平成20年度情報処理軽井沢セミナー

グリッドの認証とCSIの活用

2008.9.4
国立情報学研究所
リサーチグリッド研究開発センター
峯尾真一

目次

1. グリッドの歴史を辿る
2. セキュリティの考え方
3. 仮想組織の作り方
4. グリッド認証局の運用
5. グリッドの将来動向

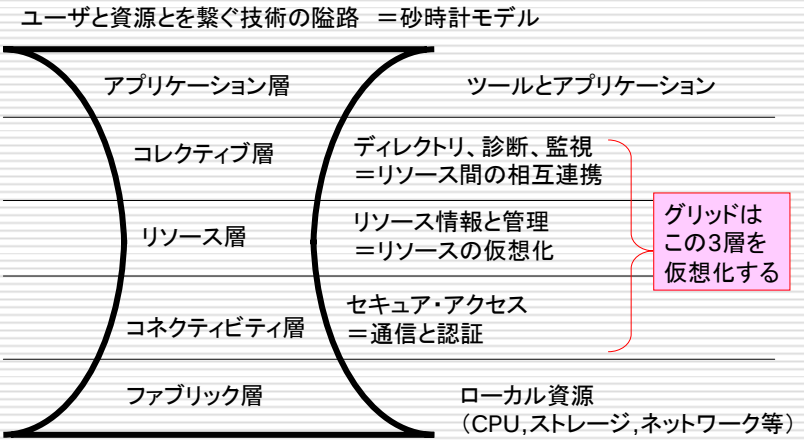
CHAPTER 1

グリッドの歴史を辿る

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)

グリッドの概念



グリッドの進化

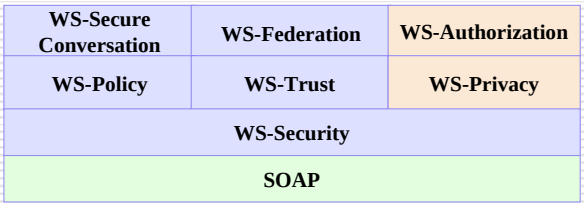
- Gridサービスをステートフルなwebサービスとして定義したOGSA (Open Grid Services Architecture)を提唱

  “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

グリッドで何ができるのか？

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
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
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
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

グリッドの事例

- LCG (LHC Computing Grid) project
  - CERNに置かれた粒子加速器を世界中の研究者で共有するためのプロジェクト
  - 15PB/年の実験データを世界中に配布するために11箇所のTier-1センターを設置、解析用のTeir-2センターは140箇所以上
  - 現在、35カ国に100,000CPUコア、57PBディスク、53PBテープドライブを有する研究共同体が実現している

CHAPTER 2

セキュリティの考え方

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

用語解説：PKI

- PKI (Public Key Infrastructure)
  - 公開鍵暗号方式を用いて電子署名、相手認証、メッセージ認証、鍵配送等を行う基盤技術
- X.509証明書フォーマット
  - ユーザの公開鍵を認証局が電子署名をして作成する公開鍵証明書の標準フォーマット
- 認証局(CA :Certificate Authority)
  - ユーザやサーバに対して、保有する公開鍵とその名前の対応を、公開鍵証明書を用いて証明する信頼できる第三者機関(Trusted Third Party)

GSI とはどんなものか？

GSI :Grid Security Infrastructure

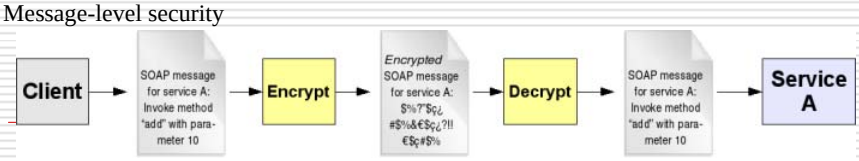
- 目的
  - GT4のセキュリティ層として、安全な通信と認可の仕組みを実現すること
- 提供する機能
  - 通信のセキュリティ
  - サービスを行う時の相互認証
  - 認可の仕組み
  - 権限委譲
  - 各レベル（コンテナ・サービス・資源）毎のセキュリティ設定
- 参考資料
  - The Globus Toolkit 4 Programmer's Tutorial
    - http://gdp.globus.org/gt4-tutorial/multiplehtml/index.html

(1) GSI:通信のセキュリティ

- Transport-level（トランスポート・レベル）とmessage-level（メッセージ・レベル）のセキュリティ・プロトコルが選択可能

Transport-level security

Message-level security



The Globus Toolkit 4 Programmer's Tutorial

セキュリティ・プロトコルの比較

	GSI Secure Conversation	GSI Secure Message	GSI Transport
Technology	WS-SecureConversation	WS-Security	TLS
Privacy (Encrypted)	YES	YES	YES
Integrity (Signed)	YES	YES	YES
Anonymous authentication	YES	NO	YES
Delegation	YES	NO	NO
Performance	Good if sending many messages	Good if sending few messages	Best

The Globus Toolkit 4 Programmer's Tutorial

(2) GSI:サービスを行う時の相互認証

- 3種類の認証方式をサポート
  - X.509証明書
    - 最も強い認証方式でGSIの機能が全て利用可能
  - ユーザ名とパスワード
    - 権限委譲等の機能が使えなくなるので通常は使わない
  - 認証無し
    - 通常は使わない

The Globus Toolkit 4 Programmer's Tutorial

(3) GSI:認可の仕組み

- サーバ側で指定できる認可方式
  - None
    - 認可判断をしない
  - Self
    - クライアントのIDがサービスのIDと同じ時のみサービスする
  - Grid-mapfile
    - 認可するユーザをGrid-mapfileに登録する
  - Identity authorization
    - クライアントのIDを基に判断する仕組みを入れる
  - Host authorization
    - 特定のホストからのサービス依頼のみ許可する
  - SAML Callout authorization
    - OGSA認可サービスへ問い合わせる

The Globus Toolkit 4 Programmer's Tutorial

用語解説：grid-mapfile

- 証明書の持ち主とローカルアカウントとの対応表
  - 証明書の名前：そのシステムに登録済みユーザ名
  - ジョブはこのユーザ名で投入される
- この対応表を作るのはシステム管理者
  - 証明書の名前を集めるのは大変
    - EGEEはこれを回避->VO単位で認可する

GSI：認可の仕組み(続)

- クライアント側で指定できる認可方式
  - None
    - 認可判断をしない
  - Self
    - サービスのIDがクライアントのIDと同じ場合のみサービスを依頼する
  - Identity authorization
    - サービスのIDを基に判断する仕組みを入れる
  - Host
    - サービスがホストの資格証明書を持っている場合のみサービスを依頼する

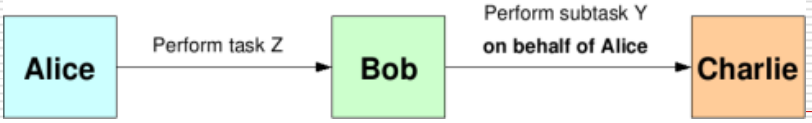
The Globus Toolkit 4 Programmer's Tutorial

GT4 GSIの機能実装図

	メッセージレベルセキュリティ（X.509証明書を用いた場合）	メッセージレベルセキュリティ（X.509証明書を用いない場合）	トランスポートレベルセキュリティ（X.509証明書を用いた場合）
認可	SAML and grid-mapfile	Grid-mapfile	SAML and grid-mapfile
権限委譲	X.509 Proxy Certificate/WS-Trust		X.509 Proxy Certificate/WS-Trust
認証	X.509 End Entity Certificate	Username/ Password	X.509 End Entity Certificate
メッセージ保護	WS-Security WS-SecureConversation	WS-Security	TLS
メッセージ形式	SOAP	SOAP	SOAP

