大阪大学でのUPKI
シングルサインオン実証実験

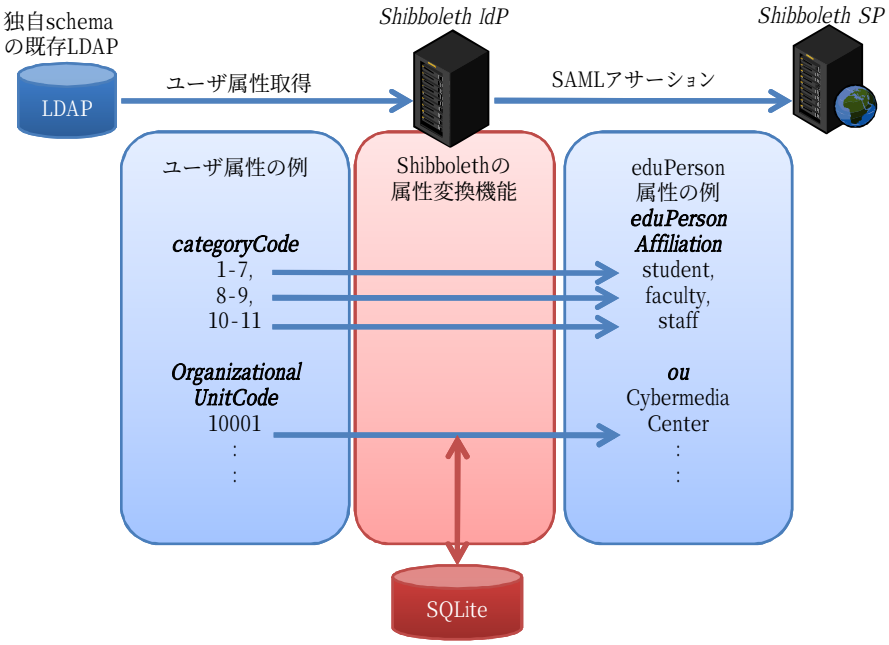
大阪大学サイバーメディアセンター

1. Identity Provider の機能調査・構築

大阪大学サイバーメディアセンターでは、学内サービスの認証基盤として構築した全学IT認証基盤を大学間認証連携およびサービス連携の基礎として発展させるため、UPKI認証連携基盤の実証実験に参加し、既存の認証基盤の拡張方針について検討を進めている。本センターでは特に既に認証基盤を構築した大学をターゲットとして、既存の認証基盤に対する変更を最小限に抑えた上で、UPKI認証連携基盤に参加する方法について検討していきたいと考えている。以下では、本学の認証基盤を例にUPKI認証連携基盤にシームレスに統合するためのアプローチについて今年度の調査状況、実証実験の実施状況について報告する。

Shibboleth IdP の属性マッピング機能の検証

各大学で構築した認証基盤で管理しているユーザ属性が eduPerson 属性に対応する属性をもっているケースは少なく、eduPerson 属性を追加して適当な値を設定する作業が必要になる。運用中のディレクトリサーバに対するデータ書き換えや新たな機能追加は作業工数が多くなるため、Shibboleth の属性変換機能で既存の属性情報から eduPerson 属性を生成しSAMLアサーションに設定する方法について調査した。調査の結果、Mapped AttributeDefinition を用いた静的な属性マッピングおよびRelationalDatabase DataConnector を用いた動的な属性マッピングにより本学で管理しているユーザ属性をeduPerson属性に変換できることを確認した。詳細についてはWikiページに報告している。

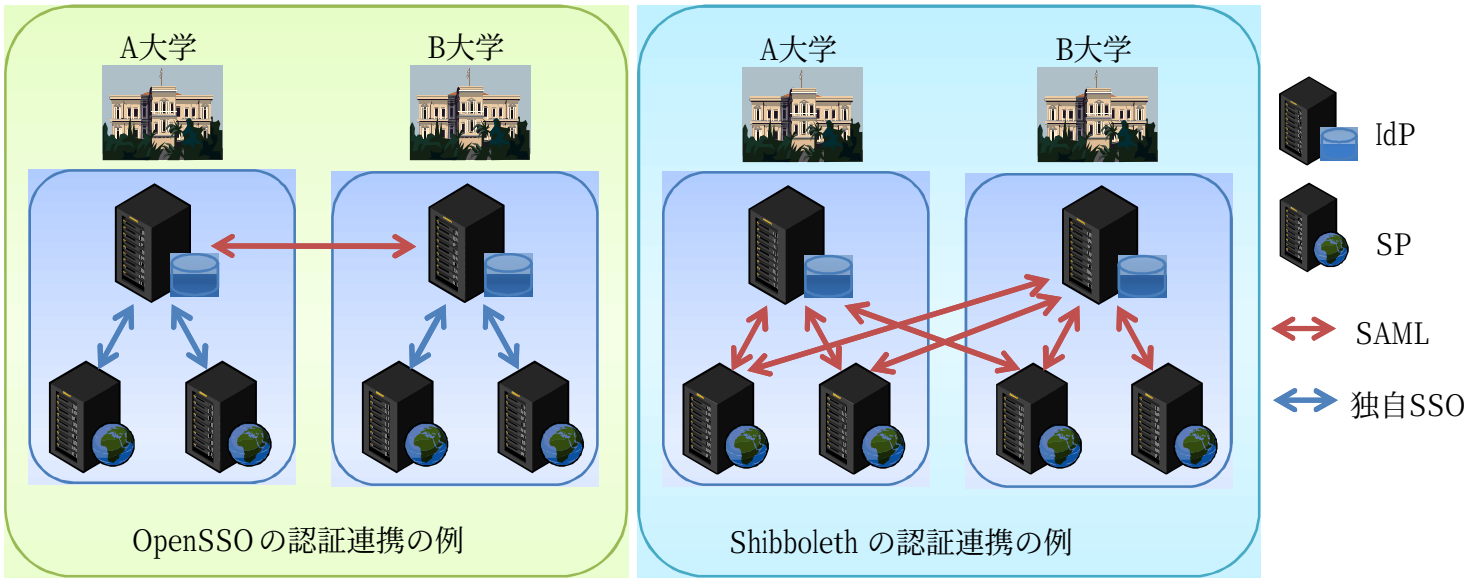


Wikiページ（http://ssowiki.nii.ac.jp/）：
「00_各参加機関の取り組み＞大阪大学＞Shibboleth 2.0 の属性マッピング機能の検証」

