“Shibbolized NAREGI Grid Middlewareによる グリッドIDフェデレーション”

CSI委託事業: 平成21年度実施報告と平成22年度の事業計画

2010/06/21

Manabu Higashida

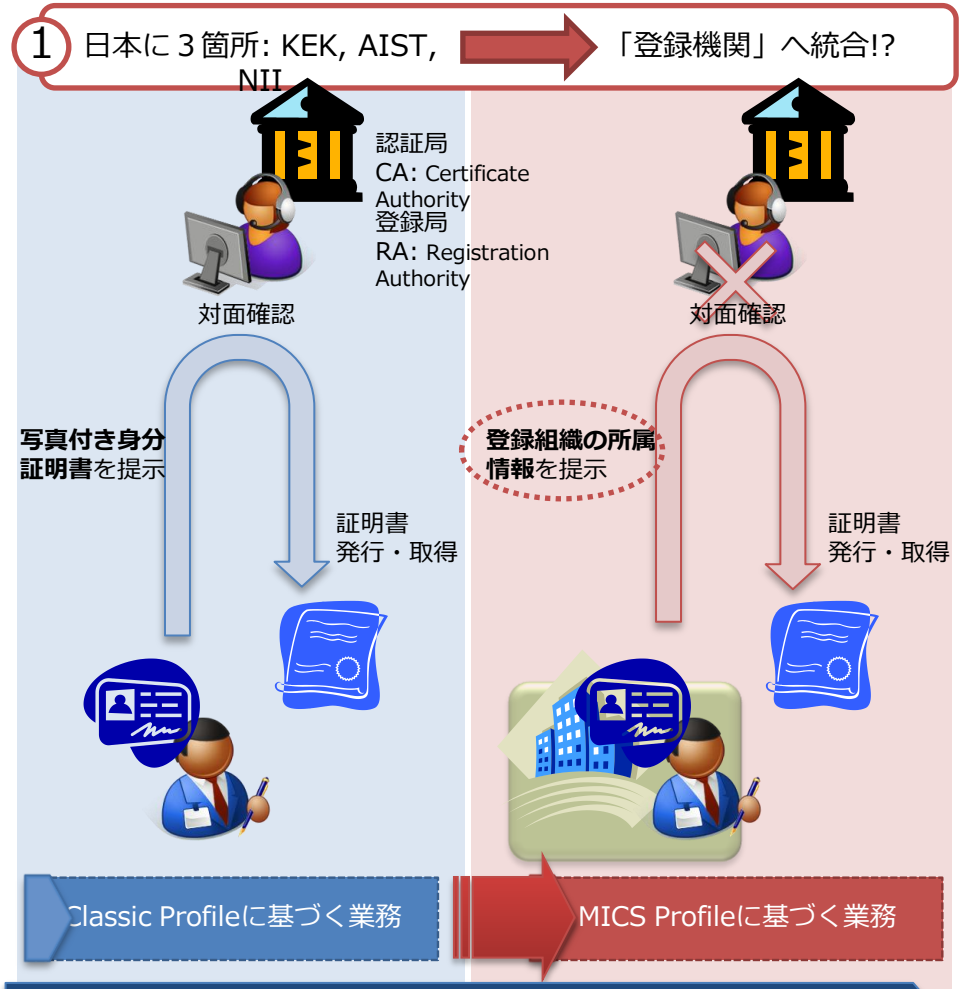
manabu@cmc.osaka-u.ac.jp

大阪大学サイバーメディアセンター

平成21年度のCSI委託事業の実施報告

1) MICSプロファイルに対応したグリッド認証局運用規定の策定

- MICSプロファイルに基づく認証局運用規程を策定すると同時に、各情報基盤センターの全国共同利用登録窓口に要求される登録局としての業務規程を策定した



MICS: Member Integrated Credential Service

平成21年度のCSI委託事業の実施報告

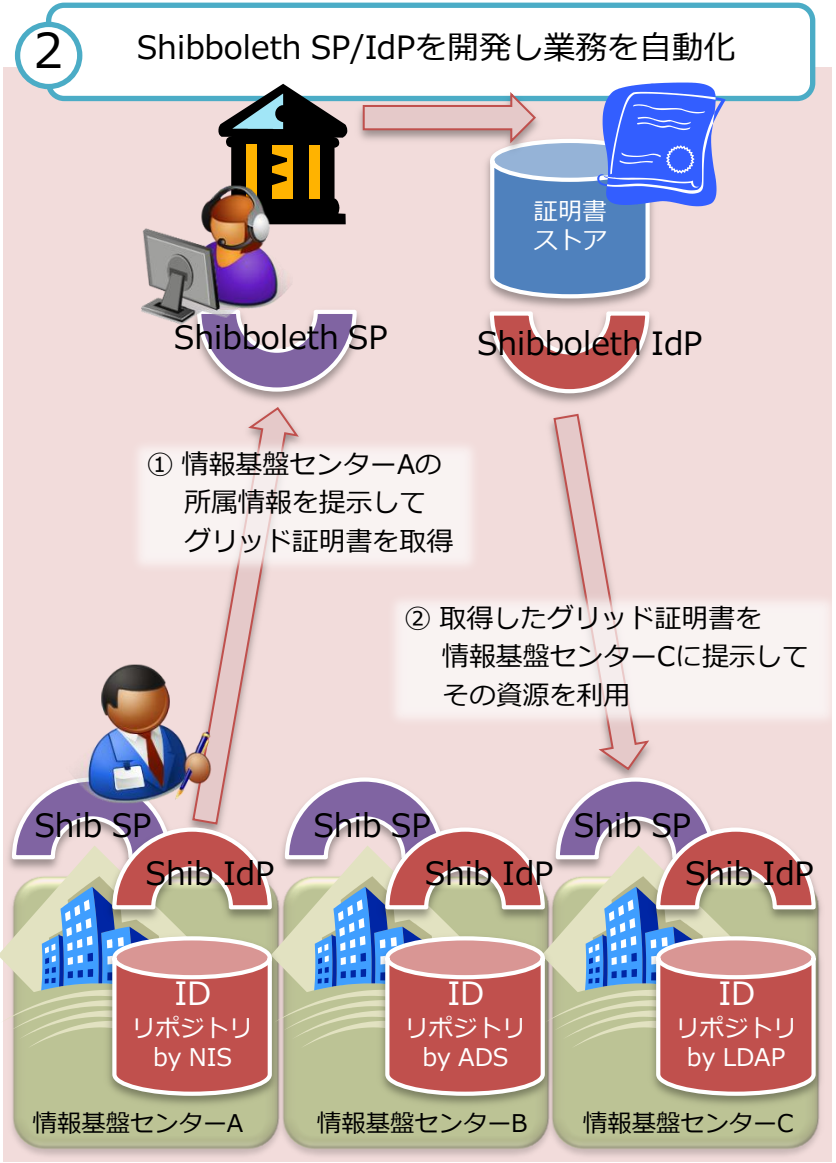
2) ShibbolethによるNAREGIミドルウェアのSingle Sign-On対応

