
セキュリティの動向

産業技術総合研究所 グリッド研究センター

田中 良夫



グリッドセキュリティの歴史、背景

● Globus Toolkit V1 が出た頃

- ▶ GSI (PKI + X.509証明書)による認証
- ▶ grid-mapfileによる認可
- ▶ Globus CAから証明書を取得
- ▶ サイト内あるいはごく限られたサイト間でのテスト
- ▶ 特に不満はなし
- ▶ GGF Security Working Group
- ▶ RFC3820 (Proxy Cert): 2001年8月～2004年5月

● 大規模グリッドプロジェクトの立ち上げ、その連携が始まって(2000年頃)...

- ▶ GTは標準ミドルウェアであり、GSI+grid-mapfileによる認証・認可
- ▶ Globus CAではなくまじめに認証局を立ち上げるようになった
- ▶ Globusを使う限り、Multi-domain PKI architectureはcross-recognition
- ▶ ポリシーのすり合わせの必要が生じた(e.g. EUDG CA Coordination Group)
- ▶ MyProxyも2000年にプロジェクト開始

グリッドセキュリティの歴史、背景(続き)

- 技術的に認証はうまくいっていたが、grid-mapfileを介してUNIXの認可モデルに落とす実装では、柔軟なアクセス制御に限界があった
 - ▶ VOMS、PERMISなどの認可システムの開発
- OGSA~OGSI~WSRF(2002年~)
 - ▶ WSのセキュリティ技術の導入
 - ◎ WS-Security, SAML, XML署名
 - ◎ Web Single Sign-onとの関係
 - ◎ delegationが鍵
- 大規模な組織では既存のIDシステムとグリッドの認証との連携が望まれた
 - ▶ Kerberos Ticket, Shibboleth ID
 - ▶ ID連携
 - ▶ Higher Education Bridge CA

グリッドセキュリティの現状と動向(まとめ)

● 認証

- ▶ GSI(X.509証明書+PKI)によるシングルサインオンと権限委譲

● 認可 & VO管理

- ▶ grid-mapfile を用いて UNIX アカウントに帰結
- ▶ VOMS (Virtual Organization Membership Service)
- ▶ PERMIS (PrivilEge and Role Management Infrastructure Standards Validation)

● 標準化

- ▶ IGTF (International Grid Trust Federation)
 - ⊗ 認証局の承認(お墨付きをあたえる)
 - ⊗ 認証プロファイルの策定
- ▶ GIN (Grid Interoperation Now) におけるVOMSを用いた相互接続実験

● 動向

- ▶ 技術開発としては、認証から認可へ
- ▶ Shibbolethを中心とするID管理システムの利用
 - ⊗ 技術開発から運用の段階に...

OGFにおけるセキュリティ関連の活動

● eScience Function

▶ Grid Operations

- ◎ Certificate Authorities Operations WG (caops-wg)
- ◎ International Grid Trust Federation (IGTF)

● Standards Function

▶ Security

- ◎ Firewall Issues RG (fi-rg)
- ◎ OGSA Authorization WG (ogsa-authz-wg)
- ◎ Levels of Assurance RG (LoA-rg)

▶ Architecture

- ◎ Open Grid Services Architecture (OGSA-wg)
 - ✦ 公開コメント中！
 - ✦ Secure Communication Profile 1.0 (4/1)
 - ✦ Secure Addressing Profile 1.0 (4/1)
 - ✦ OGSA® Basic Security Profile 2.0 (4/30)

▶ Compute

- ◎ High Performance Computing Profile (HPCP-wg)
 - ✦ GFD. 114 HPC Basic Profile, Version 1.0
 - ✦ HPC Profile Kerberos Support

OGSA-AuthZ WG

● Group Description

- ▶ The objective of the OGSA Authorization WG is to define the specifications needed to allow for basic interoperability and plug-ability of authorization components in the OGSA framework.

● Published Documents

▶ Recommendation

- Ⓢ None

▶ Informational

- Ⓢ GFD.89 Report for the GGF 15 Community Activity: Leveraging Site Infrastructure for Multi-Site Grids
 - ⊕ V. Welch et.al. Jan. 2007
- Ⓢ GFD. 67 OGSI Authorization Requirements
 - ⊕ V. Welch et.al. Mar. 2006

▶ Experimental

- Ⓢ GFD. 66 Use of SAML for OGSI Authorization
 - ⊕ V. Welch et.al. Mar. 2006
- Ⓢ GFD. 57 Attributes used in OGSI Authorization
 - ⊕ M. Thompson et.al. Jan. 2006

OGSA-AuthZ WG

Agenda @ OGF22

- ▶ Agenda Bashing (David)
- ▶ Actions from last meeting (David)
- ▶ Architecture document (David)
- ▶ Attribute Exchange profile (Valerio)
- ▶ XACML profile (David)
- ▶ WS-Trust profile (David)
- ▶ SAML attribute profile (Valerio)
- ▶ Closing down the WG (David)
- ▶ AOB (David)

Levels of Assurance RG

Group Description

- ▶ The LoA Research Group (LoA-RG) is aimed at investigating use case scenarios in the e-Science/Grid contexts, and identifying gaps in applying existing LoA definitions to such contexts.