(4) GSI:権限委譲

- どんな時に必要になるか？
  - AliceはTask ZをBobに依頼したい
  - Bobはその一部task YをCharlieに渡したい
  - CharlieはAliceを知っているがBobは知らない
  - そこでAliceはBobがAliceの代理で依頼することをCharlieに示す必要がある
- 権限委譲の方法
  - Proxy certificate（プロキシ証明書）を用いる



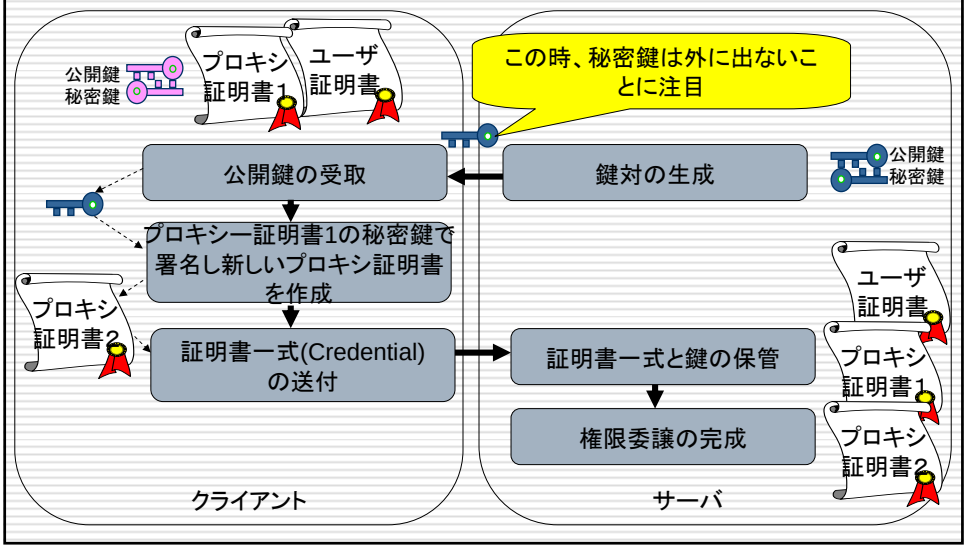
The Globus Toolkit 4 Programmer's Tutorial

用語解説：プロキシ証明書

- X.509公開鍵証明書と同じ形式で権限委譲を証明
  - 但し署名しているのは認証局ではなくエンドユーザ
- 公開鍵はプロキシ証明書毎に新しく作成される鍵ペアの片方

The Globus Toolkit 4 Programmer's Tutorial

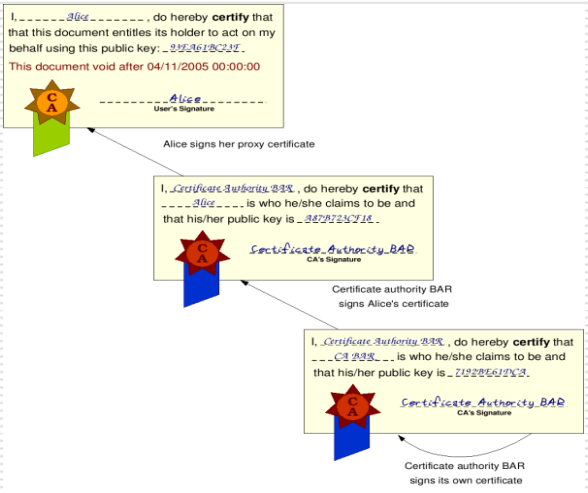
権限委譲の流れ
Credential Delegation



用語解説：Credential

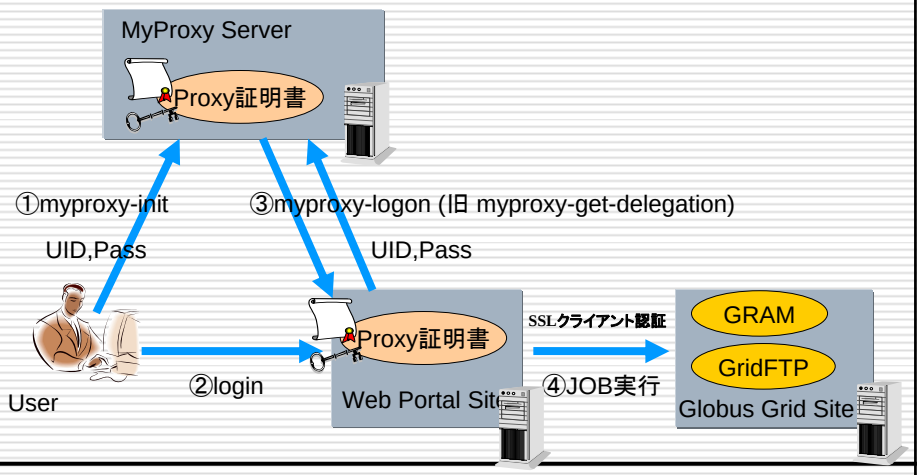
- GSIにおいては以下を含む資格証明書
  - プロキシ証明書（複数の場合もある）
  - 基になったユーザ証明書
- Credential DelegationによりSSO (Single Sign-On)を実現
  - プロキシ証明書から権限委譲の連鎖をすることにより、ユーザ自身の応答を不要とする

プロキシ証明書の検証



The Globus Toolkit 4 Programmer's Tutorial

MyProxy という名の金庫



①myproxy-initでMyProxyServerにProxy証明書を発行(UID,Passwordを入力)

