

Empowered by Innovation **NEC**

GridにおけるIDマネージメントの現状と動向

2006/06/22

日本電気株式会社
森 拓也

U can change.

Empowered by Innovation **NEC**

グリッドにおけるIDマネージメント 仮想組織

U can change.

GridにおけるIDマネジメントとは

- 仮想組織 (VO)
 - 「複数の組織にまたがった協調的な資源共有や問題解決を実現するためのルールによって定義される個人あるいは組織の集合」 - Ian Foster et al. 「The Anatomy of the Grid」 -
 - 共有のルール?
 - グリッドでの資源共有を厳密に制御
 - 誰が、何を、どのような条件で使える?
 - ルールは動的に変化するかも
 - 資源を使える人や組織の集合も動的に変わる
 - 共有の範囲が現実組織の壁を越える ← 重要!!
- どう実現?

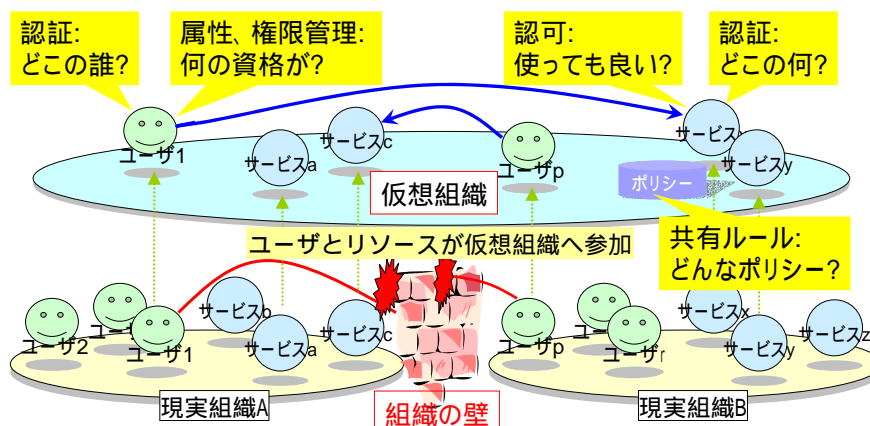
U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

3

仮想組織の実現

- 簡単に言えば、組織を跨ったリソース利用に関する認証と認可の問題...
- だけど、簡単ではない...



U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

4

認証

- ユーザやリソースが「どこ」の「誰」or「何」なのかを検証すること
 - ID&パスワード、Kerberos、PKI(公開鍵暗号基盤)、etc...
 - 何らかの秘密情報を用いることが多い
- Trusted Third Party (TTP: 信頼すべき第三者機関)を前提とするものが多い(Kerberos、PKIなど)
 - TTPが「誰」or「何」なのかを保証
 - PKIの場合は認証局(CA)がTTP
 - TTPが管理する範囲が「どこ」に相当
 - PKIの場合は認証局(CA)の認証ドメイン
- 組織が異なれば、TTPも異なる
 - 自組織が使っていないTTPは信頼に足るのか?

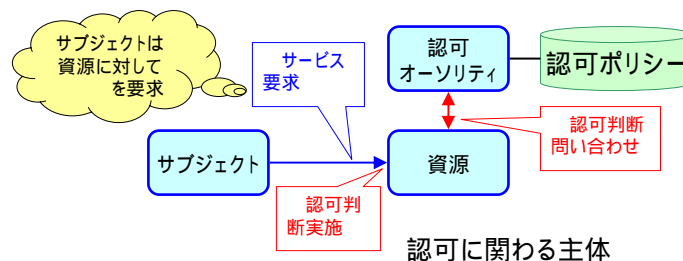
U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

5

認可(アクセス制御)

