グリッドテストベッドの構築方法
- ApGrid Testbedを例に して -

産業技術総合研究所　グリッド研究センター
田中　良夫

背景

- **グリッドはテスト段階から実用化の段階に移りつつある**
  - 主要な技術の標準化が進んでいる
    - GSI, OGSA, etc.
  - グリッドミドルウェアが枯れてきた
    - Globus Toolkit, UNICORE, Condor, etc.
- **では、グリッドを使うぞ！といっても...**
  - どこで動かすか？
  - グリッドテストベッドありますか？
  - どうやって作る？

話の目的

- **グリッドテストベッドをどうやって作るか**
  - Globus Toolkit version 2 (GT2)を使ったグリッドテストベッド
    - 社会的･政治的問題
    - 設計、実装および管理
  - ApGrid Testbedをケーススタディに、スクラッチからテストベッドを構築する方法を紹介
- **この話を通じて、GT2の各コンポーネントがどのように機能しているかを理解**

概要

I. **Globus Toolkitの紹介 (さらっと)**

II. **Grid Testbedの構築法**

  I. 一般的な話

III. **Case Study**

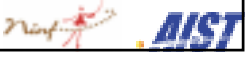
  I. ApGrid Testbedを例にして

IV. **経験および得られた知見**

  I. ApGrid Testbed上での気象予測システム

V. **まとめ**

  I. 何ができたか? 何はまだできていないか?



PART I
Globus Toolkitの紹介

several slides are by courtesy of the Globus Project

What is the Globus Toolkit?

- **A Toolkit which makes it easier to develop computational Grids**
- **Developed by the Globus Project Developer Team (ANL, USC/ISI)**
- **Defacto standard as a low level Grid middleware**
  - Most Grid testbeds are using the Globus Toolkit
- **Latest version is 2.4**
- **GT3 is also available**
  - Implementation of OGSI. Different architecture with GT2

Some notes on the Globus Toolkit (1/2)

- **Globus Toolkit is not providing a framework for anonymous computing and mega-computing**
  - Users are required
    - to have an account on servers to which the user would be mapped when accessing the servers
    - to have a user certificate issued by a trusted CA
    - to be allowed by the administrator of the server
  - Complete differences with mega-computing framework such as SETI@HOME

Some notes on the Globus Toolkit (2/2)

- **Do not think that the Globus Toolkit solves all problems on the Grid.**
  - The Globus Toolkit is a set of tools for the easy development of computational Grids and middleware
    - The Globus Toolkit includes low-level APIs and several UNIX commands
    - It is not easy to develop application programs using Globus APIs. High-level middleware helps application development.
  - Several necessary functions on the computational Grids are not supported by the Globus Toolkit.
    - Brokering, Co-scheduling, Fault Managements, etc.
  - Other supposed problems
    - using IP-unreachable resources (private IP addresses + MPICH-G2)
    - scalability (ldap, maintenance of grid-mapfiles, etc.)

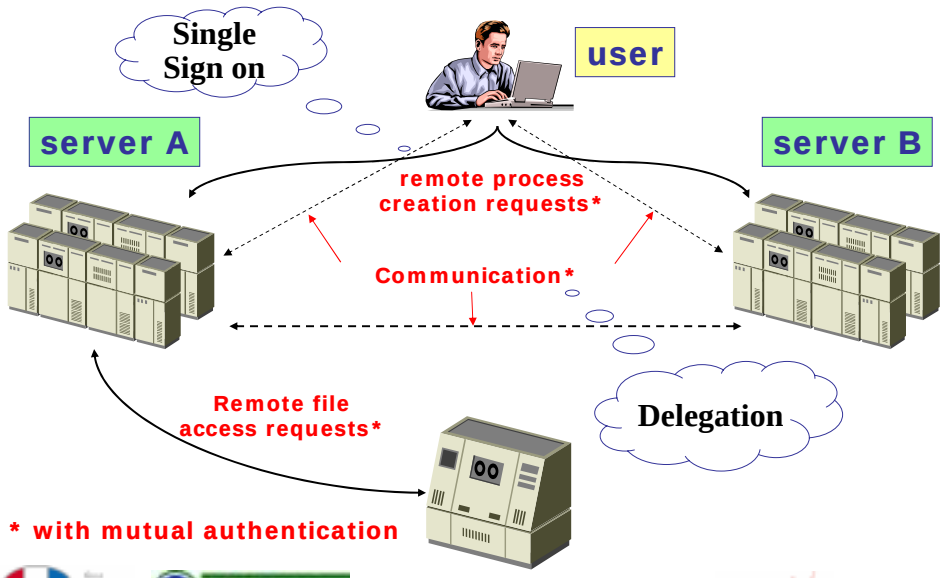
GT2 components

- **GSI: Single Sign On + delegation**
- **MDS: Information Retrieval**
  - Hierarchical Information Tree (GRIS+GIIS)
- **GRAM: Remote process invocation**
  - Three components:
    - Gatekeeper
    - Job Manager
    - Queuing System (pbs, sge, etc.)
- **Data Management:**
  - GridFTP
  - Replica management
  - GASS
- **GT2 provides C/Java APIs and Unix commands for these components**