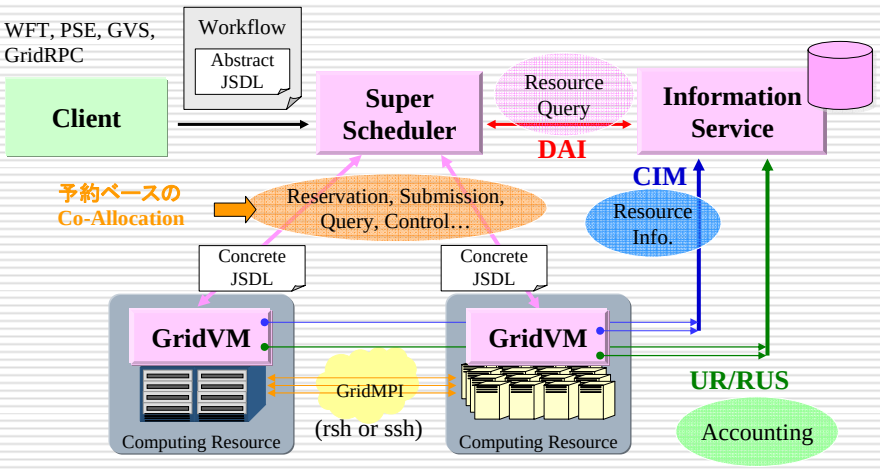
②PortalSiteにloginする。

③myproxy-logonでUID,Passwordを入力しProxy証明書を発行

④取り出したProxy証明書を利用してGlobus GridSiteでジョブ実行

GSIによるサービス連携

~ NAREGIのジョブ投入例

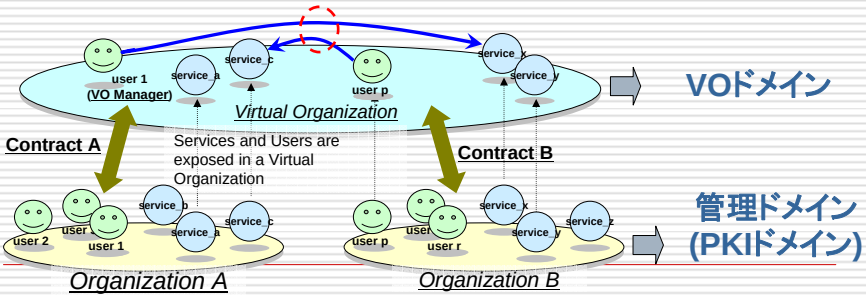


CHAPTER 3

仮想組織の作り方

仮想組織とは何か？

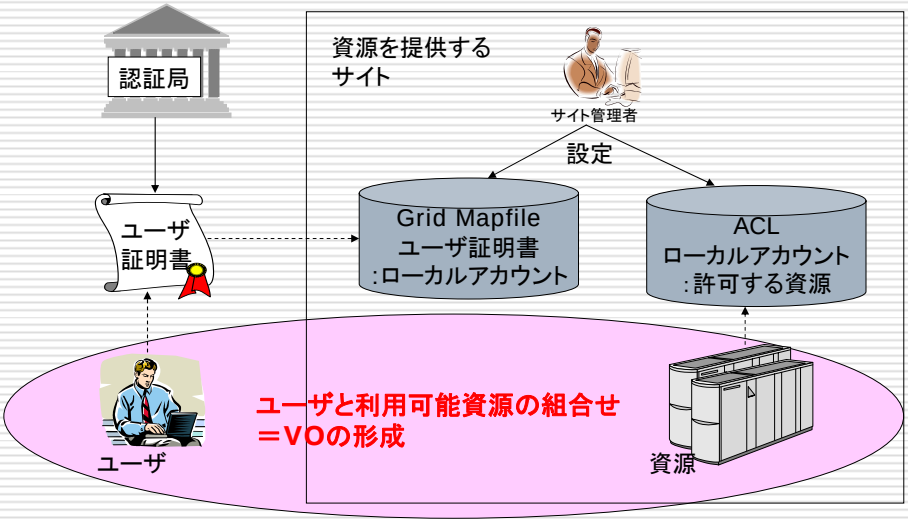
- A virtual organization (VO) is a dynamic collection of resources and users unified by a common goal and potentially spanning multiple administrative domains. (Foster, I. and Kesselman, C. Computational Grids. Foster, I. and Kesselman, C. eds.The Grid: Blueprint for a New Computing Infrastructure, Morgan 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～Globus Toolkit



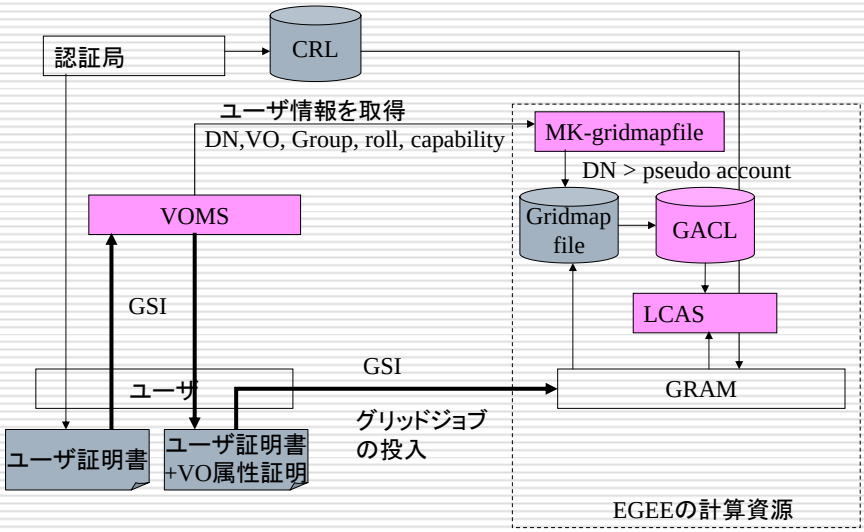
VOの作り方～NAREGIの例

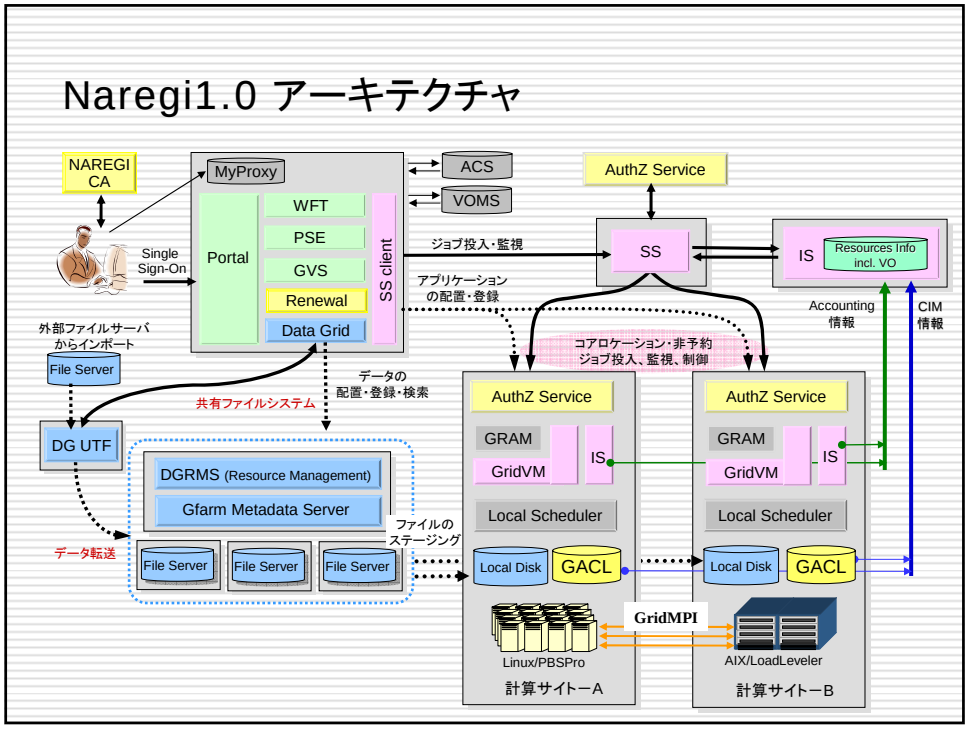
I. 所有者決定(Ownership Approach)の原則
- ✓ 資源所有者は自分の管理する資源の扱いについて全ての決定権を持つ
  - ✓ 受け入れるVO情報をIS経由でSSへ渡す
- ✓ VO管理者はそのVOに属するメンバの登録・削除・属性付与につき全ての決定権を持つ

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

VOMSの活用例

～ EGEEのジョブ投入





VOに関する責任分担(1)

- 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

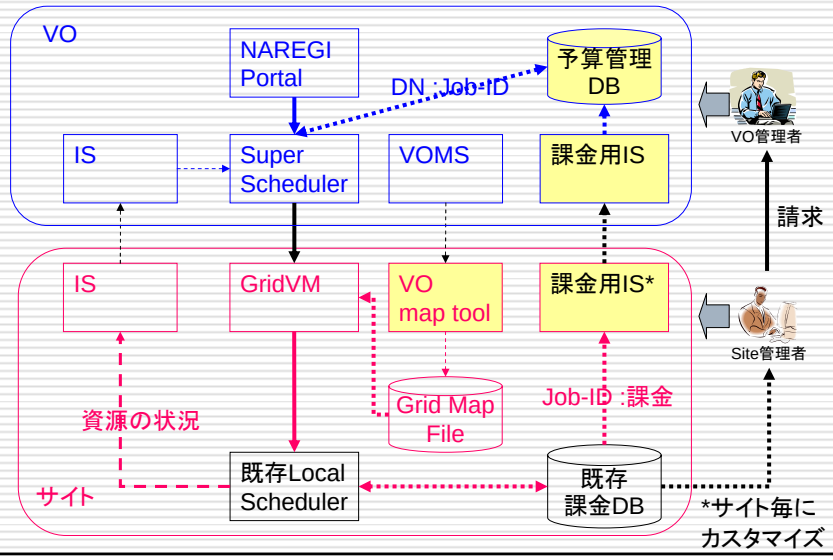
VOに関する責任分担(2)

- 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

VOに関する責任分担(3)

