第6回　東海地区CSI事業報告会

UPKIに活きるグリッドセキュリティ

～5年後の未来予想あるいは期待

2007年12月19日

国立情報学研究所

峯尾真一

CHAPTER 1

グリッドの夜明け

グリッドの誕生

- ネットワーク上に分散した計算資源やデータを“まるでコンセントにプラグを挿すだけで使える電気のように”容易に利用するための仕組み
  “The Grid :Blueprint for a New Computing Infrastructure”
  Ian Foster,Carl Kesselman (1998)
- グリッド概念の根本は、仮想組織による資源の共有と問題解決
  “*The Anatomy of the Grid”*
  Ian Foster,Carl Kesselman,Steven Tuecke (2001)

グリッドで何がうれしいのか？

1. 動的で柔軟な資源活用
2. IT資源のユーティリティ化
3. 組織の仮想化
4. オープン化＆国際標準化

1. 動的で柔軟な資源活用

- 必要な時に必要なだけの資源を瞬時に集めて利用できる
  - すなわち
    - ネット上で理論上は無限のシステム拡張性を実現できる= on demand computing
    - 最大限の利用を前提とした設備投資は不要＝効率的な投資が可能
  - もしグリッドがなければ…
    - 利用者のジョブの規模は計算センター内に導入済みの物理的な資源で決まり拡張性が無い。また実行できる範囲であっても自センターの資源が空くまで待たされ、例え他センターの資源が空いていても利用できない。
    - 計算センター運用者は、利用者の需要の瞬間最大値を満たす設備投資を続ける必要がある。

2. IT資源のユーティリティ化

- 電気や水道と同じように誰にでも簡単にあらゆるIT資源を利用することができる
  - すなわち
    - 計算機やデータはどこにあってもよい＝集める必要はない
    - すべてが同じ使い勝手＝個別の利用環境を意識する必要は無い
  - もしグリッドが無ければ…
    - ネットワーク上のどこにどんな資源（計算機やデータ）があり、どうすればアクセスできるかを正確に知らない限り利用できない。
    - 利用者は使う予定の全計算センターに利用申請を出し、センター毎に固有の利用規則や手順を覚えなければならない。
  - 例えれば…
    - ギアやクラッチを意識しなければならないマニュアルの自動車とオートマ車の違い
    - 車（計算機）の好きな人はオートマ（グリッド）を嫌う傾向にあるが、世の中一般にはオートマ車が有効かつ必要

３．組織の仮想化

- 仮想的な組織を自由に作り安全に物理的および知的資源の共有を行うことができる
  - すなわち
    - 人材も計算機もデータベースも自由に組み合わせて仮想組織が実現できる
    - ノウハウやデータの共有が可能。また意図的に囲い込むことも可能。
  - もしグリッドが無ければ…
    - 組織を超えた資源共有は原則的には不可能
    - 研究コミュニティ作りも個別に必要となり、その都度方式の調整が必要

４．オープン化＆国際標準化

- オープン化された国際標準のインターフェースを持つことができる
  - すなわち
    - 利便性・運用性・互換性・安全性が高く、構築が容易で費用対効果に優れた学術情報基盤の構築が可能＝時代はopen standard
    - Webサービスによりe-Scienceとe-Businessの融合が可能
  - もしグリッドが無ければ…
    - 互換性の無いミドルウェアが多数競合し合う状況となる。相互接続が必要な場合には、利用する予定の全てのミドルウェアを同時に導入しておく必要がある。
    - 利便性・運用性・安全性を高めるための開発を各ミドルウェア毎に重複して行うことになる
  - 例えれば…
    - グリッドはIT世界の共通言語であり、人間界の英語に相当する。完璧な言語ではないが、コミュニケーションのためには使わざるを得ない。

グリッドの進化

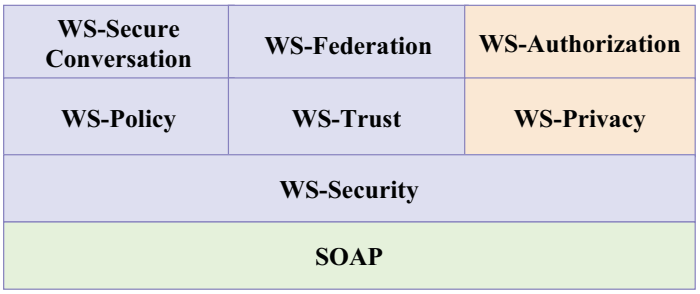
- Gridサービスをステートフルなwebサービスとして定義したOGSA (Open Grid Services Architecture)を提唱
  “The Physiology of the Grid”
  Ian Foster, Carl Kesselman, Jeffrey M. Nick, Steven Tuecke1 (2002)

e-Science meets e-Business

グリッドシンポジウム・イン関西2003
丸山不二夫 (2003年12月9日)