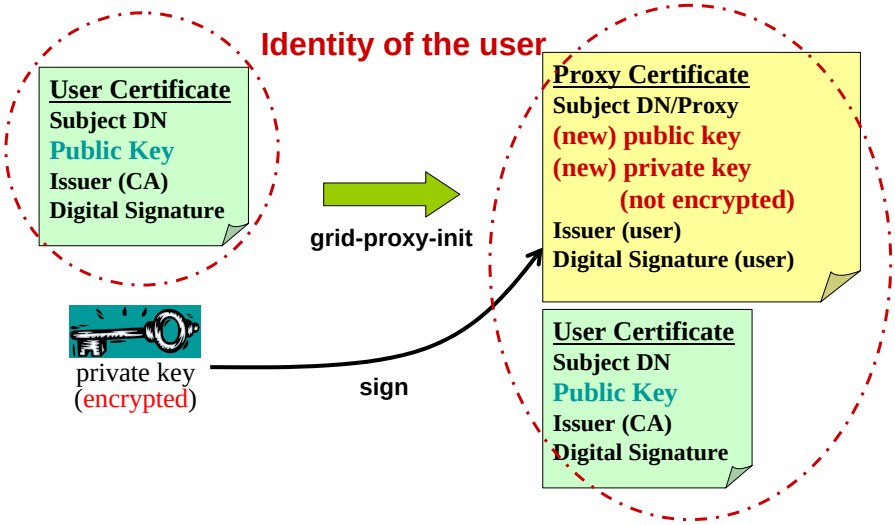
GSI: Grid Security Infrastructure

- **Authentication and authorization using standard protocols and their extensions.**
  - Authentication: Identify the entity
  - Authorization: Establishing rights
- **Standards**
  - PKI, X.509, SSL,...
- **Extensions: Single sign on and delegation**
  - Entering pass phrase is required only once
  - Implemented by proxy certificates

Requirements for security



Proxy Certificate



Requirements for users

- **Obtain a certificate issued by a trusted CA**
  - Globus CA can be used for tests
  - Run another CA for production run. The certificate and the signing policy file of the CA should be put on an appropriate directory (/etc/grid-security/certificates).
- **Run grid-proxy-init command in advance**
  - Will generate a proxy certificate. Enter PEM pass phrase for the decryption of a private key.
  - A proxy certificate will be generated in /tmp directory

Requirements for system admins.

- **CA certificate and the signing policy file are used for verifying end entity's certificate.**
  - Those files must be placed in /etc/grid-security/certificates/ directory
  - example:
    - If the server certificate is issued by AIST GTRC CA, the certificate and the signing policy file of AIST GTRC CA must be put in /etc/grid-security/certificates/ on client machine.
    - If my certificate is issued by KISTI CA, the certificate and the signing policy file of KIST CA must be put in /etc/grid-security/certificates/ on all server machines.

PART II
Grid Testbedの構築法
一般的な話

many slides are by courtesy of Bill Johnston (NASA)

Building a Multi-site, Computational and Data Grid

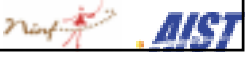
- **Like networking, successful Grids involve almost as much sociology as technology.**
- **The first step is to establish the mechanisms for promoting cooperation and mutual technical support among those who will build and manage the Grid.**
- **Establish an Engineering Working Group that involves the Grid deployment teams at each site**
  - schedule regular meetings / telecons
  - involve Globus experts in these meetings
  - establish an EngWG archived email list

Grid Resources

- **Identify the computing and storage resources to be incorporated into your Grid**
  - be sensitive to the fact that opening up systems to Grid users may turn lightly or moderately loaded systems into heavily loaded systems
  - batch schedulers may have to be installed on systems that previously did not use them in order to manage the increased load
  - carefully consider the issue of co-scheduling!
    - many potential Grid applications need this
    - only a few available schedulers provide it (e.g. PBSPro)
    - this is an important issue for building distributed systems

Build the Initial Testbed

- **Plan for a Grid Information Service / Grid Information Index Server (GIS/GIIS) at each distinct site with significant resources**
  - this is important in order to avoid single points of failure
    - if you depend on an MDS/GIIS at some other site site, and it becomes un-available, you will not be able to examine your local resources
- **The initial testbed GIS/MDS model can be independent GIISs at each site**
  - in this model
    - Either cross-site searches require explicit knowledge of each of the GIISs, which have to searched independently, or
    - All resources cross-register in each GIIS

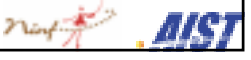


Build the Initial Testbed

- **Build Globus on test systems**
  - use PKI authentication and certificates from the Globus Certificate Authority, or some other CA, issued certificates for this test environment
    - Globus CA will expire on January 23, 2004.
    - can use the OpenSSL CA to issue your own certs manually
  - validate the access to, and operation of the GIS/GIISs at all sites

Preparing for the Transition to a Prototype-Production Grid

- **There are a number of significant issues that have to be addressed before going to even a pseudo production Grid**
  - Policy and mechanism must be established for the Grid X.509 identity certificates
  - the operational model for the Grid Information Service must be determined
    - who maintains the underlying data?
  - the model and mechanisms for user authorization must be established
    - how are the Grid mapfiles managed?
  - your Grid resource service model must be established (more later)
  - your Grid user support service model must be established
  - Documentation must be published