- 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とGACLファイルを作成する
    - 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
    - GACLファイルには受け入れ可能なVO名を登録する
    - 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。
  - 資源のアクセスポリシーをより細かく管理する場合には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

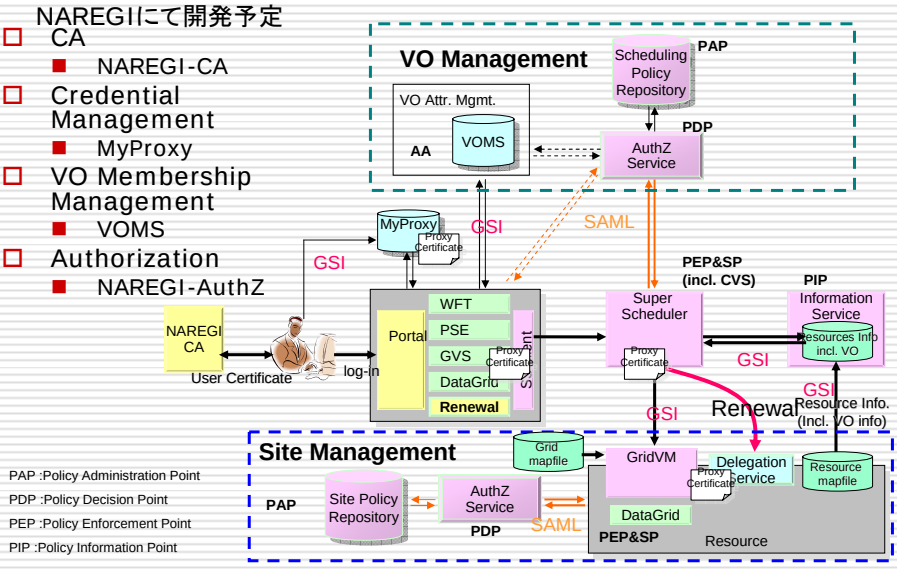
VO単位課金への利用例

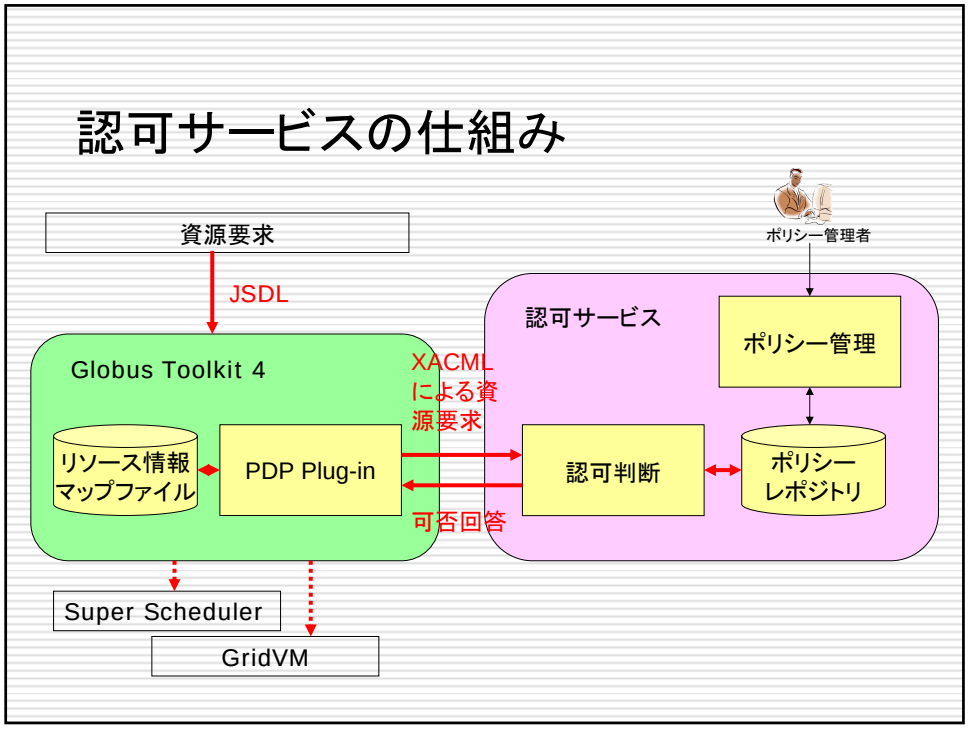


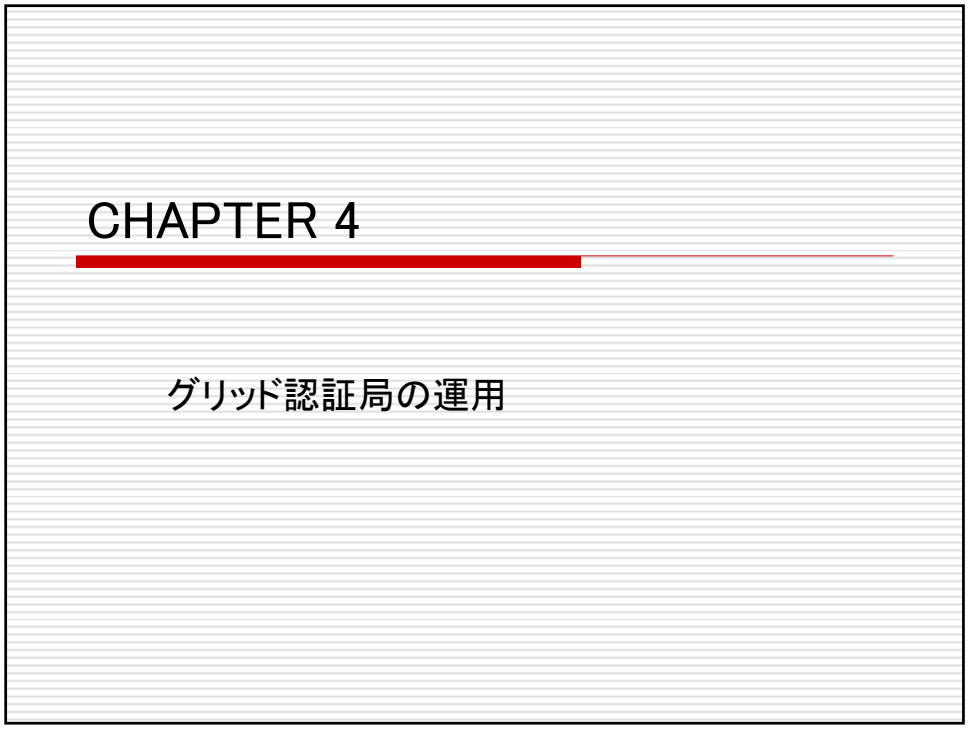
認可サービスの利用

NAREGIにて開発予定

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




認可サービスの仕組み
資源要求
JSDL
Globus Toolkit 4
リソース情報
マップファイル
PDP Plug-in
XACML
による資
源要求
可否回答
Super Scheduler
GridVM
ポリシー管理者
認可サービス
ポリシー管理
認可判断
ポリシー
レポジトリ


CHAPTER 4
グリッド認証局の運用

グリッド認証局の運用

- IGTF (International Grid Trust Federation)
  - 国際的な信頼関係構築の取り組み
- NAREGI認証局の運用事例
  - IGTF(APGRID)準拠の認証局
- UPKIにおけるグリッド認証局
  - CSIの中で構築予定

(1)IGTF

- メンバPMA (Policy Management Authority :認証局のポリシー管理を行う独立組織)は認証局の審査、承認を行う
  - あるPMAで承認されれば、自動的にすべてのPMAに信頼される
- IGTFは認証プロファイル(Authentication Profile)を管理する。
  - 証明書の用途、保証レベル、認証局の運用用件に応じた認証プロファイルを規定
- 現在の認証プロファイル
  - Classic AP (EUGrid PMA)
  - Short Lived Credential Services (SLCS) AP (TAGPMA)
  - Member Integrated Credential Services (MICS) AP (TAGPMA)
- APへの変更が提案されると、すべてのPMAに議長を通して変更が伝えられる。
- 変更はすべてのPMAで承認される必要がある。

