全国共同利用ID連携のための Shibboleth導入と NAREGIグリッド運用での評価

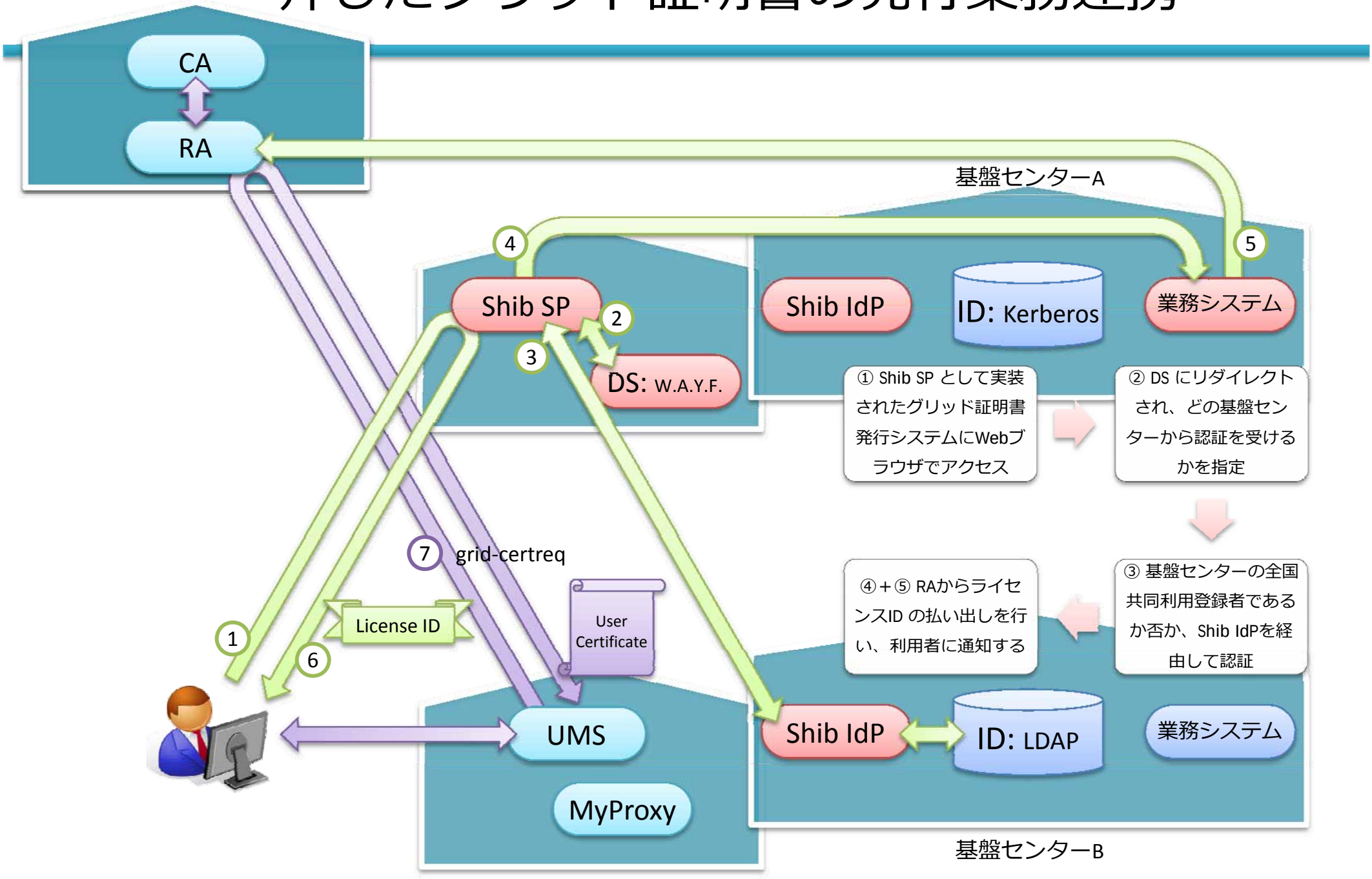
2008/12/24

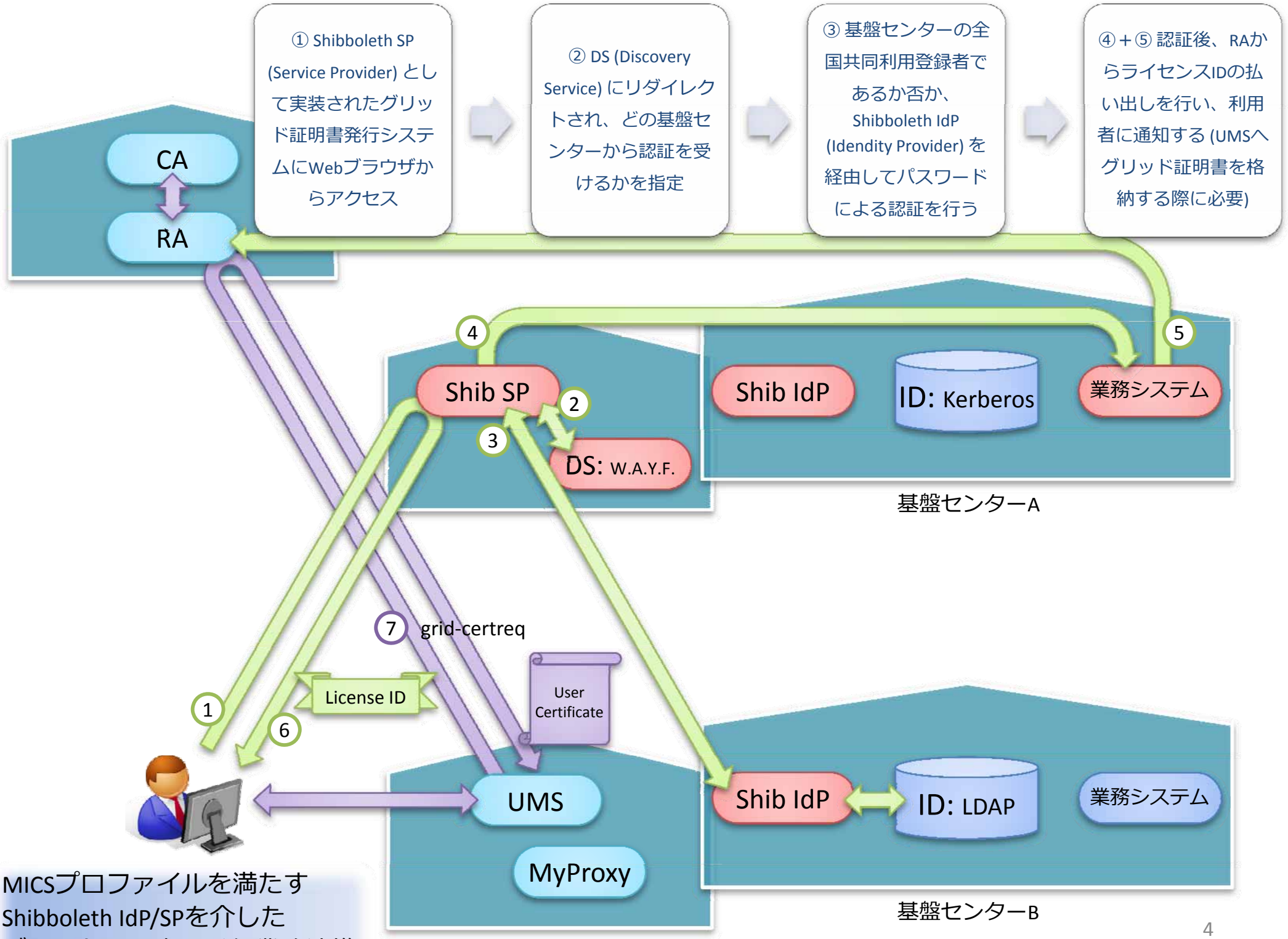
Manabu Higashida

manabu@cmc.osaka-u.ac.jp

基盤センターの
共同利用登録と連動した
グリッド認証局業務の自動化

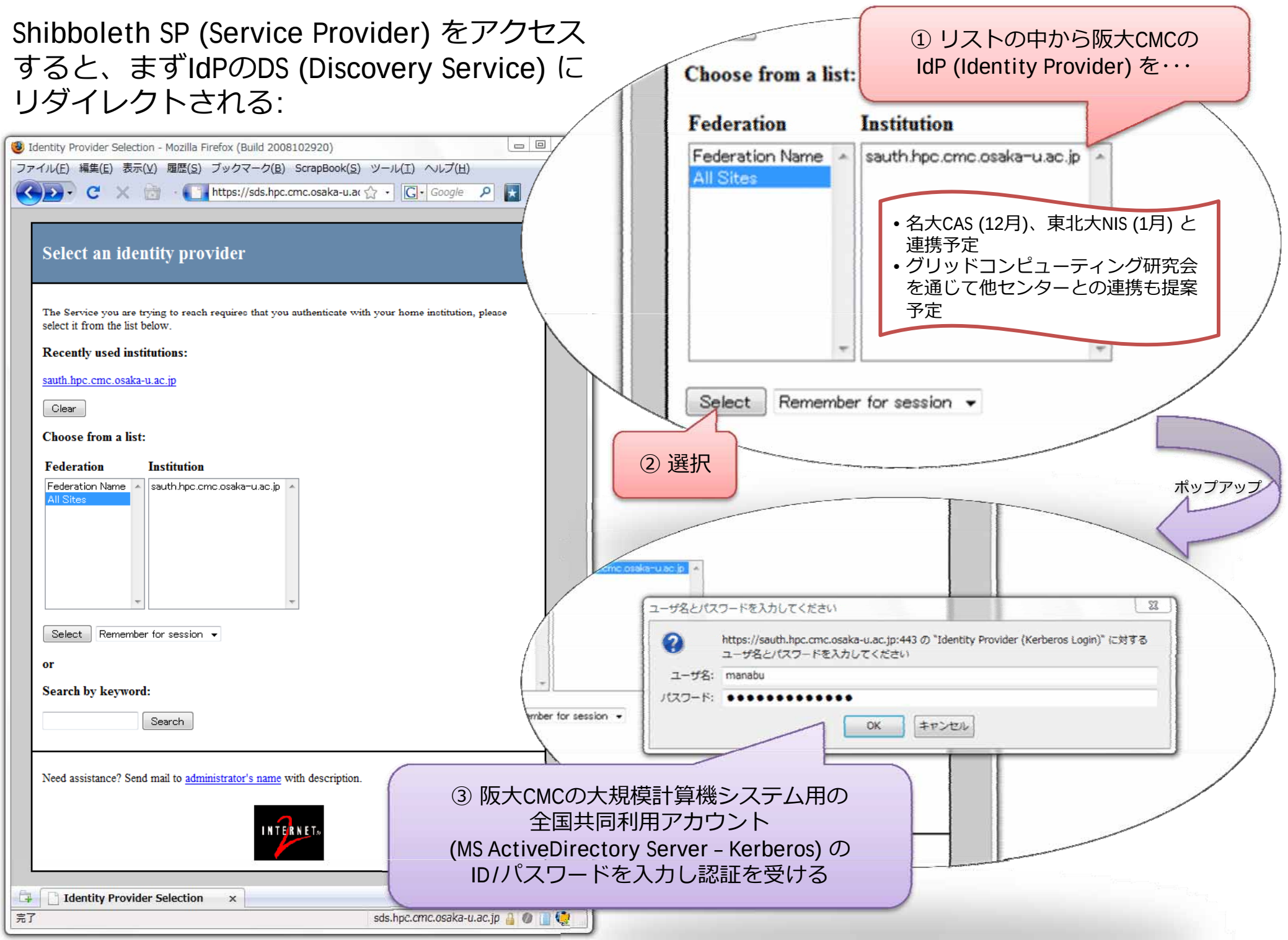
MICSプロファイルを満たすShibboleth IdP/SPを介したグリッド証明書の発行業務連携



