웹서비스 기반 그리드 보안 기술 동향

Research Trends of Grid Security Technology Based on Web Services

u-IT839의 정보보호 이슈 특집

이성현 (S.H. Lee) 바이오인식기술연구팀 Post-Doc
이재승 (J.S. Lee) 바이오인식기술연구팀 선임연구원
문기영 (K.Y. Moon) 바이오인식기술연구팀 팀장

목 차

2006년 9월 개최된 제18차 GGF 회의는 그리드 연구에 대한 새로운 출발점으로 기억될 것이다. 1999년 미국 시카고 대학의 이안 포스터 교수에 의해서 “인터넷 망을 이용하여 분산된 컴퓨터 자원의 결합을 통한 작업 수행”이 가능한 그리드가 처음으로 제안된 이후, 많은 기술 발전을 거듭하였고, 최근에는 웹서비스 기술과 그리드 기술을 접목한 개방형 그리드 서비스 구조를 제안하였다. 제18차 회의는 현재까지 개발된 그리드 기술에 본격적으로 웹서비스 기술을 도입하기 위한 선포였으며, 이에 GGF를 OGF로 개명하였다. 본 고에서는 OGSA에 대한 분석을 기반으로 그리드 웹서비스에 대해서 간략히 소개하고, 현재 그리드 웹서비스에서 보안 서비스를 제공하기 위해 연구를 진행하고 있는 웹서비스 보안 기술과 이에 대한 적용 동향을 살펴본다.

Ⅰ. 서론

1990년대 말 미국 시카고 대학의 이안 포스터(Ian Foster) 교수에 의해 처음으로 제안된 이후, 그리드 컴퓨팅 환경(grid computing environment; 이하 그리드)은 인터넷을 통해 분산된 컴퓨팅 자원의 공유를 통한 대용량 계산, 대용량 데이터베이스, 원격 회의 등의 분야에서 눈부신 발전을 거듭했으며, IT 기반의 각종 응용 과학(e-science) 및 전자거래 등이 적용에 이르기까지 상당한 기술 파급을 이루고 있다[1],[2]. 현재 그리드 기술의 연구 및 개발 동향은 OGSA를 기반으로 이루어지고 있다. OGSA의 목표는 그리드 애플리케이션이 공통적으로 제공하는 모든 서비스에 대해서 공통된 인터페이스를 규정함으로써 서로 다른 프로젝트 간의 상호연동성, 코드의 재활용을 높이고, 그리드 사용자가 작업을 수행하는 데 있어 편의성을 제공하는 데 있다. 이러한 OGSA의 기반이 되는 미들웨어 구조는 웹서비스이다. 이는 CORBA, RMI, RPC, EJB 등의 기존 미들웨어와 비교했을 때 웹서비스가 느슨하게 결합된(loosely coupled) 시스템이라는 점이 그리드를 구성하는 이기종 시스템들 간의 통산에 보다 적합하기 때문이다[3]. 이기종 시스템으로 구성된 그리드의 컴퓨팅 자원의 특성을 단일화할 수는 없지만, 웹서비스 기술을 사용하면 자원에 접근하고, 활용하는 방법을 단일화할 수 있기 때문에 그리드와 웹서비스 기술의 접목은 향후 상용 서비스를 통한 그리드의 확산에 결정적인 역할을 할 것이다.

본 고에서는 그리드 웹서비스에서 보안 서비스를 제공하기 위해 활발히 연구되고 있는 OGSA 보안 구조 및 웹서비스 보안 기술을 살펴본다. 또한, OGF 보안 작업그룹(security working group)과 글로버스(globus), EGEE, IBM 등의 그리드 관련 기관에서의 적용 현황을 살펴봄으로써 향후 그리드 웹서비스 보안 기술의 발전 방향에 대해서 살펴본다.

● 용 어 해 설 ●

가상 조직(Virtual Organization; VO): 공동의 목적이나 협업을 통한 문제 해결을 위해 개개인이나 혹은 공인이 가진 여러 컴퓨팅 자원이 하나의 가상 공간 영역으로 묶여 있는 상태.