PMAの現状

- 現在3つのPMAが存在する
  - EUGrid PMA (欧州地域担当)
  - TAG PMA (アメリカ地域担当)
  - APGrid PMA (アジア太平洋地域担当)
- 各PMAの主たる役割
  - 各地域内の認証局ポリシーの調整
  - 他のPMAとの認証局ポリシーの調整

Scope of the PMA

- 参加メンバの管理
- チャーターの策定、管理
- 認証プロファイルに基づいたminimum CA requirementsの策定、管理
- Minimum CA requirementsに基づいた認証局の承認
- 認証局の監査
- メンバ認証局の名前空間の管理
- メンバ認証局のルート証明書配布
- 認証プロファイルの策定、提案

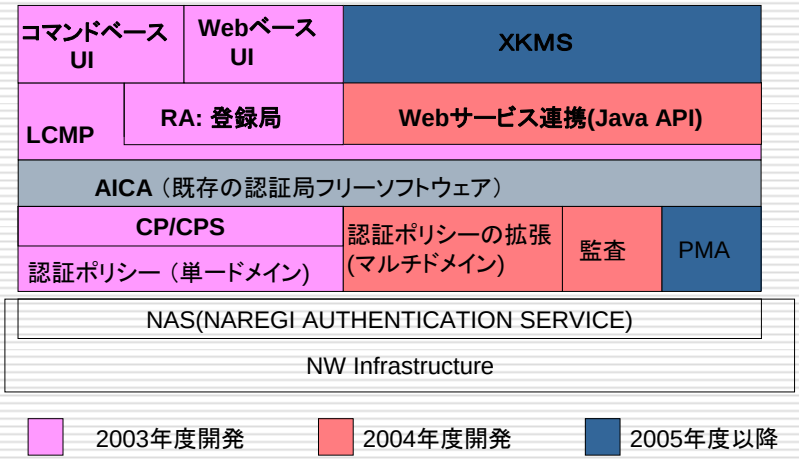
(2)NAREGI認証局の運用事例

- **NAREGI-CAとは**
- **運用概要**
  - ① 事前準備(ライセンスID一括要求)
  - ② 証明書の申し込み(ライセンスID発行要求)
  - ③ 証明書の発行申請
  - ④ 証明書の失効申請
  - ⑤ 証明書の再発行申請(失効後の再発行)
  - ⑥ Gridマップファイル作成用データの入手

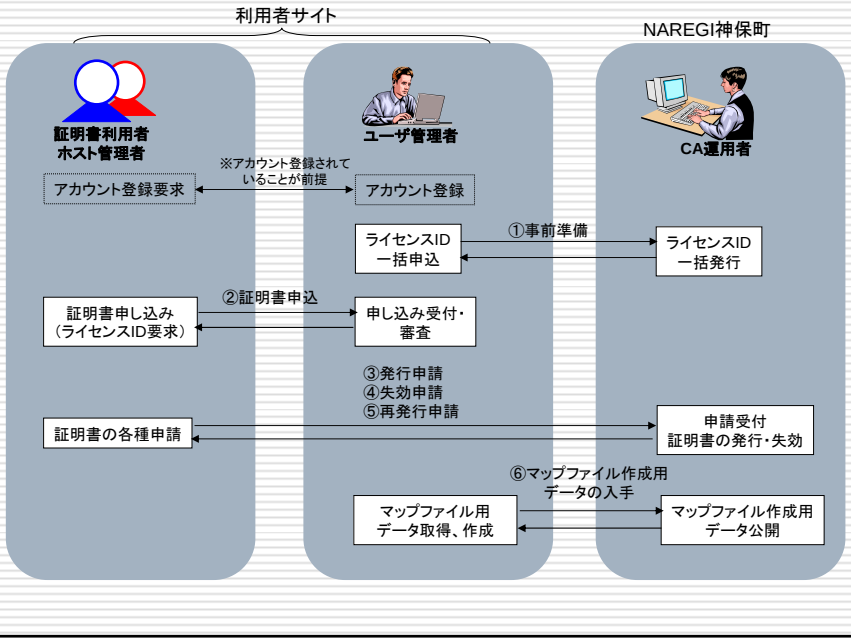
NAREGI-CA とは

- NAREGI-CAとは、NAREGI(National Research Grid Initiative)プロジェクトにより開発されたオープンソースのCAソフトウェアである。
- 2004年度より、NAREGIプロジェクトにて運用しグリッドホスト向け、ユーザ向け合計で2000枚以上の証明書発行の実績あり。
- 商用CA製品と同レベルの運用が可能になるよう、設計・開発されている。
- CAソフトウェアの開発と同時に、グリッド向けシステムに対応したCP/CPSの策定も行なった。

NAREGI-CA の開発経緯



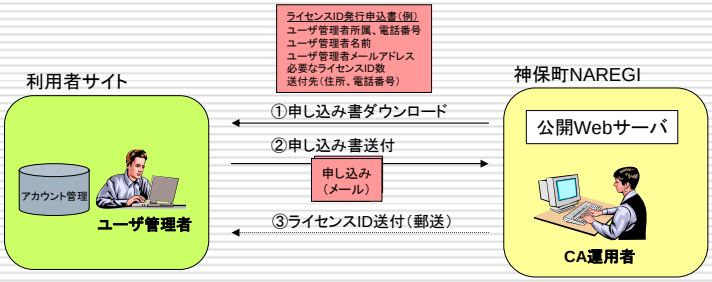
NAREGI-CA 運用概要



①事前準備

◆ユーザ管理者
・認証局よりライセンスID発行申込の用紙をダウンロードし、必要事項の記入後、メールで申し込み書を送付する。

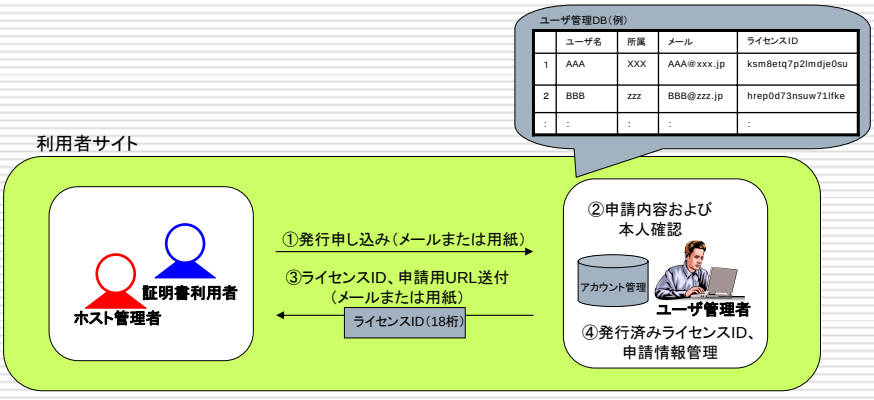
◆認証局
・ライセンスID発行申込書入手後、記載内容、申込者の確認後、要求数のライセンスIDを発行し、申込元に郵送する。



②証明書申込(ライセンスID要求)

◆証明書利用者、ホスト管理者
申込書または申し込みに必要な事項をメールまたは用紙でユーザ管理者に提出する。

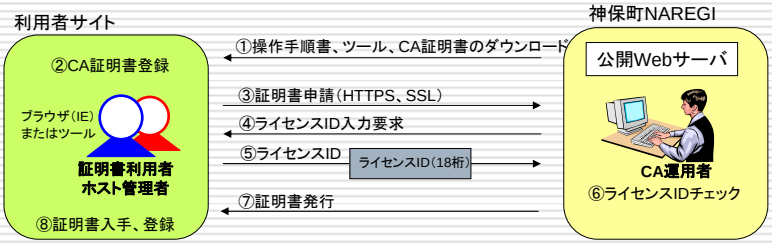
◆ユーザ管理者
・証明書利用者またはホスト管理者からの申し込みを受けると、アカウント申請時に登録した情報と、申請情報を比較し、本人であることを確認する。確認項目は、最低、利用者名・所属部門・メールアドレスを含むことを推奨する。
・発行したライセンスIDとユーザ情報は、マップファイル作成のために管理しておく。



