

担当者： 田中 良夫 (産総研)

AREA	Security
内容 状況	Grid Security Infrastructure(GSI) WGは8月に「Internet X.509 Public Key Infrastructure Proxy Certificate Profile」および「GSS-API Extensions」というドラフトを提出。 GCP WGは10月に「Global Grid Forum Certificate Policy Model」というドラフトを提出。 Grid Certificate Policy (GCP) WGはCAOPs WG(新設)に引き継がれた感じ。 Certificate Authority Operations (CAOPs) WGが新設。 (Large)Site AAA (Authentication, Authorization, Accounting)というRGが新設。
終了 Group	GSI WGおよびGCP WGはドラフトを提出し終了。
新設 Group	CAOPs WG(認証局のオペレーションについて議論するWG) Large Site AAA(大きなサイト)での認証、権限、課金当について議論するRG
今後	認証局の運用および大きなサイトでの証明書の発行・管理など、実際の状況に即した議論が行われてゆくと思われる。
所感	CPの記述や巨大なサイトでの証明書の(半自動)発行など、今までGlobus CAを使って気楽にやっていた部分を自分たちできちんとやらないといけないのは大変だとみな認識しているようだ。やろうとしているアイデアはApGridで考えているのと同じ。皆同じ事を考える。

AREA名：Security

グループ名		内容
W G	GSI	なし
	GCP	なし
	OGSA SEC	WSセキュリティ関連仕様をベースとしてOpen Grid Service のSecurity 要件を抽出。多くのレイヤーにまたがるので、WGが大きく発展する見込み。
	CAOPs	GCPの成果(Certificate Profile)をもとに、認証局の運用に関する議論を進める。今回は2セッションが開かれ、第1セッションではチャーターの確認、ドキュメントのreviewなどを行なった。第2セッションではクライアント証明書 の自動配布やオンラインCAなどの新しい機能について議論をした。
R G	(Large)Site AAA	すでに存在するサイトを例に、セキュリティに関する必要事項を収集し、文書化する。また、それらの情報を元に、Grid Toolkitが提供すべき機能等についても議論をする。今回は2セッションが開かれ、第1セッションではチャーターの確認、2ndチェアの選出、ドキュメントのreviewなどを行なった。第2セッションではAuthentication, Authorization, Accountingのそれぞれについてテーマを決めて議論を行なった。
B O F	Authorization	グリッドシステム開発者に対し、グリッド間で相互運用可能な認証システムを作成するためのガイドラインを提供する。

Global Grid Forum Certificate Policy Model (1)

- 前置き
 - GSIのベースはX.509証明書＋PKI
 - 認証局が証明書を発行
 - 認証局の運用には認証局のポリシーを明記したCertificate Policy (CP)を提示しなければならない
- この文書の概要
 - Global Grid Community (GGF)の中の様々な認証局が参考にするためのCertificate Policy
 - これを見本にしてCPを作成すればいい
 - GGFが認証局を運用するというわけではない

Global Grid Forum Certificate Policy Model (2)

1. Introduction
 - 用語の説明
 - CA, RA, End entities, Applicability,...
 - 4つのレベル
 - Rudimentary, Basic, Medium, High
2. General Provisions
 - CAやRAの義務など
3. Identification and authentication
 - 証明書を発行する前に、証明書の発行要求を識別し、認証するための手続きについて
4. Operational requirements
 - エンティティが証明書を取得する・無効化する手続きについて

Global Grid Forum Certificate Policy Model (3)

5. Physical, procedural, and personnel security controls
 - 物理的な事柄
 - 計算機、場所、災害対応など
6. Technical security controls
 - 鍵の生成、管理など
7. CA certificate
 - 秘密鍵の管理が中心
8. Certificate and CRL profile
 - 別の文書に詳しく
9. Specification administration
 - CPの管理について

担当者： 安崎 篤郎 (日立)

グループ	OGSA-SEC-WG
目的	<ul style="list-style-type: none">・OGSAでのグリッド・セキュリティの要件をリストして、順次取り組む・WS-SecurityとWS Security Roadmapを推進する。・主要成果物： The Security Architecture for Open Grid Services, OGSA Security Roadmap
状況	WSセキュリティ関連仕様(補足)をベースとし、WSとグリッドの差分を議論することが焦点であった。アーキテクチャも(現時点では?)XML-xxxやWS-xxx仕様を中心に組み立てられている。差分はVOをまたがる場合の認証やアクセス権限管理等。
進捗	The Security Architecture for Open Grid Servicesドキュメントアーキテクチャ図とビルディングブロック図が示された。後者は、WS-xxx, XML-xxxなどが中心に組み立てられている。XKMS, SAMLなども含まれており、W3CやOASISに大きく依存している。肝心のGrid Security Servicesの層は箱は用意されているものの、TBDとなっており、詳細は今後詰められることになる。
今後	AuthorizationやVOポリシーなど、すぐに話し合うべきトピックを決める。ロードマップのブロック一つずつWGを作るとたくさんできすぎるので、2つ程度のWGを作って、一つのWGが複数のブロックを担当する方向か?とにかく、必要なのはメンバからの提案である。
参加者数	50名程度
所感	セキュリティは非常に範囲が広く、各階層にまたがっていく。 本WGは発展的に、複数のWGを立ち上げていく為の準備段階のようである。

OGSA-SEC-WG

Webサービス関連セキュリティ仕様

(1)WS-Security(OASIS WSSTC)

セキュリティトークンとして, (a)UserNameトークン(ユーザ名, パスワード), (b)SAML, (c)XrML, (d)Kerberos, (e)X.509を扱える.

