グリッドにおけるセキュリティの現状と動向

産業技術総合研究所　グリッド研究センター
田中　良夫

話の内容

- グリッドにおけるセキュリティの肝
  - グリッド特有の要求事項
- 現状と動向
  - 既存研究の成果
  - 現状および動向
- 全世界的な信頼関係の構築に向けて
  - International Grid Trust Federationの紹介

グリッドにおけるセキュリティの肝

グリッド特有の要求事項

Three key functions in a Grid security model ※

- **Multiple security mechanisms**
  - VOに参加する各組織の（複数の）セキュリティ機構を利用
- **Dynamic creation of services**
  - 管理者の干渉なしに、ユーザが新しいサービスを動的に生成できる
- **Dynamic establishment of trust domains**
  - ユーザとリソースの間だけではなく、VOにおけるリソース間の信頼(trust domain)も確立する
  - それらのtrust domainは複数の組織にまたがり、動的に適応する

※ Von Welch, et.al., Security for Grid Services, HPDC-12, 2003

Security Challenges in a Grid Environment ※

- **The Integration Challenge**
  - **既存のセキュリティ技術を（相互）利用、統合**
- **The Interoperability Challenge**
  - **複数のドメイン、Hosting Environment同士が協調するために、複数のレベルでのinteroperatilityが必要**
    - Protocol level
      - **メッセージ交換の機構が必要(SOAP/HTTPなど)**
    - Policy level
      - **各サイト(party)が（相手方に望む）ポリシーを指定できる**
      - **表現されたそれぞれのポリシーは互いに理解できる**
    - Identity level
      - **ドメインをまたいでのIdentityの確立**
      - **物理的なIdentityの確立ではなく、（各ドメインにおける）IdentityとCredentialとのマッピング**

※ Nataraj Nagaratnam, et.al., Security Architecture for Open Grid Services GWD-I (draft-ggf-ogsa-sec-arch-01)




Security Challenges in a Grid Environment ※ （続き）

- **The Trust Relationship Challenge**
  - **動的かつユーザによって制御（生成、管理）されるグリッドサービスにおける問題（挑戦）**
    - Identity and authorization
      - **サービスを実行する際のidentity, privilegeを制御する**
    - Policy enforcement
      - **サービスに対するポリシーの制定、制御**
    - Assurance level discovery
      - **セキュリティのレベルを知りたい**
      - Privacy, virus protection, firewall usage, VPN, etc.
    - Policy composition
      - **ポリシは（1つのリソースオーナではなく）複数のソースにより生成**
    - Delegation

※ Nataraj Nagaratnam, et.al., Security Architecture for Open Grid Services GWD-I (draft-ggf-ogsa-sec-arch-01)



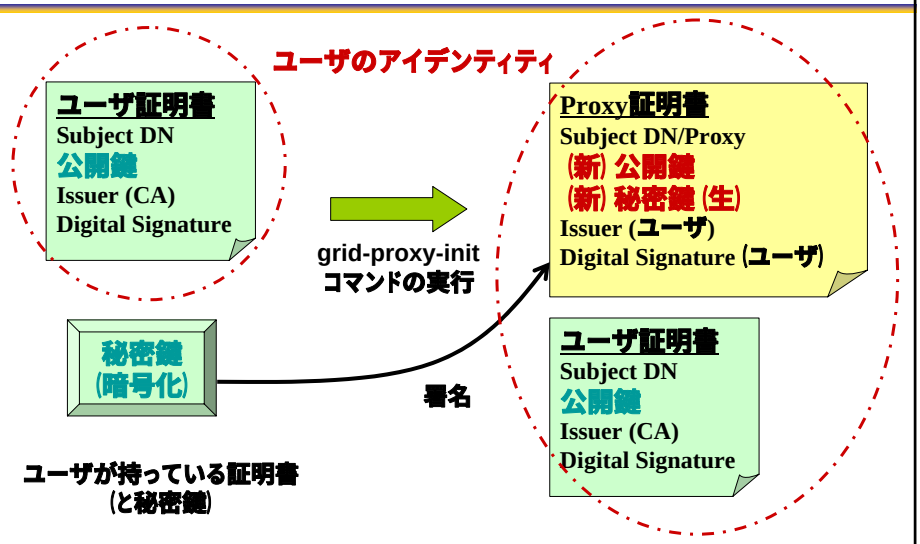

現状および動向

既存研究の成果
現状および動向

GSI: Grid Security Infrastructure

- 「グリッド」の名がつく技術の中で、もっとも偉大な成果(私見)
- PKIとX.509証明書を用いた認証および認可
  - SSL protocol や WS-Security を利用
  - ユーザ、サービス、ホストはX.509証明書を保持する必要がある
- Proxy証明書
  - X.509証明書の拡張(RFC3820)
  - シングルサインオンと委譲を実現