- NAREGIミドルウェアにU-PKIの成果を取り入れ、Shibbolethによる初期認証とSSOに対応するようNAREGI Webポータルおよび関連するライブラリなどを拡張した
  - NAREGI Webポータルや登録局のShibboleth SP化を行った

3) 阪大CMCグリッド認証局のMICS/Shibboleth対応

- 払い出した証明書と対応する属性情報を関係する情報基盤センターに通知し、各情報基盤センターのローカルアカウントとの名寄せが可能な業務フローの検討と雛形となるシステムを試作する
  - 情報基盤センター業務フローの設計と業務システム試作を行った
  - 情報基盤センター連携を想定し、UMSおよびVOMSの登録情報を共有する機能を追加した

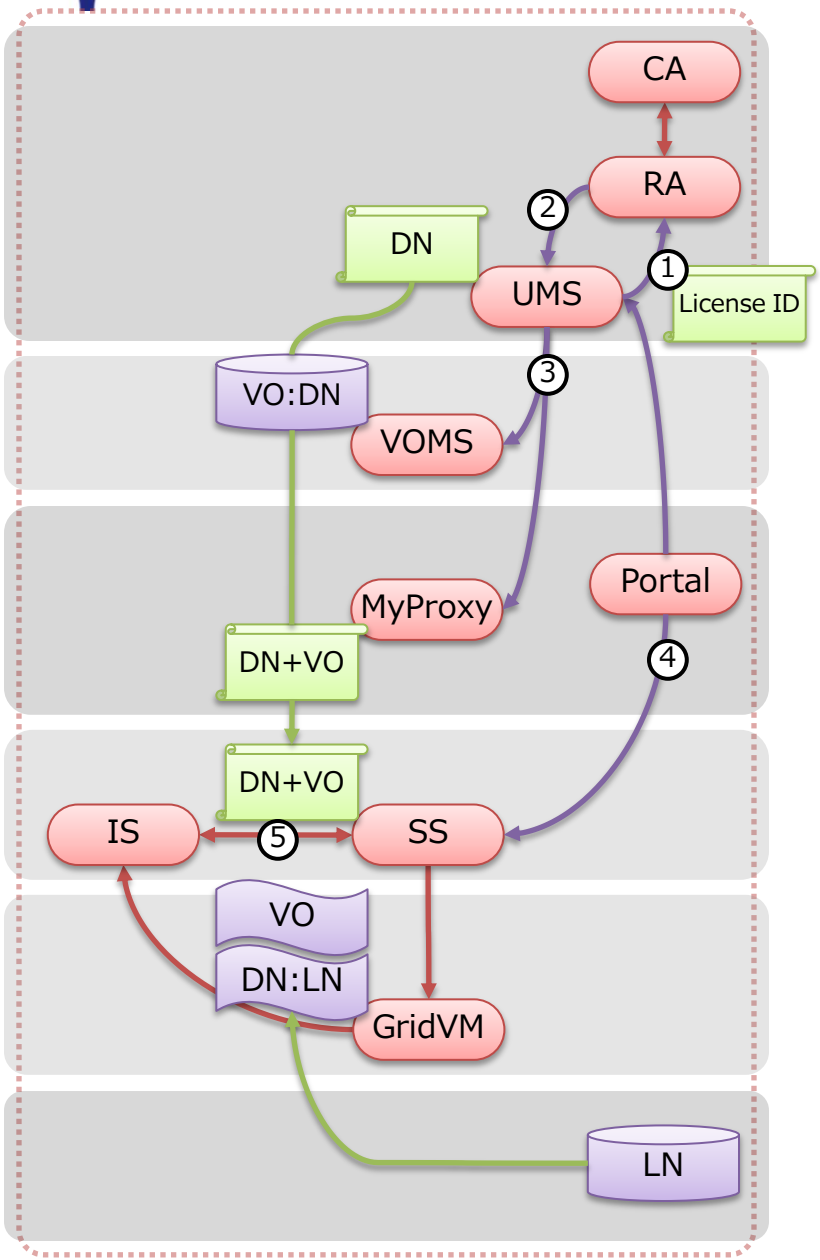
SP: Service Provider
IdP: Identity Provider



NAREGI初期認証のShibbolethによるフェデレーション

- 課題: UMSの初期認証のID管理業務が認証局へ集中
  - e.g. GPID (Grid Pack ID) の登録業務をNII GOCが負担
- 目標: Shibbolethで連携したポータル間でのシングルサインオンを実現
  - 効果: 各情報基盤センターが発行した共同利用IDで連携するUMSにシングルサインオン可能
  - 付帯効果: MICSプロファイルで業務運用されるグリッド認証局 (に付随するShibboleth SP) と連携し、証明書発行業務の完全なオンライン化

Non-Shibbolized NAREGI



① 別途、ソーシャルフローを介してLicense IDを入手しておく

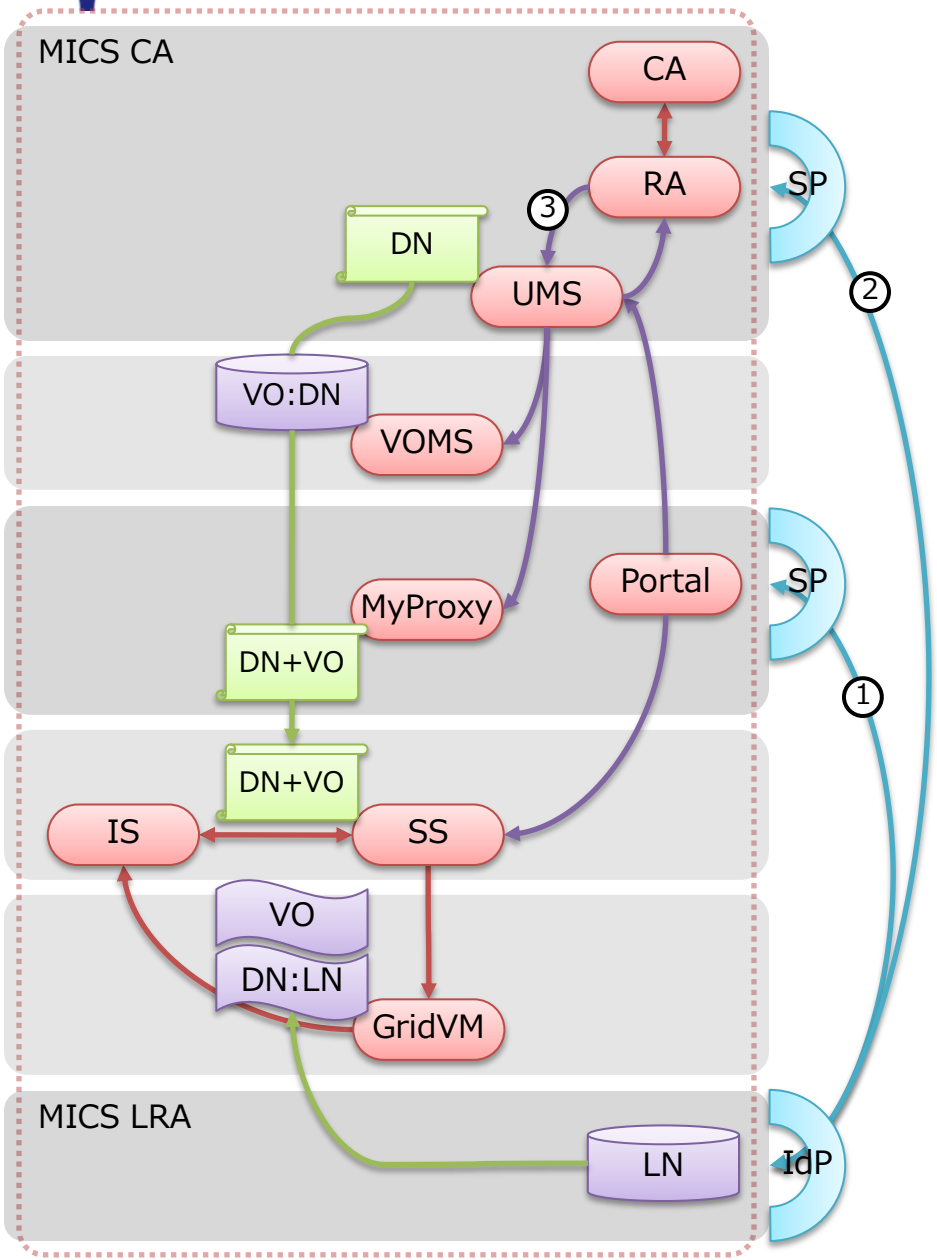
② License IDを入力しUMSへグリッド・ユーザ証明書を払い出す
- ユーザ証明書は、このとき入力するパスフレーズによって暗号化される