グリッドはwebサービスの一つになった

OGSA
(Open Grid Services Architecture)



WS-Security
メッセージの暗号化や署名の実施
WS-SecureConversation
相互認証、鍵共有、メッセージ認証・管理
WS-Trust
異なるドメインにて信頼関係の確立
WS-Policy
エンドポイントのセキュリティ要件や機能。
認証データに対してポリシーを与える。

WS-Federation
複数ドメイン間での認証情報のやりとり。
WS-Security,WS-Policy,WS-Trust, WS-Secure Conversationをベースに実現
WS-Authorization
アクセス制御の枠組み。認証データとポリシーを元に実行権限を決定する。
WS-Privacy
Webサービスでのプライバシー保護

CHAPTER 2

セキュリティはどうしよう？

何が必要か？

- 何はともあれ全てを識別すること
  - 現実世界の実体（名前）にマッピングする
    - **Identification**（識別）
- 次に安全な通信路
  - 安全な通信の3条件
    - 通信相手が本人であることが保証されること
      - **Authentication**（認証）
    - 他人に盗聴されないこと
      - **Confidentiality**（秘守性）
    - 通信内容が途中で改ざんされないこと
      - **Integrity**（完全性）
- グリッドを“サービス”と考えるとこれだけでは不足
  - システムに必要な条件
    - 限定した人にサービスを提供できること
      - **Authorization**（認可）
    - やり取りの証拠が記録できること
      - **Non-repudiation &Auditing**（事後否認防止&監査）
- 安全と言える根拠を示すこと

グリッドはどう解決しているのか

- 対象のIdentification（識別）
  - PKI（今は）
- 通信のAuthentication（認証）
  - GSI
- 通信のConfidentiality（秘守性）
  - GSI
- 通信のIntegrity（完全性）
  - GSI
- サービスのAuthorization（認可）
  - GSI (Grid-mapfile),仮想組織管理、認可サービス
- サービスのNon-repudiation &Auditing（事後否認防止&監査）
  - 監査証跡の保存等の運用による対策
- 安全の根拠
  - GSIは**PKI**を利用し、**認証局**により安全性を担保
  - 一般的なシステムやネットワークのセキュリティは別途担保されるという前提

さてGSI とはどんなものか？

GSI :Grid Security Infrastructure

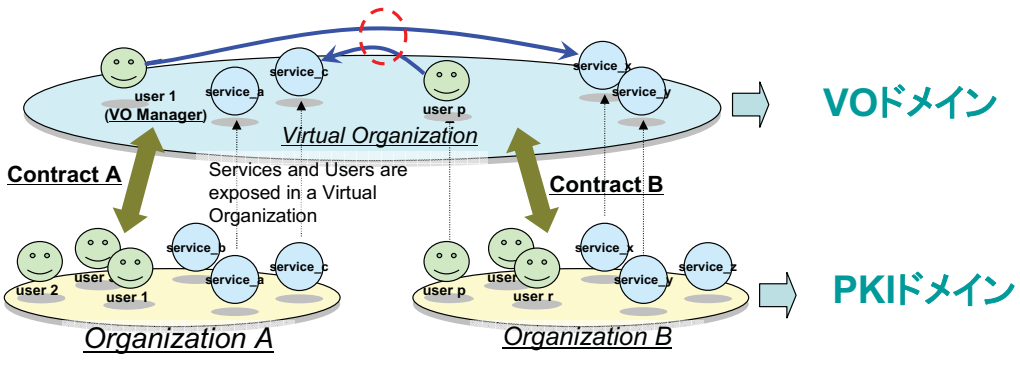
- 目的
  - GT4のセキュリティ層として、安全な通信と認可の仕組みを実現すること
- 提供する機能
  - 通信のセキュリティ
  - サービスを行う時の相互認証
  - 認可の仕組み
  - 権限委譲
  - 各レベル（コンテナ・サービス・資源）毎のセキュリティ設定
- 参考資料
  - The Globus Toolkit 4 Programmer's Tutorial
    - http://gdp.globus.org/gt4-tutorial/multiplehtml/index.html

CHAPTER 3

仮想組織とは何？

仮想組織とは何か？

- A virtual organization (VO) is a dynamic collection of resources and users unified by a common goal and potentially spanning multiple administrative domains. (Foster, I. and Kesselman, C. Computational Grids. Foster, I. and Kesselman, C. eds.The Grid: Blueprint for a New Computing Infrastructure, Morgan Kaufmann, 1999,2-48.)
- 仮想組織とは、同一の目標を達成するために選択された資源とユーザの動的な集合であり、複数の管理ドメインに跨ることが想定されている.



