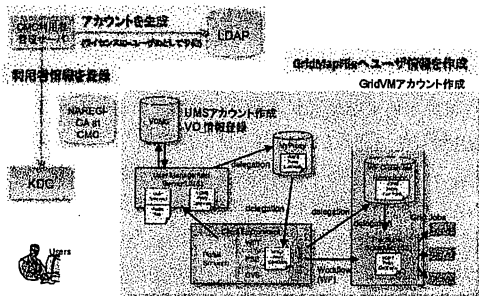


図 1 利用申請

ユーザが NAREGI を利用できるまでに必要なシステム側の作業は、CMC 利用者管理サーバから Kerberos の KDC への利用者情報の登録に加えて、UMS への証明書格納準備、VO 情報の登録、計算資源 (GridVM) のアカウント作成である (図 1)。

ユーザ証明書の発行は、一般的には、ユーザからの証明書発行要求に対して登録局が申請者の本人性を確認し、その後発行局にて証明書を発行するという手続きを踏む。CMC では、全国共同利用システムの利用申請があれば NAREGI を利用するか否かにかかわらず従来の手続きの範囲で本人性の確認を行ない、証明書の発行に必要なライセンス ID をユーザ ID などの基本情報とともに LDAP に登録する。同時に証明書の格納先である UMS のユーザアカウントの作成も行なう。これでシステム的には全てのユーザに対して何時でも証明書を発行できる状態になる。このような対応の目的は、グリッドコンピューティングを気軽に試用してもらうための、事務的手続きの簡略化である。実際に証明書を発行する／しないはユーザの判断に委ねられる。

VO に関しては、ユーザの VO 所属情報が VOMS に登録される。そもそものように VO を構成するかという重要な問題があるが、これに関しては次小節で述べる。

計算資源に対しては、計算資源全ノードにおいてアカウントを作成し、このアカウントと証明書の Subject を結びつける grid-mapfile を作成する必要がある。

以上の一連の作業は UMS, VOMS, GridVM 上で行なわれるが、これらを自動化する管理システムは非常に有益と考えられる。CMC では、このような運用管理システムにおいて、特にユーザ管理機能を重点的に開発設計した。この管理システムは、CMC 固有の問題への対応部分を切り離すことで、汎用的な NAREGI 環境へ適用可能である。

ユーザ証明書の発行プロセスは以下のとおりである (図 2)。

ユーザは KDC からチケットを得て NAREGI ポータルにアクセスする。ユーザ証明書の発行はポータルから実行できる。鍵ペアが生成され秘密鍵は UMS に格納される。LDAP 上のユーザ情報 (ライセンス ID と SubjectDN) とあわせて認証局へ証明書発行指示をし証明書を UMS に格納する。秘密鍵はパスフレーズによって暗号化されるが、このパスフレーズにはユーザ ID と適当な salt から一意に自動生成されるランダムな文字列を利用し、ユーザの入力を要求しない。

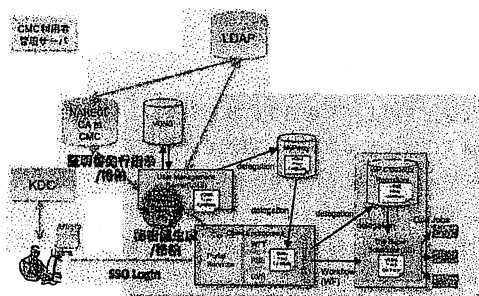


図 2 ユーザ証明書発行

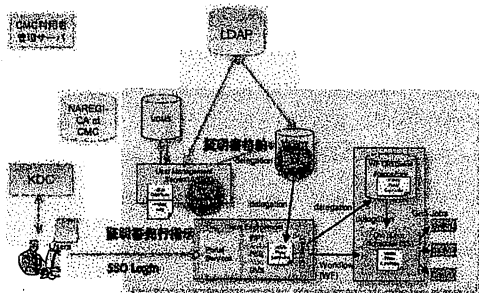


図 3 プロキシ証明書発行

プロキシ証明書の発行プロセスは以下のとおりである (図 3)。

ユーザは Kerberos のチケットで NAREGI ポータルにアクセスし、プロキシ証明書の発行要求をポータルから行なう。鍵ペアの生成および UMS のユーザ証明書により署名が行なわれ MyProxy サーバへ格納される。ここでもプロキシ証明書のペアである秘密鍵のパスフレーズはシステムが一意に自動生成し、ユーザはパスフレーズの管理を必要としない。