Trust Management

- **Trust results from clear, transparent, and negotiated policies associated with identity**
- **The nature of the policy associated with identity certificates depends a great deal on the nature of your Grid community**
  - It is relatively easy to establish policy for homogeneous communities as in a single organization
  - It is very hard to establish trust for large, heterogeneous virtual organizations involving people from multiple, international institutions

Trust Management (cont'd)

- **Assuming a PKI Based Grid Security Infrastructure (GSI)**
- **Set up, or identify, a Certification Authority to issue Grid X.509 identity certificates to users and hosts**
- **Make sure that you understand the issues associated the Certificate Policy / Certificate Practices ("CP") of the CA**
  - one thing governed by CP is the "nature" of identity verification needed to issue a certificate (this is a primary factor in determining who will be willing to accept your certificates as adequate authentication for resource access)
  - changing this aspect of the CP could well mean not just re-issuing all certificates, but requiring all users to re-apply for certificates

Trust Management (cont'd)

- **Do not try and invent your own CP**
- **The GGF is working on a standard set of CPs**
- **We are trying to establish international collaborations for Policy Management Authority and Federation of CAs at the GGF.**
  - DOE Science Grid, NASA IPG, EU Data Grid, ApGrid, etc...
  - First BOF will be held at GGF9 (Chicago, Oct.)
- **Establish and publish your Grid CP**

PKI Based Grid Security Infrastructure (GSI)

- **Pay very careful attention to the subject namespace**
  - the X.509 Distinguished Name (the full form of the certificate subject name) is based on an X.500 style hierarchical namespace
  - if you put institutional names in certificates, don't use colloquial names for institutions - consider their full organizational hierarchy in defining the naming hierarchy
  - find out if anyone else in your institution, agency, university, etc., is working on PKI (most likely in the administrative or business units) - make sure that your names do not conflict with theirs, and if possible follow the same name hierarchy conventions
  - CAs set up by the business units of your organization frequently do not have the right policies to accommodate Grid users

PKI Based Grid Security Infrastructure (GSI)

- **Think carefully about the space of entities for which you will have to issue certificates**
  - Humans
  - Hosts (systems)
  - Services (e.g. GridFTP)
  - Security domain gateways (e.g. PKI to Kerberos)
- **Each must have a clear policy and procedure described in your CA's CP/CPS**

Preparing for the Transition to a Prototype-Production Grid

- **Issue host certificates for all the resources and establish procedures for installing them**
- **Count on revoking and re-issuing all of the certificates at least once before going operational**
- **Using certificates issued by your CA, validate correct operation of the GSI/GSS libraries, GSI ssh, and GSIftp / Gridftp at all sites**

The Model for the Grid Information System

- **Index servers**
  - resources are typically named using the components of their DNS name
    - advantage is that of using an established and managed name space
  - must use separate "index" servers to define different relationships among GIISs, virtual organization, data collections, etc.
    - on the other hand, you can establish "arbitrary" relationships within the collection of indexed objects
  - this is the approach favored by the Globus R&D team


Local Authorization

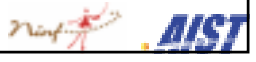
- **Establish the conventions for the Globus mapfile**
  - maps user Grid identities to system UIDs – this is the basic local authorization mechanism for each individual platform, e.g. compute and storage
  - establish the connection between user accounts on individual platforms and requests for Globus access on those systems
  - if your Grid users are to be automatically given accounts on a lot of different systems, it may make sense to centrally manage the mapfile and periodically distribute it to all systems
    - however, unless the systems are administratively homogeneous, a non-intrusive mechanism such as email to the responsible sys admins to modify the mapfile is best
  - Community Authorization Service (CAS)


Site Security Issues

- **Establish agreements on firewall issues**
  - Globus can be configured to use a restricted range of ports, but it still needs several tens, or so (depending on the level of usage of the resources behind the firewall), in the mid 700s
  - A Globus "port catalogue" is available to tell what each Globus port is used for
    - this lets you provide information that you site security folks will likely want
    - should let you estimate how many ports have to be opened (how many per process, per resource, etc.)
  - GIS/MDS also needs some ports open
  - CA typically uses a secure Web interface (port 443)
- **Develop tools/procedures to periodically check that the ports remain open**

Preparing for Users

- **Build and test your Grid incrementally**
  - very early on, identify a test case distributed application that requires reasonable bandwidth, and run it across as many widely separated systems in your Grid as possible
    - try and find problems before your users do
  - design test and validation suites that exercise your Grid in the same way that applications do
- **Establish user help mechanisms**
  - Grid user email list and / or trouble ticket system
  - Web pages with pointers to documentation
  - a Globus "Quick Start Guide" that is modified to be specific to your Grid, with examples that will work in your environment (starting with a Grid "hello world" example)

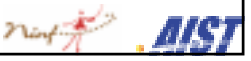


The End of the Testbed Phase

- **At this point Globus, the GIS/MDS, and the security infrastructure should all be operational on the testbed system(s). The Globus deployment team should be familiar with the install and operation issues, and the sys admins of the target resources should be engaged.**
- **Next step is to build a prototype-production environment.**

