# 月・惑星探査データを用いたセキュアGIS環境

寺薗淳也 (会津大)
中村良介 (産業総合技術研究所)
出村裕英、平田成 (会津大)
山本直孝、児玉信介 (産業総合技術研究所)
祖父江真一 (JAXA)

# 本日の講演内容

- バックグラウンドとして
  - セキュアな環境が求められるGIS
  - どのような危険が考えられるか？
- 開発システムの概要
  - Gridを利用したセキュアサイト
  - 開発システムとその現状
- 将来的な展開
  - 協働解析環境システムとしての展開

# 背景

- 地理情報システム(GIS)は、社会的なインフラとして重要性を増してきている。
  - 様々な場面で、GISを用いたシステムが活用されている。
  - 一般レベルでも、例えばGoogle EarthやYahoo! Mapのように、普通に地図情報(GIS)がアプリケーションとして使われることが多くなっている。
  - 最近は、単に地図を参照するだけではなく、ユーザ側が地図を作ったり場所を登録するといった形での、インタラクティブなシステムが一般化している。
- 掲載されている情報が増えるにつれて、その情報をセキュアに扱う必要性が増えてきている。

# 月・惑星探査データにおけるGIS

- GISという形での月・惑星探査データの参照は、最近になって始まってきたばかり。まだノウハウが足りない。
- 現在では研究目的での使用が一般的である。
  - 従って、研究目的に特有の問題が生じてくる。例えば、データは研究者グループで共有したいが、特定のグループだけでみせたい、あるいはある期日まではみせたくない、といったようなことが生じる。
  - 研究データも研究者にとっては重要な(秘匿すべき)データであり、セキュアな環境が求められる。
  - 一方で、コラボレーション(協働解析)を行うためには、ある程度の共有ができることが求められる。
  - GIS上では、単に位置情報が参照できるだけではなく、それに関連した科学データの参照ができるべきである。

# 「セキュア」の用途

- 一口で「セキュア」なサイトといっても、いろいろな可能性が考えられる。
  - 通信経路をセキュアにしたい
    →SSLなどを含めた何らかの暗号化によって保証
  - 身元を確実にしたい
    →クライアント、サーバともに証明書を利用
  - データを秘匿したい
    →上記の通信経路や身元確認に加え、サーバ側での工夫も必要になる。例えば、サーバ内のコンテンツの暗号化やアクセスレベル(ACL)設定など。

# セキュアのレベル

## サービス提供型のGISシステムの場合

- この場合には、レベルと必要性に応じたセキュリティ管理が求められる。
  - あまりに高度なセキュア環境は、サーバや通信経路に負荷をかけることになる。
  - サーバ1台に多数のアクセスがあることを前提としたセキュリティ
- ただし、通常の場合は、通信経路のセキュリティで十分である。
- 端末側、サーバ側両方をセキュア環境にすることによって、GISのセキュアレベルを高めることが可能である。(Yu et al., 2006)

# コラボレーション型GIS

## コラボレーション型のGISシステムの場合

- この「コラボレーション型」とは、GISサーバが複数存在する、または複数のソースがサーバ内に存在し、それらが互いに関係を持ってお互いの必要性を担保しあっているようなケースを指す。
- 研究型GISでいえば、研究室、ないしは研究機関ごとにGISが立ち上がっており、レイヤーとしてそれらを相互参照しつつ、ブラウザ画面上で1枚の地図としてみることができるようなシステム。
- さらに、位置情報から関連データへの参照が行える(サーバ上に関連データが存在する)。

# コラボレーション型GISに想定される脅威

- なりすまし
  - サーバのなりすまし、端末のなりすまし
  - ユーザのなりすまし
- 情報漏洩
  - 不正アクセスによる情報漏洩
  - 情報開示期限や範囲などを逸脱してしまう情報漏洩

# グリッドを利用したセキュアGIS環境の考え方

- コラボレーション型GISの場合、サーバをまとめて扱う、グリッド型のGISシステムが考えられる。
- このような場合においては、それぞれのサーバが互いに「正しい」サーバであるかどうかを認証する必要がある。
- そのためには、サーバに証明書を取得しておき、1カ所で認証することによって、関連したサーバ群がすべてそれに関連していることを証明できるようなシステムがふさわしい。
- このような方法としてグリッド化されたサーバ全体を認証するシステムとして、産業総合技術研究所で開発が進められているGeogridのモジュール “gridsite” がある。