Proxy証明書



GSIのまとめ

- ユーザはかならず証明書を取得しておく。
- 秘密鍵は大切に保管
- 認証が必要なリソースにアクセスする場合は、事前にProxy証明書を作成する。
  - (globusの場合) grid-proxy-init　コマンドの実行
  - 仮想的なログイン
  - grid-proxy-initコマンドを実行したマシン (クライアントマシン) 上にProxy証明書は作成される
- あとはProxy証明書＋delegationの機能により、single sign on ＋ 隅々までの認証 (安全性) が実現される。

既存研究の成果のまとめ

- **Proxy証明書を使ったSingle Sign On + Delegationはグリッドの普及に大きく貢献した**
  - 既存技術プラスアルファ
  - Globus Toolkitによる参照実装とその普及
  - 実際、とても便利
- **関連技術の開発**
  - My Proxy
  - Grid Portal
- **今後もProxy証明書を使ったAuthentication & delegationが基本 (by Globus Alliance)**

最近の動向

- **技術開発 (Globus World 2005より)**
  - Webサービス技術の導入
    - Gridshib, XACML
  - ポータル・ユーザ利用環境
    - PURSE, MyProxy, One-Time PW Auth & Key exchange
  - 仮想マシン
- **標準・運用 (GGF14より)**
  - OGSA AuthZ WG
    - SAMLによるAuthorization
  - Trusted Computing RG
    - TCGが中心となって設立した新設グループ
    - 耐タンパデバイスの利用等を検討
  - Firewall Issues RG
  - CAOPs
    - International Grid Trust Federation (ITGF)

Grid-Shibboleth Integration: A Policy Controlled Attribute Framework (Von Welch, Globus Alliance)

- NMIの2年プロジェクト(2004年12月に開始)
- Shibbolethが発行した属性証明をGrid(GT4)で利用
- Internet2のプロジェクトとして色々と標準技術を使っているShibbolethを認可に利用したい
- 技術的には
  - SAMLとX.509 Identity証明書の相補的な利用
  - SAMLとX.509属性証明書の相補的な利用
  - 属性管理を誰がどうやるか？などなど
- Pull Model
  - Globus ServicesがShibbolethに属性を取りに行く
  - GT4.xのWSおよびPre-WSコードに組みこまれる
  - クライアント側の修正は必要なし
- Push Model
  - ユーザがShibboleth属性を取得し、サービスに提示する。
  - VOMSやCASと同じ
- スケジュール
  - 2005年夏にFirst Release (GT4.2?)

Access Control for the Grid: XACML (Anne Anderson, Sun)

- XACML (eXtensible Access Control Markup Language)を使ったアクセス制御に関する話。
- XACMLの紹介がメイン
  - ポリシー記述言語
  - OASIS standard
  - Open source implementations by Sun Microsystems
- Globus Toolkit will ship with XACML runtime
- デモがあった(by 森さん@ANL)
- GT4.0には組み込まれない。GT4.2 or later

Portal-based Authorization Solution for the Earth System Grid SciDAC Project
(Veronika Nefedova, ANL)

- DOE Earthsystem Grid ポータルのセキュリティ機構の紹介
- PURSE (Portal-based User Registration Service)
  - MyProxyを使っている
  - 鍵生成、鍵と証明書の管理はシステムがやる
    - ユーザにはやらせない
    - Webサーバ上で鍵を生成し、ユーザに入力されたパスフレーズで秘密鍵を暗号化
    - Long Lived証明書と秘密鍵はMyProxyサーバに移す
  - ユーザはユーザ名と秘密鍵のパスフレーズで認証を受ける
  - そのパスフレーズはMyProxyサーバに対する認証にも利用
- ESG external GridFTP access
  - ユーザはPortalを介してファイルをブラウジング
  - Portalはファイルの URLとSAML AssertionをCASフォーマットで返す
  - ユーザはMyProxyからProxy証明書を取得し、SAML AssertionをProxy証明書に突っ込む
  - CAS-enabled GridFTPサーバからファイルを取り出す。




Using the MyProxy Online Credential Repository
(Jim Besney, NCSA)