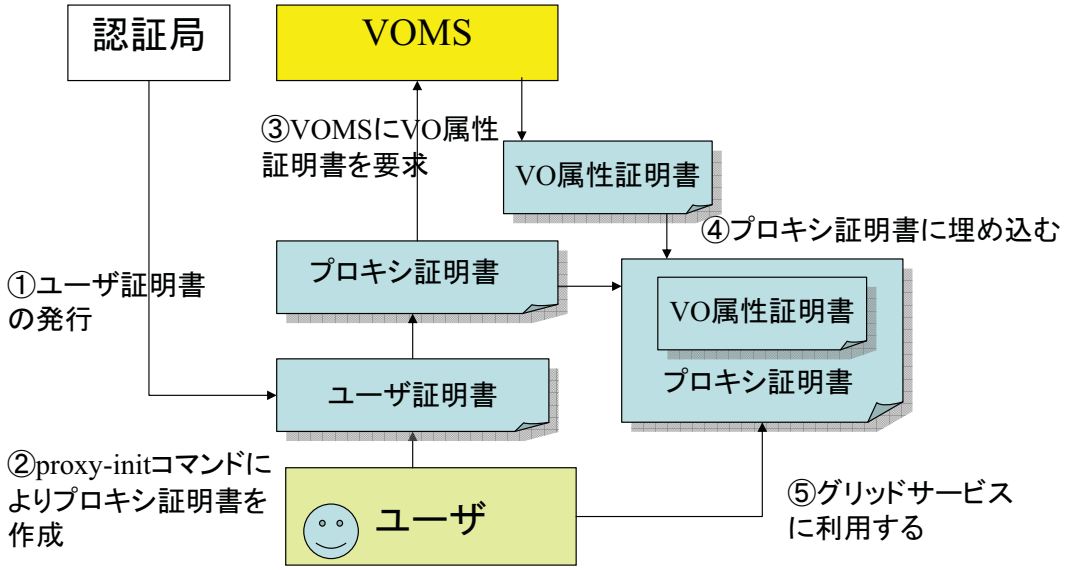
VOで実現すべきこと

- セキュリティ機能
  - VOの外からの不法なアクセスを排除するため アクセスを管理・制御可能であること
- ユーザ・資源の管理機能
  - プログラムの実行や資源の管理、ロギングなどすべてに及ぶ広範囲な管理機能を有すること
- VOポリシー管理機能
  - VOのポリシーに基づいて適切なサービスを提供可能であること
- 上記の各機能を管理ドメインを跨いで実現
  - 現実世界の組織(大学、企業あるいはその部門、提供されるサービス)ごとに独立に管理していたユーザとその役割、アクセス権限などを必要に応じて統合して 1つの仮想的なアクセス空間を提供すること

VOの作り方~NAREGIの例

- NAREGIはVOMSを採用
- VOMSとは、EU-DataGrid Projectにより開発されたVO管理ミドルウェアであり、Virtual Organization Membership Service の略称である.
- ユーザとVOの関係をGroup, Roll, Capabilityとして定義しアクセス制御を行なう。
- voms-proxy-init コマンドによりVOMS用のProxy証明書を生成し、グリッドのジョブ投入に使用する.
- VO関連情報は、Proxy証明書のX.509v3拡張情報部分に独自拡張情報として加えられ、グリッドのスケジューラや各種計算資源にて参照される.