Ⅱ. 그리드 웹서비스와 보안 서비스 개요

1. OGSA

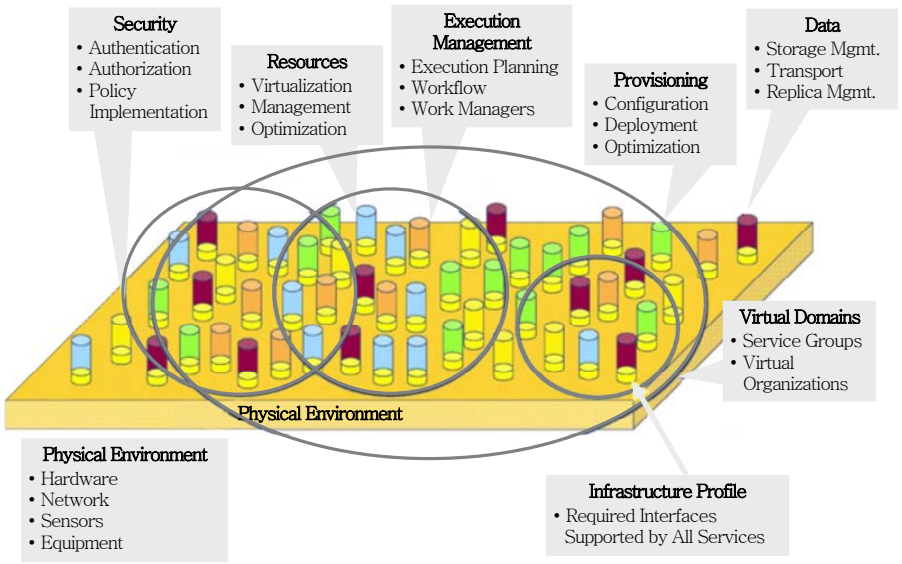
가. 개요

OGSA는 그리드를 구성하는 분산되고, 이질적인 자원에 대한 사용과 관리를 용이하게 하기 위한 목적으로 제안된 구조로 웹서비스를 기반으로 하고 있다. OGSA에서 사용되는 “분산된”, “이질적인”, “자원”이라는 용어는 그리드 연구에서 폭넓게 통용되는 용어로, “분산된”은 전역적, 다중 도메인, 결합된 자원 간의 접속 구조 등에 의해서 분산되고 연속적인 자원에 대한 의미로 사용되며, “이질적인”은 성질이 다른 자원의 구성을 의미한다. “자원”은 인위적인 물질, 실체(entity), 그리드를 구성하는 시스템 내·외부의 인위적인 결과물을 의미한다[4].

나. OGSA 프레임워크

OGSA 프레임워크는 (그림 1)과 같이 서비스의 형태, 서비스 사이의 인터페이스, 서비스와 관계된 자원의 개별적 또는 집단적 상태, 서비스 사이의 상호 작용을 논리적인 중간 계층으로 표현한 것이다. 그림에서 물리적인 환경(physical environment) 상의 원기둥은 그리드에서 제공되는 각각의 서비스를 나타내며, 의미에 따라 추가/확장/수정되어 웹서비스 상에서 구성된다. OGSA 프레임워크를 구성하기 위해서는 다음과 같은 점을 주의해야 한다.

- OGSA 내에서 기존 기능의 필요에 따라 새로운 기능을 추가하거나 구성/구축하는 적응성, 유연성, 견고함을 제공한다.
- OGSA에서 제공하는 기능을 현재 시스템에서



(그림 1) OGSA 프레임워크

제공하지 않을 경우, 그리드는 OGSA에 정의된 일부 기능을 사용하여 구성될 수 있다. 하지만 그리드에서 구성되지 않은 다른 기능을 요구할 경우 해당 기능을 이용할 수 있으며, 서비스의 하위 능력만으로 제공하는 것을 선택할 수 있다.

- OGSA는 서비스 인터페이스와 의미/행위와 이들 서비스 사이에서의 상호 작용을 기술하지만, 구체적인 제어 구조는 제공하지 않는다.
- OGSA는 하나의 서비스 구현에 계층화되지 않고 상호 작용일 수 있으며, OGSA 계층은 논리적으로 독립적 또는 객체-지향적 계층일 수 있다.

2. OGSA에서의 보안 서비스

가. 보안 서비스 개요

OGSA는 강력한 보안 프로토콜과 보안 정책을 이용하여 OGSA 서비스에 대한 접속을 제어하는 안전한 관리를 요구하며, 보안 서비스를 제공하기 위해서 다음과 같은 요구 사항을 가진다.