③ UMSにて`voms-myproxy-init`コマンドを実行し、プロキシ証明書を払い出す
- ユーザ証明書を復号化するためのパスフレーズを入力する
- プロキシ証明書を別のパスフレーズによって暗号化する

④ プロキシ証明書を委譲するために、パスフレーズを入力する

⑤ プロキシ証明書に記載されたVOとDNにマッチするGridVMへのジョブ投入が可能となる

Shibbolized NAREGI

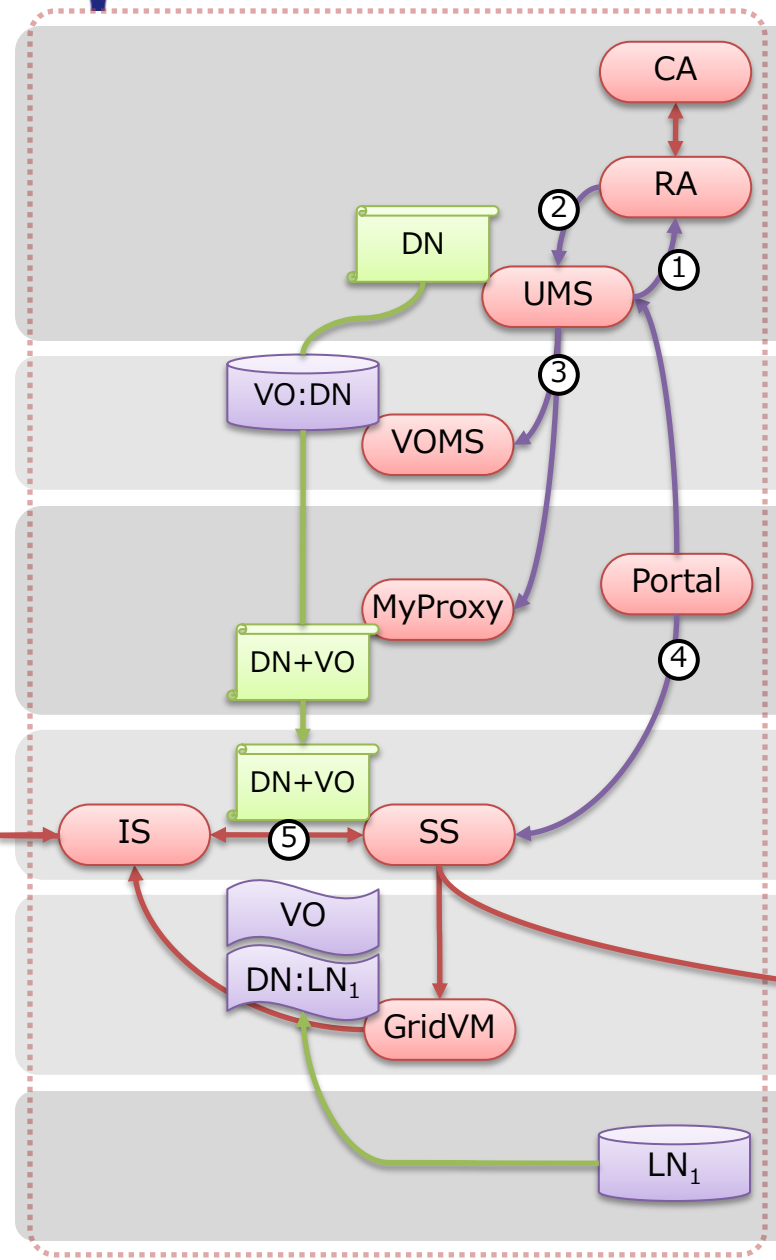


① ShibbolethフェデレーションされたIDによってポータルへログインする
- IDはMICSプロファイルに基づくLRA業務規定に従って発行されているものとする
- 規定に従うIDか否かはSAML (Security Assertion Markup Language) 属性情報によって伝達する