4.4 VO

NAREGI の仕様として、ユーザは必ず VO に所属しなければならない。したがって、NAREGI 環境を構築する上でどのような VO を立ち上げるかという問題が生じる。NAREGI において VO を構成するのは、ユーザ、リソースプロバイダおよび VO 管理者である。CMC では、ユーザは阪大の大規模計算システム利用者とし、リソースプロバイダならびに VO 管理者は CMC とする構成で VO を立ち上げる。この構成はセンターにおける基本的なものと考えられる。リソースプロバイダとして連携機関を加えることによって、ユーザの需要に柔軟に応えられる計算システムの提供が可能になり、あるいは CMC が別の組織が運用する VO にリソースプロバイダとして参加することによって計算資源を他の VO へ提供することが可能になる。

4.5 認証局

将来的に海外の研究機関との連携を行なうには、認証局のプロダクションレベルの運用が求められる。プロダクションレベルを定義するものとしては、APGrid PMA [3] の Minimum CA Requirements があり、これには認証局と登録局への要件が記述されている。日本では、産総研、NAREGI、KEK それぞれの運用する認証局がプロダクションレベルとして APGrid PMA から認定されている。近い将来の国際連携を見据え、CMC で

は、センター内に物理的に高度なセキュリティレベルの専用室を建設した。そこにサーバを設置し NAREGI-CA 2.2 で認証局を構築する。

認証局を運用していくには物理的要件だけではなく、CP/CPS (Certificate Policy/Certificate Practice Statements) が重要である。CMC では、APGrid PMA の管理する Minimum CA Requirements を満たすように CP/CPS の作成および運用体制の確立を目指したが、残念ながら完全に準拠するようにはできなかった。問題となったのは本人性の確認である。APGrid の要件では対面により本人確認をしなければならないが、センターの利用申請においては本人性の確認は利用申請時に行なうことが考えられるが、現状ではそれは書類審査により行なわれ、申請者は必ずしも利用申請受付窓口まで来る必要がない。書類審査では支払責任者と経理責任者（申請者の同一部局に所属）の押印が確認される。対面による本人性の確認を行なうにはユーザが窓口までくるか、登録局の運用要員が出向くかである。前者で対応できないユーザに対しては、後者で対応することが考えられるが、実際に運用要員が出向かなくても申請書類にある経理責任者が対面でもって申請者本人の確認を行なうことで、対面による本人性の確認を担保できる。しかしながら、課金の発生しない試用制度を利用するユーザには経理責任者の確認は不要なため、対面による本人性の確認を担保できない。

CMC では、差し当たり対面による本人性確認を担保しないで運用を開始する予定である。だが、この問題は国際連携と言わないまでも産総研、NAREGI、KEK との国内連携において解決すべきものである。

証明書のプロファイルに関しては、Minimum CA Requirements に従っている限り問題はほとんどない。ユーザ証明書の有効期間は 13ヶ月以内であり、これは年度毎に利用申請を行なう現在の運用にうまく適合する。但し、計算資源に対する証明書（ホスト証明書）も同様に有効期限は 13ヶ月以内であり、静的にリソースプロバイダとして振る舞う組織にしてみれば、もう少し長い有効期限を設定したいところである。

4.6 Campus PKI 連携

阪大では全学 IT 認証基盤を構築し、平成 19 年 1 月よりサービスを開始している。既存システムの SSO 対応を順次進めており、また、全学展開への試金石としてトライアル IC カード実験を行なっている。

UPKI (University Public Key Infrastructure) [4], [5] の基本構想では、PKI ドメインを Public PKI, Campus PKI, Grid PKI の層に分け、それぞれにおいて信頼モデル、証明書用途などが定義されている。阪大では、Campus PKI が全学 IT 認証基盤であり、前小節で構築される認証局による認証ドメインが Grid PKI に相当する。このアーキテクチャでは大学間連携は Campus PKI で実現される。したがって、Campus PKI と Grid PKI の連携は重要になる。

Campus PKI のユーザ ID を持つユーザが、Grid PKI を新たに利用する際、Grid PKI のユーザ ID を意識せずともサービスを発行・利用できることが望ましい。しかし、Grid におけるユーザ ID は、Campus PKI と別の体系となると考えられ、

少なくとも当面は Grid PKI のユーザ ID と Campus PKI のユーザ ID が同一となることはない。

そこで、CMC では、全学 IT 認証基盤による認証を行なうウェブ enroll をインターフェイスに持つグリッド証明書発行システムを開発した。本システムでは、本人性の確認を全学 IT 認証基盤の証明書により行ない、グリッド証明書の秘密鍵、公開鍵を自動生成して UMS およびユーザ端末のブラウザの証明書ストアに格納する。

本ウェブ enroll 機能により、全学 IT 認証基盤で認証されたユーザは、全学 IT 認証基盤により認証されていないユーザ、すなわち学外のユーザの証明書発行に必要となるライセンス ID を入力する手続きを省略することができる。また、証明書発行手続きにおいて、ユーザは Campus PKI のユーザ ID（大阪大学ではこれを大阪大学個人 ID と呼んでいる）による認証さえすればよく、Grid におけるユーザ ID を意識する必要がない。