OpenSSO, Access ManagerとShibboleth SPのSAML2.0連携

既存のWeb SSOサーバがある大学では別にShibbolethサーバを運用するよりは、既存のWeb SSOを用いた方がコストを低減できる可能性がある。本学でWeb SSOサーバとして採用しているSun Java System Access Managerについて、そのオープンソース版であるOpenSSOを調査し、Shibboleth SPとのSAML2.0での連携方法について検討した。OpenSSOは図に示すように想定している連携スタイルなどがShibbolethとは異なるため、SAML2.0に関して実装されている機能に相違がある。そこで、OpenSSOが提供するSDKを利用して機能をカスタマイズし、Shibboleth SPと連携可能にした。また、そこで蓄積したノウハウを用いて、Access ManagerとShibboleth SPの連携を可能にした。詳細についてはWikiページに報告している。今後の課題としては、SAML2.0での連携を前提として、OpenIDなど他のプロトコルもサポートするOpenSSO, CASといったシステムも含めて、大学における認証基盤の機能を満たすSSOシステムの構築方法について引き続き検討していく必要がある。

Wikiページ（http://ssowiki.nii.ac.jp/）：
「00_各参加機関の取り組み＞大阪大学＞OpenSSO と Shibboleth 2.0 の SAML 2.0 連携」



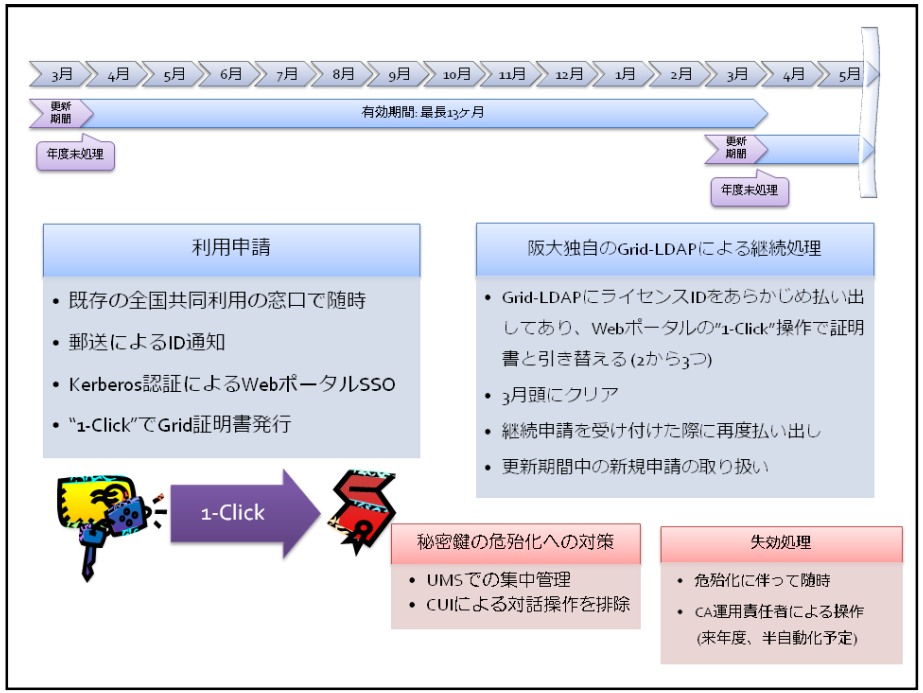
2.グリッド証明書発行SPの構築

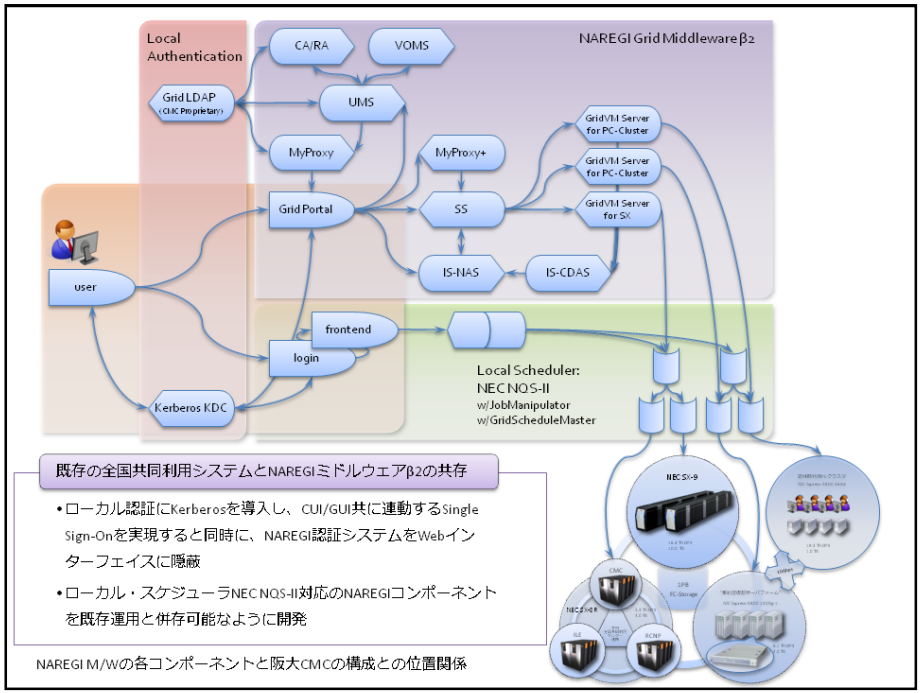
- 大阪大学サイバーメディアセンターでは、本センターの大規模計算機システムを利用するための既存の全国共同利用業務のIDデータベース (Microsoft Active Directory　Kerberos) に付随するShibboleth IdPを設置した。
- さらに、当該IdPによる認可を受けた利用者に対して本センターのグリッド認証局からグリッド証明書を発行するために必要となるライセンスIDを自動的に払い出すSPを構築し試験的なサービス提供を行っている。また、さらに、本学の全学IT認証基盤とのフェデレーションを検証した。
- このように、NISやLDAP、ADSなどによる既存のIDレポジトリにShibboleth IdPを付随して設置し、本センターと業務協力関係を結ぶことで、これまでのような人手による事務作業を省略して、本センターが発行するグリッド証明書を取得可能になる。
- このような業務フローはIGTF (International Grid Trust Federation) が規定するMICS (Member Integrated Credential Service) プロファイルによる認証局運用業務規定に合致するものと考えており、将来的にIGTF/APGrid PMA (Policy Management Authority) によってプロダクション・レベルのグリッド証明書発行業務として認定され得るものと考えている。
- これまでのClassicプロファイルに基づくグリッド証明書発行に際しては、窓口に写真付きの身分証明書を提示して本人確認を受ける必要があったが、これを既存の情報基盤センターの全国共同利用の利用登録情報で代替することが可能となり、ソーシャル・フローを大幅に簡素化し、より広範にグリッド証明書を発行可能になるものと期待している。