② Shibboleth SSOによって認証されたRAにてグリッド・ユーザ証明書を発行する

③ MICSプロファイルで業務運用することによって、License IDの受け渡しに際するソーシャルフローを介することなくユーザ証明書の発行が可能になる

グリッド配備・運用TF Phase-1の構成



大統一VO管理

- NII GOCが管理するNAREGI管理ノード群 (VOMSを含む) による一元管理
- 単一VO (`csi-grid-cc`) への資源提供

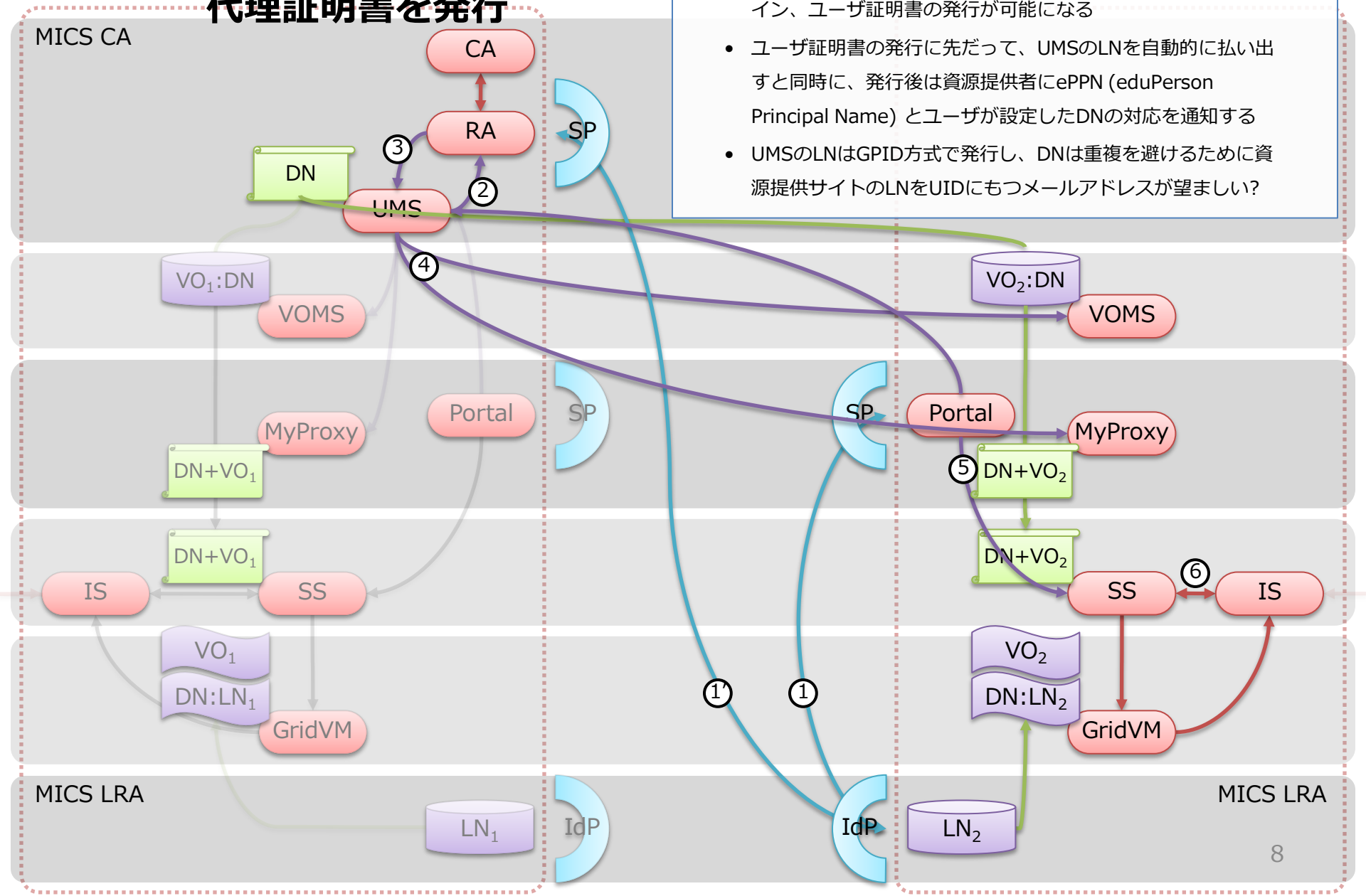
GPIDからLNへの名寄せ

- NII GOCが発行するGPID (Grid Pack ID) を取得し、NII GOCが管理するNAREGIポータルへログイン
- ユーザ証明書の発行に際して、NII GOCから資源提供者へGPID:DNを通知する (SVNリポジトリを介して)
- 資源提供者が管理するGPID:LN表と名寄せを行って`grid-mapfile` (DN:LN表) を作成

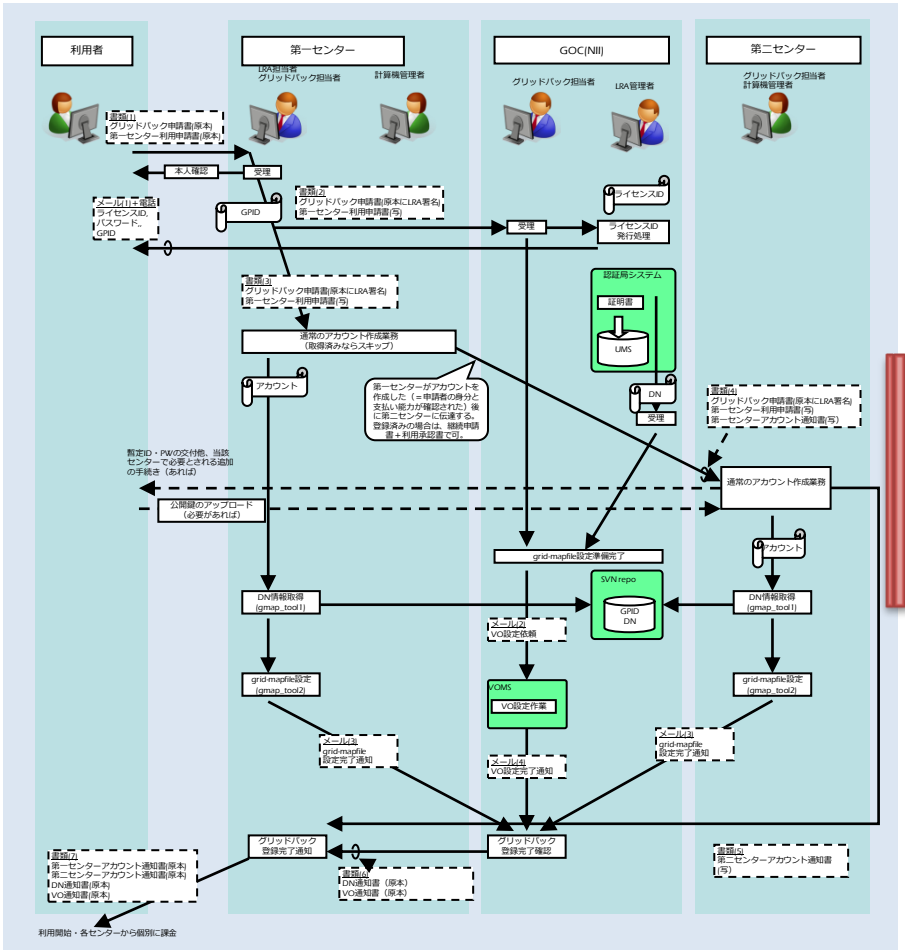
Shibboleth連携した証明書ストアから代理証明書を発行

GPID発行業務が不要に!

- 資源提供者が管理するIDによって、連携したポータルへのログイン、ユーザ証明書の発行が可能になる
- ユーザ証明書の発行に先だって、UMSのLNを自動的に払い出すと同時に、発行後は資源提供者にePPN (eduPerson Principal Name) とユーザが設定したDNの対応を通知する
- UMSのLNはGPID方式で発行し、DNは重複を避けるために資源提供サイトのLNをUIDにもつメールアドレスが望ましい?