# Gridsiteの概要

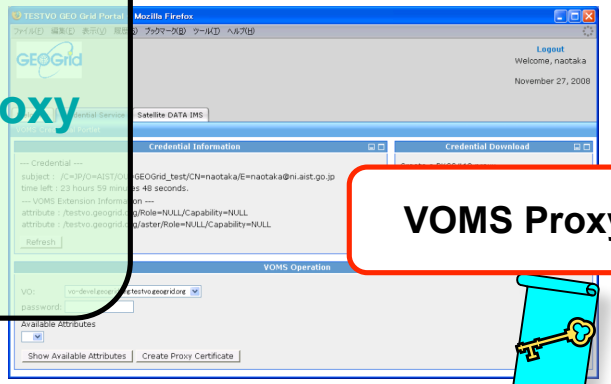
- Gridsiteは、Apacheウェブサーバのモジュールとして機能する(2.0系Apache)。
- Apache内にmod_gridsiteというモジュールをインストールすることによって、グリッドを構成しているサーバがgridsite網の1つとして認識される(VO=Virtual Organization)。
- 個々のサーバに証明書をインストールすることによって、サーバ同士が互いに認証される。
- センターサーバで認証がなされることで、VOとしての機能がスタートする(認証されない限り、アクセスが不可能)。
- さらに、公開場所などを限定したり、公開機能などをカスタマイズすることも可能である。

# OGCProxy + GridSite

ユーザ

https://portal/OGCProxy?\
URL=https://gridsite/..../service

OGCProxy




Credentialポートレット

https://gridsite/..../service

GridSite

Powered by APACHE

Contents

ACL:
/testvo.geogrid.org/aster
VO Name Group

ユーザ

$ curl ...

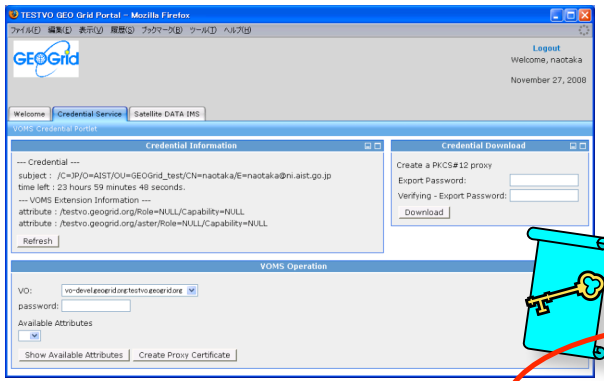
https://portal/OGCProxy?URL=https://gridsite/....