Moving from Testbed to Prototype Production Grid

- **Deploy and build Globus on at least two production computing platforms at two different sites.Establish the relationship between Globus job submission and the local batch schedulers (one queue, several queues, a Globus queue, etc.)**
- **Validate operation of this configuration**



Take Good Care of the Users as Early as Possible

- ***Establish a Grid/Globus application specialist group***
  - they should be running sample jobs as soon as the testbed is stable, and certainly as soon as the prototype-production system is operational
  - they should serve as the interface between users and the Globus system administrators to solve Globus related application problems
- ***Identify early users and have the Grid/Globus application specialists assist them in getting jobs running on the Grid***
  - On of the scaling / impediment-to-use issues currently is that the Grid services are relatively primitive (I.e., at a low level). The Grid Services and Web Grid Services work currently in progress is trying to address this.

PART III
Case Study
ApGrid Testbedを例にして

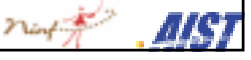
several slides are by courtesy of the Globus Project

Outline

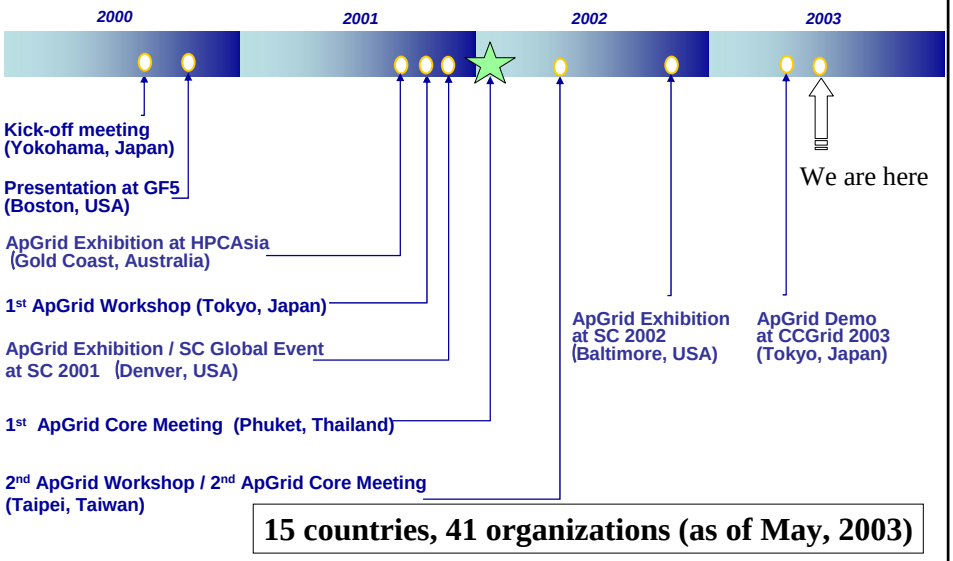
- **Brief introduction of ApGrid and the ApGrid Testbed**
- **Software architecture of the ApGrid Testbed**
- **Lessons learned**

What is ApGrid?

- Asia-Pacific Partnership for Grid Computing.
- **ApGrid focuses on**
  - Sharing resources, knowledge, technologies
  - Developing Grid technologies
  - Helping the use of our technologies in create new applications
  - Collaboration on each others work
- **Not only a Testbed**
- **Not restricted to just a few developed countries, neither to a specific network nor its related group of researchers**
- **Not a single source funded project**



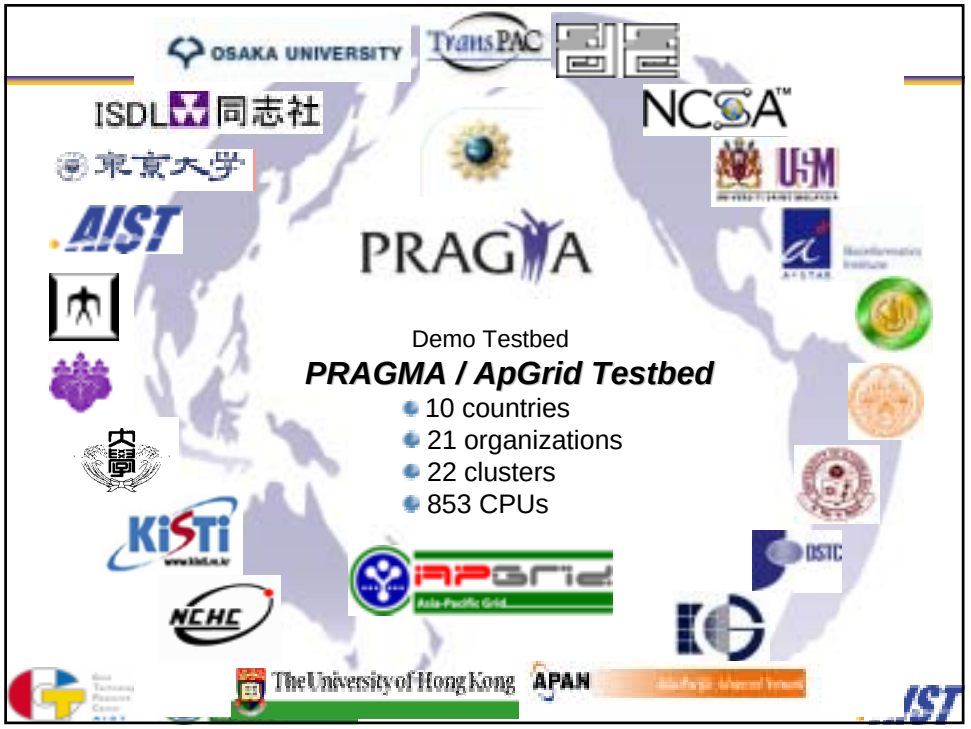
History of ApGrid



15 countries, 41 organizations (as of May, 2003)