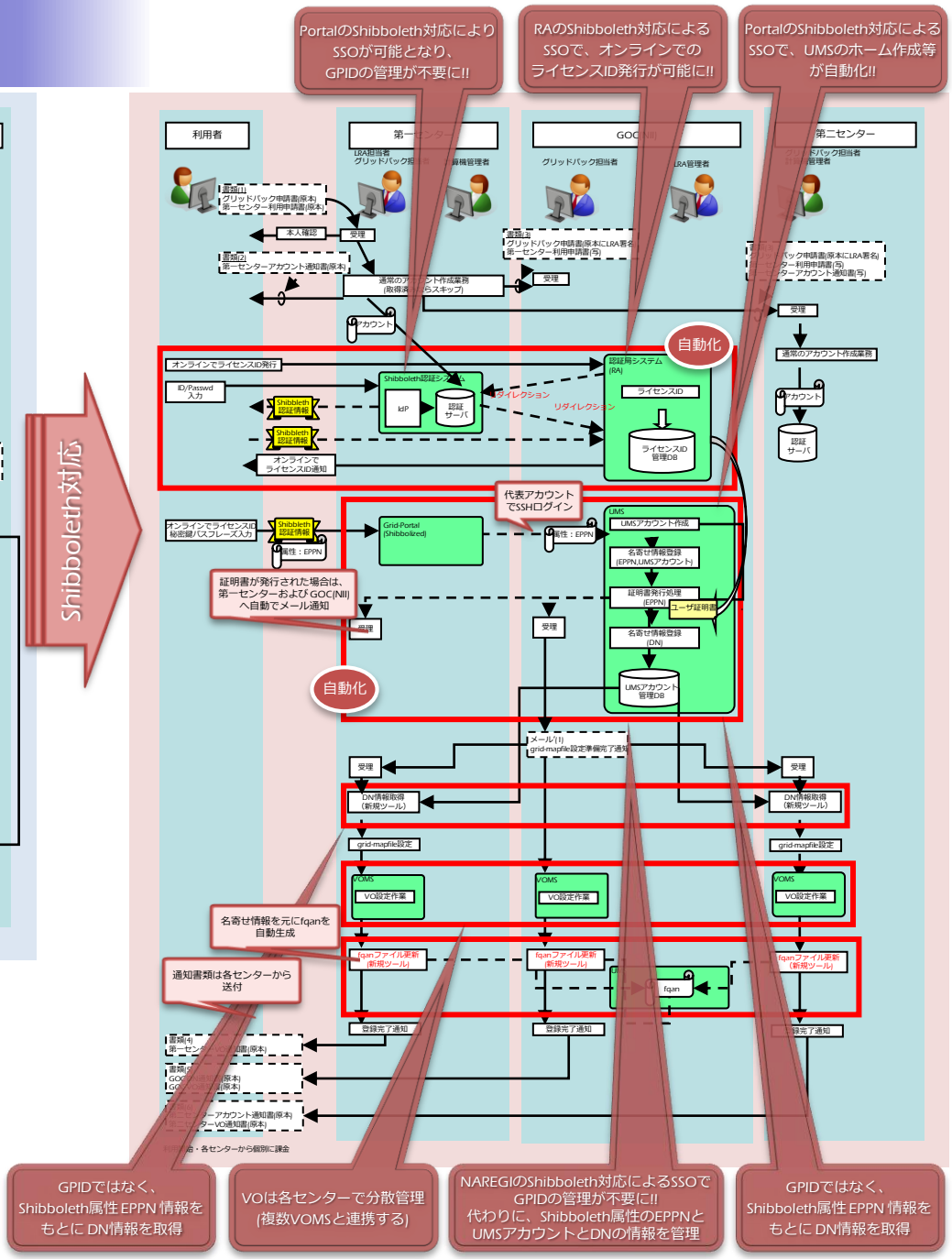


複数センターが連携する利用登録業務の Shibbolethによる自動化



平成21年度グリッド・パック業務フロー (Shibboleth未対応)

Shibboleth対応



情報基盤センターの業務システムにShibbolethによるID連携を組み込むことによって、各々の情報基盤センターがこれまで管理・維持してきた全国共同利用IDを基にグリッド証明書を発行し、シングルサインオンでグリッド・サービスの利用が可能となる。さらに、グリッド利用IDと全国共同利用IDを名寄せするグリッドマップファイルの自動生成や、VO所属情報の分散管理など認可サービスとの連携を検討している。