VOMSの利用方法



VOの基本的な運用ポリシー

I. 所有者決定（Ownership Approach）の原則
- ✓ 資源所有者は自分の管理する資源の扱いについて全ての決定権を持つ
- ✓ VO管理者はそのVOに属するメンバの登録・削除・属性付与につき全ての決定権を持つ

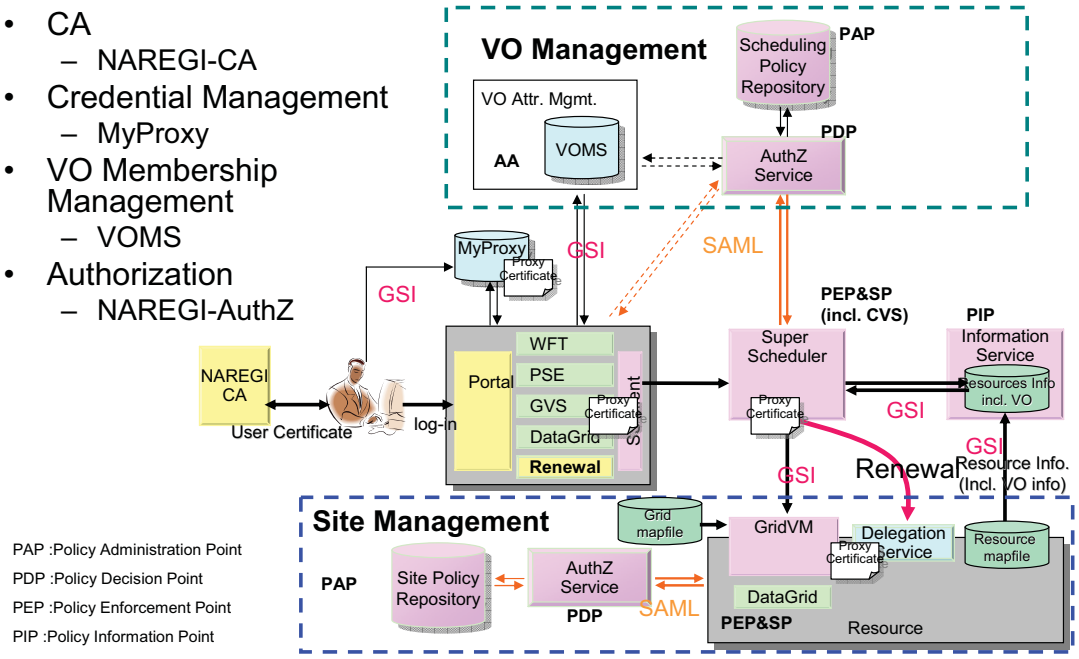
II. VOMS(VO Membership Service)互換
- ✓ X.509属性証明書の利用
- ✓ group, role, capabilityによる属性定義

III. 認可サービスの提供
- ✓ GT4コンテナの認可ハンドラから呼び出し可能
- ✓ XACMLによるアクセス制御ポリシーの定義

認可サービスの仕組み

NAREGIにて開発予定

- CA
  - NAREGI-CA
- Credential Management
  - MyProxy
- VO Membership Management
  - VOMS
- Authorization
  - NAREGI-AuthZ

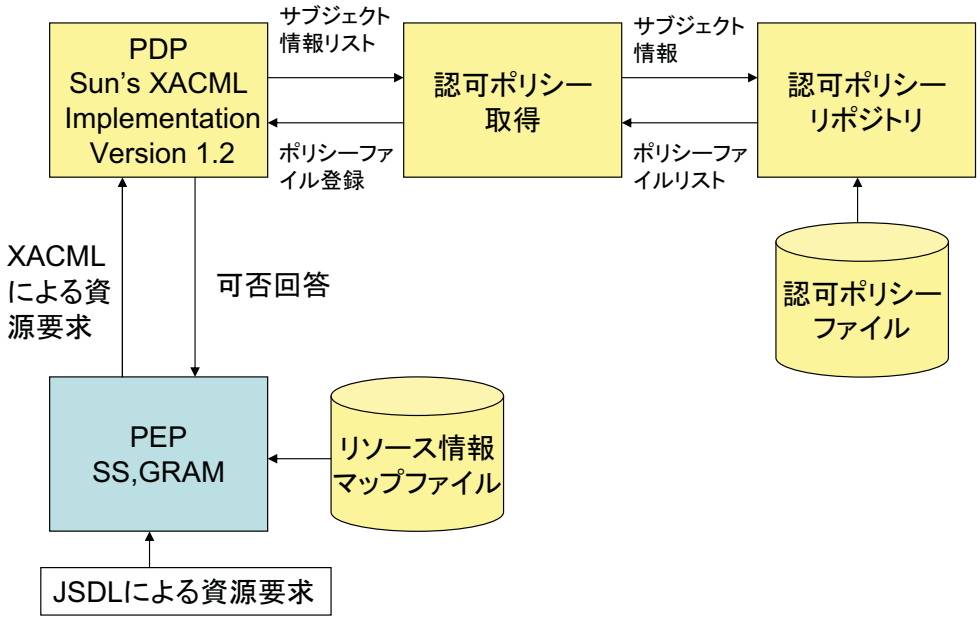


PAP :Policy Administration Point
PDP :Policy Decision Point
PEP :Policy Enforcement Point
PIP :Policy Information Point