Focus and Scope

- ▶ 保証レベルに関するクライテリアの洗い出し、NISTなどが定める既存の保証レベルとの違い、グリッドにおけるユースケースなどをまとめる。

Outputs

- ▶ A risk analysis in relation to LoA and use case gathering in an e-Science context
- ▶ A risk analysis in relation to LoA and use case gathering in an e-Science context

- **IGTF、PMAの活動とCAOPs WGは密接に連携している。**
 - ▶ CAOPsでは
 - ◎ PMAのモデル、チャーターテンプレートを策定
 - ◎ CP/CPSのテンプレートを策定
 - ◎ 証明書のプロフィールを策定
 - ▶ IGTFでは認証プロフィールを策定
- **PMAの会議**
 - ▶ EUGrid PMA: 年3回のF2F
 - ▶ TAGPMA: 年3回のF2F
 - ▶ APGrid PMA: 年1~2回のF2F+VTC
- **EUGrid PMAとTAGPMAのF2Fでは、CAOPsセッションを設けている**

CAOPs @ OGF22

- **Session 1: CAOPs (1)**
 - ▶ HSM Vendor Sessions
- **Session2: IGTF (1)**
 - ▶ Private Key Protection
 - ▶ Certificate Renewal
 - ▶ Higher Level CA Profile
- **Session3: CAOPs (2)**
 - ▶ *Grid Certificate Profile*
 - ▶ *Guidelines for Auditing Grid CAs*
 - ▶ *Authentication Service Profile*
 - ▶ *CP/CPS model template*
 - ▶ Use Cases for Relying Party Enforce Name Space Constraints
 - ▶ Election of new CAOPs chair
- **Session4: IGTF (2)**
 - ▶ BalticGrid CA
 - ▶ Robot Certificates
- **Session5: IGTF (3)**
 - ▶ OpenCA + PRQP (PKI Resource Query Protocol)
 - ▶ Identification in IGTF
 - ▶ Distribution Process Document
 - ▶ Discussion on SLCS

Grid Certificate Profile

- Authors: David Groep et.al.
- Gridで利用する証明書のプロファイルを既定
 - ▶ Root証明書
 - ▶ ユーザ証明書
 - ▶ ホスト・サービス証明書
- **MUST, MUST NOT, SHOULD, SHOULD NOT**を既定
- 例
 - ▶ X.509v3 keyUsage **MUST BE** marked as critical for user certificates
 - ▶ emailAddress field **SHOULD NOT** be included in subject name
- 公開コメントおよびそれへの対応は終了。ファイナルドキュメント(Informational Document)への段階

Guidelines for Auditing Grid CAs

● **Authors: Yoshio Tanaka and Matthew Viljoen**

● **認証局監査のガイドライン**

▶ 手順

▶ 監査項目

● **IGTF Classic Authentication Profileに基づく**

● **自己監査にも利用可能**

● **IGTFの認証局が利用している**

▶ EUGridPMA, TAGPMAの自己監査

▶ APGridPMAの外部監査

● **Informational Documentsとして、近日中にエディタ
に提出予定**

Authentication Service Profile

- Authors: Tony Genovese et.al.
- 現在IGTFでは以下の3つの認証プロファイル (Authentication Profile, AP)が規定されている
 - ▶ Classic AP
 - ▶ SLCS AP
 - ▶ MICS AP
- このドキュメントは、認証プロファイル作成のガイドライン的文書
 - ▶ 2年前のものが引っ張り出されて復活
 - ▶ 認証プロファイルとして、何が規定されているべきかななどを記述
 - ▶ 今迄の経験をもとにリバイスしていく

CP/CPS Model Template

- **Presenter: Jens Jensen (UK-eScience)**
- **RFC3647に基づいたCP/CPSのテンプレートを作ろうという提案**
 - ▶ RFC2527については、すでにある。
- **IGTF Classic APに基づいてテンプレートを作成し、認証局の立ち上げを助けてたいということ**
 - ▶ 簡単になりすぎてしまうのではという懸念も
- **ポリシーの共通化にもつながるという議論も**
 - ▶ NII-GOC CAがやろうとしていること
 - ▶ うまく協力していけないか模索する

CAOPs/IGTFに関する所感 (1/2)

- 出席者はそれほど多くないが、メンバはほぼ固定し、かなりアクティブ
 - ▶ 出席者: 18名 (最初のセッション)
 - ④ 米国、カナダ、ブラジル: 8名
 - ④ 欧州: 9名
 - ④ アジア: 1名
- IGTFの知名度も高まっている
- ドキュメント、発表はほとんど欧州
 - ▶ アジア1件、米国1件、ほかすべて欧州
- EUGridPMAはとてもアクティブ。
 - ▶ LCGの実験組からの強力なモチベーション
 - ▶ OSG系も引っ張られている
 - ▶ アジアではASGCC@TaiwanがROCをたてているが、OGFには出てきていない
- OGF, PMA会議を合わせると、年に10回IGTF関連のF2Fがある！
 - ▶ 新しい話がどんどん出てくる
 - ▶ 運用を始めて出てくる(明らかになる)問題があるということ
- アジアの弱さ
 - ▶ OGFに出てくるのは一人だけ
 - ▶ F2F会議も他に比べると量、質ともに弱い

CAOPs/IGTFに関する所感 (2/2)

- Classic APやそれに続くドキュメントなど、かなり制約がきついものが出てきている。
 - ▶ 過去に2件、MUSTをSHOULDに変更してもらったが、ほかにも制約が厳しいものがある
 - ⊙ Subject名のuniqueness
 - ⊙ Identity Vetting
 - ▶ EUGridPMA固有の話がProfileの中に入っている
 - ⊙ 1カ国あたり1認証局
 - ⊙ TACARというレポジトリの利用
- 特にClassic APのID Vettingについては、ちょっと大変
 - ▶ F2Fが必要
 - ▶ たとえば、TeraGrid CAでClassic AP Compliant CAはない
- もっと低いレベルのAPがあってもいいし、作っていくべきだと思う
 - ▶ EUGridPMAの理解を得るのは大変そう
 - ▶ TAGPMAと協力してやっていくのがいいだろう
- これからLHCの実験が始まるが、この活動が役に立つことを願っている
 - ▶ ほかの分野にも役立つはず