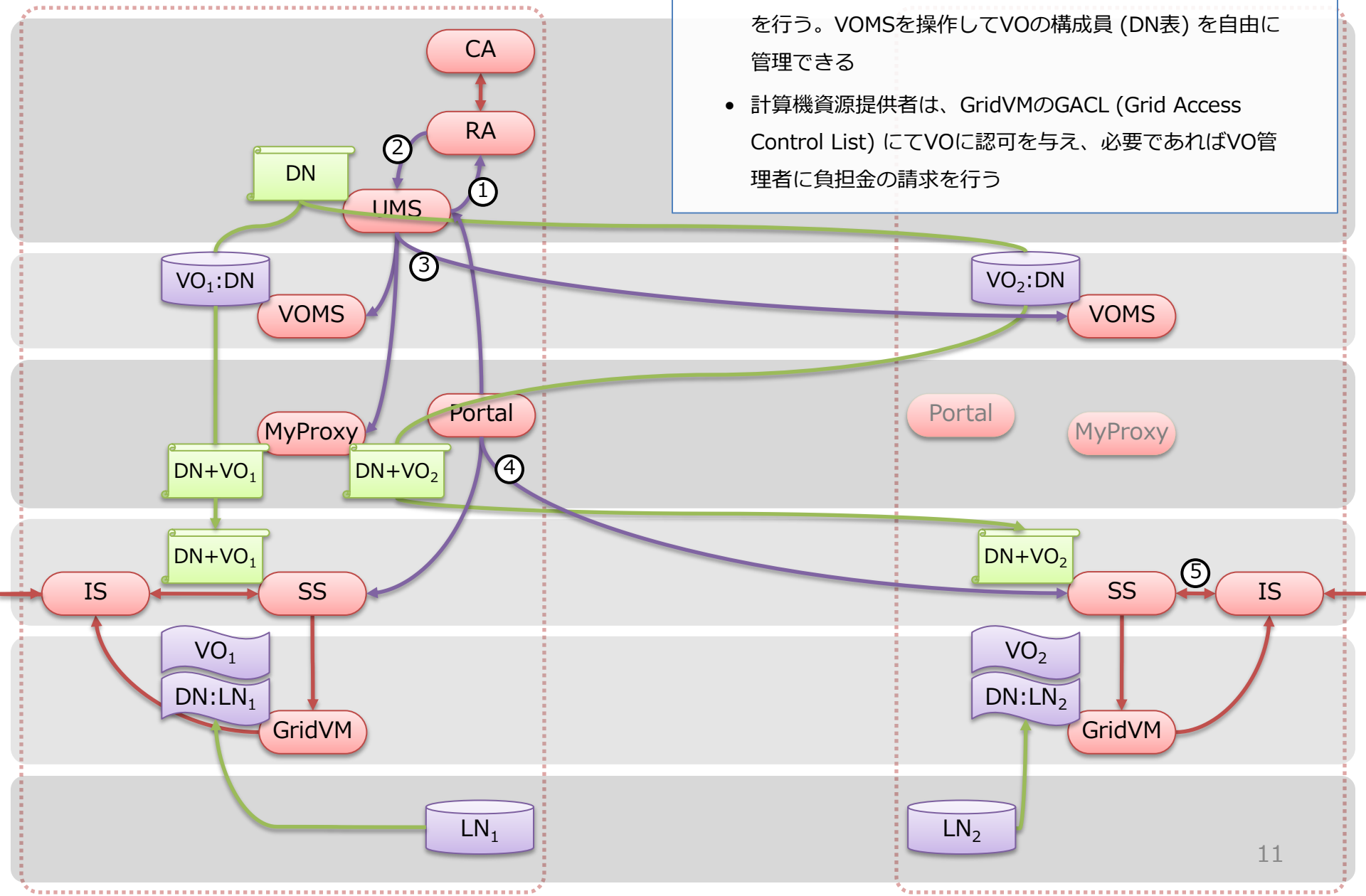
Shibbolethによる複数VO連携

- 課題: VO管理がどんぶり
  - VOMS (Virtual Organization Management Server by gLite)
    - DNがどのVOに所属しているかを管理しているが、これまで積極的に活用されていない･･･
  - `voms-myproxy-init` at UMS (User Management Server)
    - VO名を拡張領域に格納した代理証明書を発行
  - 計算機資源 (GridVM)
    - 認可はVO単位で行われている
      - GACL: Grid Access Control Listでの認可をLRPS-ISを介してSSへ通知
    - DNとLNの対応は`/etc/grid-securityt/grid-mapfile`で管理されている
      - DNがどのVOに所属しているかは関知していない
- 目標: 資源提供に際する認可 (課金) をVO単位で行い、VOの構成メンバー管理をVO管理者に委譲する
  - UMSにおけるVOMS構成情報: `/opt/glite/etc/vomses`, `${HOME}/.glite/vomses`を分散管理する手法を提案する

複数のVOの資源を連携して使う

VOの管理権限をVO管理者へ委譲

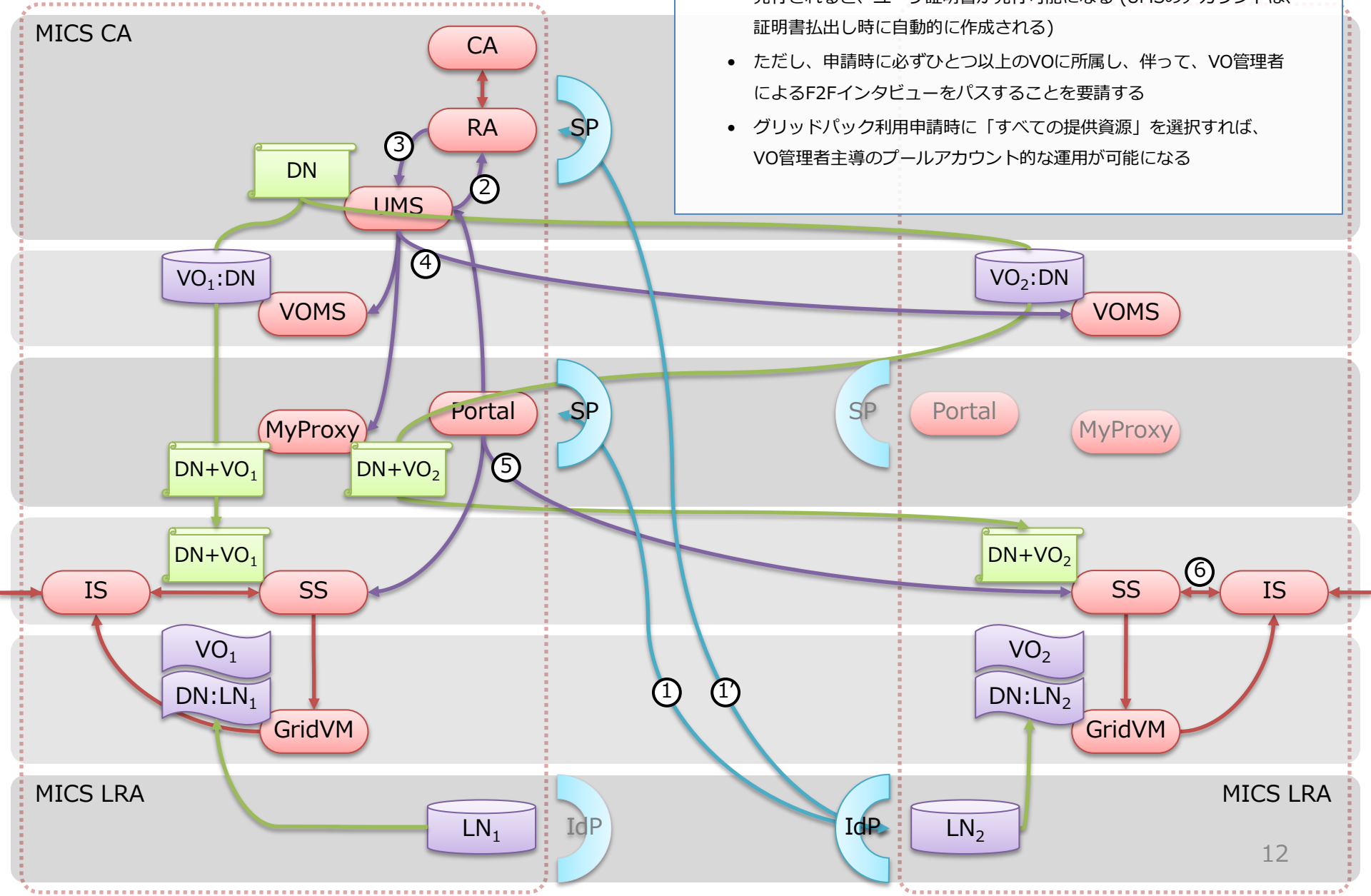
- VO管理者は、支払い責任者として計算機資源の利用申請を行う。VOMSを操作してVOの構成員 (DN表) を自由に管理できる
- 計算機資源提供者は、GridVMのGACL (Grid Access Control List) にてVOに認可を与え、必要であればVO管理者に負担金の請求を行う



Shibbolized NAREGIによる複数VO連携

グリッドパック利用者をプールアカウントへ

- グリッドパック利用申請によって各情報基盤センターのアカウントが発行されると、ユーザ証明書が発行可能になる (UMSのアカウントは、証明書払出し時に自動的に作成される)
- ただし、申請時に必ずひとつ以上のVOに所属し、伴って、VO管理者によるF2Fインタビューをパスすることを要請する
- グリッドパック利用申請時に「すべての提供資源」を選択すれば、VO管理者主導のプールアカウント的な運用が可能になる



平成22年度の事業計画

- IDフェデレーションによるグリッド認証基盤の普及

Phase-1: MICSプロファイル対応の阪大グリッド認証局 (Semi-Production Level) による試験的な配備・運用によるフィージビリ・ティスタディ
(6月～7月)