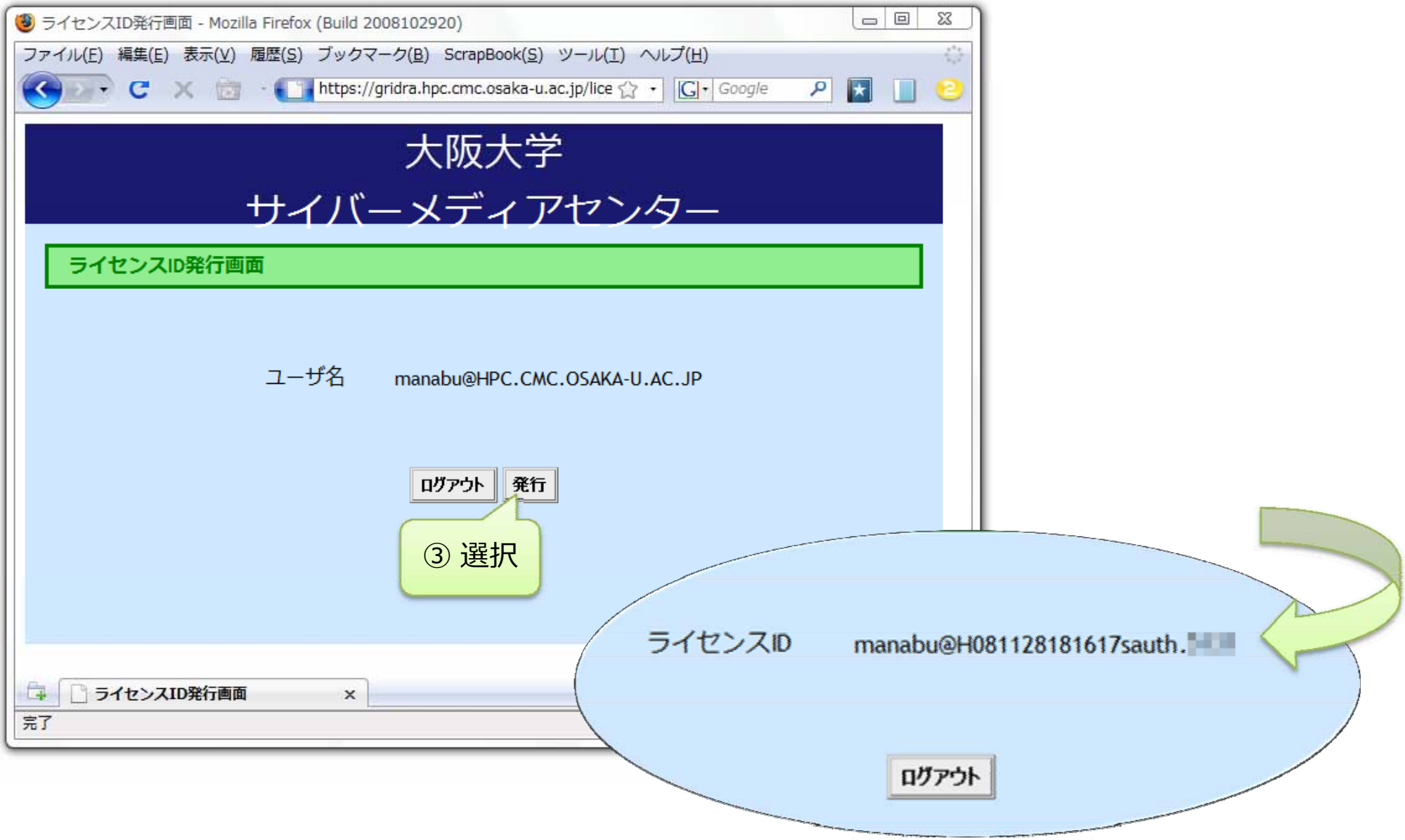


MICSプロファイルを満たす
Shibboleth IdP/SPを介した
グリッド証明書の発行業務連携

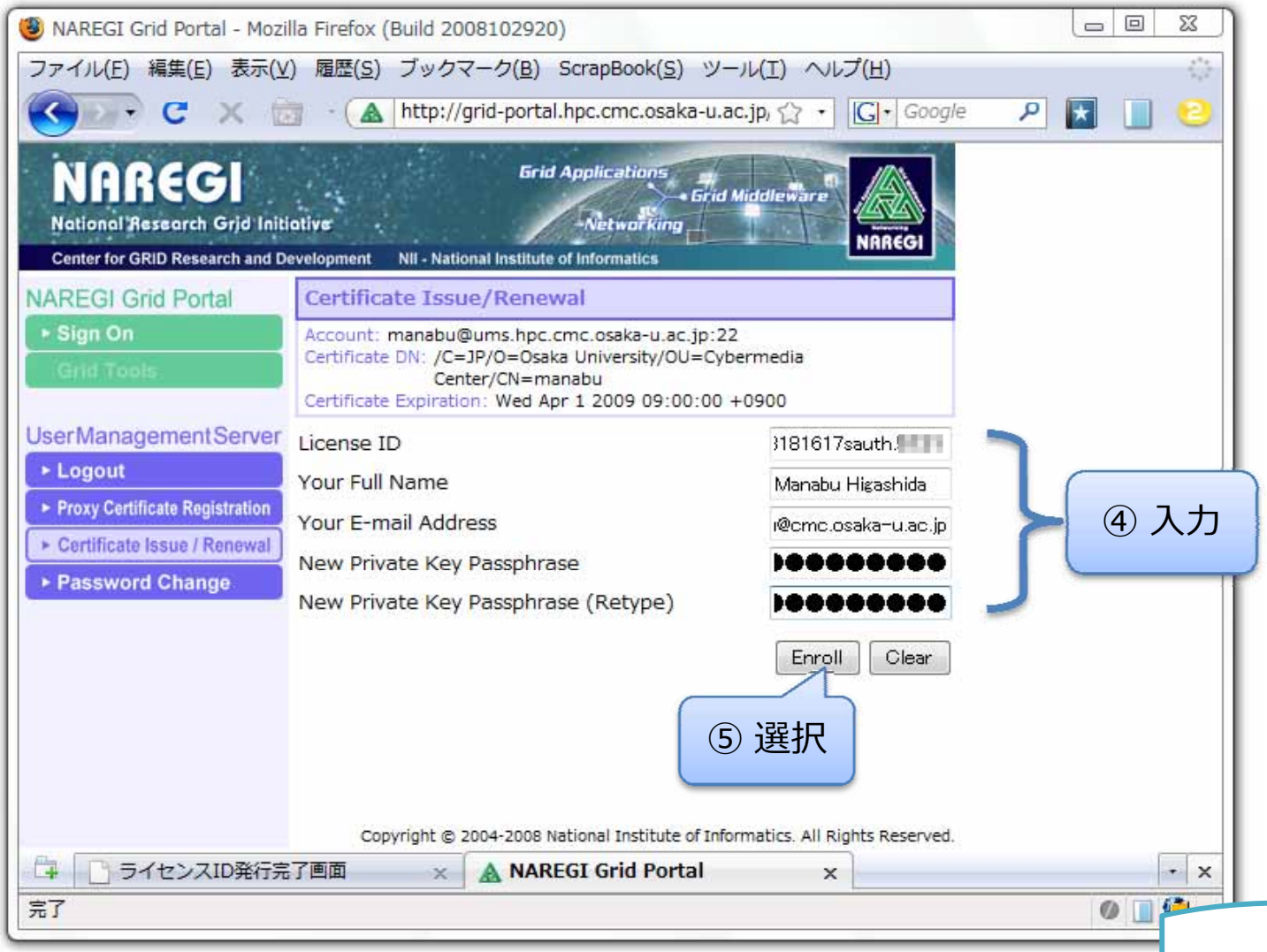
Shibboleth SP (Service Provider) をアクセスすると、まずIdPのDS (Discovery Service) にリダイレクトされる:



IdPによる認証後、Shibboleth SP (Service Provider) に戻る。
阪大グリッド認証局からユーザ証明書を発行するために
必要となるライセンスIDの発行を指示 (阪大CMC開発部分):



NAREGIポータル (Web UI) にて、取得したライセンスIDと付帯情報を入力する。
阪大グリッド認証局からユーザ証明書が発行され
付随するUMS (User Management Server) に格納される:



他センターに設置したUMSに
グリッド証明書を格納する場合は、
当該UMSのCUIにて
“grid-certreq” コマンドを実行する

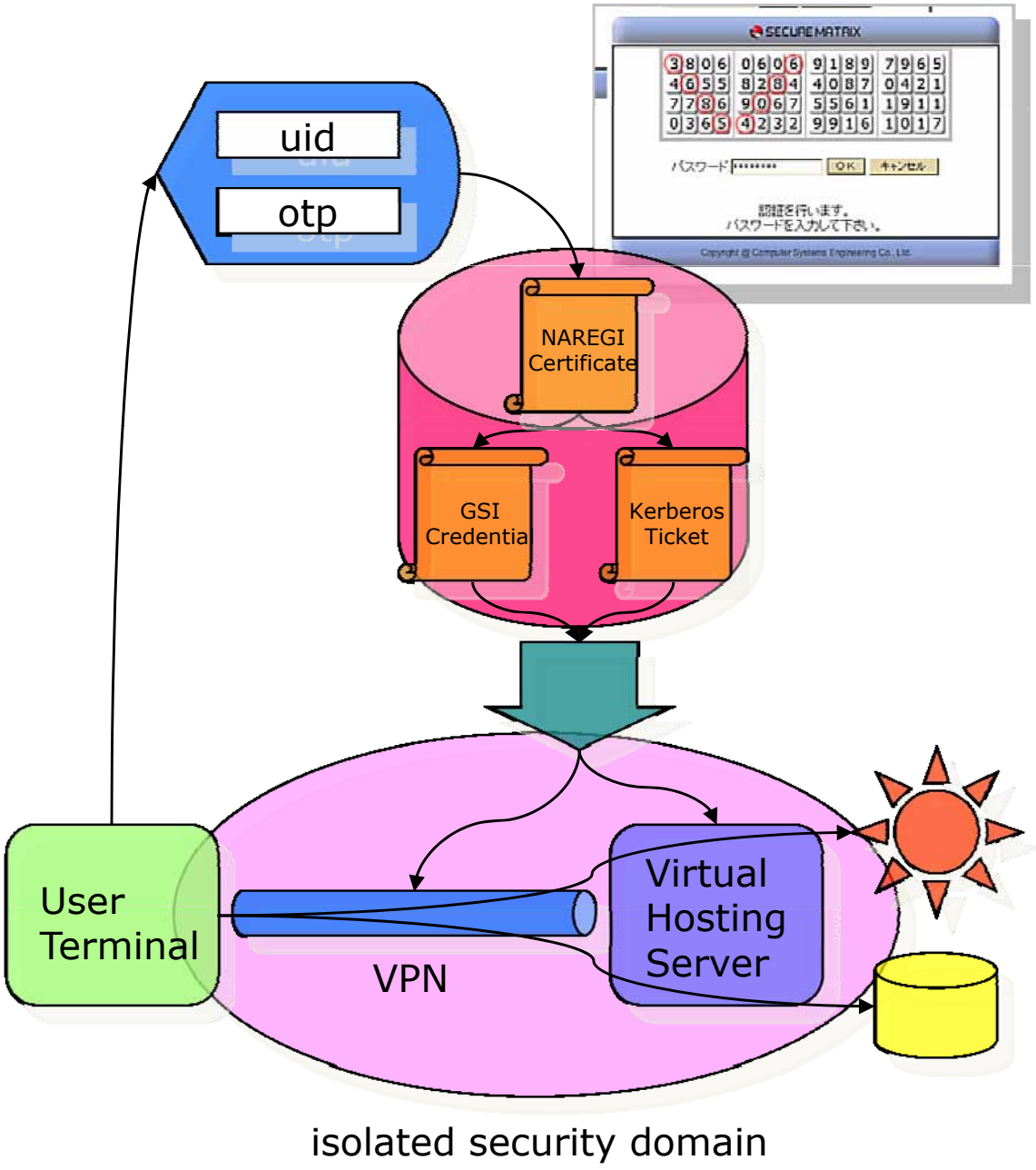
以下、ここに至った過程を
時間の許す限り・・・

セキュリティ・インシデントを教訓に: The Case of “clark/clark”

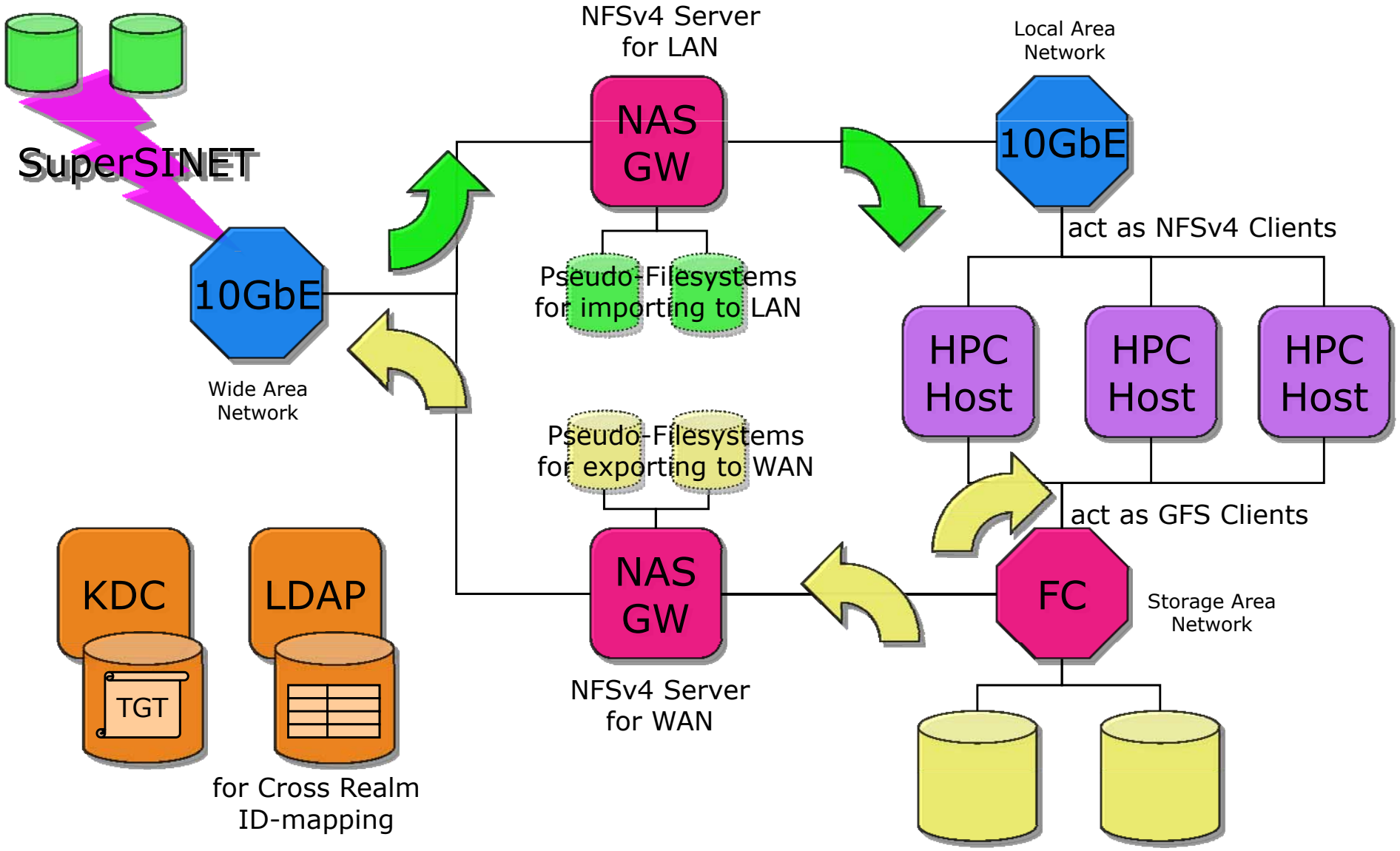
- あらまし
  - シンプルなパスワード・アタックによる侵入
    - rootkitによるカーネル・トラップでID/Password入力を盗み見される
  - 侵入者 (複数) の痕跡を洗い出してダーティなOSを再インストール
- 教訓
  - ID/Password入力の機会を最小化
    - 認証サーバを独立し、一般ユーザが利用可能なサーバとは切り離す
  - 仮想OSを導入し、ユーザ毎にプロセス空間を完全に分離する
  - IDSによる監視
    - Force10社製P10 (元 Metanetworks社製) の導入

次期システムの利用イメージ@2005

- Webポータルからシングル・サインオン
  - ユーザIDとワンタイム・パスワード
    - “SECURE MATRIX” by CSE
- 基本サービスの接続・設定を確立
  - VPN+仮想サーバによって
    すべてのサービスを媒介
    - NAS
    - HPC/Grid/Visualization
    - CGM
- ユーザ占有環境を提供
  - プライバシーとセキュリティ
    - 他の一切のユーザから隔離することで
      セキュリティ・バイオレーションが起こる
      機会を最小化
    - ハイパーバイザからの外部監視・監査
  - ユーザによる完全なカスタマイズ
    - OS、ライブラリ、アプリケーションの
      入れ替えは自由自在
    - 行き過ぎたときは、スナップショット
      によるロールバック



Global Storage Sharing with NFSv4



“Web2.0” はすべてを救う!?