- MyProxyの紹介 (いろはから)
  - 秘密鍵と証明書を自分のクライアントマシンにコピーして回らなくてもよい
- PURSE (Portal-based User Registration Service)も紹介
- 議論の対象はポータルにおける利用
  - 鍵管理をユーザに任せるのと、一括管理するのとどちらが安全か？
  - Long Lived 証明書は一括管理し、ユーザにはShort LivedなProxyのみ提供する方が安全という主張
  - ユーザは (慣れた) ユーザ名とパスワードでログインしたい
- MyProxy + SASL
  - OTPとMyProxy Passwordを使った認証
  - Kerberos ticketとMyProxy Passwordを使った認証




Secure (One-Time-) Password Authentication for the Globus Toolkit
(Olivier Chevassut, LBNL)

- **背景**
  - Long Lived証明書はData Centerに置かれる
  - Data Centerへの認証はセキュアにやりたい
    - 信頼できない場所からのアクセス
    - short lived証明書をセキュアに渡したい
    - OTPの利用 (認証と鍵交換)
- **One-Time Password authentication and Key Exchange (OPKeyX)**
  - セッション鍵作成の際にOne Time Passwordを利用
- **Globusへの組み込み**
  - OPKeyXをTransport Layerに組み込む
    - OPKeyXをTSLの鍵交換に利用
  - OPKeyXをアプリケーションレイヤに組み込む
    - OPKeyXをWS-SecureConversationの鍵交換に利用

Virtual Machines as Virtual Resources on the Grid
(Kate Kathey, ANL)

- **VMを使った仮想環境の実装**
- **VMの紹介、性能比較**
- **GRAM経由でVMを立ち上げ、ユーザのジョブを実行**
- **Xenならばさほど遜色のない性能が得られることを示していた**
- **クラスタVMもやろうとしているとのこと**

技術的動向のまとめ

- SAML，XACMLなどなどWebサービスの技術がどんどん取り入れられるようになってきている。
- Proxy証明書を使わないSingle Sign On，Delegationが実装されるだろう。
- Authorizationについてはまだまだ発展途上
- ポータルの標準的お作法が確立してきたようだ
  - Long Lived証明書はユーザに管理させない･持たせず、データセンターで管理
  - 一極集中型の弱点は認識している。でもユーザに任せるよりは良いという判断
  - そうすると、いわゆるパスワード認証にもなるので、OTPの利用が進んでいる
- VMも流行ってくると思う。

全世界的な信頼関係の構築に向けて

International Grid Trust Federationの紹介

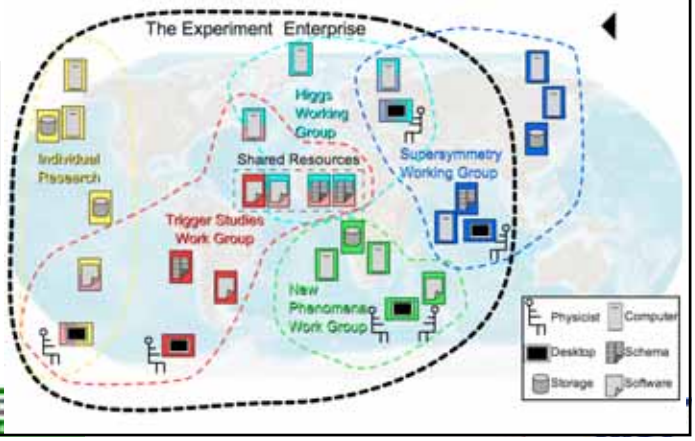
現状

- **技術的には実用レベルに達しつつある**
  - ハードウェア基盤の整備が進む
    - ネットワーク、高性能計算機、大規模ストレージ等の整備
  - 基盤ソフトウェア（ミドルウェア）の研究成果
    - 高品質かつ高性能なオープンソースソフトウェアが開発、公開されている
  - 応用分野と情報分野の連携による大規模アプリケーションの開発
    - 様々な分野でノウハウが蓄積されてきている
- **各コミュニティ内における基盤整備は進み、研究も急速に進んでいる**
  - 共通ミドルウェアの選定/開発、配備
  - アプリケーションの開発
  - 実証実験

グリッドにおけるセキュリティ基盤の構築

- **現状はX.509証明書とPKI（公開鍵暗号）を用いた認証が一般的**
  - 各組織は認証局を運用し、ユーザや計算サーバ等に証明書を発行
  - 各組織は互いの認証局を信頼しあうことにより、他組織のユーザ・計算サーバ等を認証