- ユーザ(サブジェクト)によるリソースに対するサービス(特定の操作)の要求を許可・拒絶するかの判断とその実施
- グリッドでの認可モデルでは、認可に関わる主体として、サブジェクトとリソースと認可オーソリティを規定
- オーソリティは認可ポリシーを元に認可判断を行い、リソース側でその認可判断を実施する
- ポリシーは、{サブジェクトの情報、リソースの情報、リソースに対する操作(action)}の組み合わせに対するOK・NGの形で記述



U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

6

ポリシー、認可属性の管理

- ポリシー記述の種類
 - IDベース:
サブジェクトのID(識別子)を用いて記述
 - 属性ベース:
サブジェクトの属性(認可属性)を用いて記述
 - 役割ベース:
サブジェクトの役割を用いて記述
 - 権限ベース:
サブジェクトが持つ権限を用いて記述
役割、権限ベースのポリシーは認可属性ベースのポリシーの一種とみなすこともできる
- ポリシーやサブジェクトに付与する認可属性の管理も組織ごとに行われる
ポリシーや認可属性に使われる語彙が組織によりまちまち

U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

7

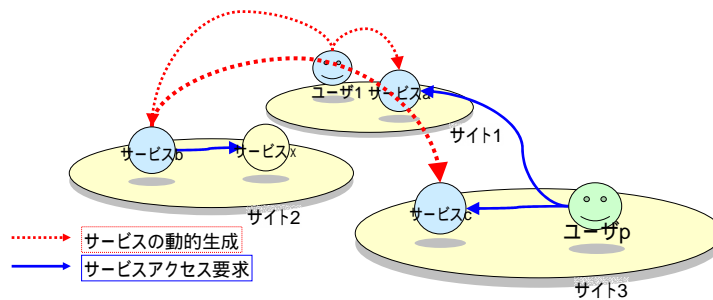
Empowered by Innovation

NEC

グリッドにおけるIDマネージメント 現状

U can change.

Gridのシナリオ



- ユーザはサイトをまたがり動的にサービスを生成
- ユーザが生成したサービスは他のサービスをアクセス
- ユーザが生成したサービスは後にさらに別のサービスを生成
- ユーザが生成したサービスは他のサービスからのアクセスを適切に制御

U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

9

Grid特有の要求

- サイトをまたがる認証と認可の実現
 - ユーザがサイトをまたがりサービスを生成
 - ユーザがサイトをまたがりサービスをアクセス
- シングルサインオンの実現
 - ユーザが複数のサービスをほぼ同時に生成
 - ユーザが生成したサービスがさらに別のサービスを生成
 - ユーザが生成したサービスが別のサービスをアクセス
- 権限委譲(デレゲーション)
 - サービスはユーザに成り代わって動作
 - ユーザが生成したサービスがさらに別のサービスを生成
 - サービスにユーザの権限を委譲することが必要

U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

10

Gridの現状 認証

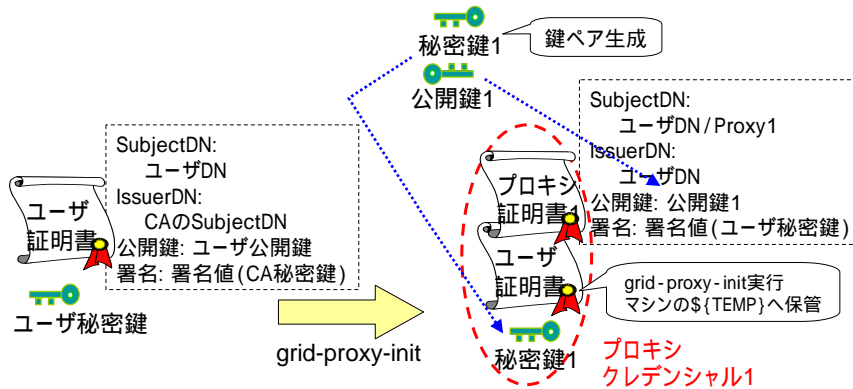
- GSI(Grid Security Infrastructure)
 - PKI、X.509証明書ベースの認証方式
 - プロキシ証明書(IETF RFC 3820)を用いてサブジェクトを認証
 - 認証が必要なリソース利用時に事前にローカルでプロキシ証明書を生成(grid-proxy-initコマンドを実行)
 - サブジェクトのIDはプロキシ証明書を署名しているエンド・エンティティ証明書のサブジェクト名から取得
- Transport Layer Security (TLS)
 - TLS/SSLの相互認証でプロキシ証明書を認証に利用
 - GSI-Transportと呼ばれる
- Message Level Security (MLS)
 - WS-Security + XML署名でメッセージ認証
 - GSI Secure Conversation: SOAPレベルでのセッション鍵交換のハンドシェイク時に双方向で発信者認証
 - GSI Secure Message: サービスへのアクセスの際の要求と応答の往復メッセージで双方向で発信者認証