ApGrid Testbed – features -

- **Truly multi national/political/institutional VO**
  - not an application-driven testbed
  - differences in languages, culture, policy, interests, …
- **Donation (Contribution) based**
  - Not a single source funded for the development
  - Each institution contributes his own share
  - bottom-up approach
- **We can**
  - have experiences on running international VO
  - verify the feasibility of this approach for the testbed development



ApGrid Testbed – status and plans -

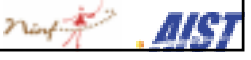
- **Resources**
  - 853 CPUs from 21 institutions
    - Most resources are not dedicated to the ApGrid Testbed.
  - many AG nodes, 1 virtual venue server
  - Special devices (MEG, Ultra High Voltage Microscope, etc.)
- **Going to be a production Grid**
  - Most current participants are developers of Grid middleware rather than application people
  - Should be used for running REAL applications
    - increase CPUs
    - keep it stable
    - provide documents

Design Policy

- **Security is based on GSI**
- **Information service is provided by MDS**
  - Use Globus Toolkit Ver.2 as a common software infrastructure

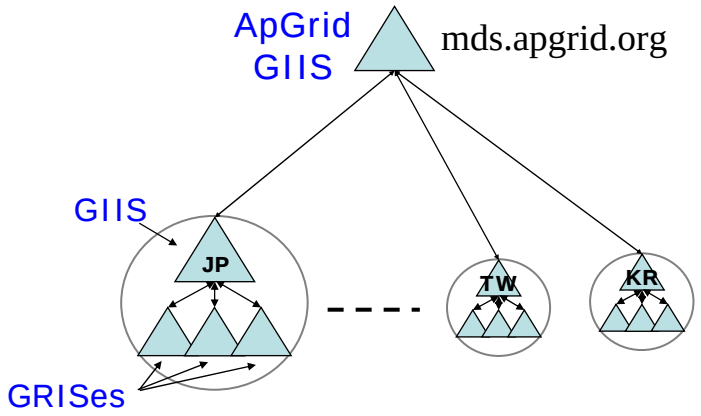
Testbed Developments – Security Infrastructure -

- **Certificates and CAs**
  - Users and resources have to have their certificates issued by a trusted CA.
  - The ApGrid Testbed runs CAs and issues certificates for users and resources.
- **ApGrid CA?**
  - The ApGrid Testbed allows multiple root CAs.
  - Each country/organization/project may run its own CA and these could be root CAs on the ApGrid Testbed.
  - Certificates, signing policy files of the ApGrid CAs are put on the ApGrid home page and can be downloaded via https access.
  - Planning to establish ApGrid PMA and collaborate with other communities.



Testbed Developments – Information Services -

- **Based on MDS (GRIS/GIIS)**



Requirements for users

- **obtain a user certificate**
- **be permitted accesses to resources by the resource providers**
  - need to have an account and an entry to grid-mapfile on each server
- **Put certificates of all CAs by which server certificates are issued.**

Requirements for resource providers

- **Install GT2 on every server**
- **Decide your policy**
  - which CA will be trusted?
  - to whom is your resource opened?
  - make limitations such as max job running time, etc.?
  - …
- **Give appropriate accounts and add entries to grid-mapfile for the users**
  - Possible policies:
    - Give accounts for all individuals
    - Give a common account for each institution
- **Accept job requests via the Globus Gatekeeper**
- **Provide information via GRIS/GIIS**
- **Push the sites' GIIS to the ApGrid GIIS**



How to contribute to the ApGrid Testbed

1. **Install ApGrid Recommended Software**
   1. Configure GRIS/GIIS
   2. Put trusted CA's cert. and policy files
2. **Provide Users' Guide for ApGrid users**
   1. Resource information
   2. How to get an account
   3. Contact information
   4. etc.
3. **Administrative work**
   1. Create accounts
   2. Add entries to grid-mapfile
   3. etc.