- ターミナル・エミュレータもWebサービス化?
  - RFB on Web Browser (VNC Java Viewer)
    - 携帯電話でも使える!?
  - AjaxTermは全てを解決するか?
    - http://antony.lesuisse.org/qweb/trac/wiki/AjaxTerm
      - Latain-1のみ対応: UTF-8? 日本語?
- 泥臭いターミナル・サービスはまだ必要…
  - Windows Active DirectoryはKerberos+LDAPによるアイデンティティ・マネジメントと判明!
    - Windowsクライアントを全て取り込める!?
      - PKIによる初期認証も可能らしい…
    - MacOS XもADSとの親和性を謳い始めた
      - http://www.apple.com/jp/macosx/features/windows/
      - http://www.apple.com/jp/server/macosx/features/windowsservices.html
    - Linux Distro’sもほぼKerberos対応

着実にkerberizeされつつあるかも…

- Microsoft Active Directory
  - 最も普及しているKerberosベースのアイデンティティ・マネジメント
    - KDC (Key distribution Center) として相互運用性が高い
    - SPNEGO-ready
      - IE 5.0.1 and IIS 5.0
- MIT Kerberos for Windows
  - 3.0は不安定だった…
  - 3.1 on β
- Windowsクライアント
  - Firefox 1.5、PuTTY、WinSCP、FileZillaなど
- KX.509/KPKCS11、Kerberized MyProxy

SPNEGO – **S**imple and **P**rotected GSSAPI **Nego**tiation Mechanism

- RFC-2478/4178
  - MS方言では “**S**ecurer **P**rotocol **Neg**otiation”
- SPNEGO-awareなWebサーバ (ポータル) にアクセスしてKerberosクレデンシャルを取得しSSOを実現
  - Apache2
    - mod_auth_krb (http://sourceforge.net/projects/modauthkerb)
      - Microsoft推奨?
        - » http://support.microsoft.com/?id=555092
    - mod_spnego (http://sourceforge.net/projects/modgssapache)
    - mod_auth_vas (http://rc.vintela.com/topics/mod_auth_vas/)
  - Apache2 for Windows
    - mod_auth_sspi (http://sourceforge.net/projects/mod-auth-sspi)

API問題 (SSPI vs. GSSAPI)

- RFC-2048/2743 GSSAPI (Generic Security Service API)
  - MS方言 SSPI (Security Service Provider Interface)
    - NTLMなどに対応するため?
    - SPNEGO対応によりプロトコルとしてはGSSAPIと互換性あり
  - Windowsクライアントのバリエーション
    - MS SSPI にのみ対応したアプリケーション
      - IE、Webフォルダ (a.k.a.「マイネットワーク」) を含むすべてのMSアプリケーション
      - Firefox 1.0
    - MIT GSSAPI にのみ対応したアプリケーション
      - WinSCP (http://winscp.net/ 、次期リリースでSSPI対応)
      - FileZilla (http://sourceforge.net/projects/filezilla/)
    - 両者に対応しているアプリケーション
      - Firefox 1.5 (設定が面倒なのでXPIを作る必要あり)
      - PuTTY
        - » CSS版 at http://www.certifiedsecuritysolutions.com/downloads.html
        - » Vintela版 at http://rc.vintela.com/topics/putty/

ccache (Credential Cache) 問題

- MSの「独自」実装 vs. MIT (vs. Heimdal)
  - LSA: Local Security Authority サブシステムにクレデンシャルを格納
    - MITのGSSAPIからもアクセス可能
      - 手動でインポート: `ms2mit.exe`
      - 自動でインポート: `NetIDMgr` a.k.a. “Network Identity Manager”
        - ３.１からちゃんと動く? (βテスト中…)
    - MITのccacheからMS LSAにエクスポート (`mit2ms.exe`) も可能
      - 副作用は起きないか?

Kerberos and PKI Integration – Efforts Since 1995

- PK-INIT
  - Kerberosのpre-authentication (`kinit`) をPKIで
    - やっとRFC-4556 (2006/10/06現在: Standards Track) に…
    - Draft-39の実装: Microsoft (Since Draft-9)、Heimdal
- PK-CROSS
  - Cross-Realm環境構築の認証 (鍵交換) をPKIで
    - draft-ietf-cat-kerberos-pk-cross-08
- PK-APP (?)
  - Kerberosのクレデンシャルから PKIの証明書 (短期間) を取得
    - KX.509
    - MyProxy

基盤センターにおけるSingle Sign-On

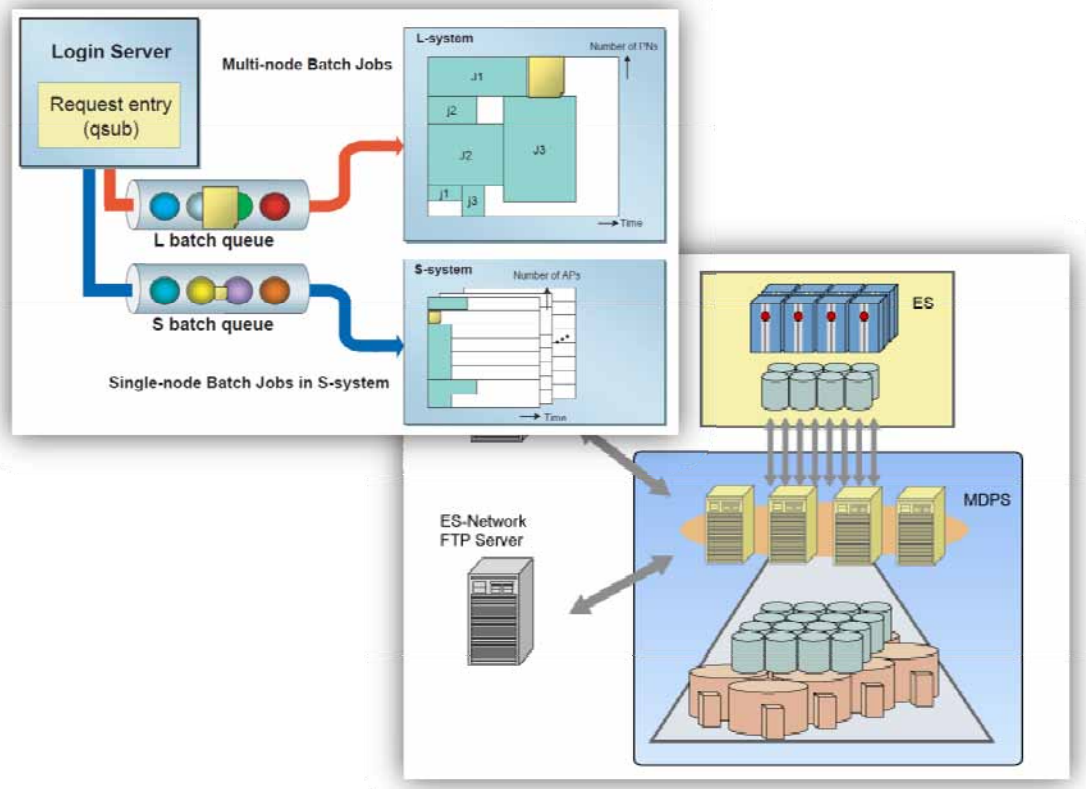
- 安全・安心なPre Authenticationの保障
  - 利用者に対して･･･
  - 連携を必要とする多組織に対して･･･
    - 全国共同利用施設としての登録業務実績
- 非Webアプリケーションとの互換性
  - Webサービス化の追従を許さない先鋭性
    - 高性能
    - 大規模

Lessons from operation in the Earth Simulator

- Authentication
  - Two-Factor Authentication
    - One Time Password, combination of
      - PIN or Passphrase
      - Pseudo-random number, periodically being generated from Security Token

- Job Management
  - NQS-II with node-by-node resource reservation
- File Sharing
  - Multiple gateways to pass with different credentials

http://www.jamstec.go.jp/es/en/system/scheduling.html



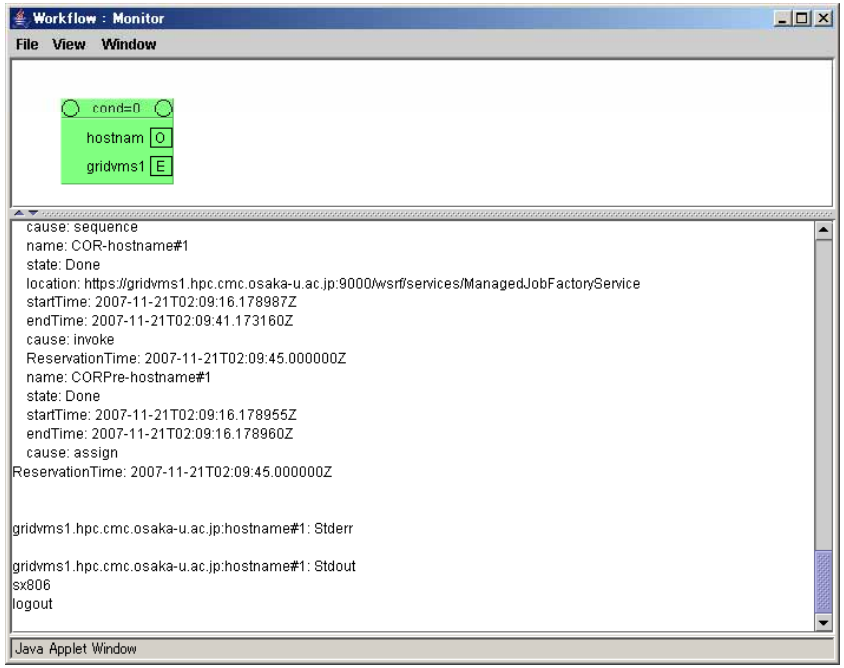
http://www.jamstec.go.jp/jamstec-j/spod/system/hardware.ja/mdps.html

阪大CMCの取り組み

- ✓ “Grid Operation” を単純化・簡素化し、既存のセンター運用業務へ取り込む
  - すべての高性能計算機資源をGrid資源として提供
    - ベクトル型スーパーコンピュータへのミドルウェアの移植
    - PCクラスタをセンター運用に耐えうる品質に引き上げる
  - すべての利用登録者にGrid PKI証明書を発行
    - CMC以外の学内共同利用センターからの登録者も含む
      - レーザーエネルギー学研究センター (ILE)
      - 核物理研究センター (RCNP)

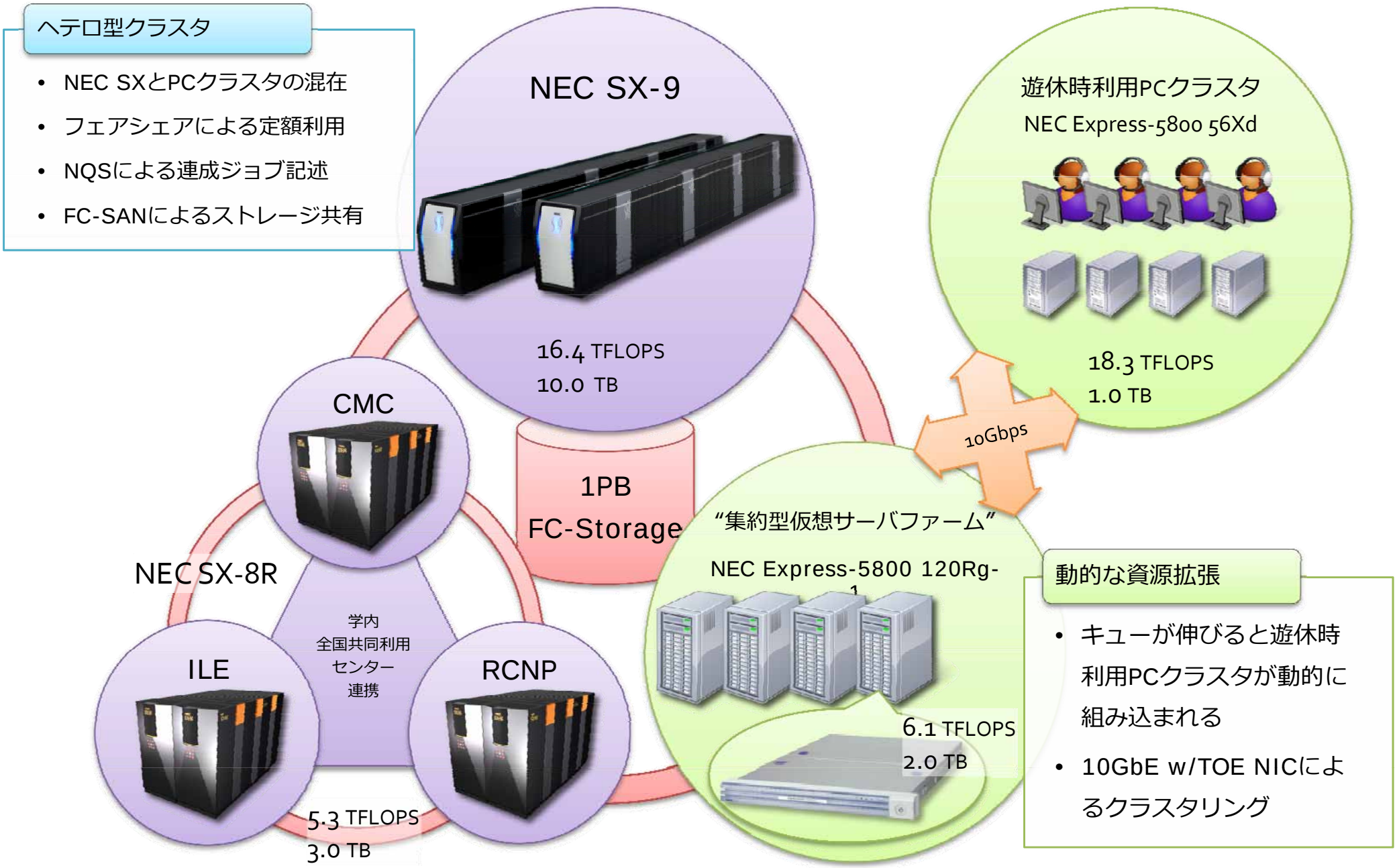
すべての高性能計算機資源を Grid資源として提供

- ✓ ローカルスケジューラの統一と NAREGI GridVM対応 (CSI委託事業として)
  - NEC NQS-II
    - 対応機種
      - SX: SUPER-UX
      - PC Cluster: SuSE Enterprise Linux, OpenSuSE
    - 多段キュー: Faire Share Queue + Job Assigned Map
      - フェアシェア型定額制
      - 飽き資源情報の提供と実行予約