Gridの現状 権限委譲

- GSI(Grid Security Infrastructure)
 - プロキシクレデンシャル(プロキシの秘密鍵+プロキシ証明書(RFC 3820)を利用)
 - 認証時のハンドシェイク中にリモート側で鍵ペアとプロキシ証明書発行要求(プロキシCSR)を生成
 - 認証時のハンドシェイク中にローカル側でCSRに署名しプロキシ証明書を発行
 - 以上によりリモート側のプロセスへプロキシクレデンシャル発行
- TLS – GSI-Transportでサポート
- MLS – GSI-SecureConversationでサポート

GSI - プロキシ証明書の生成

- grid-proxy-initコマンドで作成
 - 新たに鍵ペアを生成
 - ユーザの秘密鍵でプロキシ証明書へ署名
 - プロキシ証明書の有効期限は12時間(デフォルト値)
- プロキシ証明書はシングルサインオン + delegationに利用
 - 認証はプロキシクレデンシャル、識別はユーザ証明書を利用

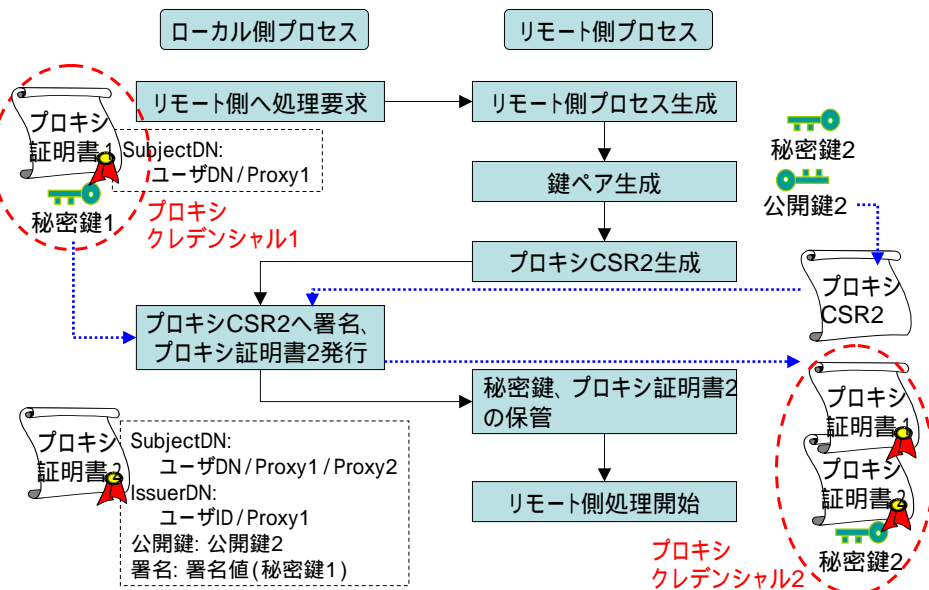


U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

13

GSI - デレゲーションの流れ



U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

14

Gridの現状 認可、認可属性管理

- grid-mapfile
 - ユーザのSubjectDNからリソース(UNIX)のローカルアカウントへのマッピング
 - grid-mapfileのエントリがあることによりリソース利用を許可
- CAS: Community Authorization Service
 - Globus Allianceが配布
 - VOのユーザとリソースを管理(グループで管理)
 - ユーザグループに対してリソースへのアクセス権限を付与
 - リソースアクセスに対する認可判断
 - CASプロキシ証明書の拡張領域にSAMLの AuthorizationDecisionStatement を埋め込む

http://www.globus.org/grid_software/security/
http://www.globus.org/grid_software/security/cas.php