ApGrid Testbed – Software Infrastructure -

- **Minimum Software: Globus Toolkit 2.2 (or later)**
  - Security is based on GSI
  - Information Service is based on MDS
- **The ApGrid Recommended Package will include**
  - GPT 2.2.5
  - Globus Toolkit 2.4.2
  - MPICH-G2 (MPICH 1.2.5.1)
  - Ninf-G 1.1.1
  - Iperf 1.6.5
  - SCMSWeb 2.1
  - + installation tool

Configuration of GIIS
- Define name of the VO -

Add the following contents to $GLOBUS_LOCATION/etc/grid-info-slapd.conf

```
database        giis
suffix          "Mds-Vo-name=AIST, o=Grid"
conf            /usr/local/gt2/etc/grid-info-site-giis.conf
policyfile      /usr/local/gt2/etc/grid-info-site-
policy.conf
anonymousbind     yes
access to * by * write
```

Need to change $GLOBUS_LOCATION/etc/grid-info-site-policy.conf so that the GIIS can accept registration from GRISes

Configuration of GRIS
- Example: Register to the ApGrid MDS -

Add the following contents to
$GLOBUS_LOCATION/etc/grid-info-resource-register.conf

```
dn: Mds-Vo-Op-name=register,   Mds-Vo-name=ApGrid, o=Grid
regtype: mdsreg2
reghn: mds.apgrid.org
regport: 2135
regperiod: 600
type: ldap
hn: koume.hpcc.jp
port: 2135
rootdn: Mds-Vo-name=AIST, o=Grid
…
```

PART IV
経験および得られた知見
ApGrid Testbed上での気象予測システム

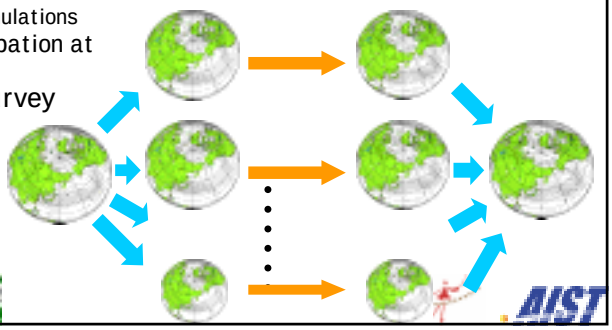
several slides are by courtesy of the Globus Project

Weather Prediction System on the ApGrid Testbed

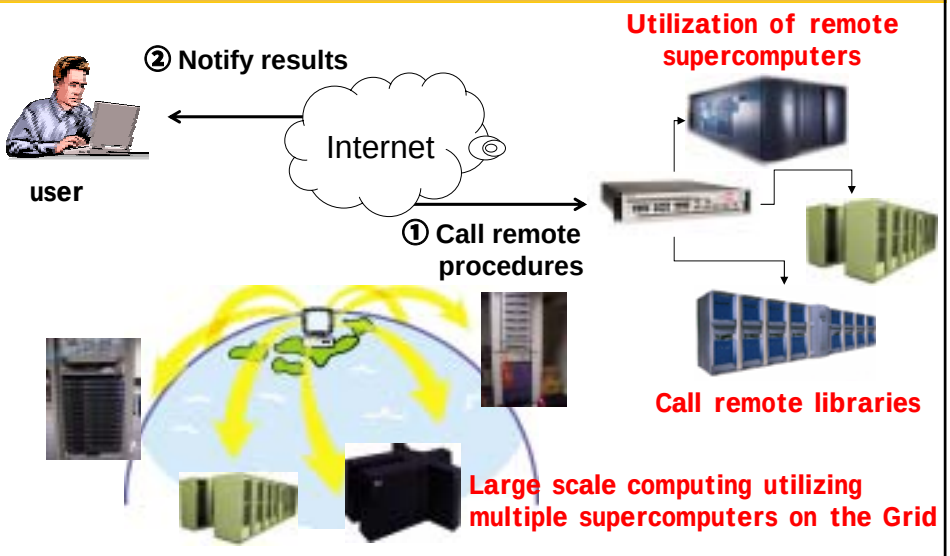
- **Application:** **Weather Prediction**
  - Originally developed by Dr. Tanaka (U. of Tsukuba)
- **Portal:** **Grid PSE Builder**
- **Middleware used for the implementation of Grid-enabled climate simulation:** **Ninf-G**
  - GridRPC middleware based on the Globus Toolkit which is used for gridifying the original (sequential) application
- **Resources:** **Provided by ApGrid/PRAGMA organiations**
  - 853 cpus (10 countries/21 organizations/22 clusters)

Application: Weather Prediction

- **Goal**
  - Short- to Middle- term, global weather prediction
    - Winding of Jet-Stream
    - Blocking phenomenon of high atmospheric pressure
- **Barotropic S-Model**
  - Climate simulation model proposed by Prof. Tanaka (U. of Tsukuba)
  - Simple and precise
    Modeling complicated 3D turbulence as a horizontal one
    Keep high precision over long periods
    - Taking a statistical ensemble mean
      - ~ several 100 simulations
    - Introducing perturbation at every time step
  - Typical parameter survey



Middleware: Ninf-G (GridRPC System)



Standard GridRPC API is proposed at the GGF GridRPC WG.