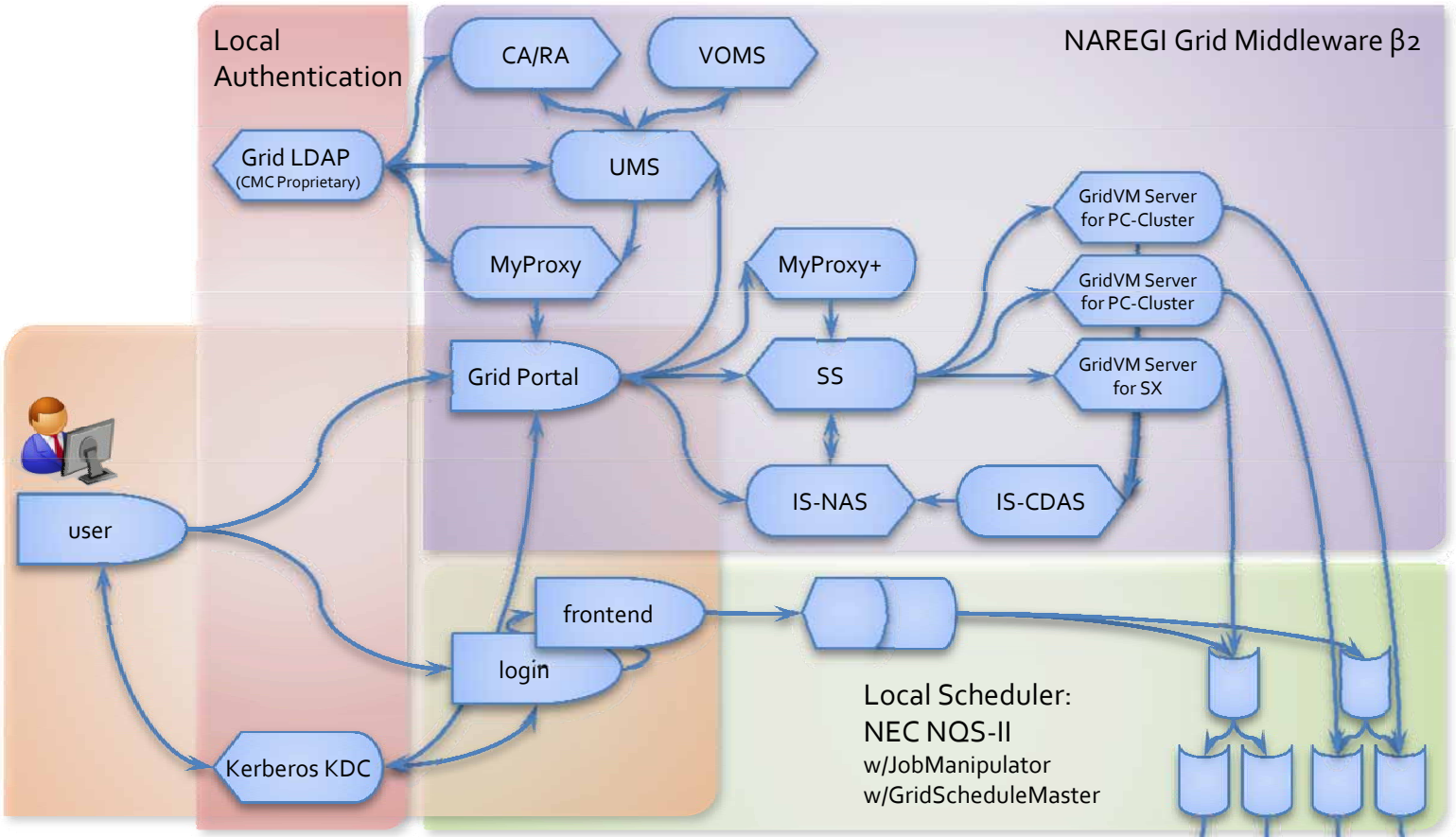


SXもGrid資源として提供
（現時点ではGridMPI未対応）

阪大CMCの大規模計算機システム構成　Total: 46.1 TFLOPS, 16.0 TB

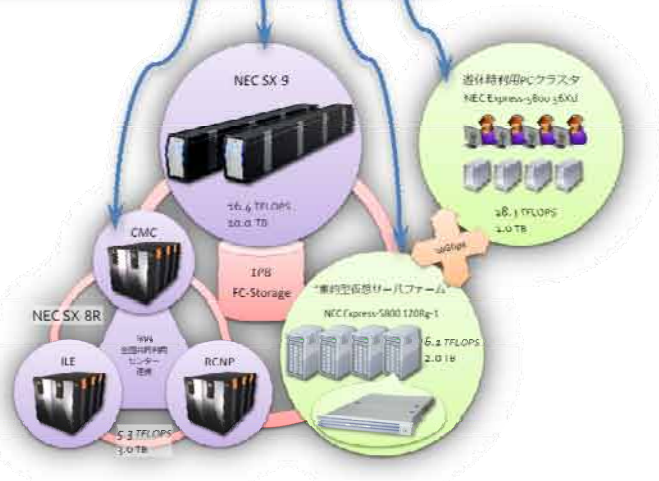


NAREGI M/Wの各コンポーネントと阪大CMCの構成との位置関係



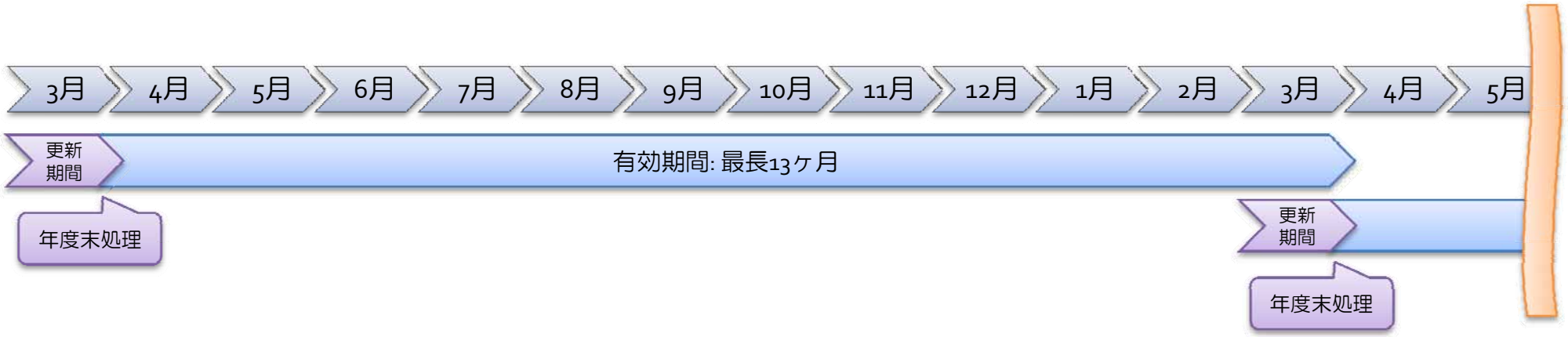
既存の全国共同利用システムとNAREGIミドルウェアβ2の共存

- ローカル認証にKerberosを導入し、CUI/GUI共に連動するSingle Sign-Onを実現すると同時に、NAREGI認証システムをWebインターフェイスに隠蔽
- ローカル・スケジューラNEC NQS-II対応のNAREGIコンポーネントを既存運用と併存可能なように開発



すべての利用登録者に Grid PKI証明書を発行

- ✓ NAREGI-CAによるGrid PKIの構築と阪大CMC認証局CP/CPS策定 (v1.1)
  - AP Grid PMA minimum CA requirements準拠?!
    - 秘密のCA室
    - 本人性の検証・確認は簡素化
      - 支払責任者・経理責任者の印鑑で十分じゃないの?!
  - Web I/FとKerberos認証によるソーシャル・エンジニアリング・フローの簡素化
    - License IDによる申請者の検証を隠蔽
    - Passphraseによる秘密鍵の暗号化を隠蔽
    - Campus CAからKerberos PKINIT (RFC4556) によるGrid CAへのフェデレーションを視野に
  - 業務に乗らない、簡素化・隠蔽できない処理も･･･
    - 失効処理
- ✓ RA業務を共同利用掛の通常業務に組み込む
  - NEC DEVIAS ▶ NAVIAS (仮称)



利用申請

- 既存の全国共同利用の窓口で随時
- 郵送によるID通知
- Kerberos認証によるWebポータルSSO
- “1-Click”でGrid証明書発行

阪大独自のGrid-LDAPによる継続処理

- Grid-LDAPにライセンスIDをあらかじめ払い出してありWebポータルの”1-Click”操作で証明書と引き替える(2から3つ)
- 3月頭にクリア
- 継続申請を受け付けた際に再度払い出し
- 更新期間中の新規申請の取り扱い