阪大CMCのアプローチ – その1

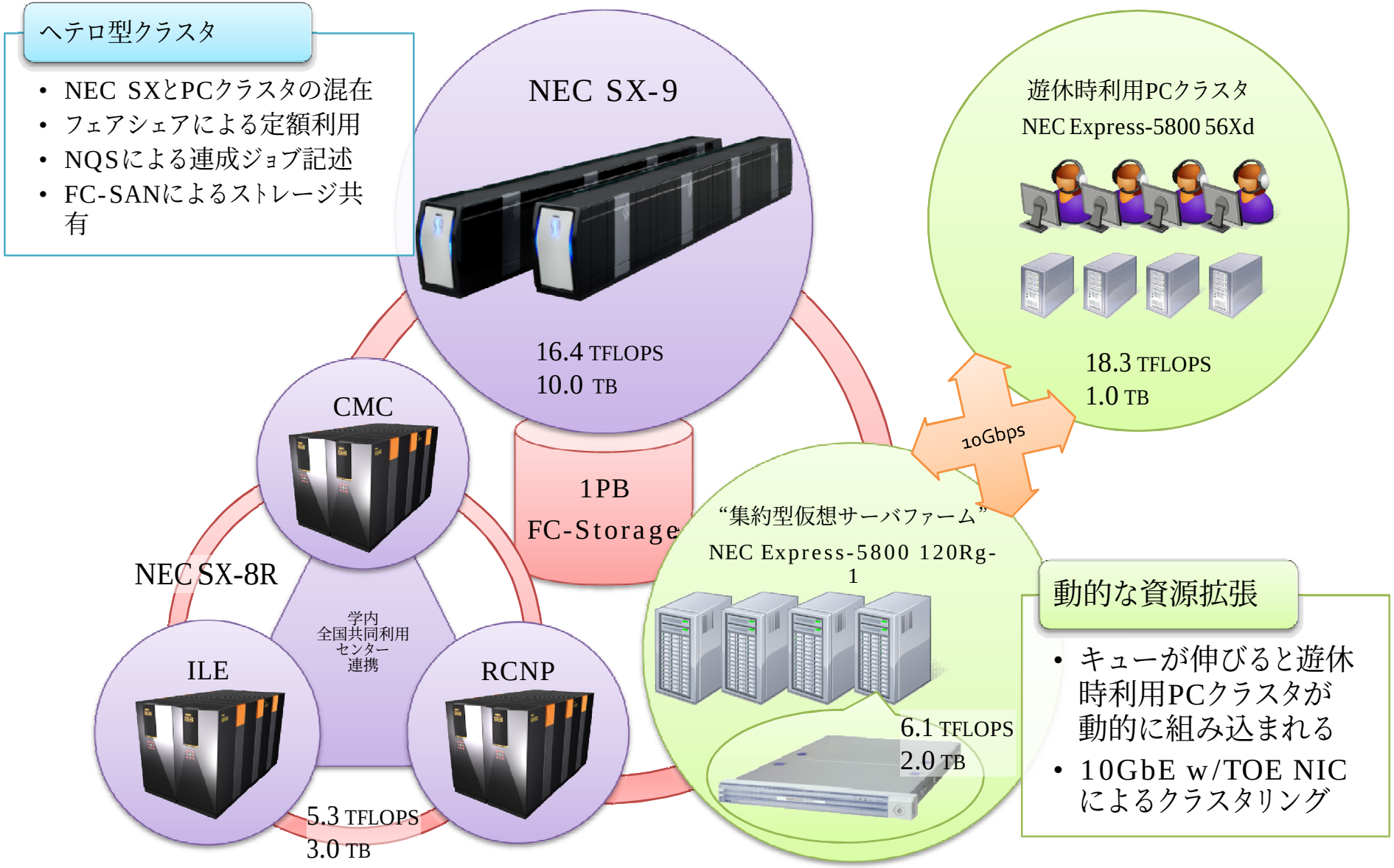
「NAREGI連携なんて無理」と考えていた頃･･･阪大だけでも

- 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

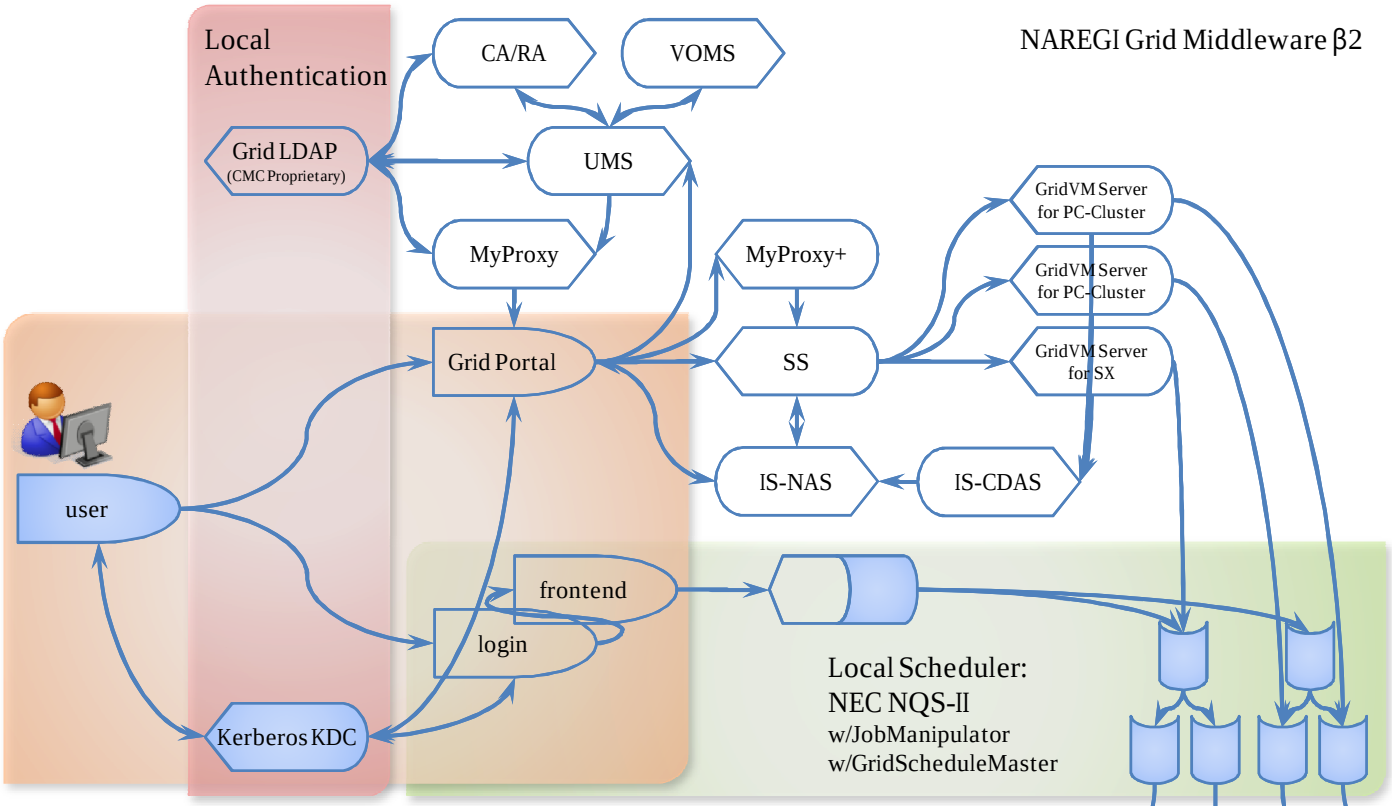


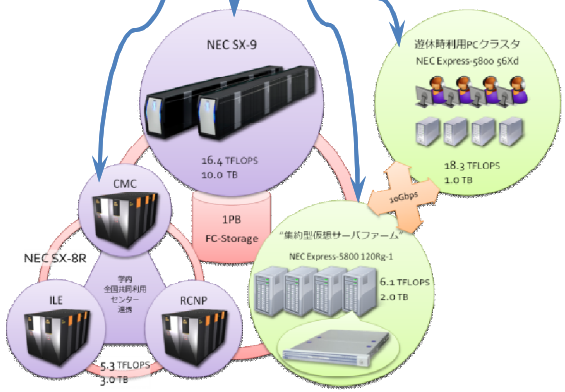


阪大CMCの大規模計算機システム構成　Total: 46.1 TFLOPS, 16.0 TB



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

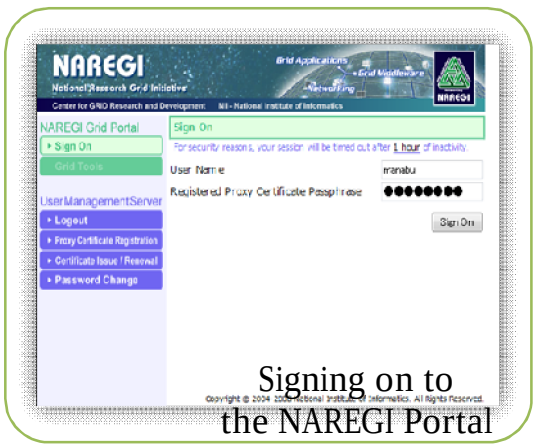
- ローカル認証にKerberosを導入し、CUI/GUI共に連動するSingle Sign-Onを実現すると同時に、NAREGI認証システムをWebインターフェイスに隠蔽
- ローカル・スケジューラNEC NQS-II対応のNAREGIコンポーネントを既存運用と併存可能なように開発

NAREGIグリッドミドルウェアの認証メカニズム

- シングルサインオンは行わない･･･
  - UMS (User Management Server)
    - ローカルアカウントで初期認証
    - 別途、RAから発行されたライセンスIDで認証を行ってグリッド用ユーザ証明書を払い出し
  - Grid Portal
    - UMSから払い出したプロキシ証明書を復号化するパスフレーズによって認証
- 2007年度、阪大CMCでは、これらの認証をKerberosクレデンシャルに基づくシングルサインオンに置き換えた
  - 残念ながら、NAREGIミドルウェア最終版の発注仕様決定後だったため貢献できず･･･

Issuing Grid User Certificate with "License ID" pre-obtained from the RA and storing it to the UMS (first time)

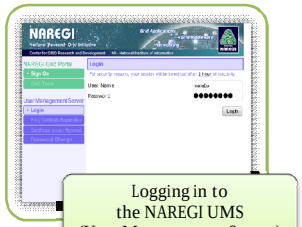
Issuing Proxy Certificate with decrypting Grid User Certificate



Logging in to the NAREGI UMS (User Management Server) with its local account