U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

15

Gridの現状 認可、認可属性管理

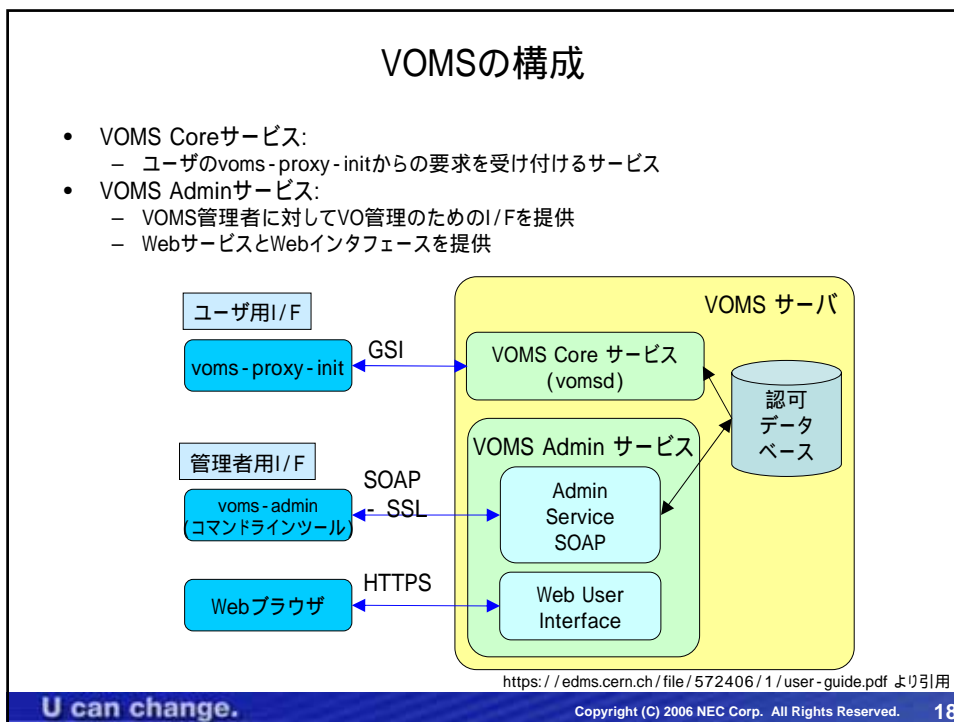
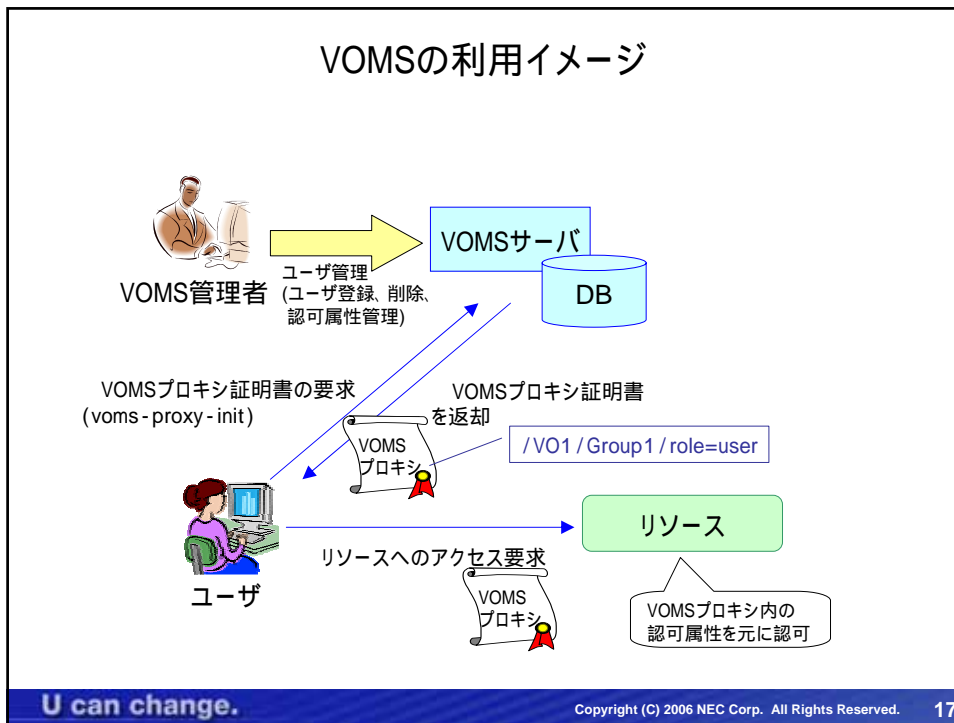
- VOMS: Virtual Organization Membership Service
 - EDG (Europe Data Grid) プロジェクトで開発、EGEE (Enabling Grid for E-Science in Europe) へ引継ぎ
 - VOのユーザとユーザの認可属性(グループ、役割、Capability)を管理
 - VOのユーザの認可属性を含むVOMSプロキシ証明書を発行
 - プロキシ証明書の拡張領域に認可属性を格納
 - 認可属性はFully Qualified Attribute Name (FQAN) という書式で記述
 - /VO名/グループ名/role="役割名"
 - /VO名/グループ名/capability="Capability名"
 - リソースはVOMSプロキシ証明書の認可属性を元に認可
 - GT2ベースの認可ミドルウェアとしてLCAS、LCMAPSが利用可能