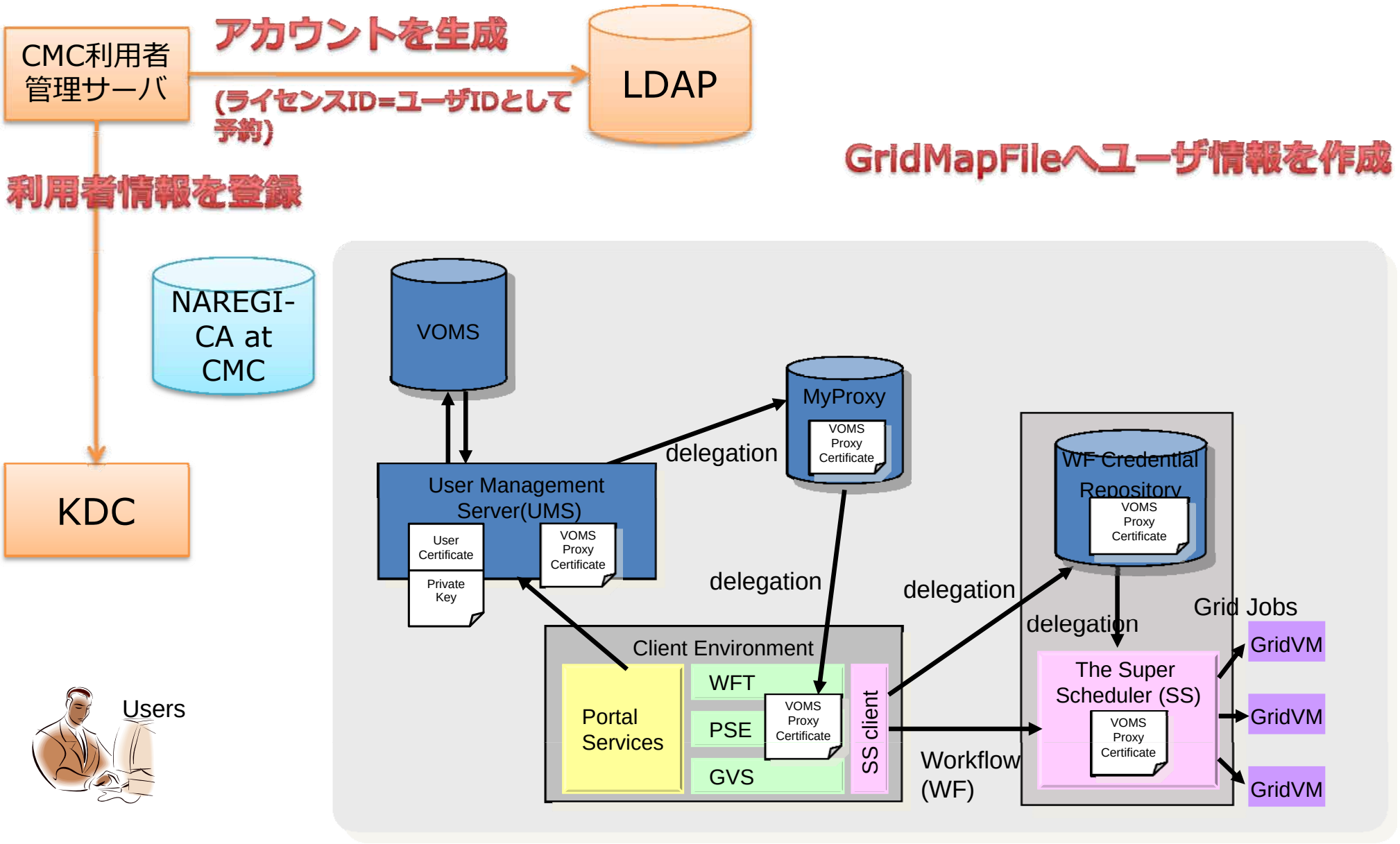
秘密鍵の危殆化への対策

- UMSでの集中管理
- CUIによる対話操作を排除

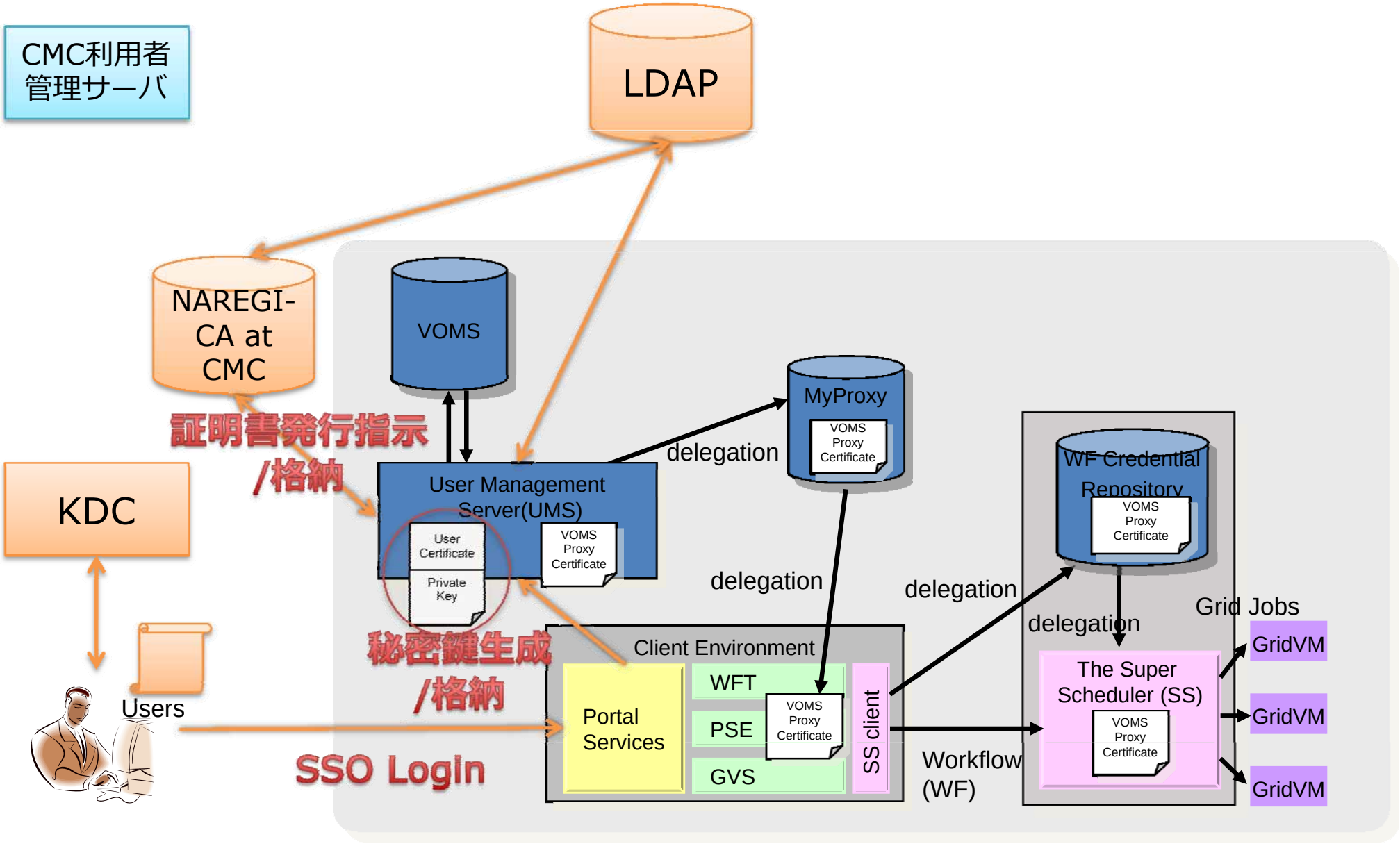
失効処理

- 危殆化に伴って随時
- CA運用責任者による操作

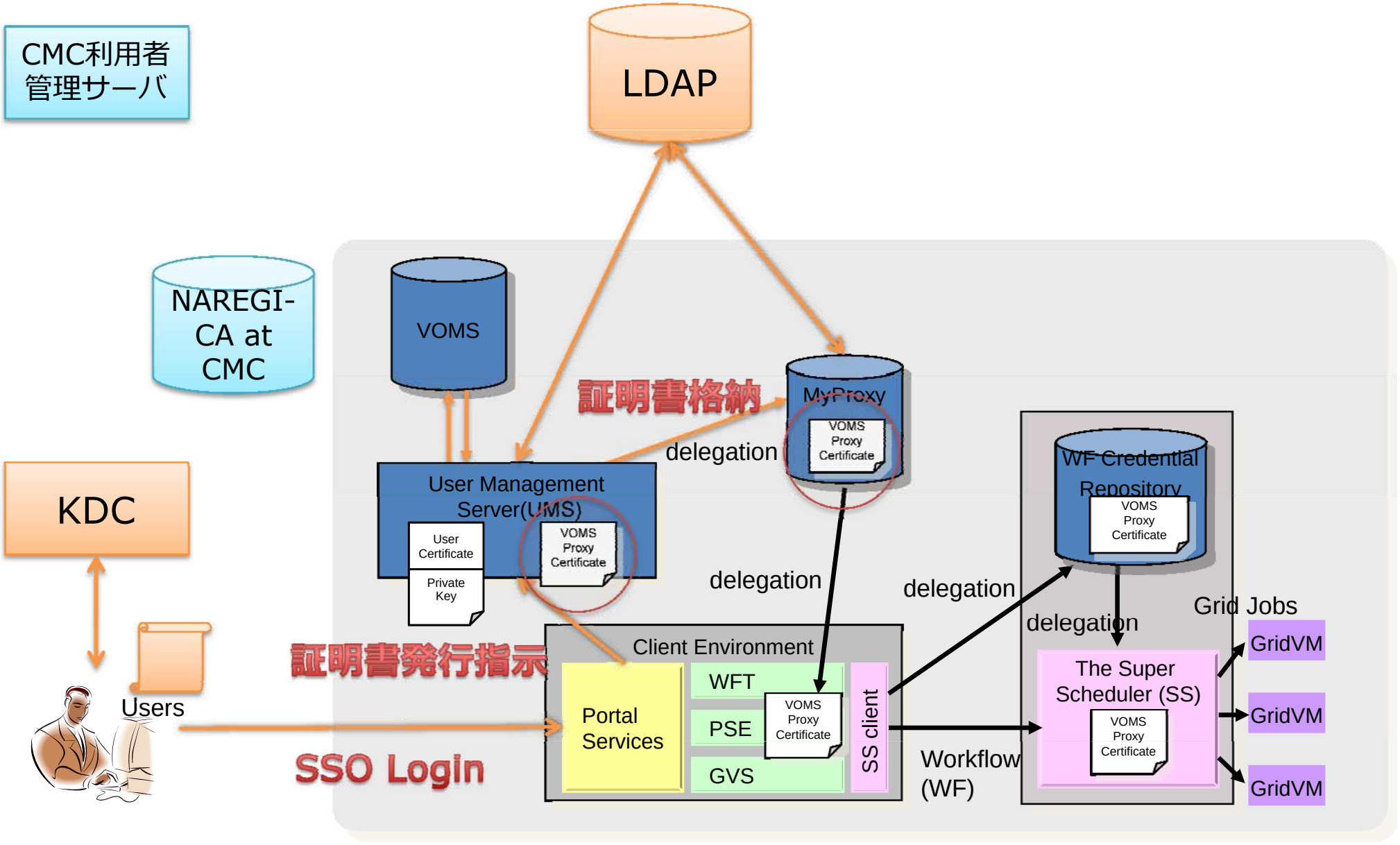
NAREGI-β2: 利用申請



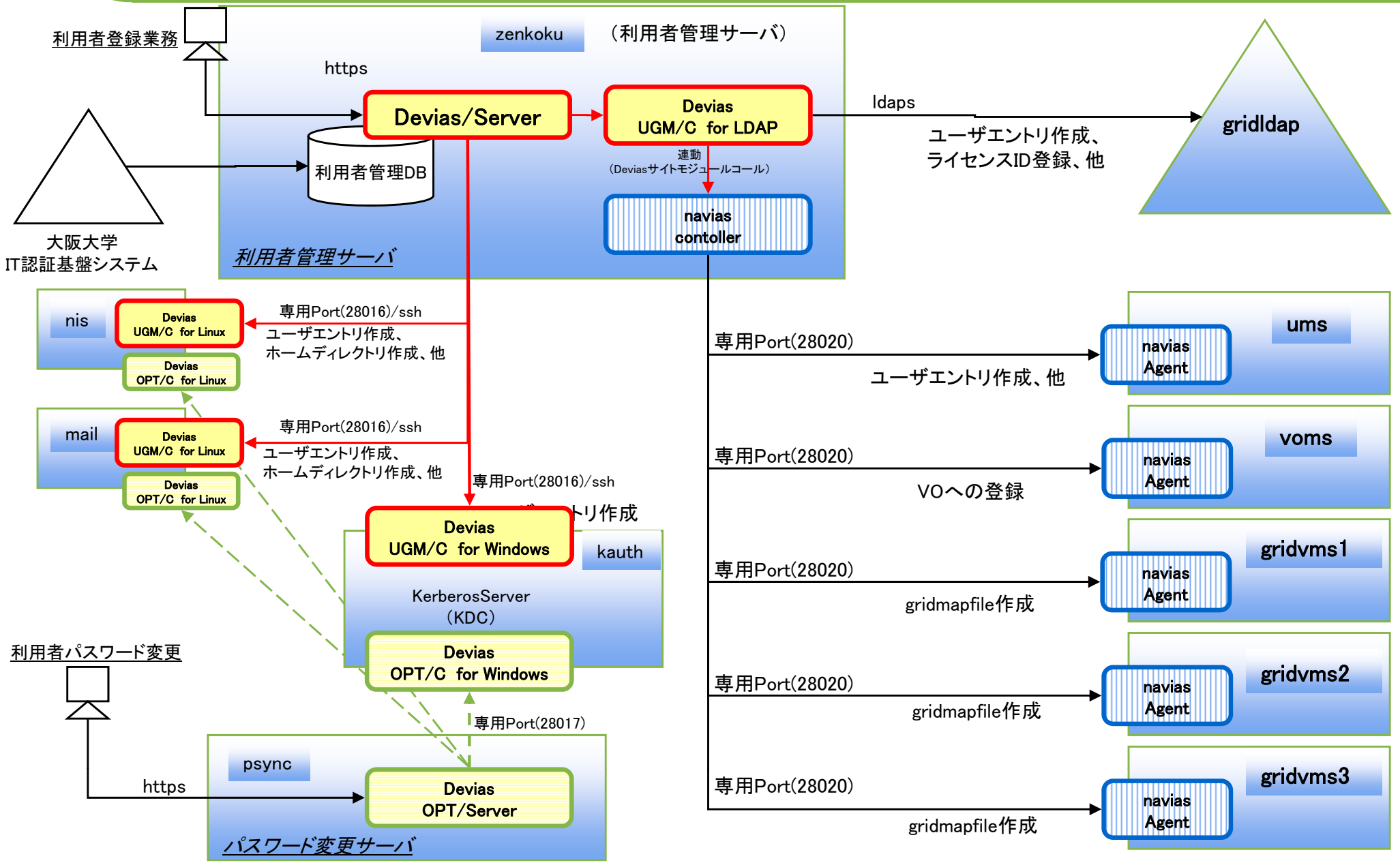
NAREGI-β2: 証明書発行



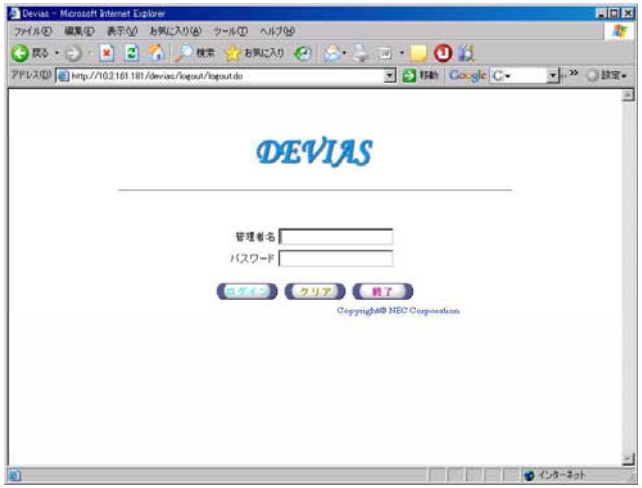
NAREGI-β2: Proxy証明書発行

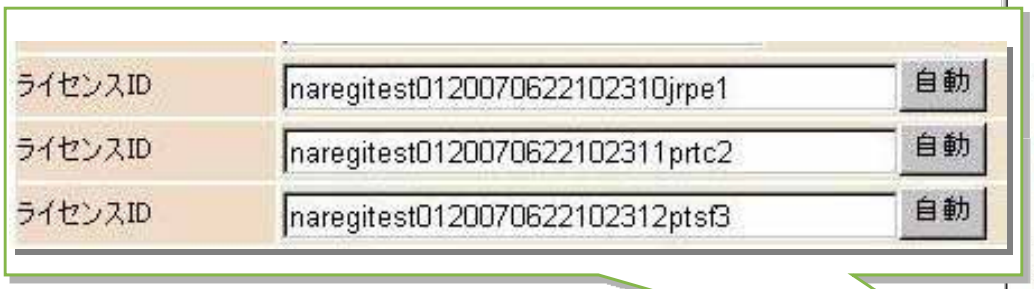


システム概念図

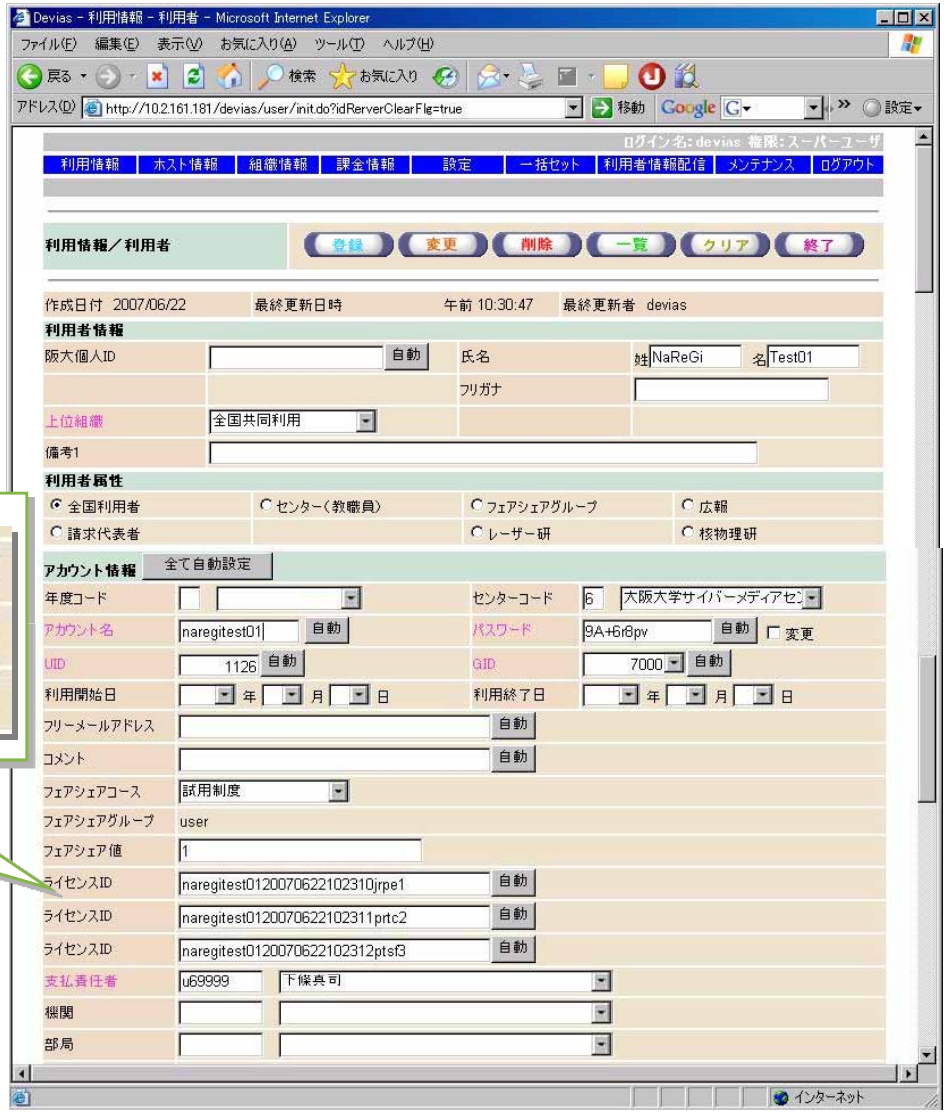

利用者登録業務
zenkoku
（利用者管理サーバ）
https
Devias/Server
Devias
UGM/C for LDAP
ldaps
gridldap
ユーザエントリ作成、
ライセンスID登録、他
利用者管理DB
連動
（Deviasサイトモジュールコール）
navias
contoller
大阪大学
IT認証基盤システム
利用者管理サーバ
nis
Devias
UGM/C for Linux
Devias
OPT/C for Linux
専用Port(28016)/ssh
ユーザエントリ作成、
ホームディレクトリ作成、他
mail
Devias
UGM/C for Linux
Devias
OPT/C for Linux
専用Port(28016)/ssh
ユーザエントリ作成、
ホームディレクトリ作成、他
専用Port(28016)/ssh
Devias
UGM/C for Windows
kauth
KerberosServer
（KDC）
Devias
OPT/C for Windows
利用者パスワード変更
https
専用Port(28017)
psync
Devias
OPT/Server
パスワード変更サーバ
専用Port(28020)
ユーザエントリ作成、他
navias
Agent
ums
専用Port(28020)
VOへの登録
navias
Agent
voms
専用Port(28020)
gridmapfile作成
navias
Agent
gridvms1
専用Port(28020)
gridmapfile作成
navias
Agent
gridvms2
専用Port(28020)
gridmapfile作成
navias
Agent
gridvms3

