様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 5 月 17 日現在

研究種目：若手研究(B)
研究期間：2008～2009
課題番号：20700062
研究課題名（和文）
グリッド認証基盤に適応した XML データ保護・管理機構に関する研究
研究課題名（英文）
A study on XML data protection and management structure for Grid authentication infrastructure
研究代表者
伊達　進（DATE SUSUMU）
大阪大学・サイバーメディアセンター・准教授
研究者番号：20346175

研究成果の概要（和文）：
本研究は、XML(eXtensible Markup Language)によって記述される科学データや情報のグリッド上での安全な共有のため、グリッドにおける認証技術 GSI（Grid Security Infrastructure）との連携により、XML 要素レベルでのデータ暗号化および電子署名によるデータ機密性と完全性を保障する XML データ保護・管理機構を設計、実装した。具体的には、グリッドの事実上標準であるミドルウェア Globus のサービス要素技術 WS-GRAM、および VOMS (Virtual Organization Membership Service)を連動させることで、XML 要素レベルでのデータ暗号化および電子署名によるデータ機密性と完全性を保証する XML データ保護・管理機構のプロトタイピングに成功した。

研究成果の概要（英文）：
In this research, an XML data protection and management structure has been designed and implemented. The structure guarantees the confidentiality and integrity of data through the use of encryption and signature on the basis of XML element, by leveraging GSI (Grid Security Infrastructure) for XML-based scientific data and information exchanged on a Grid. Specifically, the structure was prototyped using WS-GRAM and VOMS (Virtual Organization Membership Service).

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,900,000	570,000	2,470,000
2009 年度	1,500,000	450,000	1,950,000
年度			
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：総合領域
科研費の分科・細目：計算機システム・ネットワーク
キーワード：　グリッド、アクセス制御、XML データ、GSI、PERMIS

１．研究開始当初の背景

地理的に分散する複数の研究機関や大学の保有する計算資源、およびデータ資源を、その物理的な組織構造に関わらず仮想組織（VO：Virtual Organization）として形成し、それらを安全かつ高利便に共有可能にするグリッドが、次世代科学のための研究環境を構築する基盤技術として研究者らの注目を集めている。そのような背景から、特に科学研究に関連するデータや情報などデータ資源の共有に着目したグリッドを構築しようとする動きが世界規模で活発化している。

また、このようなデータ資源の共有に向けた試みの活発化と連動し、グリッド上でのデータセキュリティ技術の必要性と重要性が急速に高まっている。一般的に、グリッドでは、複数の組織から様々なセキュリティ要件をもつデータ資源が集約され、そのユーザの属性も多様に異なる。しかし、今日のグリッドにおけるセキュリティ技術では、グリッドでのデファクトスタンダード（事実上標準）認証技術 GSI によって異質かつ多様な計算資源およびデータ資源へのシングルサインオン機能を提供するものの、多様なユーザ属性とデータセキュリティ要件を十分に考慮し、柔軟かつ頑強にデータを保護・管理する汎用的なメカニズムはいまだ実現されていない。

２．研究の目的

申請者は、本申請書執筆時までに、本申請研究を推進する上で基礎となるグリッド認証基盤に適応した XML データに対するアクセス制御およびデータフィルタリング機構(図１)のプロトタイプ構築を実施している(文献[1])。当該機構は、認証基盤技術である GSI および認可技術 PERMIS をシームレスに連動させることにより、ユーザの役割(Role)に応じてデータベース内に格納された XML データを要素レベルでフィルタリングし、アクセスを制御する仕組みを提供する。XML データのフィルタリングには、ユーザの持つ役割に応じて、あらかじめ役割ごとに用意されているスタイルシートを適用する。これによりユーザの役割に応じた適切な XML 要素セットからなる XML データを生成する。本申請研究では、このアクセス制御およびデータフィルタリング機構との連携を視野に入れ、グリッド認証基盤に適応し、XML 要素レベルでのデータ暗号化および電子署名によるデータの機密性と完全性を保障する XML データ保護・管理機構を実現する。これにより、グリッド環境上で研究者らによる、XML データ化された様々なデータ、情報、知見の安全な共有を促進し、今後の科学研究への貢献を目指す。