実質的には「認証局を信頼しあう組織」が仮想的な組織を構成する



multi PKI domain の構築における問題点

- **アーキテクチャ**
  - Cross Certification, Cross Recognition, Bridged CA など、いくつか提案されている。それぞれPros/Consがある。
- **本質的な問題は技術面ではなくポリシーのすり合わせ**
  - すべての認証局は同じレベルで運営されるべき
    - 如何に認証局が安全に運営されているか？
      - HSMによる鍵管理、CAマシンの管理など
    - …
  - すべての認証局はポリシーの整合性を確保すべき
    - 如何に認証局はユーザを識別するか？
      - 面接？電話？….
    - …
- **Policy Management Authority (PMA) は認証局のポリシーおよび運用に関する整合性を取る調整機関**




PMA (Policy Management Authority)

- **複数の認証領域間におけるポリシー整合をとるための調整機関**
- **PMAの例**
  - カナダ政府PMA（12のCAのポリシーを整合）
  - International Grid Policy Management Authority (http://www.gridpma.org)

The goal of the Grid PMA will be to harmonize these various PMAs policies to allow for a global trust relationship to be established

- European Grid PMA
- Asia Pacific Grid PMA
- Americas Grid PMAs
  - DOE Grids
  - Grid Canada
  - NCSA Alliance
  - NASA IPG

Grid PMAは、国際的な信頼関係を確立するための種々のPMAを協調する




PMAの現状

- **現在3つのPMAが存在する**
  - EUGrid PMA (established May 2004)
    - Former: EUDG WP6 CA Coordination Group (started in 2002)
  - TAG PMA (going to be established)
    - Former: DOEGrid PMA (started in 2002)
  - APGrid PMA (established June 2004)
    - Unofficially started in 2003
- **各PMAの主たる役割**
  - **各地域内の認証局ポリシーの調整**
  - **他のPMAとの認証局ポリシーの調整**

Regional PMAがやろうとしていること

- **地域内のセキュリティ基盤およびPMA同士の連携・協力による全世界的なセキュリティ基盤の構築に向けて**
  - **認証局の運用要件の洗い出しおよび標準化**
  - **認証局の承認手順の確立および標準化**
  - **認証局の監査項目、監査手順の確立および標準化**
  - **所属認証局が管理する名前空間の監視**
  - **所属認証局の情報提供**
  - **PMAの運用に関するガイドラインの作成**

International Grid Trust Federation (IGTF)

- **GGF CAOPs WGで始まった活動**
  - (文字通り) グリッドにおける信頼の連合 (の構築)
- **GGF7@Tokyo, March 2003**
  - First meeting with EU, DOE, and AP members
  - Agreed with working on forming the Grid PMA.
    - develop minimum requirements
    - develop GridPMA charter
- **世界的な枠組みの構築に向けて議論を開始**
  - 2004年9月のブリュッセル会合
    - DOEGrid PMA, EUGrid PMA, APGrid PMAが議論を開始
    - 各PMAが地域を代表して世界的な枠組みを構築していくことで同意
    - 互いの認証局運用要件を査読する事からはじめることで同意
  - 2005年3月のソウル会合
    - PMA間で互いが認めた認証局同士を実験的に信頼しあうことに同意
    - International Grid Trust Federationについて文書化を開始
    - 監査方法についてAPGrid PMAが提案
  - 2005年5月のタリン会合
    - 具体的な信頼の手順
    - 認証局運用要件および監査手順の標準化など

IGTF/PMAの役割 (例)

- **Can EGEE trust your CA?**
  - How is the procedure for reviewing/accrediting your CA?
  - Does your CA need to be reviewed by individual organizations in EGEE?
  - If the other CA in Asia wish to be trusted by EGEE, is separate review necessary?
  - APGridPMA will accredit your CA. EGEE does not need to review/accredit your CA.
- **Can your organization trust CAs in EGEE?**
  - How is the procedure for reviewing?
  - Do you need to review all CAs in EGEE?
  - EUGridPMA will accredit CAs. Both you and APGridPMA do not need to review/accredit CAs in EGEE.
- **If you will launch a new CA that is expected to be trusted by organizations in EGEE, how should you design policy and practices of your CA?**
  - APGrid PMA provides minimum CA requirements.