詳細は <http://edg-wp2.web.cern.ch/edg-wp2/security/voms/> などを参照

U can change.

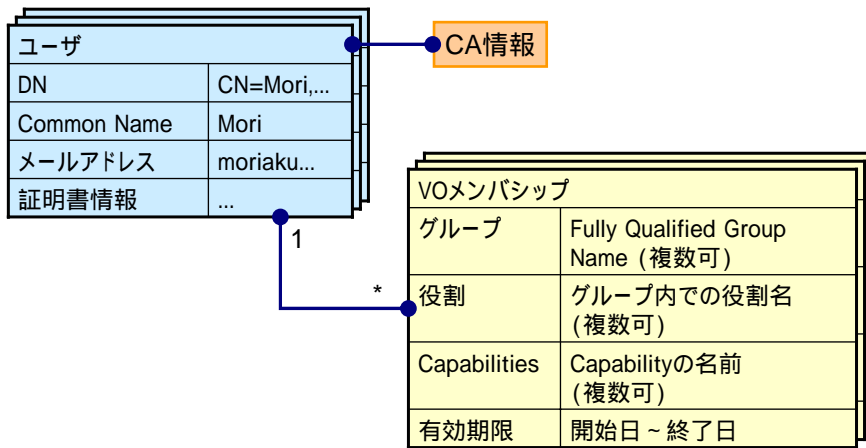
Copyright (C) 2006 NEC Corp. All Rights Reserved.