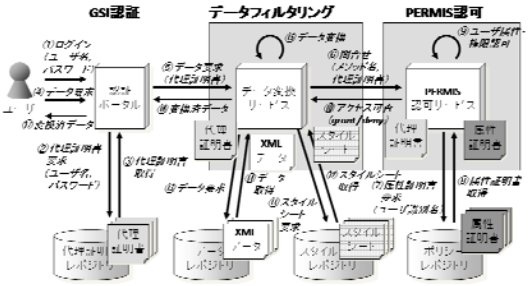

図１GSI-PERMIS によるアクセス制御機構およびデータフィルタリング機構

３．研究の方法

本研究では、上述の目的を達成するため、マイルストーンとなる以下の３つの課題を設定し、実施する。

［課題１］セキュリティ情報伝達モデルと XML データ保護・管理機構の設計

広域グリッド上でユーザが科学研究を行う際の一般的なワークフロー、すなわちデータ取得、解析計算、解析結果の解釈からなる作業ステップにおけるデータアクセスパターンを考慮し、ユーザのクレデンシャル（信用）情報、X.509 証明書および X.509 属性証明書に含まれるユーザ属性情報などをグリッド上で安全に伝達するセキュリティ情報伝達モデルを設計する。また、セキュリティ情報伝達モデルに基づく、XML データ保護・管理機構の設計を行う。

［課題２］XML データ保護・管理機構のプロトタイプ作成

上記課題１で構築したモデルに基づく XML データ保護・管理機構のプロトタイプを作成する。

［課題３］アクセス制御およびフィルタリング機構と連動する XML データ保護・管理機構の実装

課題２でプロトタイプ開発を行う XML データ保護・管理機構と、図１に示されるアクセス制御およびデータフィルタリング機構を連動させることにより、多様なユーザ属性とデー

タセキュリティ要件に柔軟かつ頑強に XML データを保護・管理するデータセキュリティ技術を完成させる。

４．研究成果

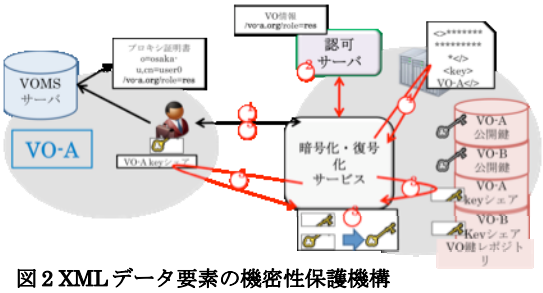

図２XML データ要素の機密性保護機構

図 2 に本研究でプロトタイプ開発した機構のアーキテクチャを示す．本機構は，VOMS サーバ，暗号サービス，認可サーバ，VO 鍵レポジトリから構成される．VOMS サーバは各 VO に設置され，ユーザがグリッド認証時に作成するプロキシ証明書にユーザの VO 情報を追記する．暗号化・復号化サービスは，ユーザからの要求を受けて,VO 鍵の取得および復元，XML データ要素の暗号化，復号化を行う．認可サーバは，暗号化・復号化サービスと連携し，ユーザの VO 情報を基に認可を行う．

本機構はこれら 4 つのコンポネントが連動し，次の通り動作する．まず，ユーザは GSI によるプロキシ証明書の発行，VOMS サーバによるプロキシ証明書への VO 情報の追記により認証を行う．次に，ユーザは，XML データ要素の暗号化または復号化を暗号化・復号化サービスへ要求する．ユーザからの要求を受けた暗号化・復号化サービスは，認可サーバを呼び出し，認可された場合には認可サーバが取得したユーザの VO 情報を受け取る．暗号化・復号化サービスは VO 情報に基づいて，ユーザの所属する VO の公開鍵，もしくは VO の秘密鍵のシェアを VO 鍵レポジトリから検索する．復号化の場合，これに加えて，ユーザからも VO の秘密鍵のシェアを取得し，VO の秘密鍵を復元する．最後に，取得した鍵を用いて，ユーザに指定された XML データ要素を暗号化または復号化する．

本研究で提案する XML データ要素の機密性保護機構は，VO の公開鍵と VO の秘密鍵の導入，および VO の秘密鍵の分散管理により，鍵の漏洩による致命的なセキュリティリスクを軽減している．本機構では，ユーザと VO 鍵レポジトリからの VO 秘密鍵のシェアが同時に発生しない限り本機構の保証するデータの機密性は損なわれない．また，ユーザが管理する VO の秘密鍵のシェアだけでは VO の秘密鍵を復元することはできないため，ユーザの負う鍵の管理責任は，ユーザが VO の秘密鍵を管理する場合と比較して小さくなる．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計１件）

* 野崎一徳, 伊達進, 馬場健一, 中川真志, 下條真司, “発音解析のための大規模可視化情報プラットフォーム”, 情報処理学会論文誌 コンピューティングシステム(ACS27), 査読有, pp. 189-200, 2009.

〔学会発表〕（計１件）

* Masahiro Yamada, Kohei Ichikawa, Susumu Date, Shinji Shimojo, “A Confidentiality Protection Mechanism for XML Data Element Leveraging GSI and VOMS”, 18th Pacific Rim Applications and Grid Middleware Assembly Workshop, San Diego, USA, March 3-4, 2010.

６．研究組織
(1)研究代表者

伊達　進（DATE SUSUMU）
大阪大学・サイバーメディアセンター・
准教授
研究者番号：20346175

(2)研究分担者
なし

(3)連携研究者
なし