(2)Policy表現

WS-QoP(Quality of Protection)(OASISに議論グループ有り)

WS-Policy (まだ仕様はない)

(3)フェデレーション

WS-Federation (ロードマップのブロックの一つ. まだ仕様はない)

(4)その他

Trust, Secure conversationなど, ロードマップの
ブロックとして示されていて, まだ仕様はない。

グリッド固有部分を特定し, 拡張・修正することがWGの目標。
標準化については, 他の標準化団体にリエゾンを送り込むか,
GGF本体で行う。(本WGのチャーターには標準化は含まれていない)

担当者： 田中 良夫 (産総研)

グループ	CAOPs WG
目的	X.509ユーザ証明書を使った認証および認証局の運用に関して必要な手続きやガイドライン等をまとめ、今後の相互利用への手引きとする。
状況	GCP WGが提出したドラフトGGF Certificate Policy Modelは認証局のポリシーステートメントのGGFモデルとして提案されたが、これを元に実際に認証局を運用する際に必要な事柄等について議論を進めようということで結成された。
進捗	GCPのドキュメントなど、Security Areaの過去のWGからのドキュメントの蓄積が多くあり、また、過去のWGのメンバがそのまま継続して参加しているため、新設ということを感じさせずにチャーターの確認やドキュメントのreviewなどをサクサクとこなしていった。
今後	今年10月来年5月をめどに、いくつかのドキュメントを書き上げる。 基本的にはMLを通じて議論を進める
参加者数	30人
所感	GSI WG～GCP WGと引き継がれたWGであるが、GSI WGにおけるProxy Cert.拡張等の技術的な話から、認証局の運用といった実務的な話に変わってきたことが、グリッドの実用化が現実のものとなっていると感じさせた。

CAOPs WG

- CAOPsについてすでに同じような活動をしているところは、
 - European Data Grid
 - Federal Bridge
 - Internet 2 (focus on campus needs)
- このWGは秘密鍵の管理については言及しない
- このWGで扱うべき事柄は
 - Certificate Policy/Certificate Practices
 - Policy Management Authority charter
 - Cross trust models
 - Certificate Profiles
 - Certificate Revocation List Management
 - Physical Security Management
 - Disaster Recovery
- クライアント証明書の自動取得に関する話
 - 自動ツール、バックアップ、ファイル複製などに利用可能
- Online CAについて
 - CAの証明書などをLDAPに突っ込む
- Certificate Revocation Listについて
 - EU Data Gridは1日に1度チェック
 - Globus CAは6000の証明書を発行して、CRLには600登録されている

担当者： 田中 良夫 (産総研)

グループ	Site AAA RG
目的	すでに存在するサイトを例に、セキュリティに関する必要事項を収集し、文書化する。また、それらの情報を元に、Grid Toolkitが提供すべき機能等についても議論をする。
状況	当初はLarge Site AAAだったが、「Largeというのは計算資源か、人の数か、どこからがLargeなのか…」などの指摘があり、Largeを取った。GGF5でBOFがあったとのことであるが、そちらには出席していなかったなのでこのWG結成の経緯は不明。
進捗	第二チェアの選出、チャーターの確認等を行なった。また、EUDG, PPDG, Internet2のrequirementが示された。しかし、その後の議論はあまり進展がなく成果はあまりなかった。
今後	GGF7までにはreviewのためのドキュメントを仕上げ、GGF8で終了
参加者数	30～50人
所感	CAOPsに比べると話の道筋(このWGの目的)が分かりにくかった。各サイトのrequirementを洗い出してから分かるが、それがどう活用されていくのかが不明。あまり興味をもてなかった。

Site AAA RG

- 既存のサイトとして、以下の3つのサイトについてドキュメントがある
 - European Data Grid
 - Particle Physics Data Grid
 - Internet 2
- Authenticationについては、ユーザがどのように秘密鍵を管理するかということと、世界中の認証局間でagreementを交換する必要性を中心に議論
- AuthorizationおよびAccountingについてはあまり議論(進捗)なし。

担当者： 新島 秀人 (日本アイ・ビー・エム)

グループ	BOF: Authorization
目的	グリッドシステム開発者に対し、グリッド間で相互運用可能な認証システムを作成するためのガイドラインを提供する。
状況	チャーターの決定とグループの体制とについて作業中。 他グループとの協業体制、スケジュールについても作成中。
進捗	スケジュールに関しては当初の予定より半年～1年早いタイミングで最終版のドキュメント完成を目指すことを確認。
今後	チャーターについてはメーリングリストにて回覧する。 GGF7でサマリードキュメント発行。GGF8で最終版のドキュメント発行を目指す。(当初の予定ではGGF10で最終版ドキュメント発行の予定であった)
参加者数	30名程度
所感	立ち見参加が多数出るほど盛況であり、このグループ(エリア)に対する関心の高さが伺えた。これまでの標準技術をベースにしっかりと構築していこうと言う方向性が感じられ、今後に期待が持てるグループであると感じた。