③証明書の発行申請

◆証明書利用者、ホスト管理者
・操作手順書、申請ツール等をWebサーバよりダウンロードする。
・IEまたは、申請ツールにより、認証局への証明書の発行申請を行う。
このとき、2の証明書申込時に入手したライセンスIDを入力する。

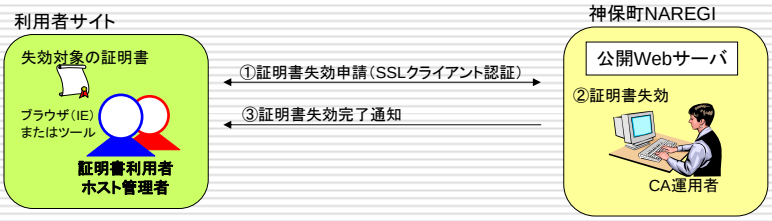
◆認証局
・証明書利用者またはホスト管理者からの発行申請に対し、ライセンスIDをチェックし、有効なライセンスIDであれば証明書を発行する。



④証明書の失効申請

◆証明書利用者、ホスト管理者
・IEまたは、申請ツールにより、認証局への証明書の失効申請を行う。
◆認証局
・証明書利用者またはホスト管理者からの失効申請に対し、クライアント証明書による認証後、証明書を失効する。

注）失効申請時、申請者の確認のためのSSL認証は、失効対象の証明書、秘密鍵を利用する。



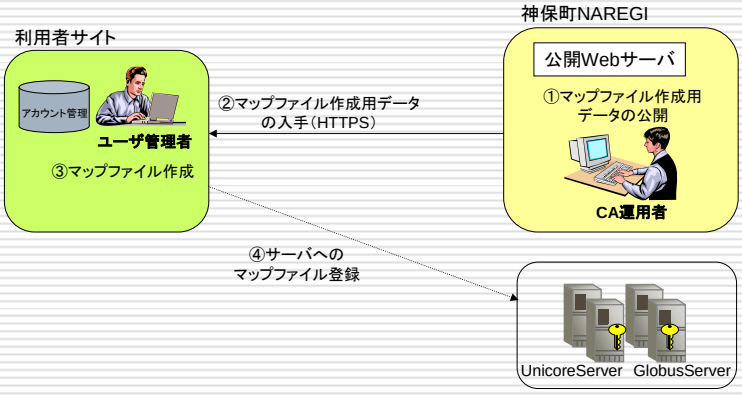
⑤証明書の再発行申請（失効後の再発行）

◆証明書利用者、ホスト管理者は、初期発行と同様に、証明書の発行申し込み（ライセンスID要求）、証明書の発行申請を行う。

⑥Gridマップファイル作成用データ取得

◆認証局
・証明書発行または再発行時、マップファイル作成用データとして、ライセンスIDと証明書情報（サブジェクト）をWebサーバに公開する。

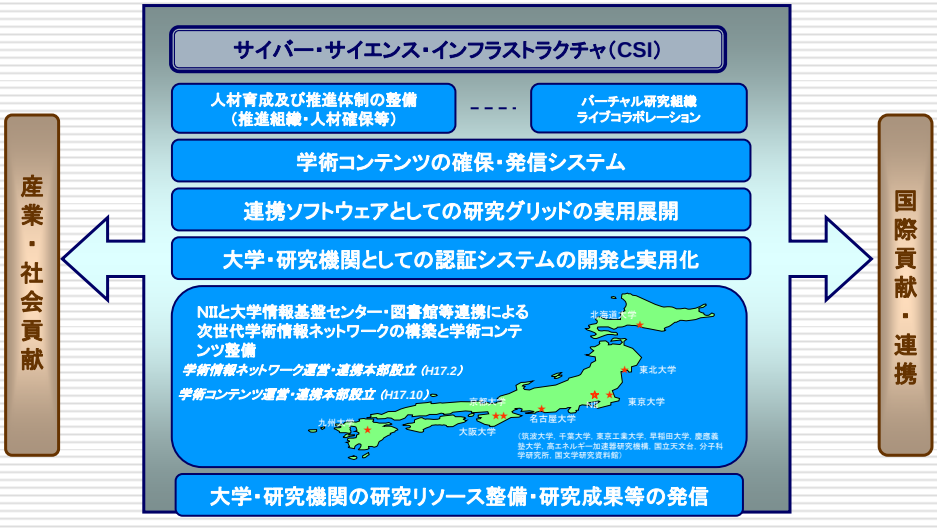
◆ユーザ管理者
・定期的に認証局のWebサーバより、マップファイル作成用データを入手する。
入手したファイルが更新されているかどうかをチェックする。（ファイル内容、サイズ比較など）
更新がある場合は、マップファイルを作成し、サーバへ登録する。



(3)UPKIにおけるグリッド認証局

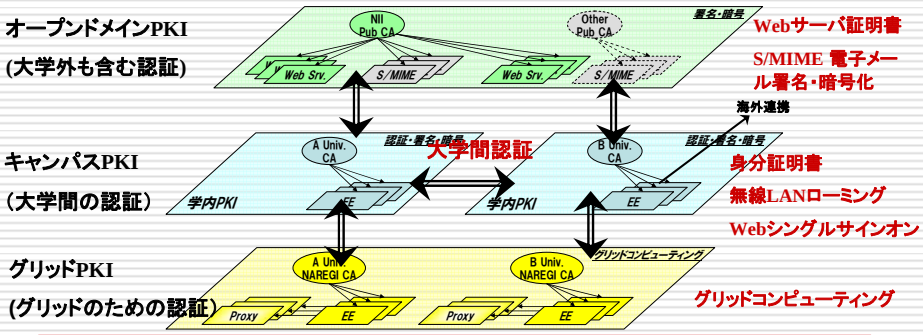
- UPKI構築計画
- UPKIの基本アーキテクチャ
- NAREGI-CAの強化機能
- 将来の発展可能性