Signing on to the NAREGI Portal with decrypting issued Proxy Certificate

Original NAREGI Authentication Flow



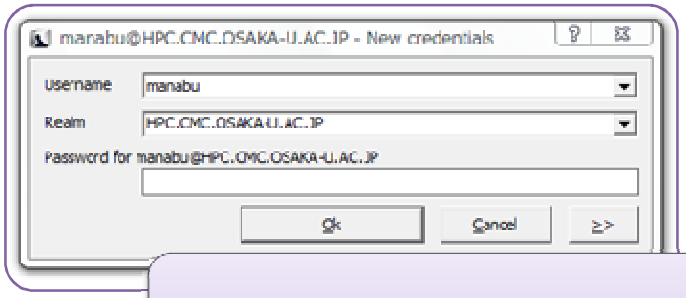
Logging in to
the NAREGI UMS
(User Management Server)
with its local account

Issuing Proxy Certificate
with decrypting
Grid User Certificate

Signing on to
the NAREGI Portal
with decrypting
issued Proxy Certificate

Original NAREGI Authentication Flow

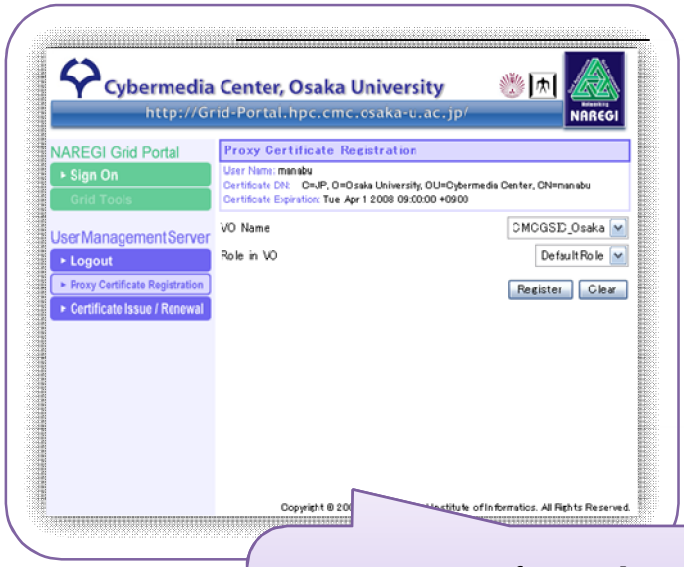
Our Replacement using Kerberized SSO



Obtaining Kerberos Credential for SSO
to the NAREGI UMS and Portal

Showing Kerberos Credential,
Grid User Certificate is able to issue
for all users without exchanging
“License ID” (first time)

Showing Kerberos Credential,
no decryption is needed
on issuing Proxy Certificate
and signing on to the NAREGI Portal



Note: Certificates have been
encrypted by a system generated
passphrase,
users don’t aware and don’t bother

最初に行う初期認証が十分に強固であるべき

- 阪大CMCの全国共同利用アカウント
  - KerberosによるSSO+12文字のパスワード
  - IGTF (International Grid Trust Federation) が規定するプロダクション・レベルのグリッド用ユーザ証明書を操作するために十分な強度
    - APGrid PMA議長の田中さんと議論しMICSプロファイルとして認定を受け得ることを示唆される

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?