VOに関する責任分担案

- 利用者
  - 認証局からユーザ証明書を発行してもらい、Proxy証明書を作成してMyProxyへ登録しておく
  - VOMSへVO属性証明書の発行を依頼し、Proxy証明書の拡張部分へ埋め込む
- VO管理者
  - 管理したいVOに対応したVOMSを運用する
  - VOMSを用いてVOメンバの登録・削除・属性付与を行う
  - サイト管理者との間で資源利用に関する契約を結ぶ
  - SSに対して特別な認可ポリシーを設定したい場合は、認可サービスを運用する
    - SSにリソース情報マップファイルを、Scheduling Policy Repositoryに認可ポリシーファイルを設定する
- サイト管理者
  - 管理したい資源毎にGridVM, サイト毎にISを運用する
  - 受け入れるVOについて、(例えばVOMSの情報を基に)grid mapfileを作成する
    - Grid mapfileには、ユーザ証明書のDNとローカルアカウントの対応を定義する
    - 定義の方法はサイトのポリシーによるが、個別のユーザ識別を行う場合と、VO毎に一括したプールアカウントを適用する場合とがある
    - 課金については、サイトの独自機能として構築することが前提となる。VO単位の課金方法の一例を次ページに示す
  - 受け入れるVOについて、VO管理者との契約を基にGACLファイルを作成する
    - GACLファイルには、VO毎の資源利用可能性を定義する
    - この情報を、サイトのISは定期的(規定値では5分間隔)に読み出し、IS全体で共有する
    - SS はブローカリング時にプロキシ証明書に記載されているVO名を元に IS の情報を検索し、そのVOが利用できる資源を知る
  - 資源のアクセスポリシーを管理するため認可サービスを運用する
    - GRAM(GridVM)にリソース情報マップファイルを、Site Policy Repositoryに認可ポリシーファイルを設定する