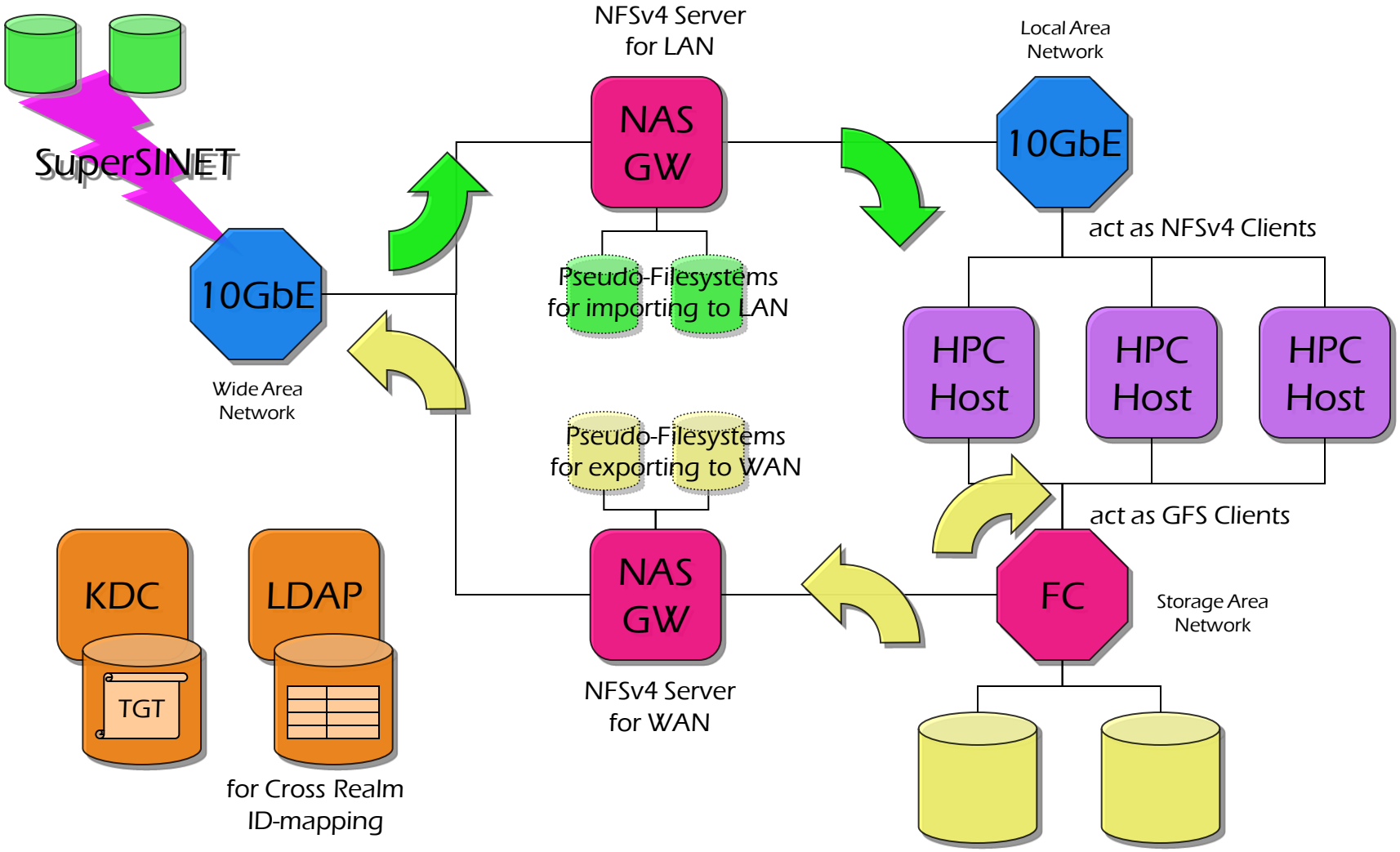
- 連携予定機関: 九大、東工大、東北大、京大
- サービス展開: GSI (Globus Security Infrastructure) 認証による GSI-SSH (対話型処理), Gfarm (ストレージ共有)、GRAM (ジョブ実行)

Phase-2: NIIグリッド認証局 (Production Level) と学術認証フェデレーション “GakuNin” と連携した本格的な配備・運用

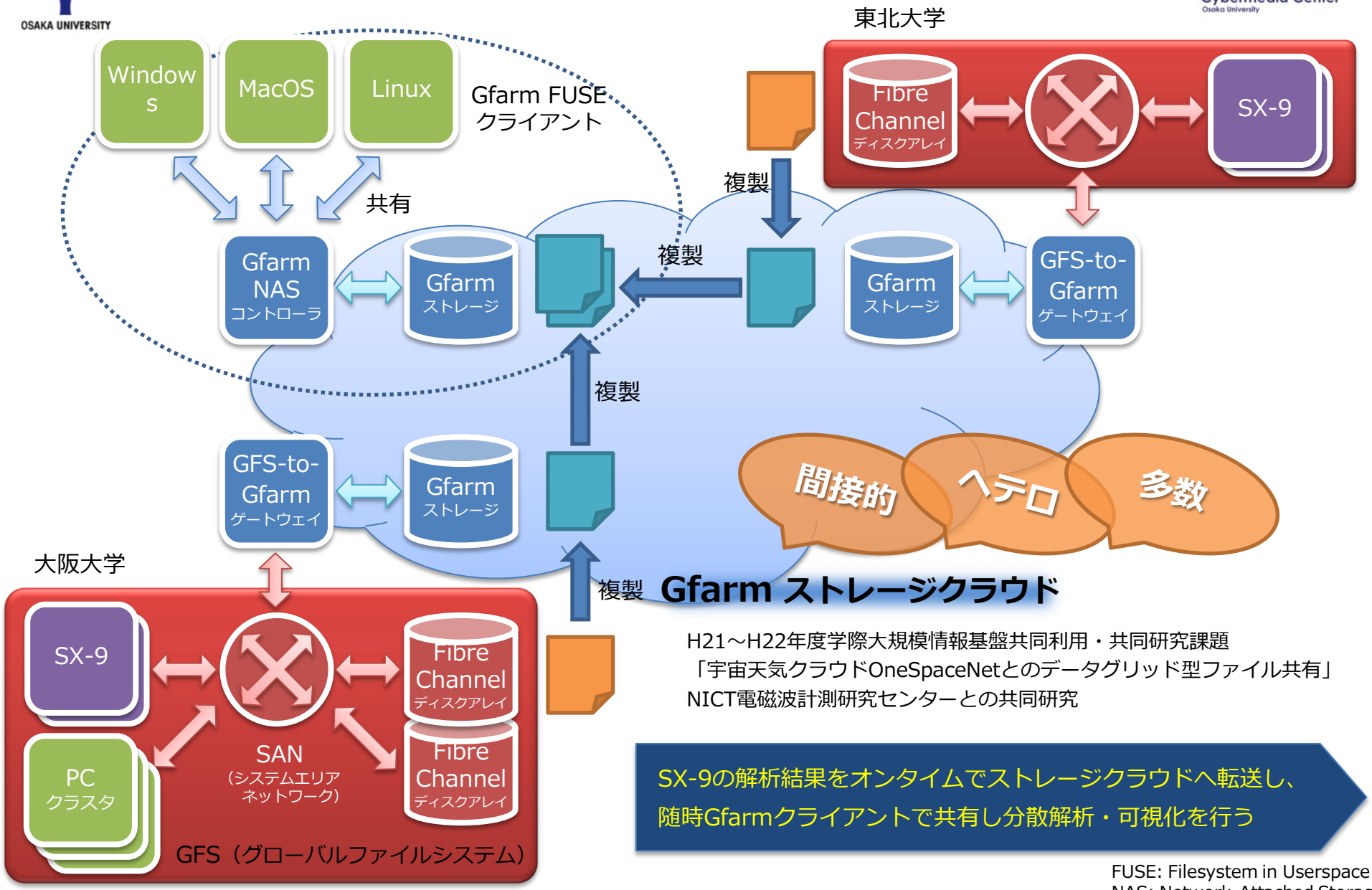
➠グリッドIDフェデレーションの業務化を視野に!!