利用者管理システム（利用者登録画面）





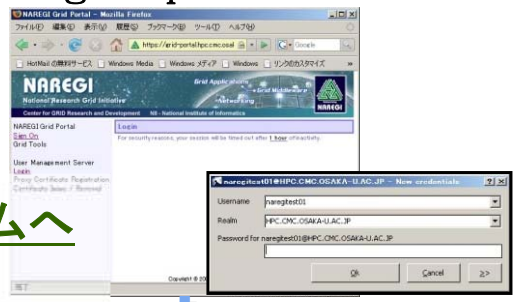
Grid-ldapへ登録するライセンスIDを自動生成する。



ユーザ自身による証明書発行（Webエンロール）

ユーザ証明書発行処理シーケンス

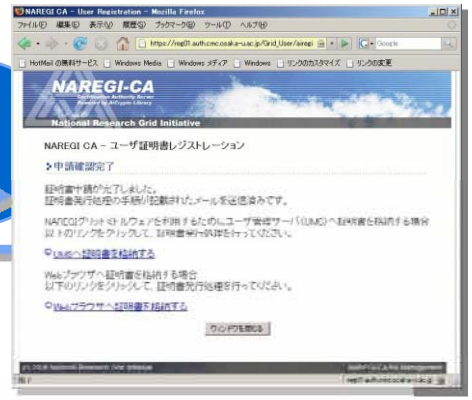
grid-portal

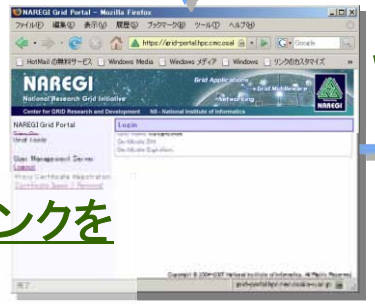


1．GRIDポータルシステムへログイン

バックグラウンドで
利用者のユーザ証明書発行に関する
申請処理と承認処理が自動で処理されます。

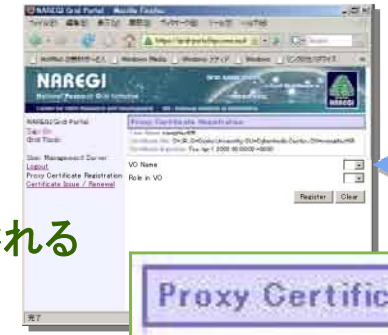
gridra





Webエンロールシステムへジャンプ
（Kerberos SSO）

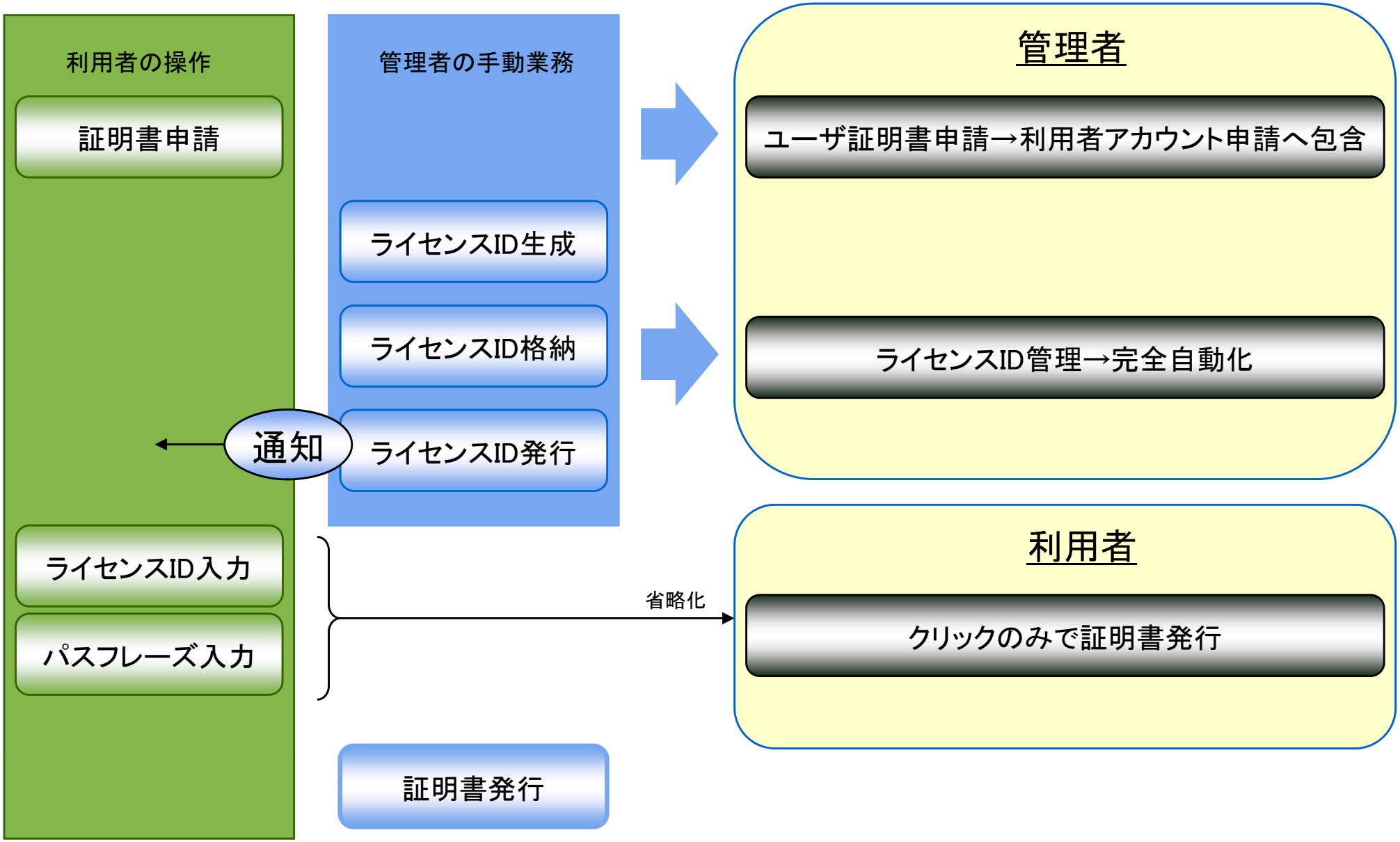
2．ユーザ証明書発行リンクをクリック



3．ユーザ証明書発行処理
（ボタン押下のみ）

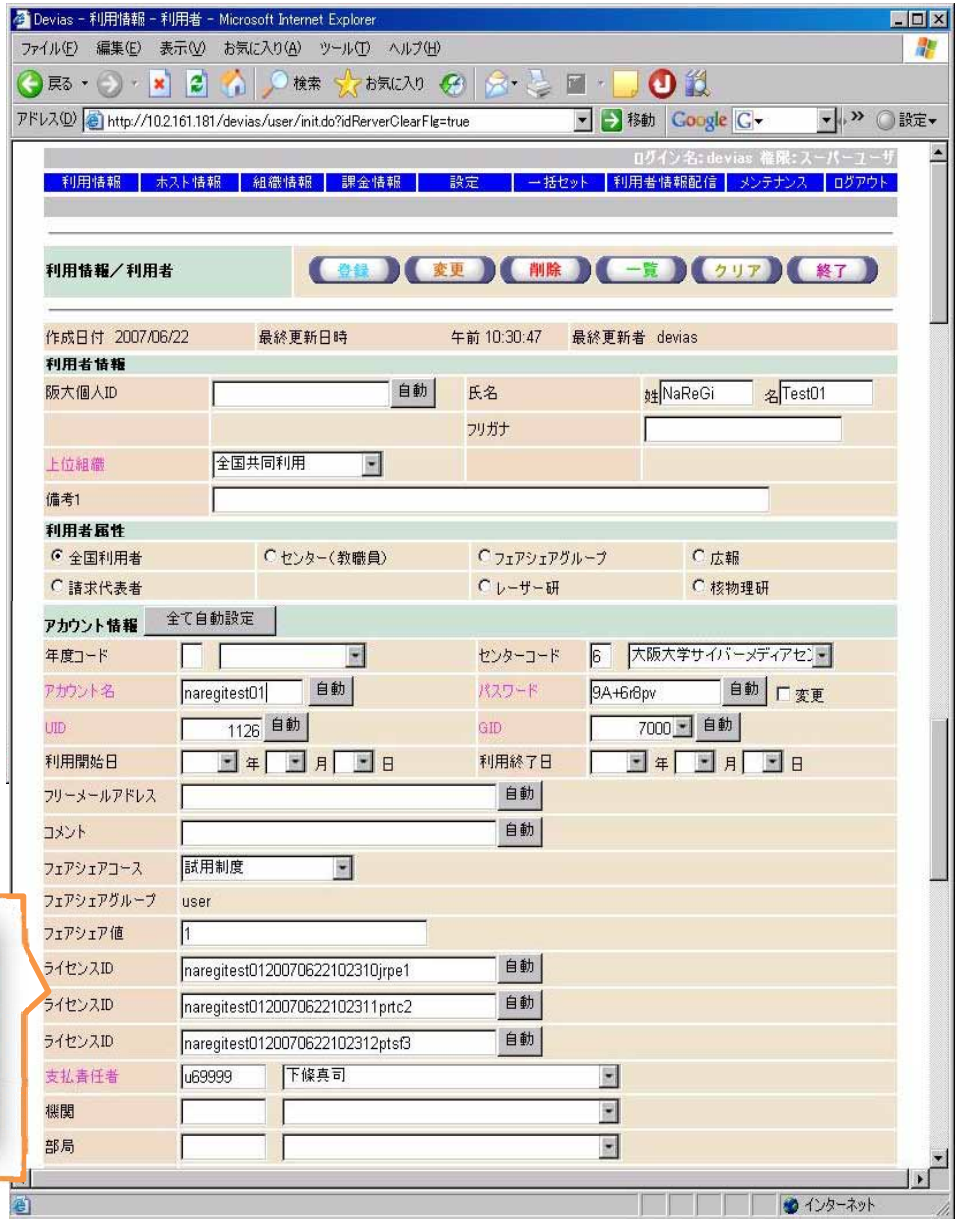
ユーザ証明書が生成される

運用性及び操作性の簡易化･効率化



阪大CMCの業務システム

- ✓ 共同利用掛が利用者登録に使っている管理者システム (NEC製DEVIAS)
  - 管理者インターフェイスに、グリッド証明書発行に必要な「ライセンスID」の払い出しや「所属VO」の設定項目を追加
  - バックエンド処理システムに、Unixアカウントの発行などと同様に、グリッドマップファイルの生成などのグリッド用の処理を追加
- ✓ APGrid PMAが「MICSプロファイル」による業務を承認し、古の「共通利用番号制」が復活すれば、すべての全国共同利用ユーザにグリッド証明書を発行できる準備はある!?

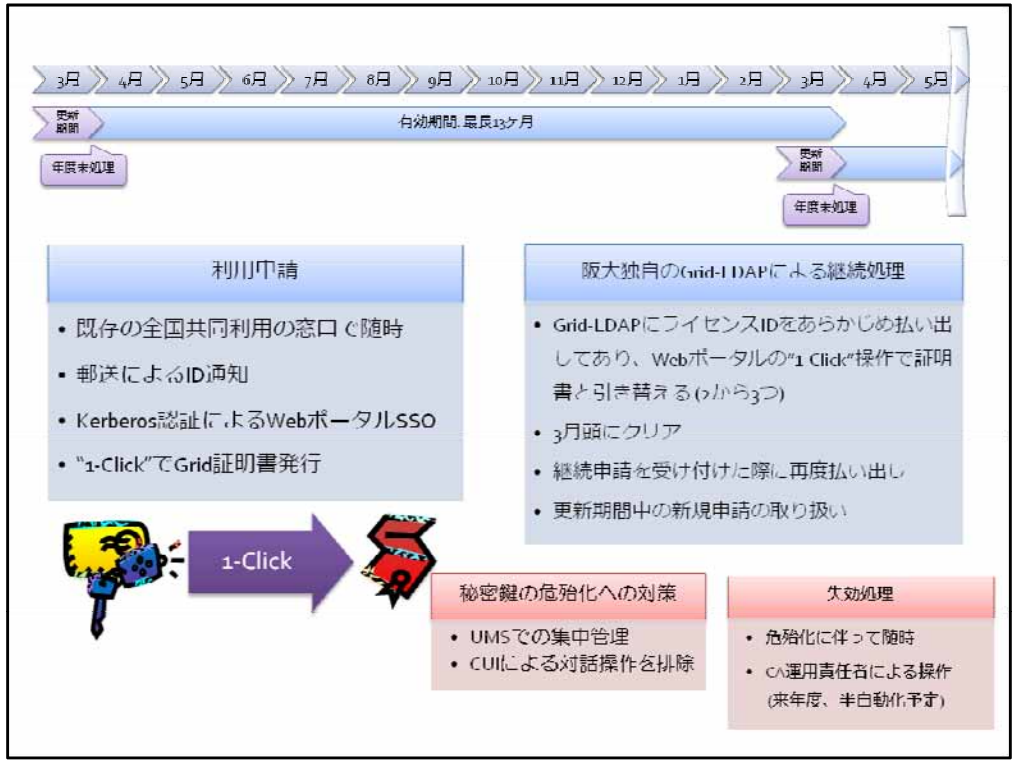


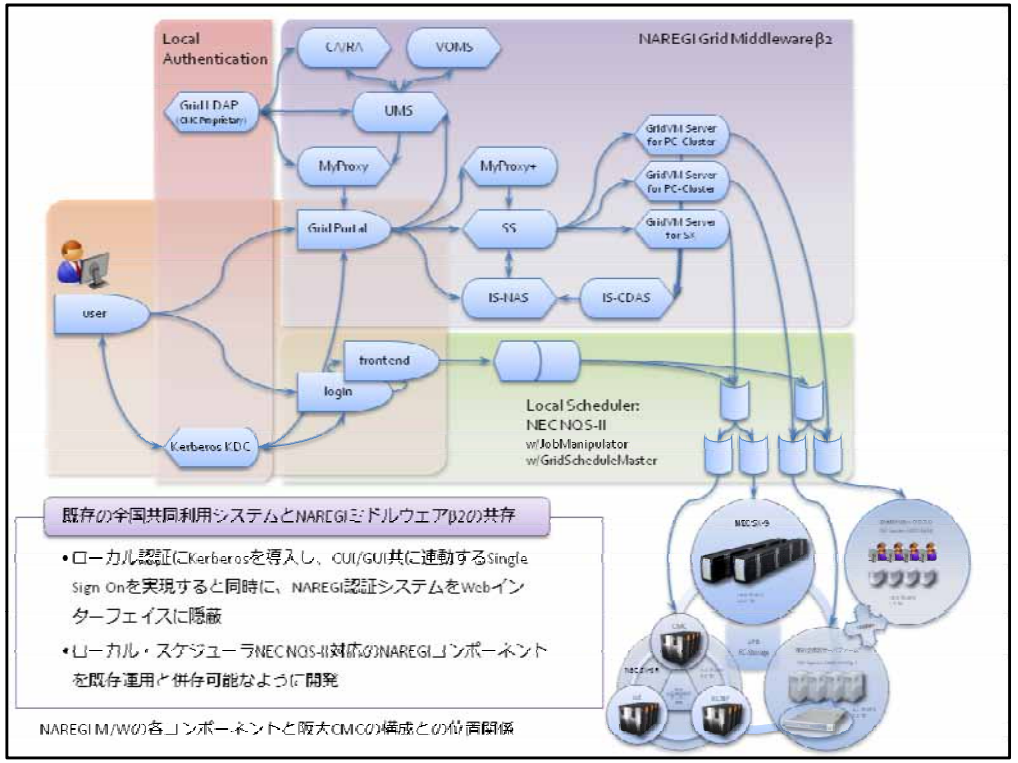
そう思っていた時期が
ありました・・・

阪大CMCのアプローチ – その1

「NAREGI連携なんて無理」と考えていた頃･･･阪大だけでも

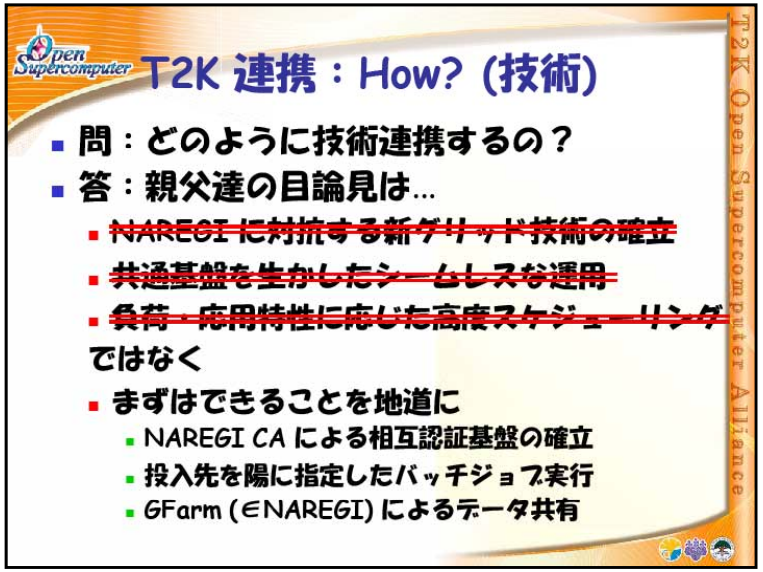
- 第1段階
  - すべての登録ユーザにグリッド証明書を
    - “1-click” によるグリッド証明書発行
  - すべての計算機資源をグリッドに提供
    - ローカルスケジューラのパイプキューを閉塞・開放することで提供資源を適宜制御