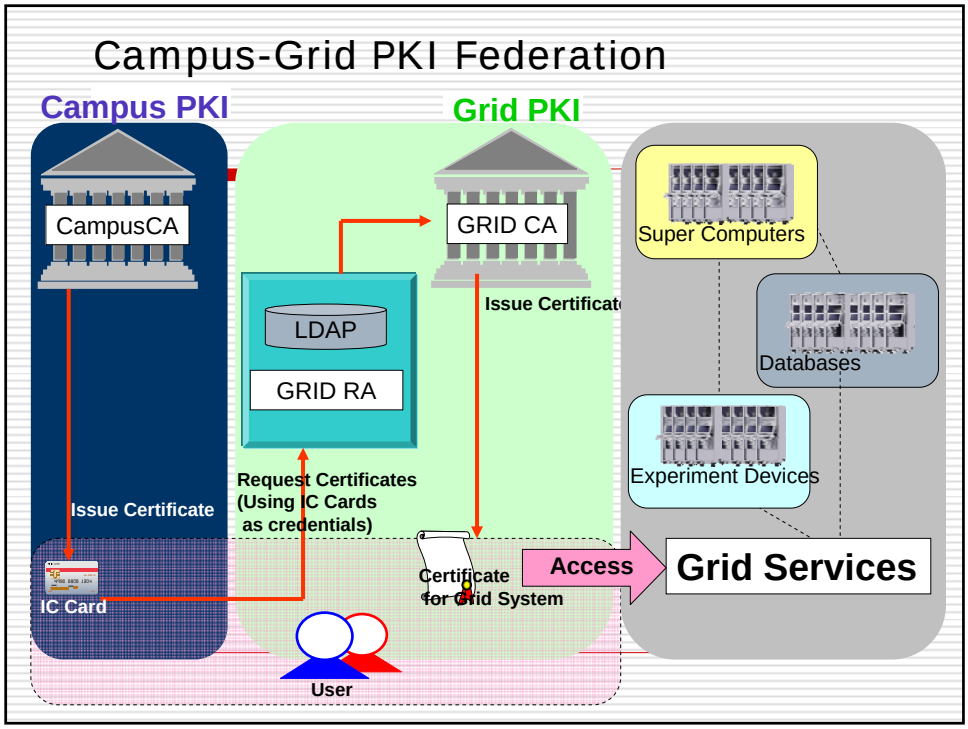
UPKIの構築計画



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





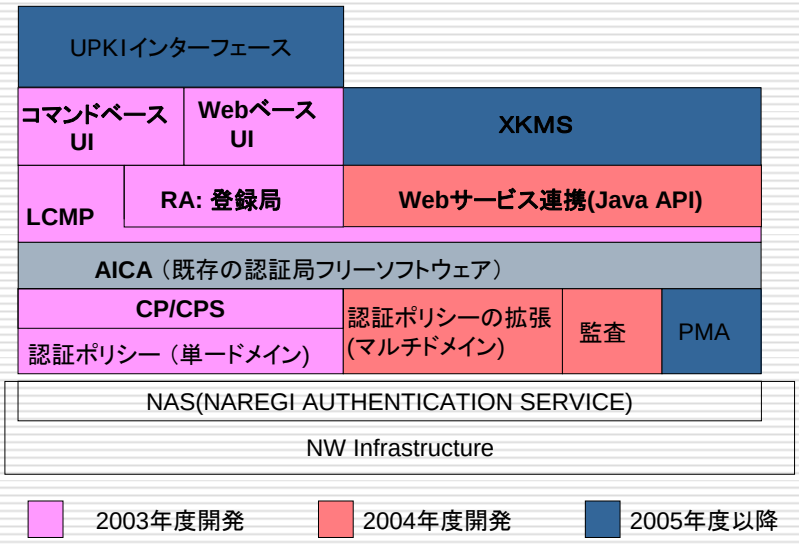
NAREGI-CAの強化機能

① RA (Registration Authority：登録局)機能の権限分離

② チャレンジPIN対応

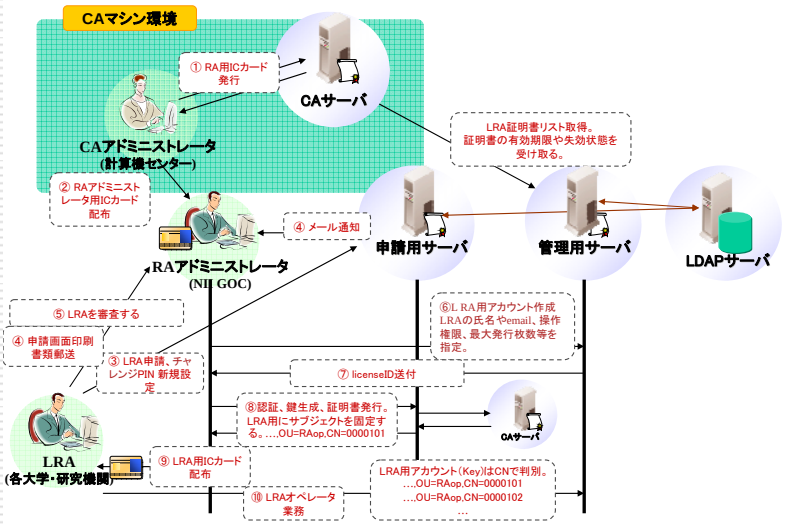
③ 学内認証局と連携したグリッド向け証明書発行インターフェース

NAREGI-CA のUPKI用強化



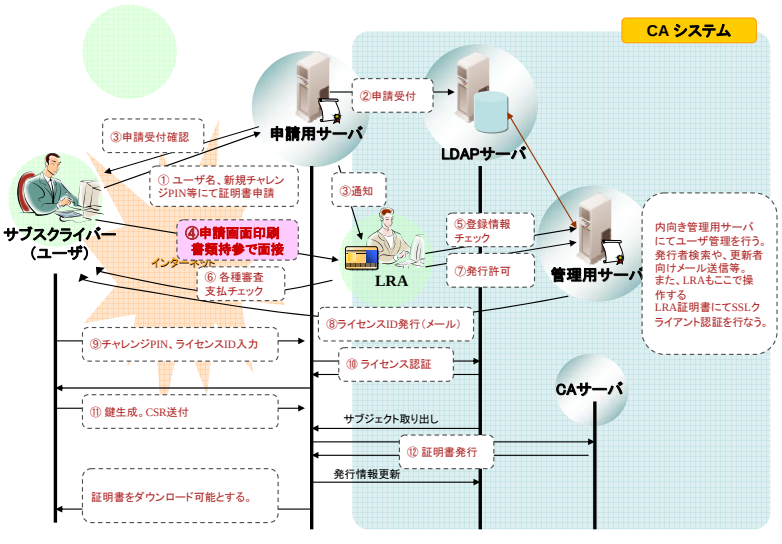
①RA機能の権限分離

各大学・研究機関にLRA (Local RA)を認定し、管理サーバのアクセス権を設定



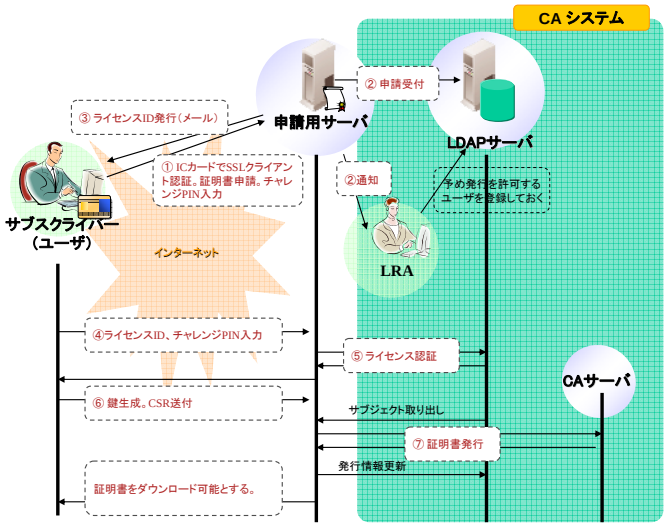
②チャレンジPIN対応

APGRID PMAの信頼性基準を満たすために、ユーザの面接が必要



③学内認証局と連携したグリッド向け証明書発行インターフェース

キャンパスPKI側ではAPGRID PMA準拠の本人確認をしているのが条件



CHAPTER 5

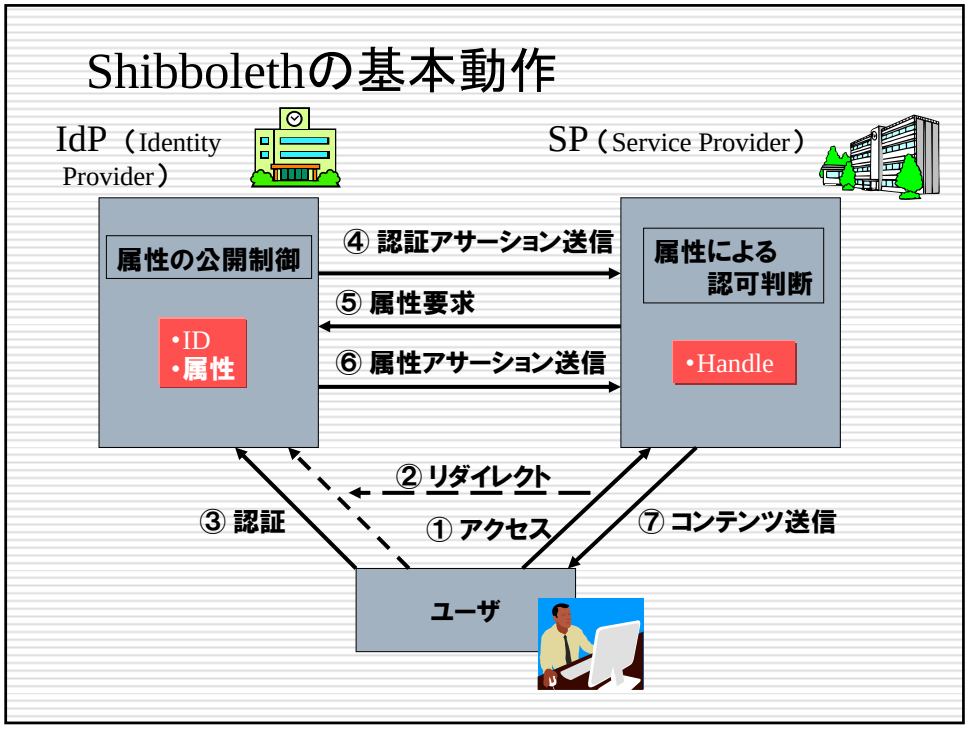
グリッドの将来動向

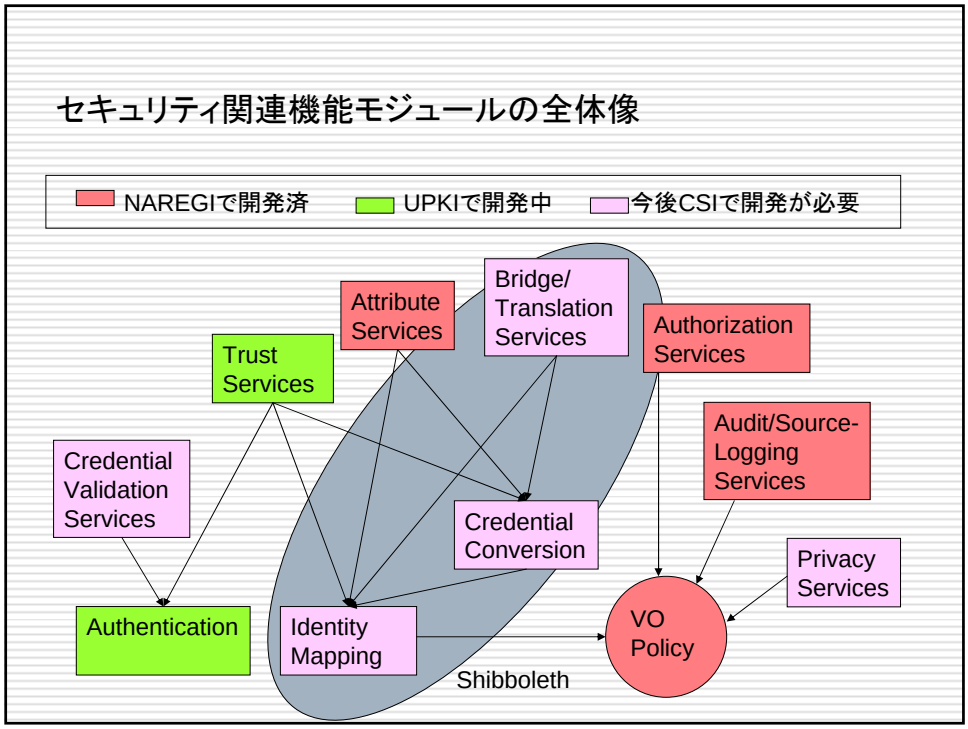
将来動向①：ID管理との連携

- 目的
  - グリッドのID管理と各教育・研究機関のID管理を連携させる
- 提供される機能
  - 管理ドメインを跨るIDのフェデレーション
  - プライバシー保護
- 実装方法
  - Shibboleth活用の可能性を検討中

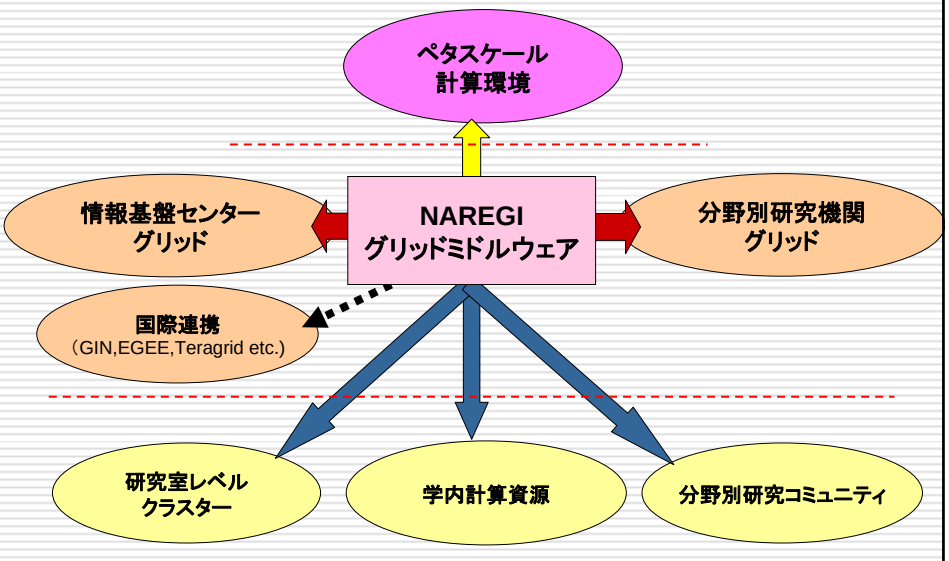
Shibboleth

- 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
IdP（Identity Provider）
SP（Service Provider）