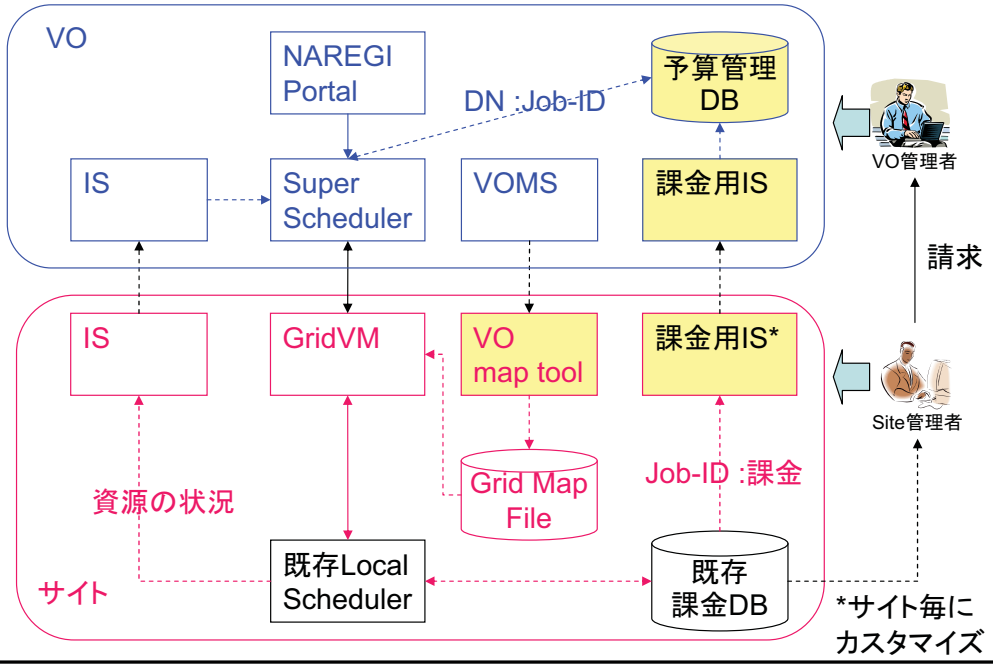
認可サービスの運用例



VO属性の利用ポリシー案

- groupとroleを指定
  - VO>group>roleの階層構造を前提とする
    - 一枚の属性証明書に記述するのはVO:group:roleの各項目一つ
  - group名はVO管理者が自由に決める
  - roleとして"VO管理者/group管理者/role無"を指定可能
- 想定される利用
  - IS
    - ISがサイト毎のISからサイト情報を収集する時に、サイト管理者のポ リシーを反映させたアクセス制御を行う。認可サービスを適用する。
    - 「VO管理者」属性を確認し、ポリシーを適用する
  - PSE
    - ソフトウェアの管理や利用のために、ソフトウェア毎の排他的なアクセス管理を行う。但し認可サービスは使わず、独自にポリシーを組み込む。
    - ソフトウェア毎にgroupを定義する
    - 「group管理者」属性を確認し、対応するソフトウェア管理を可能とする
      - 「VO管理者」の権限は「group管理者」の権限を包含する
    - 「group」属性を確認し、対応するソフトウェアを利用可能とする
    - 一つのユーザセッションの間、VO:group:roleは不変である

VO単位課金への利用例



CHAPTER 4

5年後の姿

5年後の姿

- OGSAによる標準化
  - OGSA(Open Grid Services Architecture：2002年2月に開かれたGGF4にてIBM社が提案)によりSOAPやWSDLなどWEBサービス技術を基盤としてグリッドの全ての機能をサービス化
- IGTF (International Grid Trust Federation)による国際認証連携
  - APGRID、EUGRID、TAGにより世界を3分割管理
  - 日本の認証局はAPGRIDの認可を受ければ証明書が世界中で有効となる
- ID管理との連携
  - 管理ドメインを跨るIDのフェデレーション機能としてプライバシー保護を重視するShibbolethが主流になるかもしれない
- NIIによるCSI (Cyber Science Infrastructure)構築
  - UPKIによる相互信頼の基盤の確立
  - NAREGIグリッドミドルウェアによるe-Science基盤の確立
    - 全国規模の研究・開発・運用体制の構築