Middleware: Ninf-G (cont'd)

- **RPC library on the Grid**
  - Built on top of Globus Toolkit
    - MDS: managing stub information
    - GRAM: invocation of server programs
    - GSI: secure communication between a client and a server
  - Simple and easy-to-use programming interface
    - Hiding complicated mechanism of the grid
    - Providing RPC semantics

```
for (i = start; i <= end; i++) {
  /* sequential search */
  SDP_search(argv[1], i, &value[i]); }
```

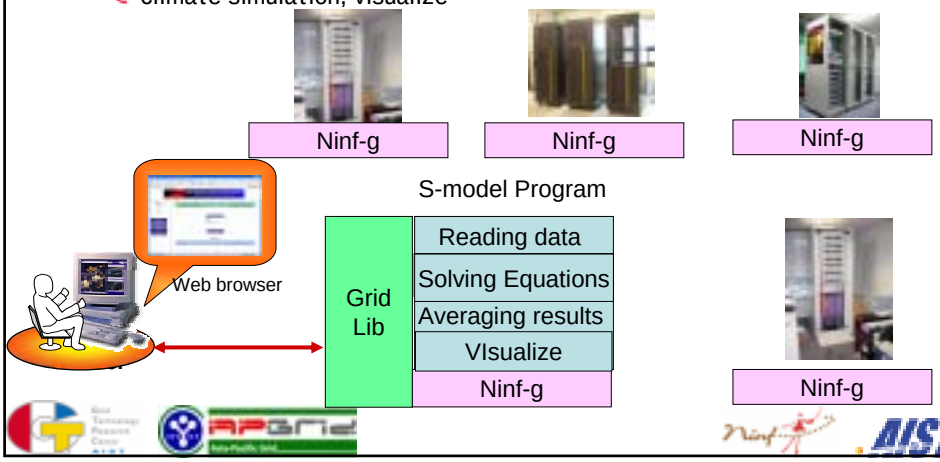
⇩

```
grpc_function_handle_init(&hdl, …, "SDP/search");
for (i = start; i <= end; i++) {
  /* parallel search using async. call */
  grpc_call_async(&hdl, argv[1], i, &value[i]): }
```

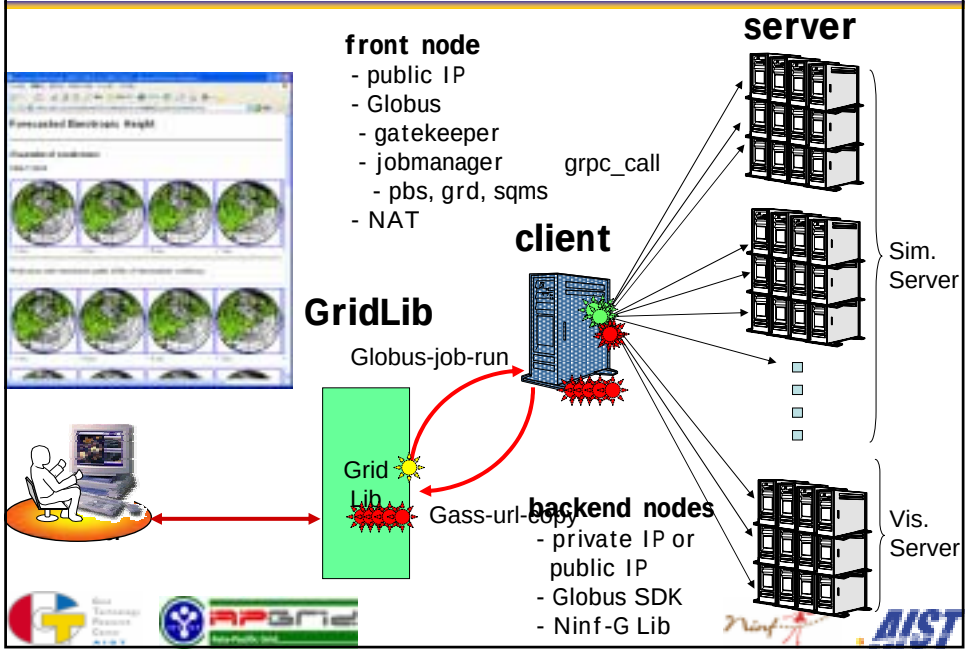
Requires no detailed knowledge on Grid infrastructure

Ninfy the original (seq.) weather prediction

- **Dividing a program into two parts as a client-server system**
  - Client:
    - Pre-processing: reading input data
    - Post-processing: averaging results of ensembles
  - Server
    - climate simulation, visualize



Behavior of the weather prediction system

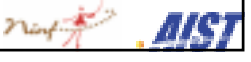


Lessons Learned

- **We have to pay much efforts for initiation**
  - Problems on installation of GT2/PBS/jobmanger-pbs,grd
    - Failed in lookup service of hostname/IP addresses
      - Both for internet and intranet
      - Add host entries in /etc/hosts in our resources
    - failed in rsh/ssh server to/from backend nodes
      - .rhosts, ssh key, mismatch of hostname
    - pbs_rcp was located in NFS mounted (nosuid) volume
    - bugs in jobmanager scripts (jobmanager-grd is not formally released)
  - GT2 has poor interface with queuing system

Lessons Learned (cont'd)

- **We have to pay much efforts for initiation (cont'd)**
  - What I asked
    - Open firewall/TCP Wrapper
    - Additionally build Info SDK bundle with gcc32dbg
    - Add ${GLOBUS_LOCATION}/lib to /etc/ld.so.conf and run ldconfig (this can be avoided by specifying link option)
    - change configuration of xinetd/inetd
    - Enable NAT

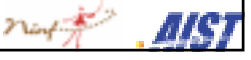


Lessons Learned (cont'd)