Global Storage Sharing with NFSv4

2005年の試案



データグリッド型ストレージ共有



H21～H22年度学際大規模情報基盤共同利用・共同研究課題
「宇宙天気クラウドOneSpaceNetとのデータグリッド型ファイル共有」
NICT電磁波計測研究センターとの共同研究

SX-9の解析結果をオンタイムでストレージクラウドへ転送し、
随時Gfarmクライアントで共有し分散解析・可視化を行う

FUSE: Filesystem in Userspace
NAS: Network-Attached Storag


acer
soc-cfarm-n31
soc-cfarm-n30
APC
Smart-UPS
1500
DELL
PowerConnect
6224
NEC
Express5800/120Lj

ディペンダブルな広域SAN共有

ベクトルコンピューティングクラウド

東北大学

Fibre Channel ディスクアレイ

SX-9

ToE NIC

SINET3

800km往復による
20ms以上の遅延
と揺らぎ、欠落など

JGN2+

OpenFlow Switch

GFS-to-iSCSI ゲートウェイ

OpenFlow Switch

大阪大学

SX-9

PC クラスタ

SAN (システムエリアネットワーク)

Fibre Channel ディスクアレイ

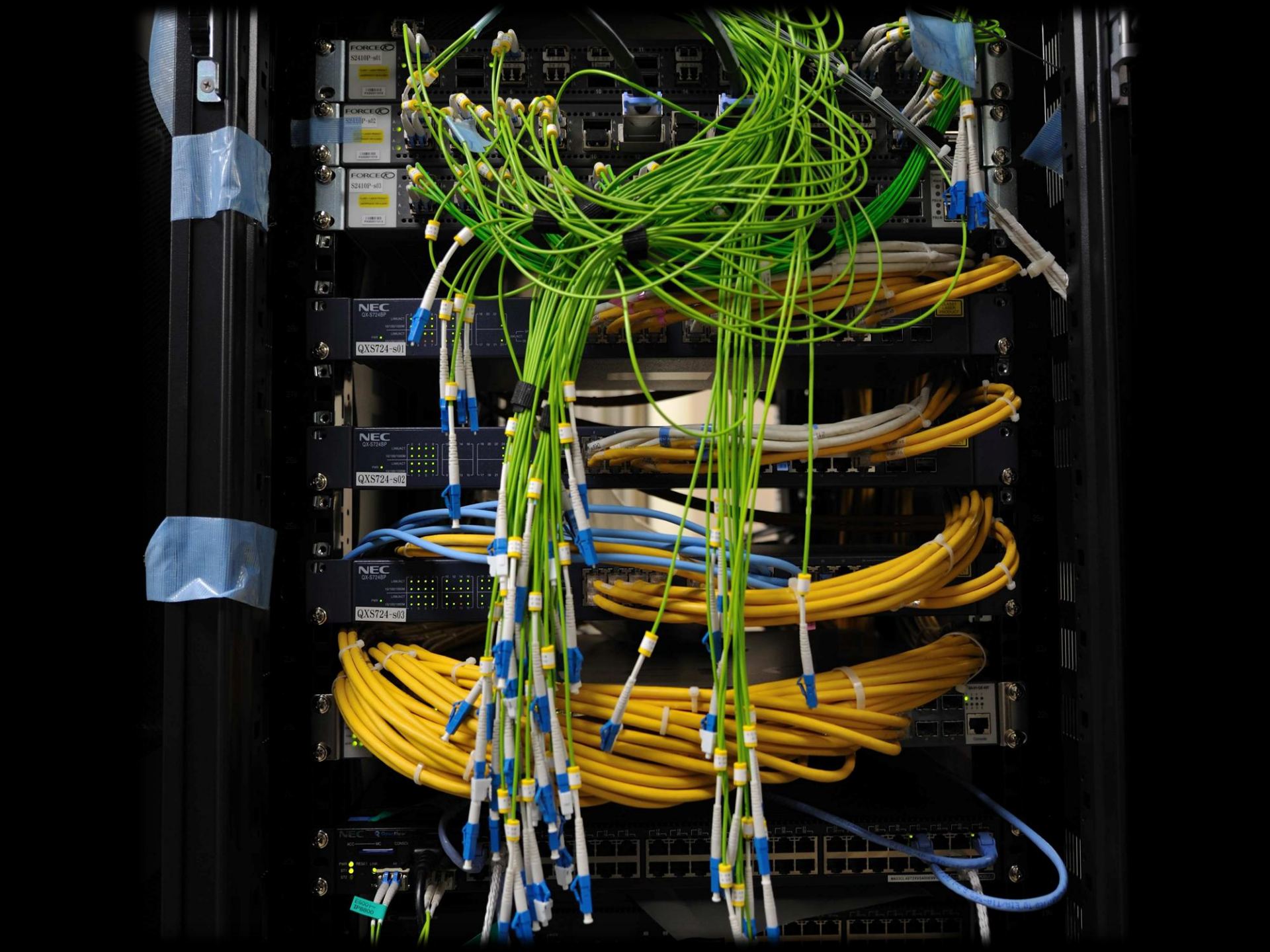
Fibre Channel ディスクアレイ

GFS（グローバルファイルシステム）

大阪-仙台間での20ミリ秒を越える往復遅延を有する
LFN (Long Fat Network) を介しても
1Gbps (100MB/s) を越える転送性能の実現を目指すとともに、
OpenFlow技術を導入することにより
SINET3とJGN2+を動的に使い分け
よりディペンダブルな広域ストレージ共有を実現する

SX-9にToE NICを増設し、FibreChannel SANをEthernetに延長する
ゲートウェイ装置を介して、遠隔地のストレージを直接参照する

ToE: TCP Offload Engine
NIC: Network Interface Card


FORCE10
S2410P-s01
FORCE10
S2410P-s02
FORCE10
S2410P-s03
NEC
QX-S724BP
QXS724-s01
NEC
QX-S724BP
QXS724-s02
NEC
QX-S724BP
QXS724-s03


SA-01-GE-48T
Console
PWR
RESET
ST1
WA03CL48T2XVS400E991003
CLASS1 LASER PROD