- 인증/인가(authentication/authorization): 인증은 개개의 실체와 서비스가 성립될 수 있도록 요구되며, 서비스 제공자는 각 서비스 정책에 따른 인가 메커니즘을 반드시 제공해야 한다. OGSA 기반 그리드는 각 도메인과 개인 사용자를 위한 보안 정책을 가지고 있으며, 인가는 다양한 접근 제어 모델의 구현을 통해서 제공되어야 한다.
- 다중 보안 구조(multiple security infrastructure): 그리드의 분산된 연산은 다중 보안 구조의 통합과 상호운용을 필요로 한다. 따라서, OGSA에서 제공하는 보안 서비스는 현존하는 모든 보안 구조와 보안 모델의 통합과 상호 운용을 필요로 한다.
- 경계 보안 솔루션(perimeter security solutions): OGSA를 구성하는 자원에 대한 접속은 조직의 경계를 벗어날 수 있다. OGSA는 자원이 위치하고 있는 조직의 로컬 보안 메커니즘을 손상시키는 일 없이 교차 도메인에서 상호작용하는 동안 로컬 도메인을 보호할 수 있어야 한다.
- 분리(isolation): OGSA에서 공유되는 자원에 대해 사용자, 성능, 제공 콘텐츠에 대한 다양한 분리를 보증해야 한다.
- 위임(delegation): 서비스 요청자와 제공자로부터 접속 측에 권한을 위임하기 위한 메커니즘이 요구된다. 위임되는 권한의 한정과 권한 생명주기의 제한과 같은 위임 권한의 오용에 대한 대비

책을 마련해야 한다(또는 오용에 대한 위험을 최소화해야 한다).

- 보안 정책 교환(security policy exchange): 서비스 요청자와 제공자 사이의 보안 정책 구문협상을 위해 동적인 보안 정책 교환이 가능해야 한다.
- 침입탐지/보호/보안 로깅(intrusion detection/protection/secure logging): 강력한 모니터링은 침입 탐지와 오용, 바이러스 또는 웜 공격을 포함하는 보안 위협 대응과 식별을 위해서 요구된다. 이를 통해 보안 위협의 공격 경로와 임의 영역과 기능의 보호가 가능하다.

나. 보안 서비스 목적

OGSA 보안 서비스의 목적은 OGSA를 구성하는 가상 자원 조직에 대해 보안과 연계된 정책 시행을 용이하게 하기 위한 것이다. 일반적으로 보안 정책 시행의 목적은 상위 계층의 비즈니스 목적들이 달성될 수 있는 것을 보장하는 것이다. 보안 정책은 그리드에서 수행하는 작업에 대한 메시지 무결성과 비밀성, 실체 인증, 제한된 위임, 인가, 보안 로깅과 감사, 책임 분리, 침입 탐지, 신뢰와 보증, 보안 위협 대응과 같은 보안 서비스를 제공하기 위한 목적으로 작성된다. OGSA 보안 구조에서 각 구성 요소는 그리드를 구성하는 시스템들이 안전하게 동작하는 것을 가능하게 하기 위해서 일반적인 보안 모델과 메커니즘, 프로토콜, 플랫폼과 기술 등의 통합을 지원해야 하며, 현존하는 보안 구조와 교차 플랫폼(cross-platform), 호스팅 환경의 통합을 지원해야 한다. 또한, 복수의 도메인들과 호스팅 환경을 가로지르는 서비스는 서로 상호작용할 필요가 있다. 또한, 그리드에서 어떤 작업은 애플리케이션 실행 이전에 사이트들에 대한 신뢰 관계 형성을 불가능하게 할 수 있다. 주어진 모든 도메인들이 필요한 다른 보안 구조(예를 들어, Kerberos 또는 PKI)의 보안 메커니즘 중에서 어떤 형태를 통하여 요구되는 신뢰 관계의 실현을 필요로 할 수도 있다. 따라서, 구성 요소는 현존하는 보안 구조와 플랫폼을 교차하는 호스팅 환경에 대한 통합을 제공할 수 있어야 한다.