CMC では今後、さらに Kerberos 認証における事前認証において PKI 認証を併用する PKINIT 方式への対応も検討している。

5. ま と め

CMC では、全国共同利用施設としての大規模計算機システムへ NAREGI ミドルウェアの導入を検討し、CMC でのポリシーに反する問題点を解決する適用手法を示した。現在、本稿で述べた手法に基づいて NAREGI 環境を構築中である。したがって、適用システムの評価は今後の課題となる。

第 4.2 節において、Kerberos 認証を前提とした上での NAREGI ポータルへのアクセス手法について説明し、状況によっては NAREGI ポータル上で複数のパスワード/パスフレーズの入力を要することを指摘した。提案手法では、NAREGI で利用する証明書のパスフレーズを自動生成させることにより、認証時のユーザとのインタラクションを極力抑えた。ユーザは証明書のパスフレーズの管理から解放される。一見すると、セキュリティレベルが下がったように思えるかもしれないが、これらの設計は Kerberos における認証情報の集中管理の思想に則っている。外部の攻撃者が NAREGI ポータルに直接アクセスしての総当たり攻撃は成立しない。何故なら Kerberos 認証を通らない限り、ポータルシステムに内在する認証以外の脆弱性を除けば、NAREGI ポータルへアクセスできずポータル機能が利用できないからである。

NAREGI ポータルにおけるパスフレーズの入力を出来るだけ少なくする試みは、NAREGI の開発チームでも議論されており、NAREGI バージョン 1 では UMS が廃止されユーザ証明書をユーザ端末に格納することで実現されるようである（事実上 1 回の入力で済ませられる）。しかしながら、証明書の格納場所としてユーザ端末であることは、昨今のデータ流出事件が相変わらず世間を賑わしていることを踏まえると、むしろ危険である。ユーザ端末ではなく IC カードに格納する場合は、秘密鍵が漏洩ないし複製される危険はかなり下がると考えられるので、許容できる選択肢となる。ユーザ端末しか格納場所がない場合、利便性のためにユーザ自身の手によって秘密鍵が複

製され、他の端末へ格納されることもあり得る。このような状況下では、運用管理の観点からはユーザによる秘密鍵の管理を信用することはできない。CMC では証明書の格納場所として UMS または IC カードに限定することを CP/CPS に明記している。管理者側での集中管理か、あるいはユーザ個人の管理を信頼する場合でも IC カードのような局所的な格納媒体を前提とするポリシーである。したがって、NAREGI バージョン 1 がリリースされた時点でも、証明書の格納場所としてユーザ端末は認めず、差し当たっては UMS と IC カードの両方を格納場所とする運用になると考えられる。

VO の形成には、研究分野という括りによる自然な構成がある。例えば、全国の大学に点在するナノサイエンスの研究者で構成され、協力研究機関がリソースプロバイダとなるようなナノサイエンス VO を考えることができる。これらの仮想組織への情報基盤センターとしての関り方は、リソースプロバイダとして参加するだけではなく、VO の管理者として VO のホスティングサービスを提供できる可能性がある。いわゆる e-Science 研究支援においては VO のホスティングサービスだけではなく、広域分散するデータの共有を可能とするデータグリッド環境サービスを展開できる。現時点では、コンピューティンググリッドに比べてデータグリッドのサービス形態は明確ではないが、今後の最重要検討課題である。

CMC では、平成 19 年 5 月に NAREGI β 2 がリリースされるのに合わせて大規模計算機での NAREGI コンピューティング環境の運用を開始する。システムの評価を行なうことはもちろんのこと、データグリッドサービスあるいは NAREGI に留まらない広い意味でのグリッドコンピューティングサービスの展開が今後の検討課題である。

謝 辞

本研究を進めるにあたりご支援いただきました国立情報学研究所グリッド研究開発推進拠点の皆さまに深く感謝いたします。

本研究の一部は、国立情報学研究所委託事業「最先端学術情報基盤の構築に関する研究開発と調査」の一環として行なわれた成果である。

文 献

- [1] National REsearch Grid Initiative (NAREGI). <http://www.naregi.org/>
- [2] Globus Toolkit 4. <http://www.globus.org/toolkit/>
- [3] APGrid PMA (Asa Pacific Grid Policy Management Authority). <http://www.apgridpma.org/>
- [4] UPKI (University Public Key Infrastructure). <http://upki-portal.nii.ac.jp/>
- [5] 島岡政基, 谷本茂明, 片岡俊幸, 峯尾真一, 曾根原登, 寺西裕一, 飯田勝吉, 岡部寿男, “大学間連携のための全国共同電子認証基盤 UPKI における認証連携方式の検討”, 信学技報, vol. 106, no. 62, IA2006-3, pp. 13-18, 2006 年 5 月.