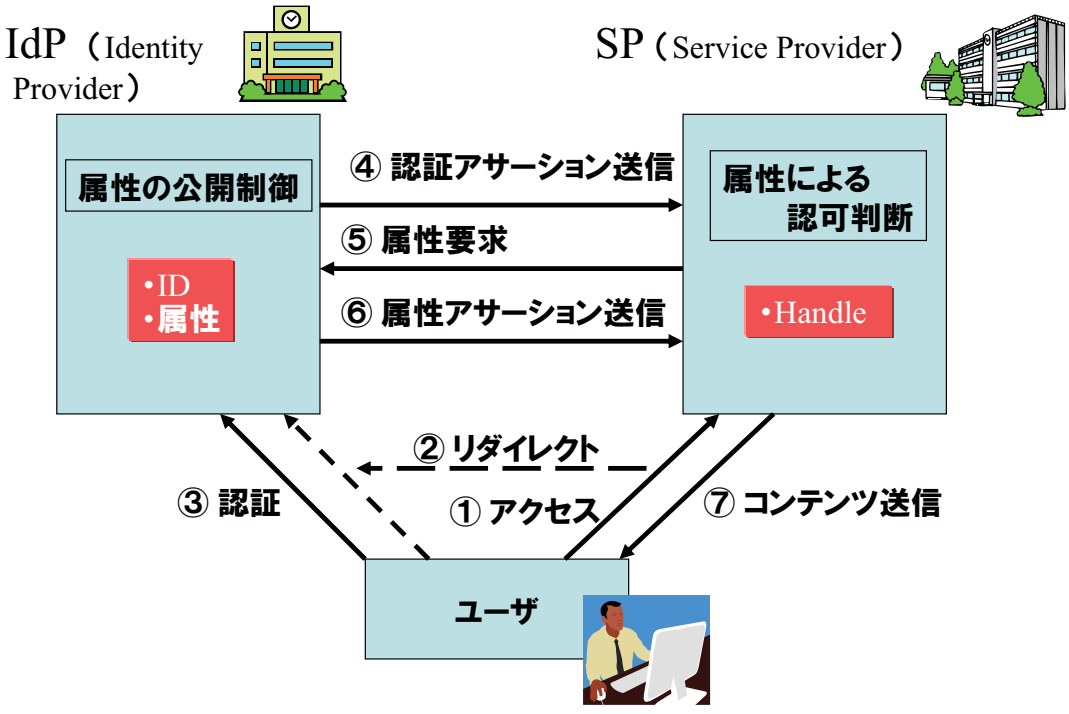
ApGrid PMA

- 2004年6月に設立されたアジア・太平洋地域のPMA（Policy Management Authority：認証局のポリシーおよび運用に関する整合性を取る調整機関）
- ApGrid PMAの認可を受けるためには、信頼レベルの高い運用を継続し毎年監査を受けなければならない
- 現在認可を受けているのは、NAREGI, AIST, KEKの各認証局であり、NIIは将来NAREGI認証局を引き継いでUPKIのグリッド認証基盤とする予定

Shibboleth~ ID管理との連携

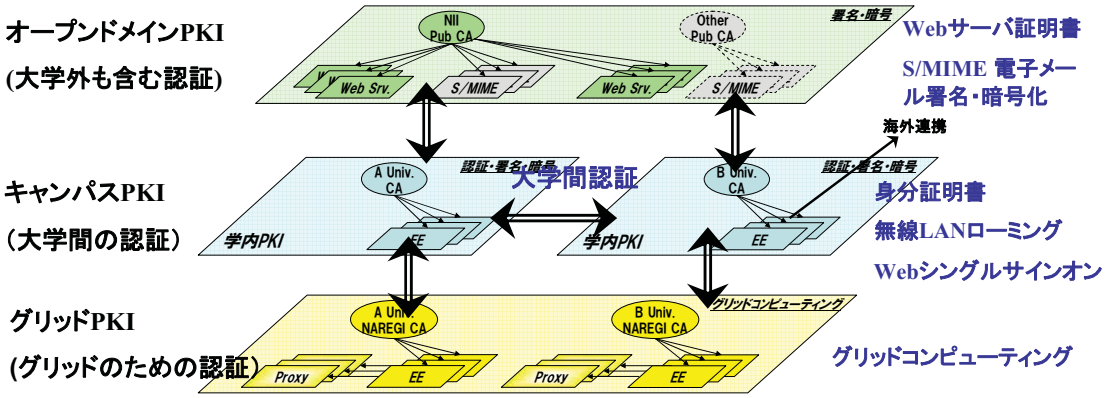
- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト
- SAML、eduPerson等の標準仕様を利用した、認可のための属性交換を行う標準仕様とオープンソフト
- 最新はShibboleth V1.3
- Shibboleth V2.0（SAML2.0ベース）は未リリース
- 米国、欧州でShibbolethのFederationが運用、拡大