APGrid PMA: Asia Pacific Grid PMA

- アジア太平洋地域におけるPMA
- 2004年6月1日設立
- 議長は産総研田中
- Minimum CA requirementsを定義
- APGrid PMA は2つのレベルを規定
  - Experimental-level CA
    - テスト用認証局であり、ルーズな運用が認められる
    - 地域内のみでのみ信頼可能
  - Production-level CA
    - 厳密な運用が求められる
    - 欧米のコミュニティにも信頼されるレベル

APGridPMA: Status (Members and CAs)

Affiliation	Name	Production CA	Experimental CA	LCG?
AIST / Japan	Yoshio Tanaka	in operation	will close	no
ASCC / Taiwan	Eric Yen	in operation	none	yes
KISTI / Korea	Jae-Hyuck Kwak	in operation	in operation	yes
CAS / China	Kai Nan	in operation	in operation	no
IHEP / China	Gonxing Sun	CP under review	none	yes
VPAC/Australia	Damon Smith	planning	in operation	yes
NCHC / Taiwan	Julian Yu-Chung Chen	planning	in operation	no
Osaka U / Japan	Susumu Date	planning	in operation	no
SDSC / USA	Mason Katz	no plan	planning	no
HKU / HongKong	Chen Lin, Elaine	no plan	in operation	no
U of Hyd / India	Arun Agarwal	no plan	in operation	no
USM / Malaysia	Boon Yaik	no plan	in operation	no
BII / Singapore	Kishore Sakharkar	no plan	in operation	no

＊NAREGIが加盟申請中

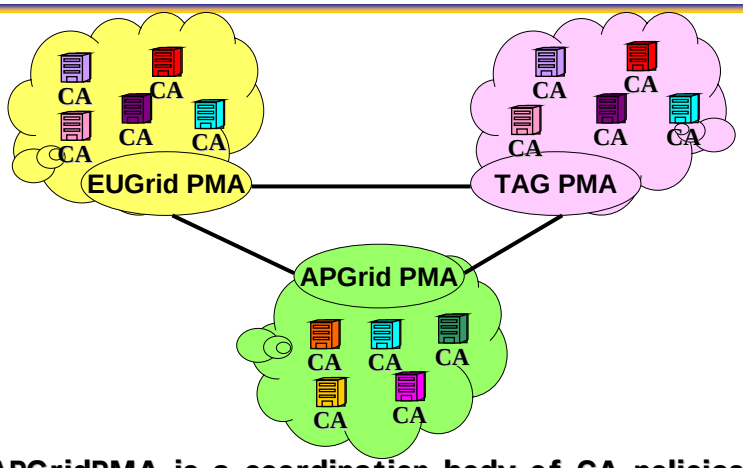
IGTFの現状

- CAOPs WGにおいてCharterの査読中
  - Federationとは？
    - 目的
    - 初期メンバ (APGrid PMA, EUGrid PMA, TAGPMA)
  - IGTFの役割
  - 各PMAの役割
- いくつかの問題については言及していない
  - CA証明書の配布方法等
- 各PMAは8月初旬までに、Charterの承認／否認を決定
- 実働について
  - (EUGrid PMAに倣い) CA RPMを配布
  - メーリングリスト構築
    - IGTF-PMA@gridpma.org
    - IGTF-General@gridpma.org
  - IGTFのChairは各PMAのチェアで持ち回り
  - 各PMAのミーティングには互いに参加しましょうという感じ

解決すべき問題

- CA証明書・ポリシーファイルの配布方法
  - RPMで良い？
    - どこからどうやって配布？
    - 確認方法は？署名？
- PMA内の認証局の承認・監査
- PMA間の承認・監査
  - サンプリング？
- PMA内・PMA間の情報共有
  - CRLの配布等
- ポリシー、minimum CA requirementsの更新手順は？

Summary



- **APGridPMA is a coordination body of CA policies in Asia Pacific.**
- **APGridPMA is collaborating with EUGrid PMA and TAGPMA for International Grid Trust Federation.**

More Information

- **APGrid PMA**
  - http://www.apgridpma.org/
- **EUGrid PMA**
  - http://www.eugridpma.org/
- **TAGPMA**
  - http://www.tagpma.org/
- **GridPMA**
  - http://www.gridpma.org/
- **ApGrid**
  - http://www.apgrid.org/
- **PRAGMA**
  - http://www.pragma-grid.net/
- **GTRC/AIST**
  - http://www.gtrc.aist.go.jp/
- **My email address**
  - yoshio.tanaka@aist.go.jp