1. Intro: MICS AP Goals

- Leverage existing IdM infrastructures.
- Generate end entity certificates based on a membership or authentication system maintained by an organization or federation that last at most 1 year and 1 month.
- MICS CA maps IdM identity to an X.509 Grid certificate identity.
- Define minimum security requirements.

TACC 10th EUGridPMAMtg Istanbul 30May07 2

MICS CA Examples

- NCSA MICS CA
  - Provisionally accredited for TeraGrid
    - Replaces F2F vetting with long-standing NSF Allocations Peer Review process
- TACC MICS CA
  - Seeking full accreditation for operation within Texas; applies to more than one grid organization
  - 1st recognized IdM: UT-System Federation
  - 2nd candidate IdM: Texas A&M University System

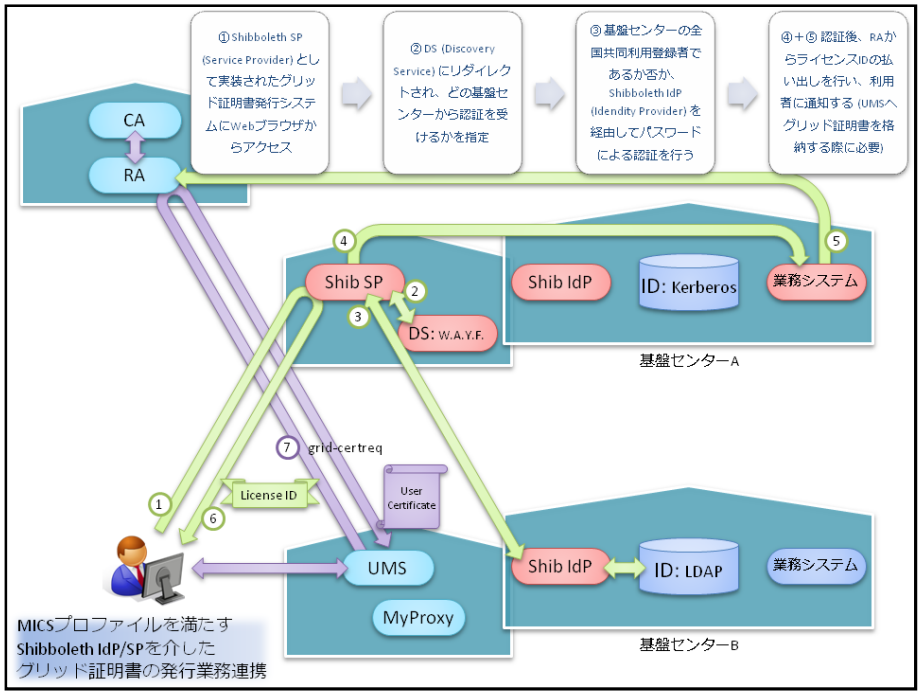
TACC 10th EUGridPMAMtg Istanbul 30May07 17

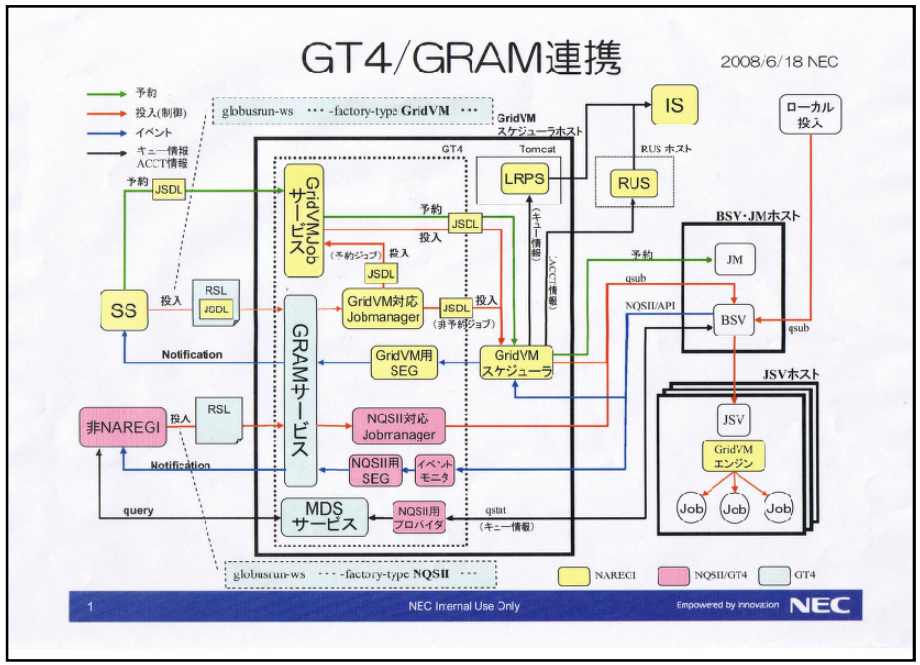
"IGTF Accrediation Review of MICS Authentication Profile (Update)"
by Marg Murray, TACC, 2007/05/30