16



VOMSによるユーザの管理

- ユーザは複数のVOのメンバシップを保持可能
- 証明書のDN名を用いてユーザを識別し、VOメンバシップを確認



U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

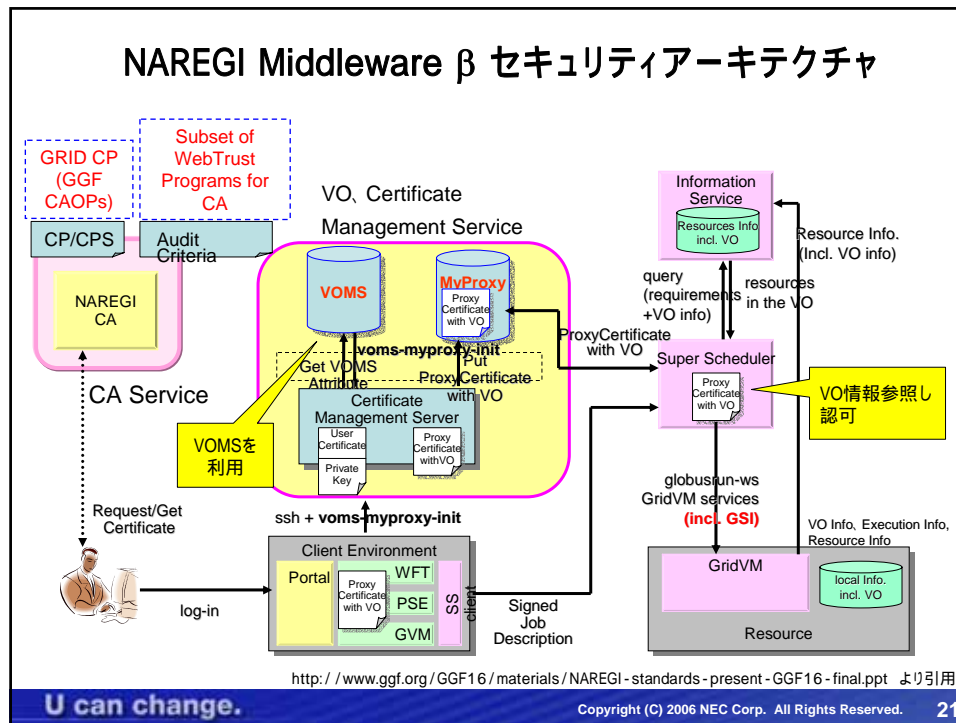
19

Empowered by Innovation

NEC

グリッドにおけるIDマネージメント 動向

U can change.



GridShibプロジェクト

- Shibboleth:
 - 米国Internet2による大学間認証連携の基盤
 - SAML1.1ベースの認証連携と属性交換機能を提供
 - 現在はSAML2.0ベースのShibboleth2の開発を目指す
- GridShib:
 - NSF(全米科学財団)が出資し、NCSA、シカゴ大、アルゴンヌ国立研究所が主導するプロジェクト
 - Shibbolethが発行する属性をGlobus Toolkitでの認可に利用することが狙い
 - 認証は従来どおりGSIを用いた認証を踏襲
 - 詳細は <http://gridshib.globus.org/> を参照

GIN: Grid Interoperation Now

- 現在運用されているGridを相互接続しようとする試み
 - EGEE、TeraGrid、など
- VO管理はVOMSを利用する方針
 - VOの名前空間管理、属性名の相互運用性などが議論
 - EGEE内にGIN VOMSサーバを整備
- IGTF (International Grid Trust Federation) により認証されたCAを利用する方針
- 今後GINの場での相互接続性の検証が加速していくことが予想

まとめ

- グリッドにおけるIDマネージメントを仮想組織(VO)での認証、認可の管理という観点で紹介した
 - 認証(SSO)、権限委譲はGSIが広く使われている
 - 認可(権限管理)に関してはVOMSが広く使われている
 - 学術系グリッドではGSI + VOMSという組み合わせで相互運用を図るという流れが強まっている
 - 基本的にサイト間である程度の信頼を前提としてシステムが成り立っている
 - リモートサイトに置かれるプロキシクレデンシャルは安全
 - サイトの管理者は信頼する
 - 上記の前提が成り立つ範囲で、GSI+VOMSの仕組みはかなりうまく機能しており、今後より広く利用されるようになると思われる

Empowered by Innovation

NEC

U can change.

Copyright (C) 2006 NEC Corp. All Rights Reserved.

25