GridSite

PKCS#12

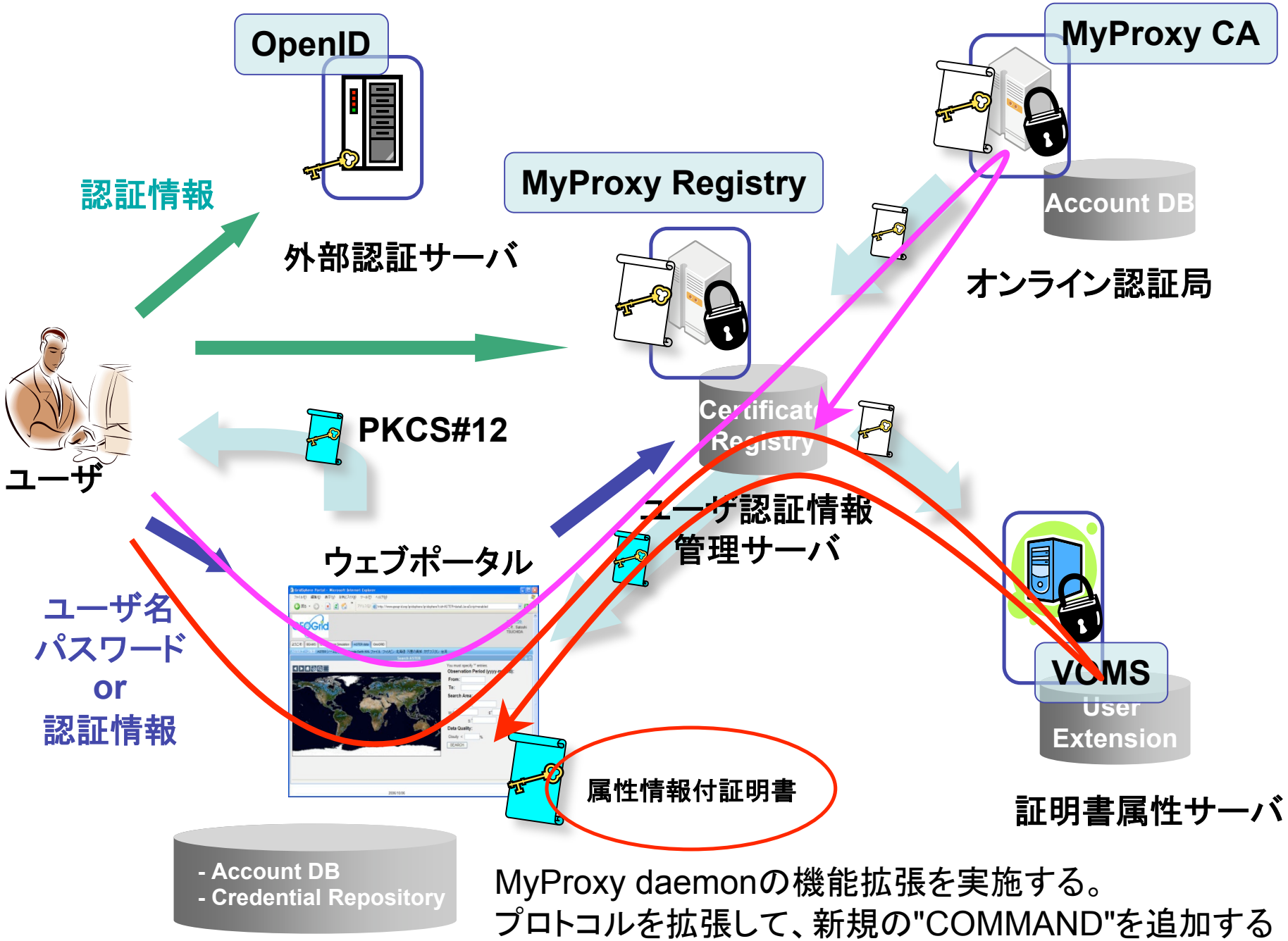
gridsiteで保護する。

/testvo.geogrid.org/aster




Credentialポートレット

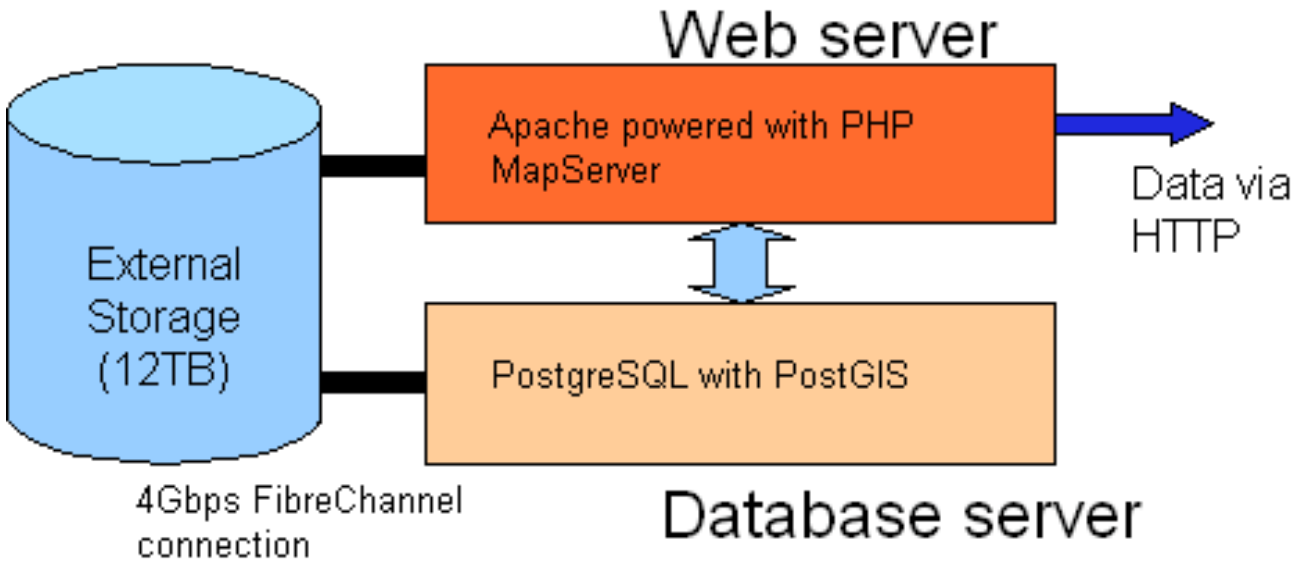
VOMS Proxy




MyProxy daemonの機能拡張を実施する。
プロトコルを拡張して、新規の"COMMAND"を追加する

# システム構成

- DBサーバとウェブサーバ、合計2台からなるサーバ
- 両サーバのバックエンドに、12TBの外付けストレージをファイバーチャネル接続
- ネットワーク接続はJGNIIplusを利用