- **Difficulties caused by the bottom-up approach for building ApGrid Testbed and the problems on the installation of the Globus Toolkit.**
  - Most resources are not dedicated to the ApGrid Testbed.
    - There may be busy resources
    - Need grid level scheduler, fancy Grid reservation system?
  - Incompatibility between different version of GT2

Lessons Learned (cont'd)

- **Performance Problems**
  - Overhead caused by MDS lookup
    - it takes several 10 seconds
    - Added a new feature to Ninf-G so as to bypass MDS lookup
  - Default polling interval of the Globus jobmanager (30 seconds) is not appropriate for running fine-grain applications.
    - AIST and Doshisha U. have changed the interval to 5 seconds (need to re-compile jobmanager)



Lessons Learned (cont'd)

- **Performance Problems (cont'd)**
  - Time for initialization of function handles cannot be negligible
    - Overhead caused by not only by MDS lookup but also hitting gatekeeper (GSI authentication) and a jobmanager invocation
    - Current Ninf-G implementation needs to hit gatekeeper for initialization of function handles one-by-one
      - Although Globus GRAM enables to invoke multiple jobs at one contact to gatekeeper, GRAM API is not sufficient to control each jobs.
    - Used multithreading for initialization to improve performance
    - Ninf-G2 will provide a new feature which supports efficient initialization of multiple function handles.

Lessons Learned (cont'd)

- **We observed that Ninf-G apps did not work correctly due to un-expected configuration of clusters**
  - Failed in GSI auth. for establishing connection for file transfers using GASS.
    - Backend nodes do not have host certs.
    - Added a new feature to Ninf-G which allows to use non-secure connection
  - Due to the configuration of local scheduler (PBS), Ninf-G executables were not activated.
    - Example:
      - PBS jobmanager on a 16 nodes cluster
      - Call grpc_call 16 times on the cluster. App. developer expected to invoke 16 Ninf-G executables simultaneously.
      - Configuration of PBS Queue Manager set the max number of simultaneous job invocation for each user a 9
      - 9 Ninf-G executables were launched, however 7 were not activated
    - Added a new feature to Ninf-G so as to set timeout for initialization of a function handle.

Lessons Learned (cont'd)

- **Some resources are not stable**
  - example: If I call many (more than 20) RPCs, some of them fails (but sometimes all will done)
  - not yet resolved
  - GT2? Ninf-G? OS? Hardware?
- **Other instability**
  - Version up of software (gt2, pbs, etc.) without notification
    - realized when the application would fail.
    - it worked well yesterday, but I'm not sure whether it works or not today
- **We could adapt for these instability by dynamic task allocation.**

PART V

まとめ

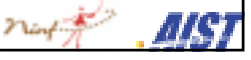
何ができたか? 何はまだできていないか?

Summary

- **Difficulties are caused by not technical problems but sociological/political problems**
- **Each site has its own policy**
  - account management
  - firewalls
  - trusted CAs
  - …
- **Differences in interests**
  - Application, middleware, networking, etc.
- **Differences in culture, language, etc.**
  - Human interaction is very important

Summary (cont'd)

- **What has been done?**
  - Resource sharing between more than 10 sites (around 500cpus)
  - Use GT2 as a common software
  - Run Ninf-G applications
- **What hasn't?**
  - I could use, but it is difficult for others
    - I was given an account at each site by personal communication
  - Formalize "how to use the Grid Testbed"
  - Provide documentation
  - Keep the testbed stable
  - Tools for management
    - Browse information
    - CA/Cert. management

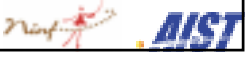


Summary (cont'd)

- **Activities at the GGF**
  - Production Grid Management RG
    - Draft a Case Study Document (ApGrid Testbed)
  - Groups in the Security Area
    - Policy Management Authority RG (not yet approved)
      - Discuss with representatives from DOE Science Grid, NASA IPG, EUDG, etc.
    - Federation/publishing of CAs (will kick off)
      - I'll be one of co-chairs

For more info

- **ApGird**
  - http://www.apgrid.org/
  - discuss@apgrid.org
- **Ninf/Ninf-G**
  - http://ninf.apgrid.org/
  - ninf@apgrid.org
- **GGF**
  - http://www.globalgridforum.org/



Acknowledgements

"Asia Grid Initiative", Special Coordination Funds for Promoting Science and Technology (MEXT, Japan)


Colin Enticott (Monash U)
Chee Shin YEO (Melbourne)


CHEN Lin, Elaine (HKU)


Arun Agarwal (Hyderbad)


Kento Aida (TITECH)
Ken'ichiro Shirose (TITECH)
Susumu Date (Osaka)
Yusuke Tanimura (Doshisha)
Yoshihiro Nakajima (Tsukuba)
Toshihiro Iwabuchi (Waseda)
Yuuki Horita (U. Tokyo)
Support Staffs (AIST)


Nazarul annuar nasirin (USM)


Nigel Teow (BII)


Gee-Bum Koo (KISTI)


Julian Yu-Chung Chen (NCHC)


Sugree Phatanapherom (KU)
Suriya Uru-ek-olan (KMITNB)


Mason Katz (SDSC)

JP/KR/TW NOC Team