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

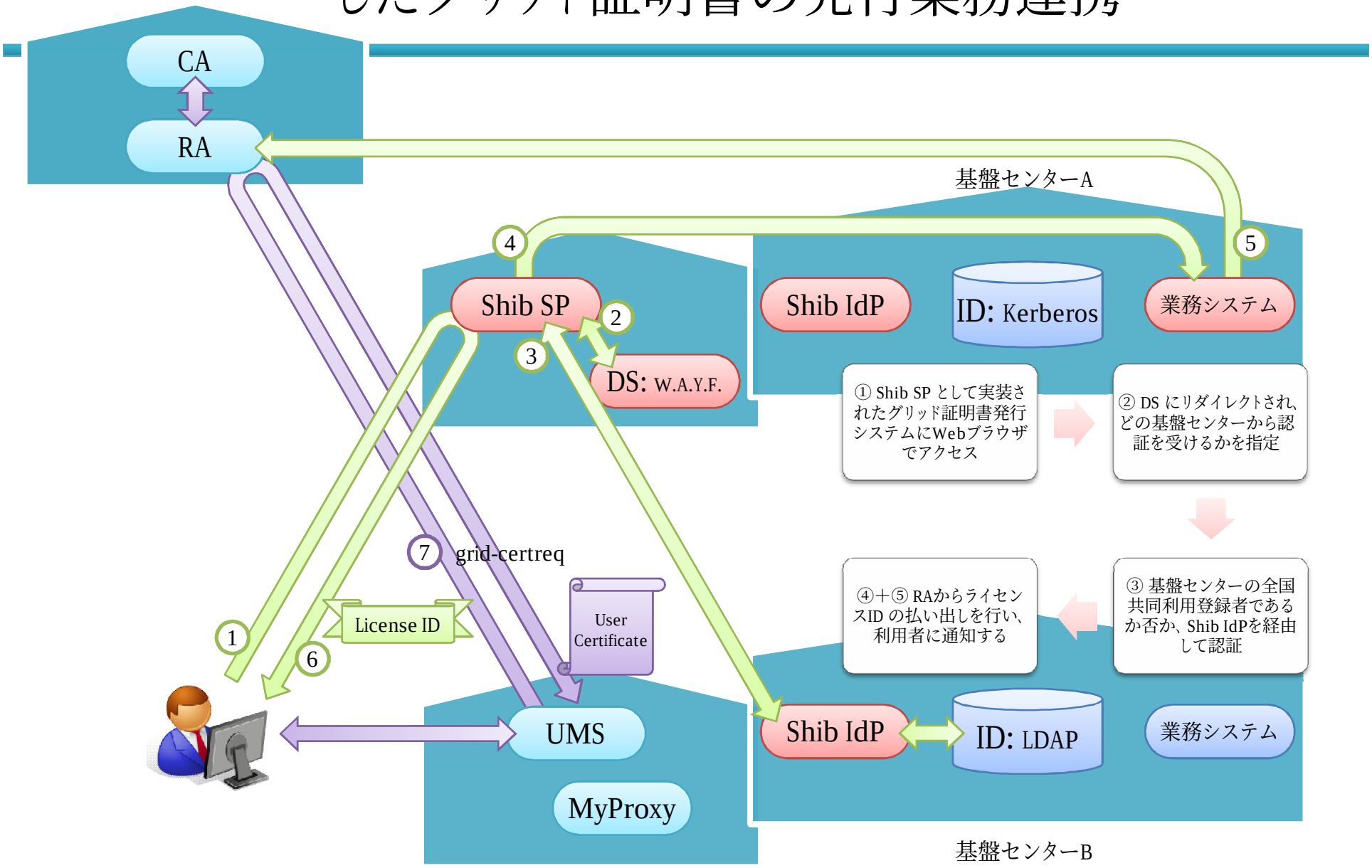




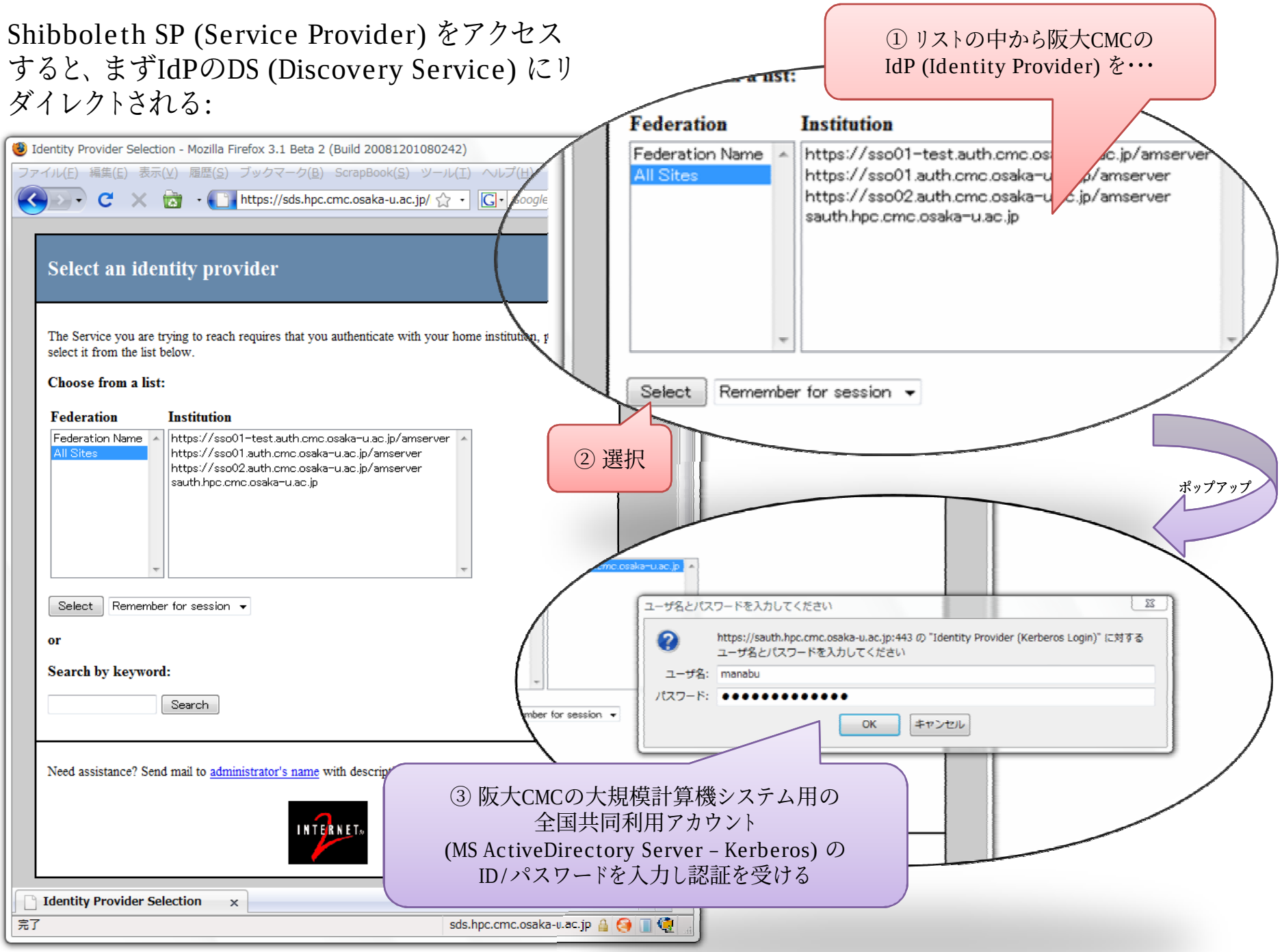
NAREGIミドルウェアとShibboleth

- シングルサインオンの実現
  - NAREGI Grid Portalへの接続時 (検討中)
  - グリッド用ユーザ証明書の払出し時 (本年度の成果)
- 現時点で実現できていない点
  - グリッド用ユーザ証明書やプロキシ証明書を複合化するパスフレーズによる認証の一元化
    - 他センターのグリッド認証局が発行したグリッド用ユーザ証明書を格納するUMSとの互換性を保つ必要性からパスフレーズなしの認証とすることは難しい・・・
- Shibbolethによるフェデレーションだけでは解消できない問題点
  - 資源提供を行う拠点間でのDN (Designated Name) とLN (Local Name) の対応管理