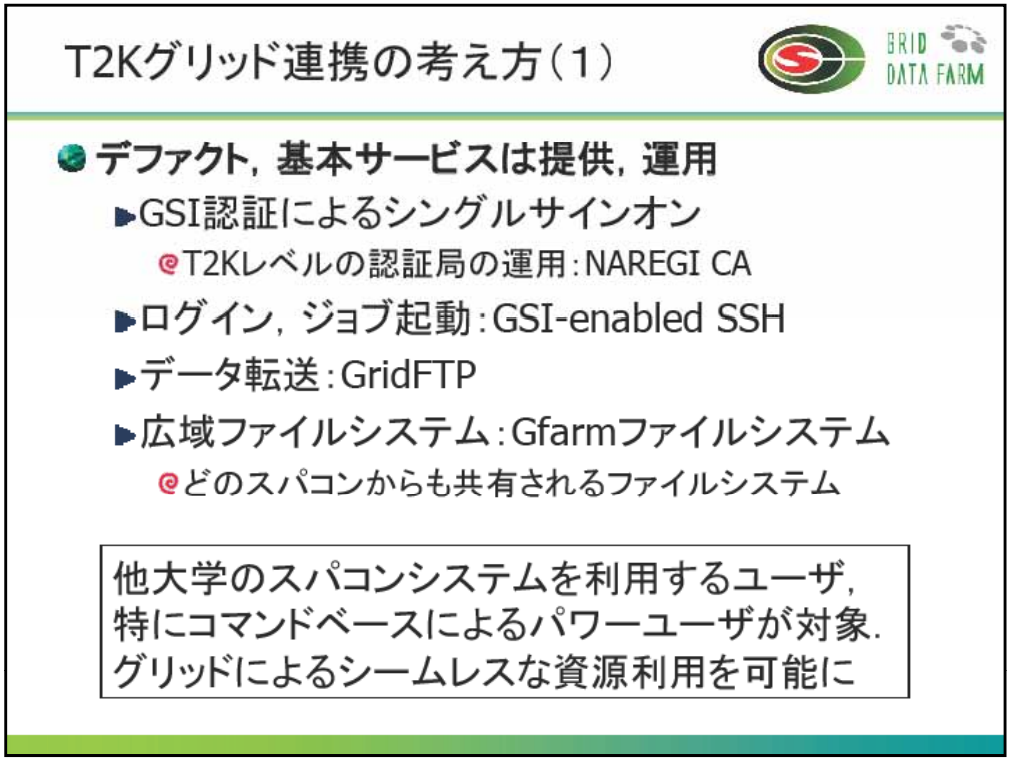


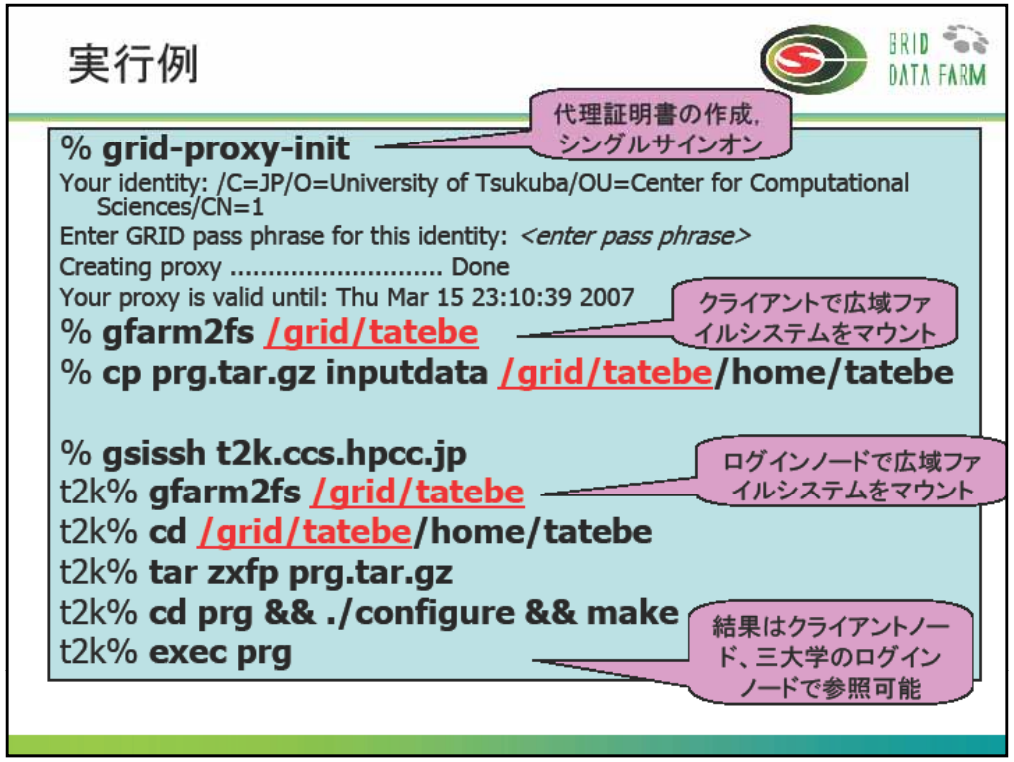
T2Kのアプローチ

- NAREGI CAによる相互認証基盤の確立
- 投入先を陽に指定したバッチジョブ実行
- Gfarmによるデータ共有



中島 浩, “T2k連携とグリッド運用”,
T2Kシンポジウムつくば 2008.



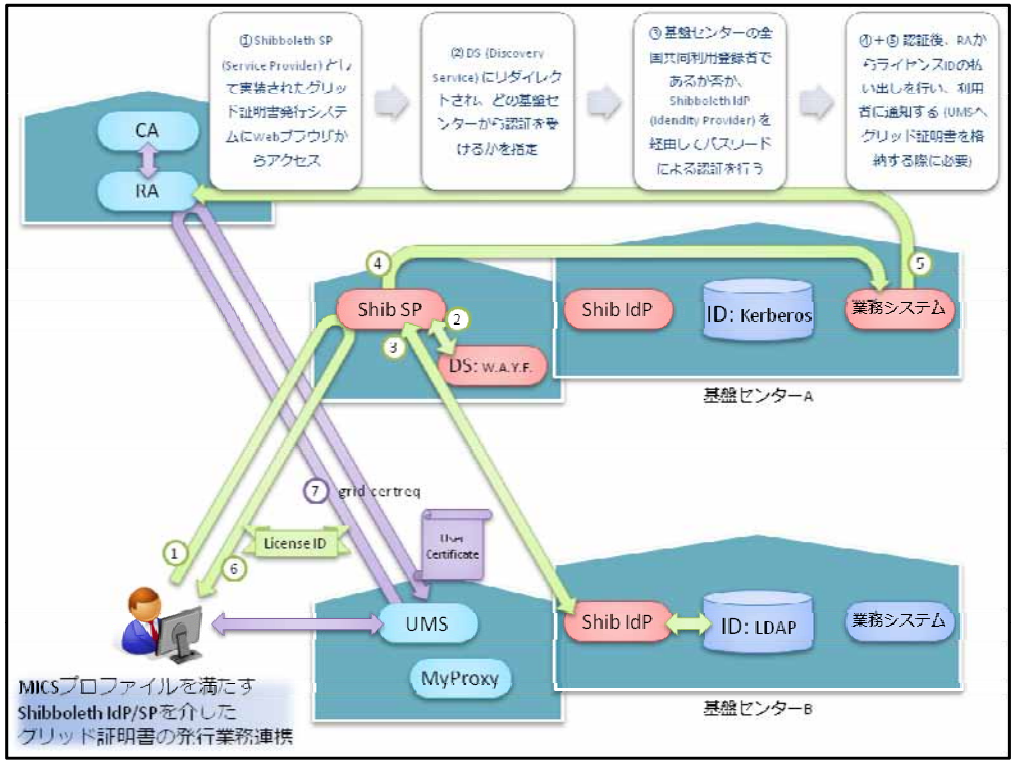


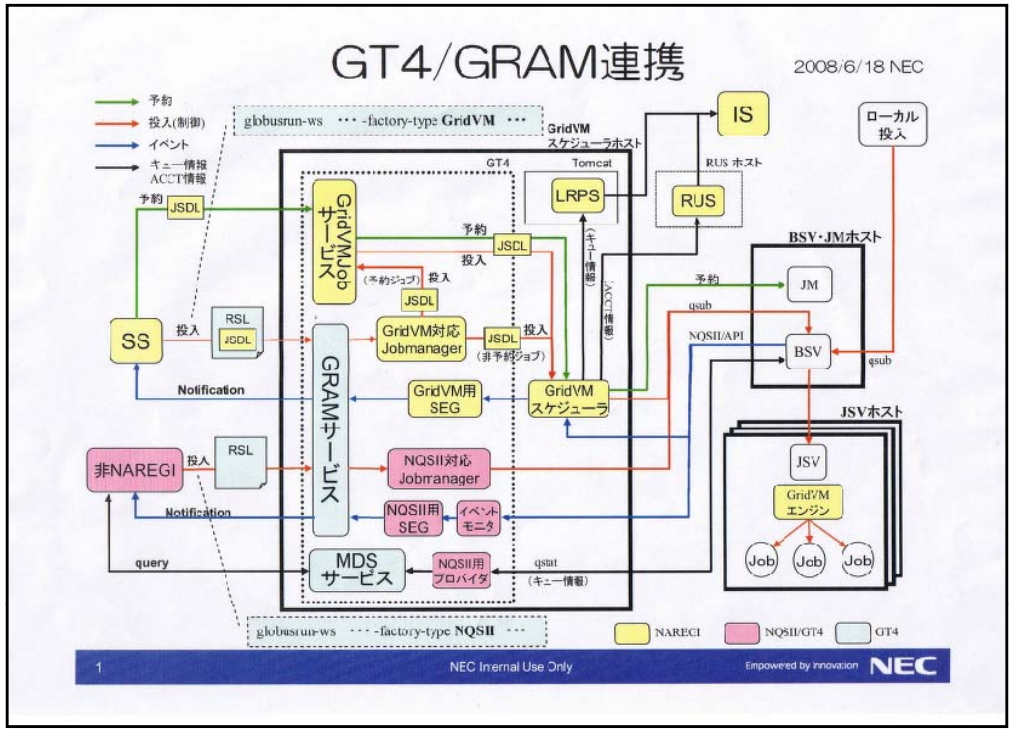
建部 修見, “T2k連携とグリッド運用”, T2Kシンポジウムつくば 2008.

阪大CMCのアプローチ - その2

T2Kグリッド連携の刺激を受けて共存を考え始める

- 第2段階
  - 他の基盤センターの登録ユーザにもグリッド証明書を発行
    - MICSプロファイルを満たすShibboleth SP/IdPによる連携
  - 提供資源を非排他的に共有
    - ローカルスケジューラの予約マップをメタスケジューラに後方からインジェクション





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

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
  - もしかしたらRESTfulなグリッドが流行っているかも
- 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

“RESTful” なグリッド

“Web2.0” はすべてを救う!?

- ターミナル・エミュレータもWebサービス化?
  - RFB on Web Browser (VNC Java Viewer)
    - 携帯電話でも使える!?
  - AjaxTermは全てを解決するか?
    - http://antony.lesuisse.org/qweb/trac/wiki/AjaxTerm
      - Latain-1のみ対応: UTF-8? 日本語?
- 泥臭いターミナル・サービスはまだ必要...
  - Windows Active DirectoryはKerberos+LDAPによるアイデンティティ・マネジメントと判明!
    - Windowsクライアントを全て取り込める!?
      - PKIによる初期認証も可能らしい...
    - MacOS XもADSとの親和性を謳い始めた
      - http://www.apple.com/jp/macosx/features/windows/
      - http://www.apple.com/jp/server/macosx/features/windowsservices.html
    - Linux Distro’sもほぼKerberos対応

MICS業務規定

グリッド認証局の業務負担

- プロダクションレベル認証局の登録窓口 (RA) への負荷の一極集中
  - 歩くRAと呼ばれた人もいたが・・・
- LRA
  - 窓口の分散
    - 基盤センターの共同利用掛 (システム管理掛)
  - それでも利用者は窓口で首実検
    - Photo ID and/or Official Document

対面による本人性の審査・確認

5-1. Issue 1

- User Identification
  - APGrid PMA minimum CA requirements;
    "In order for an RA to validate the identity of a person, the subject must contact the RA personally and present photo-id and/or valid official documents showing that the subject is an acceptable end entity as defined in the CP/CPS document of the CA."
  - Campus PKI CPS template;
    "The information of students or faculties will be collected on admission and stored in database in universities. Campus PKI CA will issue campus certificate by using and trusting the collected information in the database"
    -> Is it proper and feasible to use Campus certificate as an identification for issuing grid certificate?
    -> Add a following term to Campus PKI CPS template?
    "photo-id and/or valid official documents in the case of using campus certificate as an identification for grid certificate."

UPKI

23

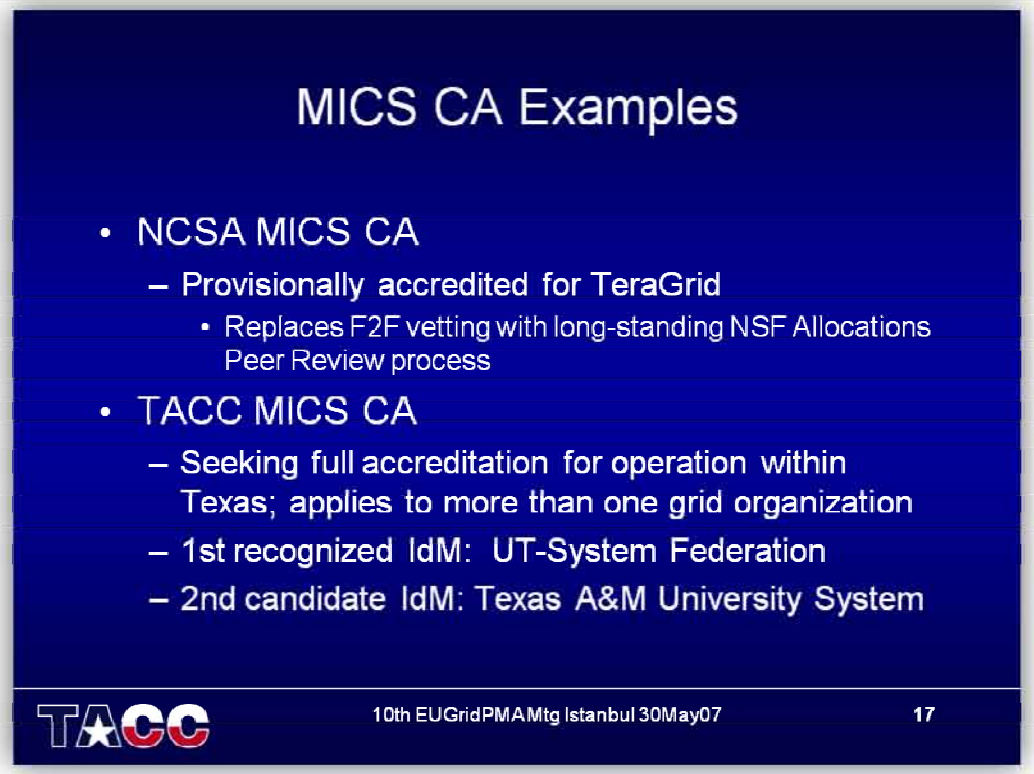
"Federation of Campus PKI and Grid PKI for Academic GOC Management Conformable to AP Grid PMA"
by Toshiyuki Kataoka and others at APAN-24

- ✓ 対面による審査 (“must contact and present”ー会って見せる) は、これまでの大型計算機センター運用では要請されてこなかった･･･
  - 大学や研究機関に所属
  - 支払責任者、経理責任者の印鑑 (支払の担保)
- ✓ 当面、Grid PKIにおいては、これまでの業務の延長でなんら問題ないのではないだろうか?!
  - 阪大CMC認証局CP/CPS第1版
    - 現時点で対面による確認を要請すれば発行できる対象を狭めてしまう･･･
    - RAが整備された段階でCP/CPSを「国際化」すればよいのではないか?!
      - Campus PKIのRAは「対面性」を要請していない?!
- ✓ “Production Level CA”と相互認証してもらえるのか?!
  - 国内: NII, KEK, 産総研
  - VOを統括する機関がROアカウントとの対応付けに際してCP/CPSが許容できるか検証してくれる?!