# 現在のシステム

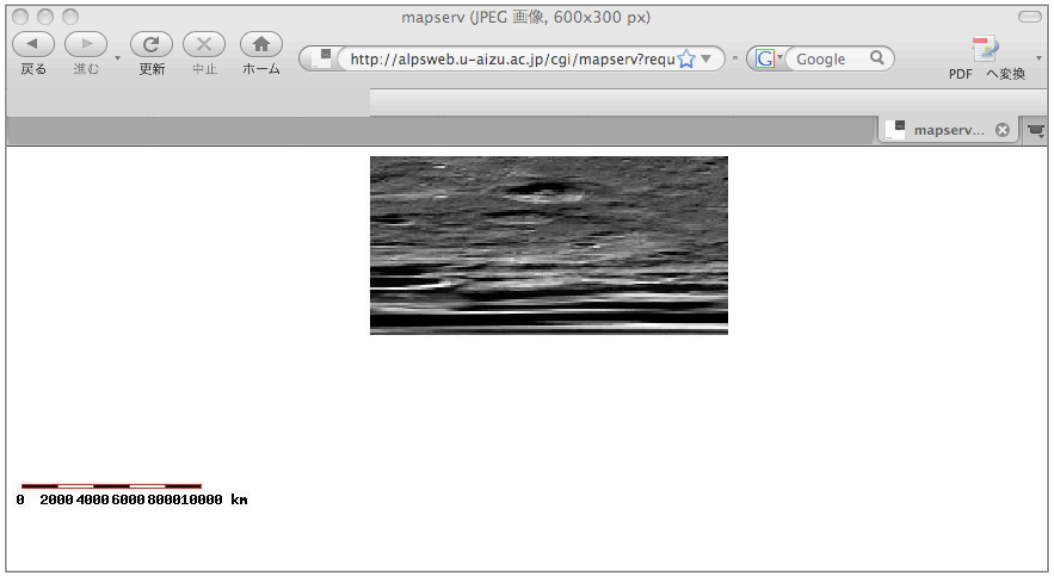
- サーバは会津大学の情報センター内に設置されている。
- 設備の都合で、外部との回線接続速度は100Mbps
- 1Uのサーバ2台(富士通 PRIMAGY RX200)
- CPUはIntel Xeon L5410、OSはRed Hat Enterprise Linux 4。

# ソフトウェア

- 以下のようなソフトウェアでシステムが構築されている。
  - Apache 2.0.63
  - MapServer 5.2.1
  - PostgreSQL 8.3＋PostGIS 1.3
  - PHP 5.2.8
- MapServerは、WMS機能が有効になっており、現在試験的な画像表示などが行えるようになっている
  - 画像変換などの主要なライブラリがリンクされている。
  - 現在のところ、静的表示、およびWMSの試験的表示が行えるようになっている。
  - PostgreSQL/PostGISとの連携は現在構築中。

# WMS機能

- MapServerについては、主要な機能がすべて実行できるように構築されている(画像変換、投影など)
- 現在、WMSサーバ機能およびWMSクライアント機能が実装されており、試験的にWMSサーバ機能が実行できている。




試験画像でテストしたWMS機能(画像はクレメンタインの月表面画像。ただし、座標がまだ正確ではない)


# セキュア環境

- 最初に、gridシステムにログインする必要がある。
  - ログインしないと、ウェブサイトとして認証されず、表示させることができない。
- そのあとは、ユーザ側からは通常通りブラウズすることが可能。
- ウェブサイトのユーザがログインする必要はない。
  - もちろん、ログインなどのユーザインタフェースを組み合わせることで、さらにセキュアな環境を構築することはできる。
  - サーバアクセスはhttp://である(https://ではない)

# 今後の展開

- WMS機能の充実
  - もちろん、WMS自体により多くのデータを加えることで、真のGISシステムを実現できる。
  - 「かぐや」の観測結果などを含め、理学的な成果を含めたデータを蓄積する。
  - 一方で、過去の探査データ(Lunar Orbiterやクレメンタイン)も蓄積できるようにしていく(ULCN2005, LOIRPなど)。
  - バックエンドにRDBMSを連携できるようにしておく(これについては、すでにDB用マシンにPostGISを用意している)
  - MapServerそのもののファインチューニング(サポートする画像を増やす、など)

# 今後の展開

- 協働解析環境としての機能
  - GIS機能をベースに、研究者がコミュニケーションをとる機能をプラス。
  - ウェブベースでのデータの受け渡しのインタフェース(もちろん、セキュリティに考慮)、音声やテキストチャットなどによるコミュニケーション機能を付加
  - それらのデータをRDBMSと連携させることで、データ管理機能、再利用可能性を強化