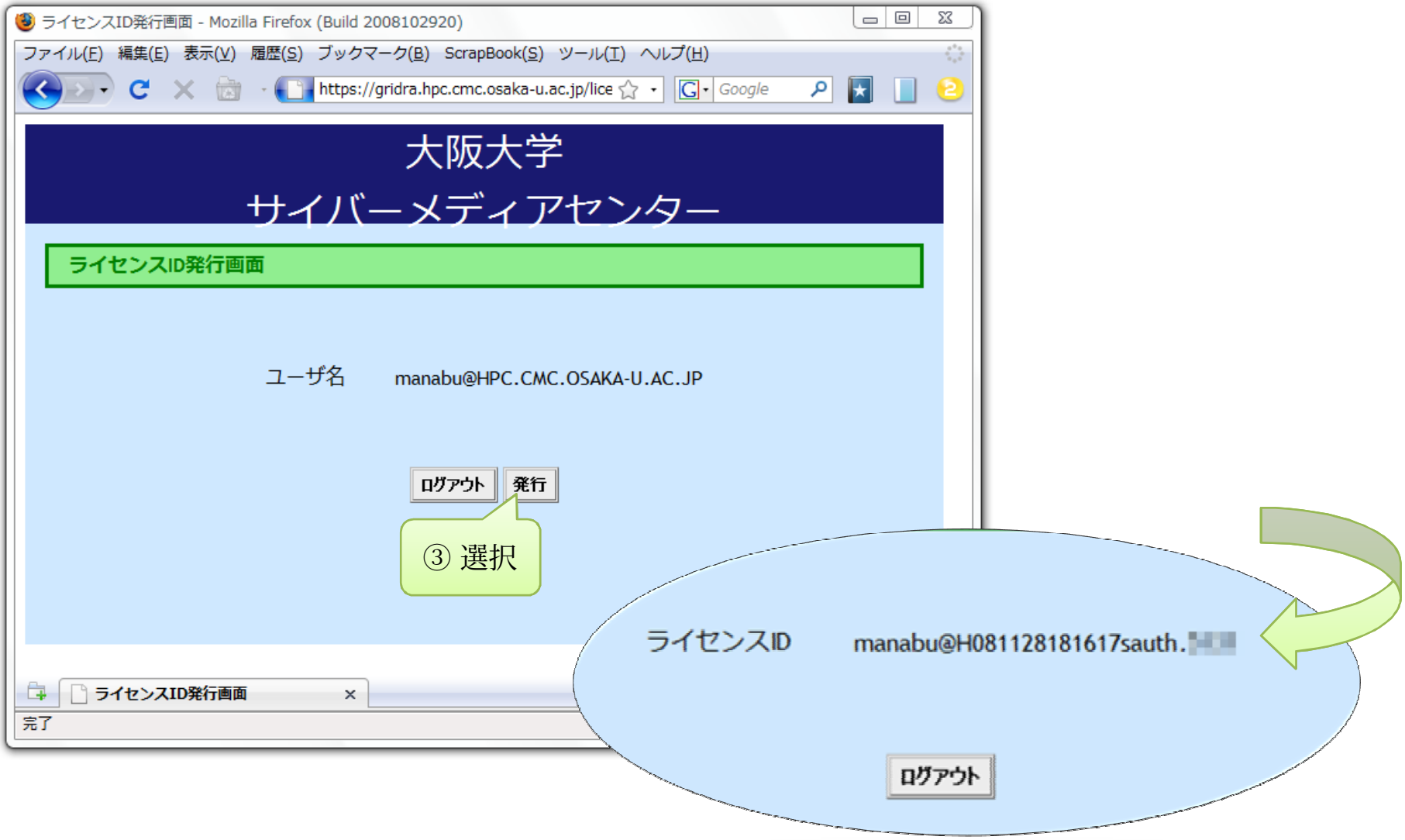
MICSプロファイルを満たすShibboleth IdP/SPを介したグリッド証明書の発行業務連携



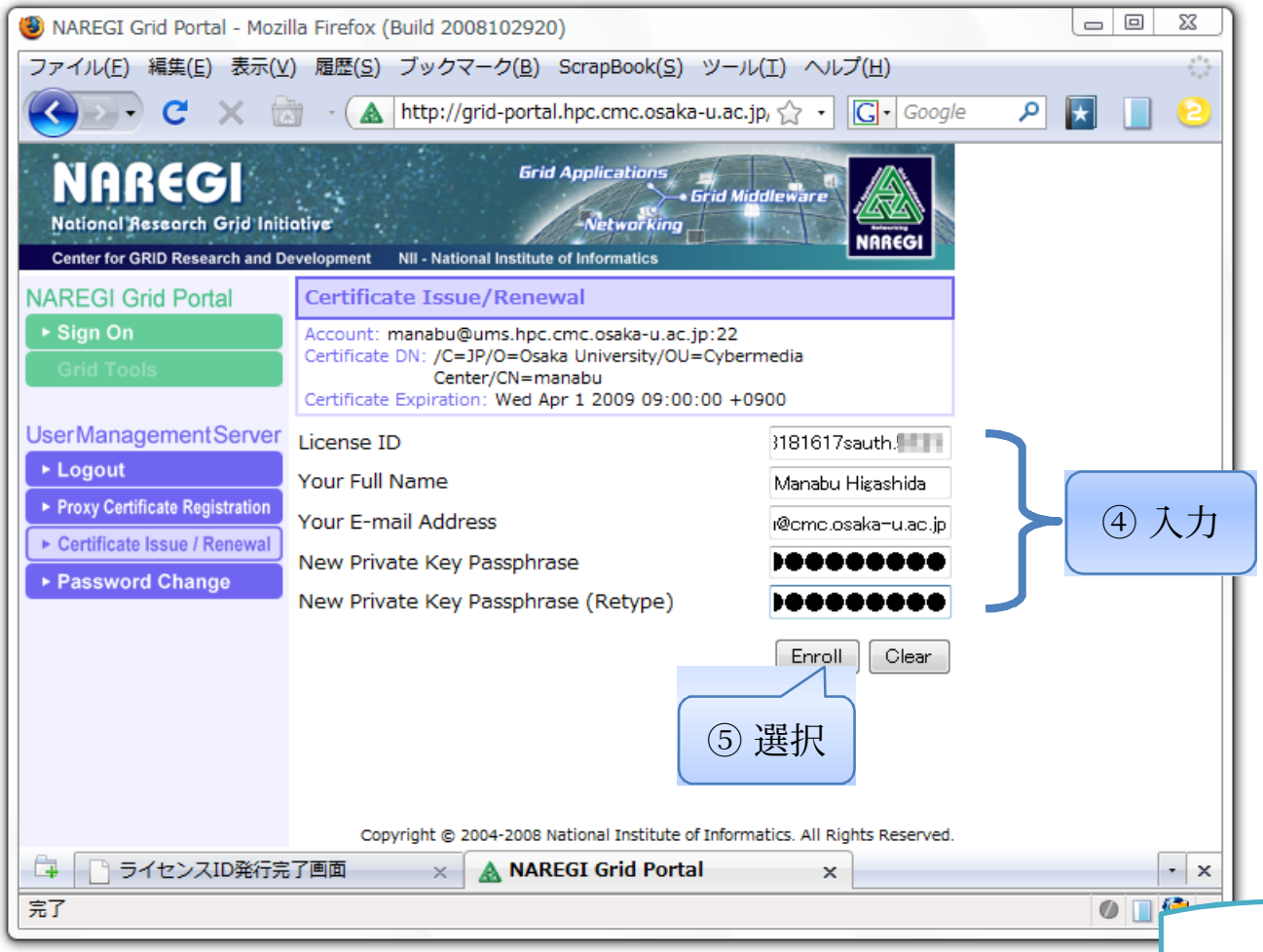
Shibboleth SP (Service Provider) をアクセスすると、まずIdPのDS (Discovery Service) にリダイレクトされる:



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):

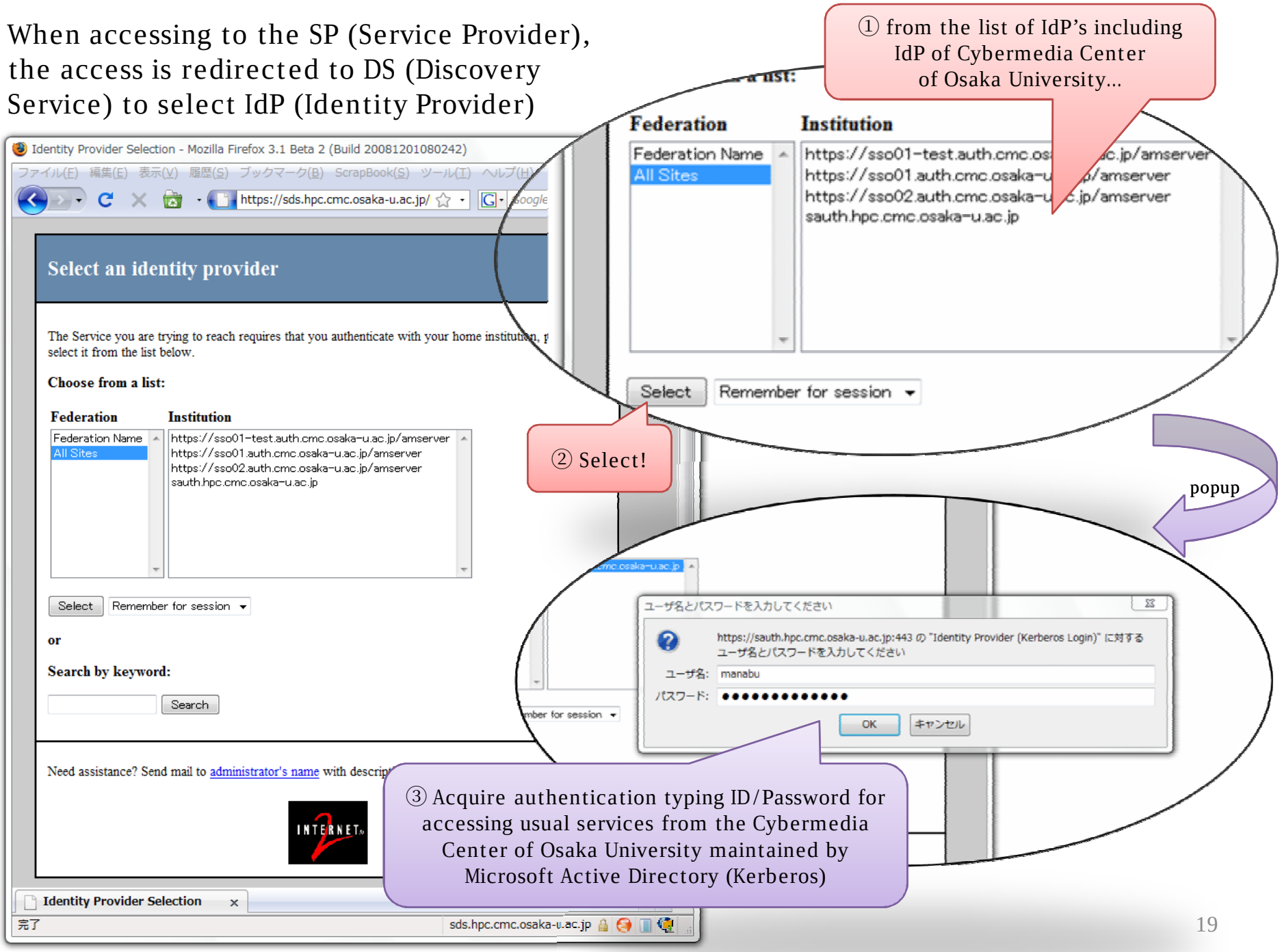


NAREGIポータル (Web UI) にて、取得したライセンスIDと付帯情報を入力する。
阪大グリッド認証局からユーザ証明書が発行され
付随するUMS (User Management Server) に格納される:



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

When accessing to the SP (Service Provider), the access is redirected to DS (Discovery Service) to select IdP (Identity Provider)



Shibbolethで実現できること、できないこと

- Shibbolethで実現できる
  - ID/パスワードに基づくフェデレーション
- Shibbolethだけでは実現できない
  - DN (またはShibbolethのEPPN属性) と各サービス提供拠点のローカルアカウントの「名寄せ」
  - EGEEが採用しているプールアカウント (LCAS/LCMAPS) とVOMS (VO Management Server) との連携で解決できる？
    - 現時点でNAREGIミドルウェアはgrid-mapfileによる「名寄せ」にのみ対応
    - 計算機資源提供を行う情報基盤センターのAUPとの整合性？