MICSプロファイル

Member Integrated X.509 PKI Credential Service

- ✓ 「1年1ヶ月」以上存続している既存の認証基盤と連動してグリッド証明書を発行する
  - The initial vetting of identity for any entity in the primary authentication system that is valid for certification should be based on a face-to-face meeting and should be confirmed via photo-identification and/or similar valid official documents.
- ✓ 導入例
  - TeraGridのNCSAグリッド認証局 (仮承認?)
    - ➢ NCSAがこれまで行ってきた「ピアレビュー」によるアカウント発行の枠組みを活かす
  - TACCのグリッド認証局
    - ➢ Classicプロファイルのグリッド認証局と併存?



"IGTF Accrediation Review of MICS Authentication Profile (Update)"
by Marg Murray, TACC, 2007/05/30

MICSはすべてを救う!?

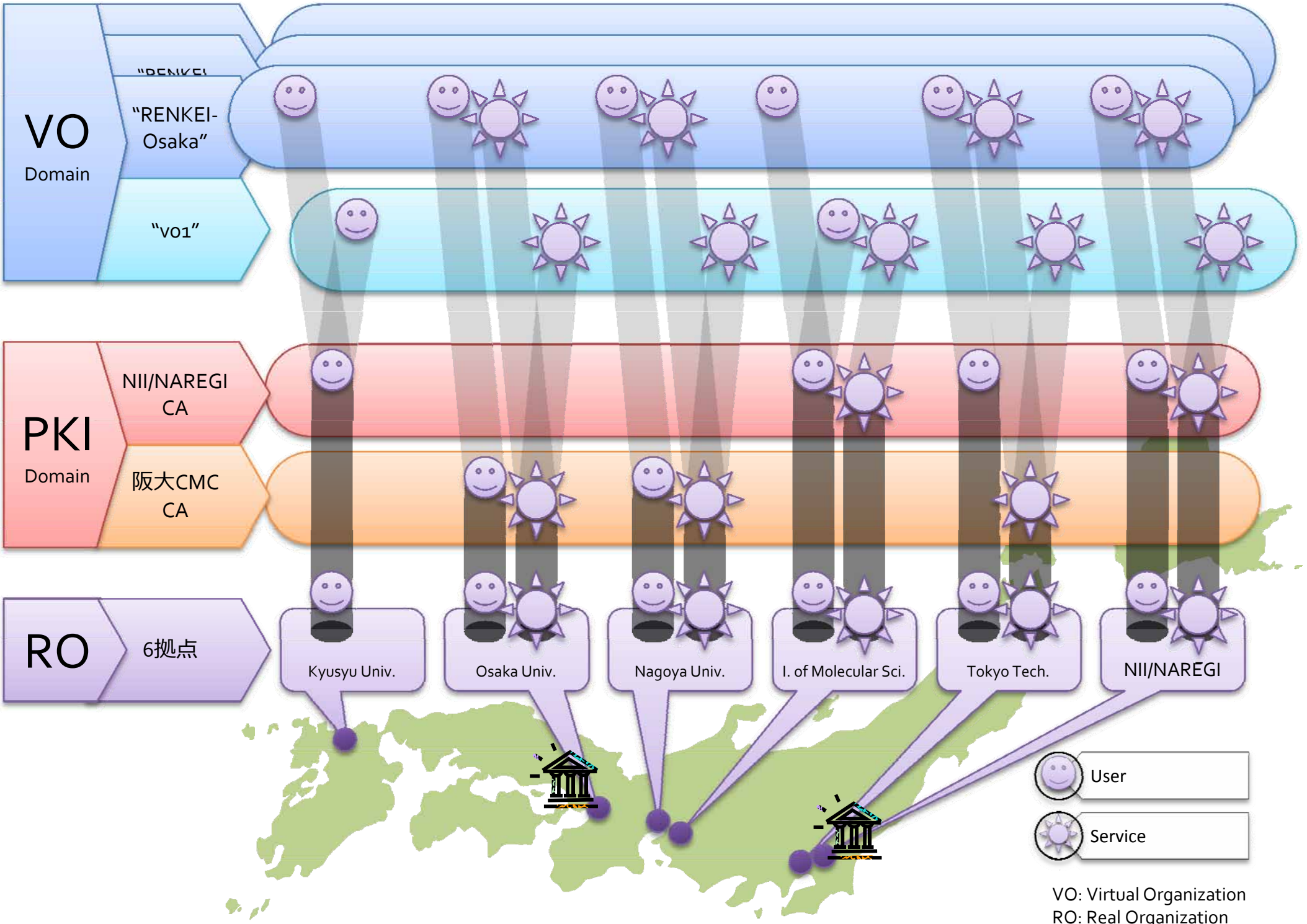
- 米国では、NSFが一元的に資金提供
  - NCSAが利用登録窓口を一手に引き受けてきた
  - PI (Principal Investigator) への権限委譲
- 日本では、旧大型計算機センター、現各種情報基盤センターが全国共同利用の窓口

Shibbolethによる
IDフェデレーション

VO管理者への
VO管理権限の委譲

VOの普及過程遷移

- Phase-0 (2006-)
  - 阪大独自の取り組み
    - すべての利用登録者にGrid PKI証明書を発行 (できるようにLicense IDを発行)
      - Default VO: “CMC_Osaka”
      - 証明書SubjectDN ↔ UID ↳ 課金グループ
        - » `grid-mapfile`を課金システム “NAVIAS” (仮称) が自動生成
- Phase-1 (2007/06-)
  - 東工大との連携 (+九大+NII)
    - 阪大へ利用申請し、東工大のUIDを紐付ける
      - 阪大がVOホスティング: “CMCGSIC_Osaka”
      - 証明書SubjectDN@阪大 ↔ UID@阪大 ↳ 課金グループ@阪大
証明書SubjectDN@阪大 ↔ UID@東工大 ↳ 課金グループ@東工大
        - » `grid-mapfie`は手動で変更する必要あり
        - » ユーザ情報のセキュアな伝達手段の確立が必要
        - » これらを開発するなら費用負担発生･･･
- Phase-2
  - VO連携



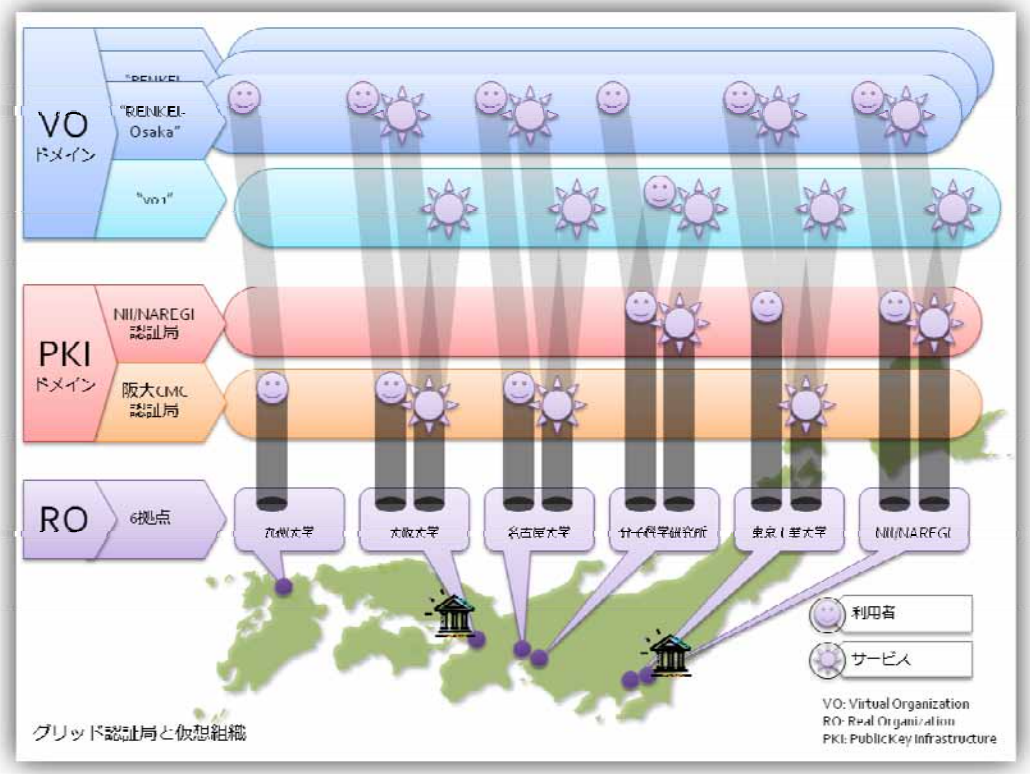
Grid Certificate Authorities and Virtual Organization

VO: Virtual Organization
RO: Real Organization
PKI: Public Key Infrastructure

“Registration Agency” 構想に向けて

今回のアカウンティング・ポリシー

- ローカル・アカウントを発行し、grid-mapfileで証明書と紐付ける
  - 大阪大学: 通常の全国共同利用アカウント発行にグリッド証明書が付随
  - 東京工業大学: 通常の全国共同利用アカウントを発行し、別途発行されたグリッド証明書を紐付け
  - その他: 一時アカウントを発行

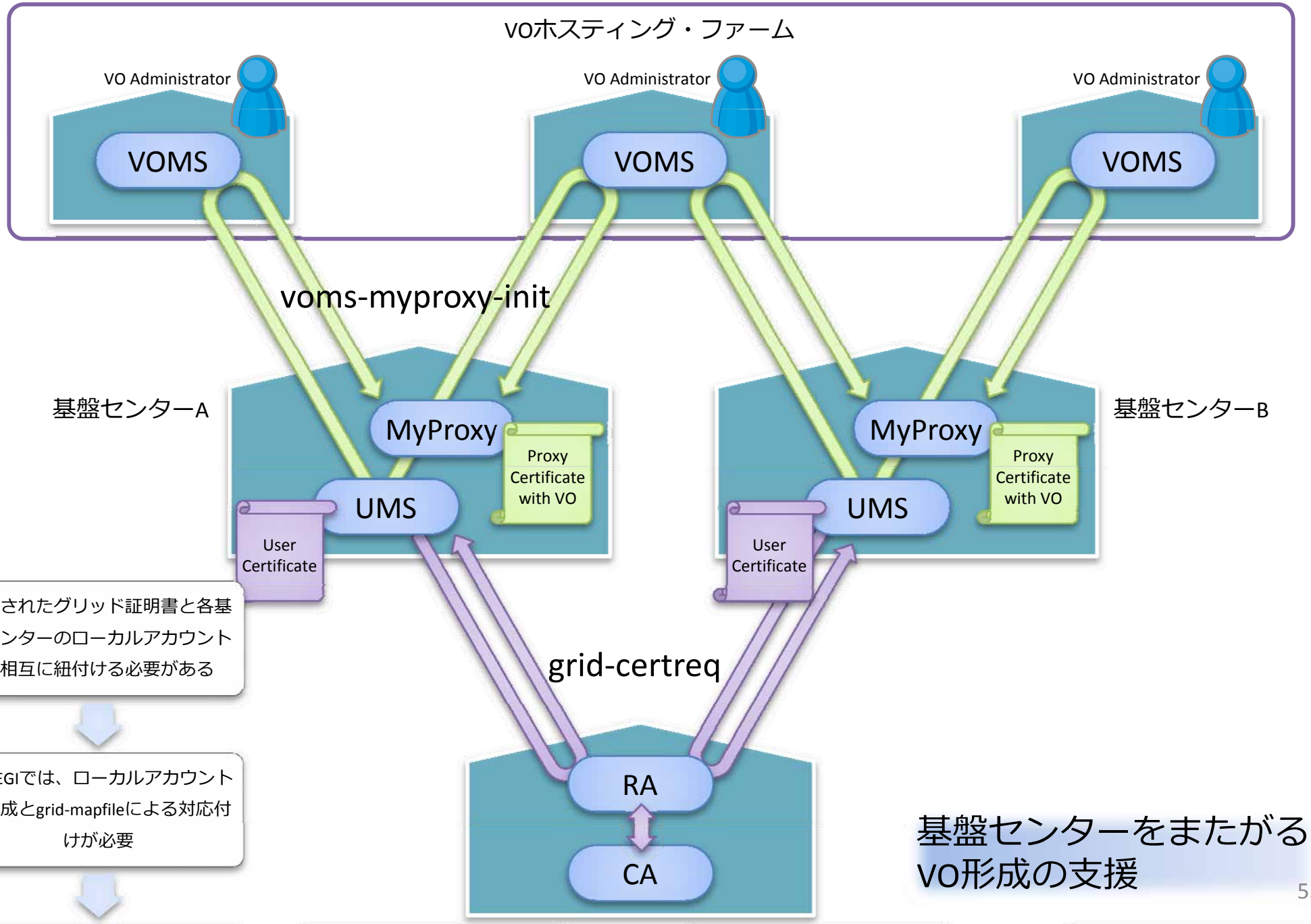


グリッド認証局と仮想組織

代理店業務

- NII/NAREGIにて連携アカウントの代理発行業務
- 各拠点のアカウント発行に必要な情報を包括して収集
  - 氏名、職名、所属、研究分野、メールアドレス、電話番号など
- 各拠点に一括して代理申請
- 各拠点にて証明書との紐付けを行う

「料金相殺」制度の導入検討



発行されたグリッド証明書と各基盤センターのローカルアカウントを相互に紐付ける必要がある

NAREGIでは、ローカルアカウントの作成とgrid-mapfileによる対応付けが必要

egeeのように、プールアカウントで対応するという方針もあるが、LCAS/LCMAPSのような拡張が必要

そもそもVOMSをどうホスティングするか?

VO管理者にすべてのVO管理権限を委譲するか?

各基盤センターで、どのVOに資源提供するかの認可制御と課金をいかに行うか?:

基盤センターをまたがるVO形成の支援

- 認証局
  - 現時点でサービスしている認証局
    - プロダクションレベル (Classic Profile)
      - AIST, KEK, NII/NAREGI
    - セミプロダクションレベル (MICS Profile – 非公認)
      - 阪大CMC
    - プライベート認証局
      - T2K筑波
  - 京速コンの登録機関との位置関係を想定して検討すべき
    - 東大?、兵庫県?
- 既存の基盤センター業務システムとの連携
  - U-PKIのSSO実証実験に阪大CMCが提供するShibboleth SPと各基盤センターのIdPとの連携
    - LDAP: OK, Kerberos (ActiveDirectory Server): OK, NIS: OK?
- VO運用
  - 実アカウントか?
    - GT, NAREGI
  - プールアカウントか? ← 課金は?
    - egee LCAS/LCMAPS
- 管理ノード
  - 昨年度の連携実証にて様々な構成での相互運用性を検証済み
- 計算ノード (GridVM)
  - 通常運用とNAREGIへの資源提供は併存
    - 本年度実施予定の機能拡張 (東北大＋阪大にて)
      - ローカルスケジューラ (NEC NQS-IIを想定) への直接的な予約とNAREGI SSからの予約が非排他的に共存
      - GridMPI以外のMPI対応 (ただし同一GridVM内のみ)
    - 課金情報はローカルスケジューラ (またはOSの課金機能) で採取
  - 問題はそれ (NEC NQS-II) 以外
    - PBS Pro, LoadLeveler
    - T2K (Torque+SCore, SGE, Parallelnavi), KEK (LSF)