属性の公開制御
•ID
•属性
④ 認証アサーション送信
⑤ 属性要求
⑥ 属性アサーション送信
属性による認可判断
•Handle
② リダイレクト
③ 認証
① アクセス
⑦ コンテンツ送信
ユーザ


セキュリティ関連機能モジュールの全体像
NAREGIで開発済
UPKIで開発中
今後CSIで開発が必要
Attribute Services
Bridge/ Translation Services
Authorization Services
Trust Services
Audit/Source-Logging Services
Credential Validation Services
Credential Conversion
Privacy Services
Authentication
Identity Mapping
VO Policy
Shibboleth

将来動向②次世代計算研究環境としてのグリッドの展開



将来動向③NII GOC 計画

- グリッド用CA運用(仮称NII GOC CA)
  - 国内の研究教育機関を対象としたCAの運用
  - 国際的(APGRID PMA準拠)証明書の発行
  - UPKIとの連携
- ユーザサポート
  - ヘルプデスク
    - 技術支援(NAREGIミドルウェア)
    - 障害対応(問題の切り分け、対応依頼)
  - ツール開発・運用(モニタリング、VO管理)
- ユーザトレーニング
  - セミナー等開催

グリッド用CA運用（仮称NII GOC CA)

- 目的
  - 国内の研究教育機関を対象としたCAの運用
- 業務
  - 国際的に通用するグリッド証明書（仮称NII GOC証明書）の発行
    - APGRID PMA準拠
  - RA業務を分散し、負荷分散と利用者の利便性を図る
- キャンパスPKIとの連携
  - キャンパスPKIの証明書からNII GOC証明書を自動発行
  - NAREGI-CAの強化機能を活用
  - 大学にLRA (Local RA)を設置し、電子申請を実現

CSI (Cyber Science Infrastructure)の構築

産学連携によるイノベーションダイナミクスの創出へ