Shibbolethの基本動作



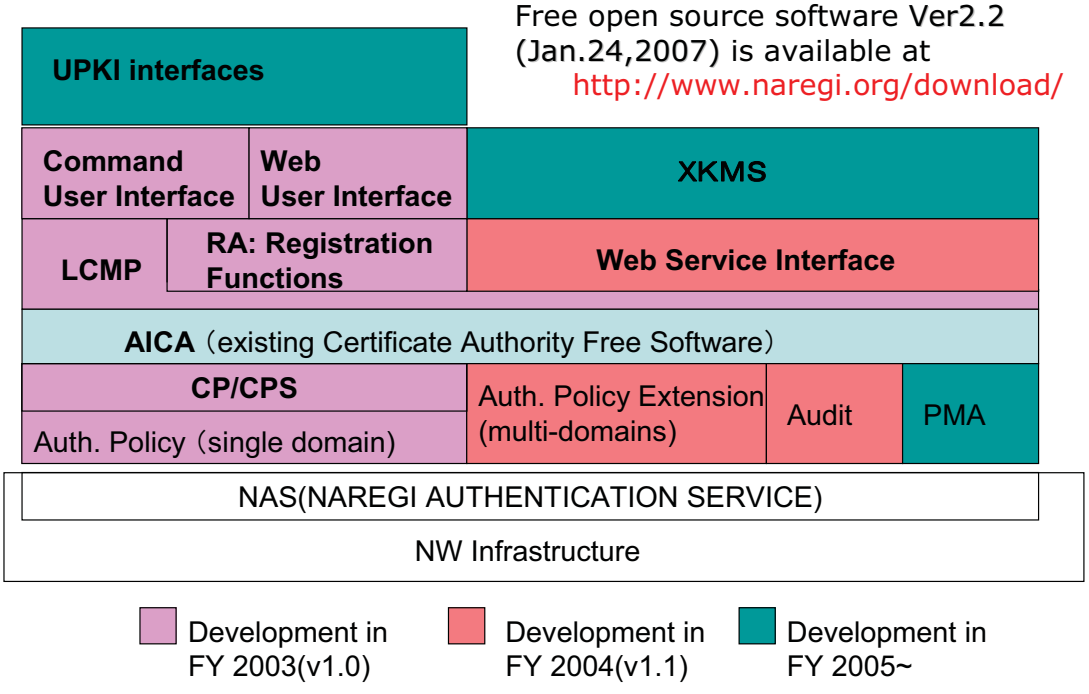
UPKIの基本アーキテクチャ

- 3階層のPKI (Public Key Infrastructure)による役割分担と連携

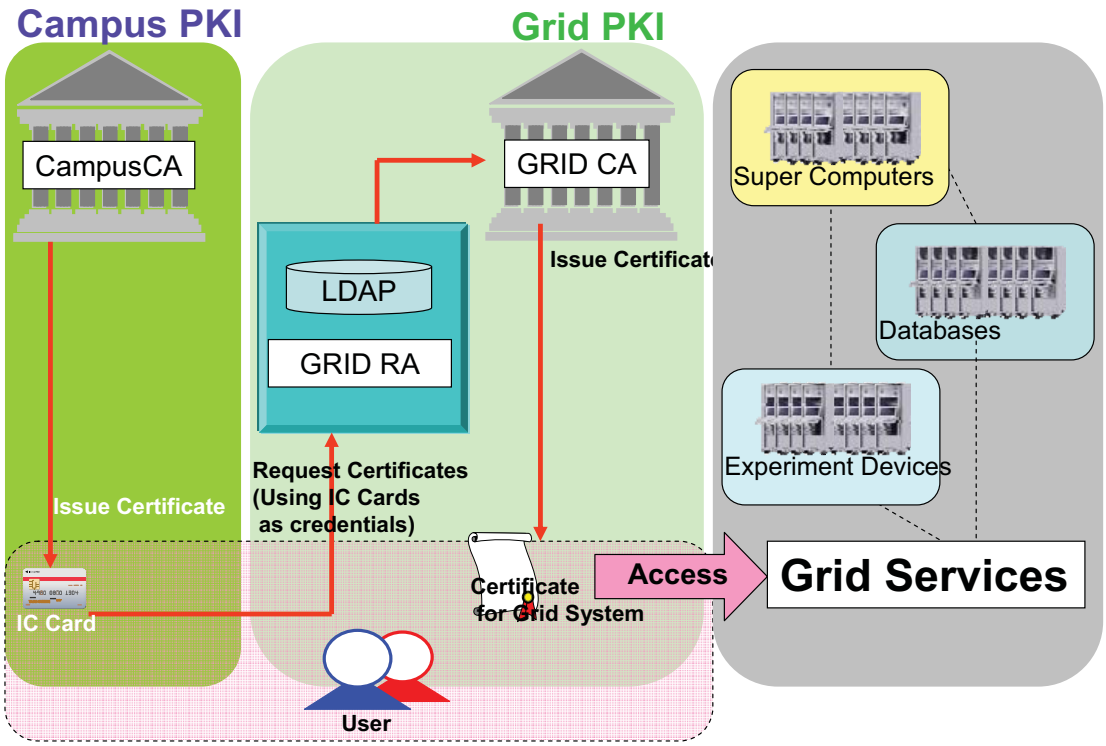


Software Stack of NAREGI-CA

Free open source software Ver2.2 (Jan.24,2007) is available at
http://www.naregi.org/download/



Campus-Grid PKI Federation



将来の姿のお手本はEGEEにあり

共通業務・調整を行う組織

利用者の近くに支援組織

Support Structures & Processes

- Operations Coordination Centre
- Regional Operations Centres
- Global Grid User Support
- EGEE Network Operations Centre
- Operational Security Coordination Team
- Training activities

Test-beds & Services

- Production Service
- Pre-production service
- Certification test-beds
- Training infrastructure

Security & Policy Groups

- Joint Security Policy Group
- EuGridPMA (& IGTF)
- Grid Security Vulnerability Group
- Operations Advisory Group

「次世代学術情報基盤」のイメージ（Super-CSI :Super Cyber Science Infrastructure）

仮想組織はサイバースペースにおいて研究・開発コミュニティを活性化