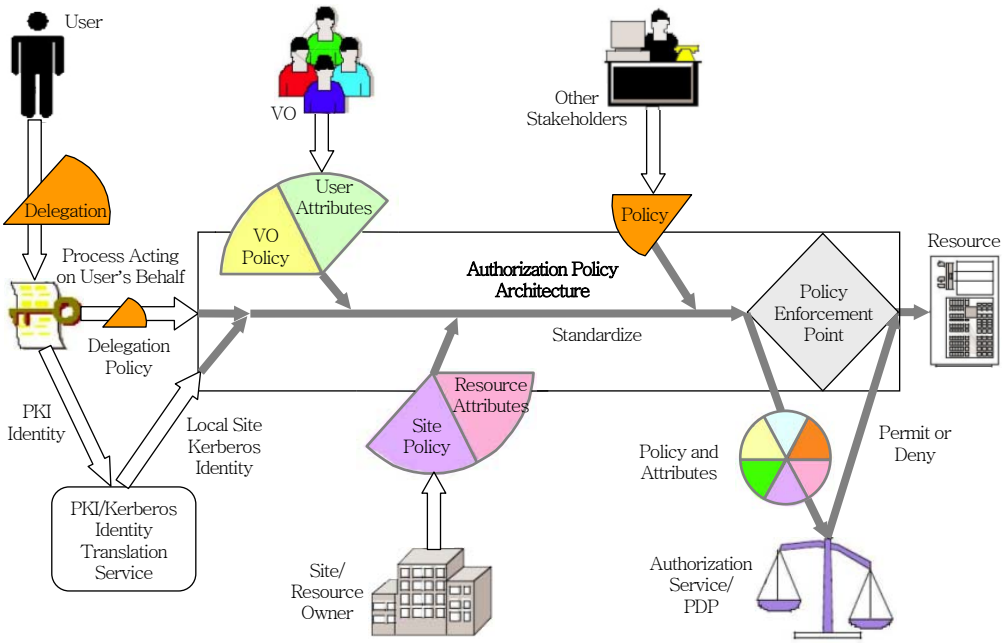
다. 보안 서비스 모델

OGSA 보안 서비스 모델은 수학적 의미의 형식적 보안 모델이 아니라, 보안 서비스를 기술할 수 있는 언어를 제공하는 것을 의미하고, 보안 정책에 대한 일반적인 이해를 획득하는 정책 시행을 의미한다.

일반적으로 실체는 사용자, 소유자, 서비스 등을 의미하며, 각 구문에서 상호작용 메커니즘을 이용할 수 있다. 이에 대한 예는 메일, 전화, HTTP, SOAP, SSL/TLS 등과 같은 서로 다른 통신 방법이다.

모든 실체의 메커니즘과 구문은 속성 또는 특징 집합으로 기술된다. 이들 속성 형태와 값은 실체에 대한 유일한 식별을 위해 사용될 수도 있고, 분류 또는 그룹화를 위해 사용될 수 있다. 또한, 어떤 속성은 불가피하게(또는 반드시) 사용될 수 있다. 불가피한 속성은 외부 기관의 참조 없이 자신의 객체를 식별할 수 있으며, 이의 예는 비밀키/공개키 쌍, 지문과 같은 공유된 비밀이다. 모든 다른 속성 값은 발행자 또는 속성 기관에 의해서 실체의 불가피한 속성 경계에 위치한다. 보안 정책은 다른 객체, 상호작용 메커니즘과 구문, 구성된 속성값 상의 특정 제약과 속성, 속성들 사이의 관계에 대한 구문이다. 정책 구문(또는 규칙)은 실체들(예를 들어, 객체, 사용자 속성 등), 자원과 환경 특성(예를 들어, 시간, 지역, 목적, 신뢰 레벨 등) 등에 대해서 표현할 수 있다. 이들 보안 정책은 인증, 인가, 위임, 신뢰, 보증, 신원 매핑 등을 포함한 다양한 형태를 가지고 있다.

(그림 2)는 보안 정책 관리, 표현, 공개, 발견, 통신, 검증, 실행, 조정과 같은 작업을 용이하게 수행하기 위한 상호 작용 과정으로 각 실체에 대한 보안 서비스로 정의한다. 다시 말해, 그림에서 정책 시행 자체가 궁극적인 목표이고, 보안 서비스는 이 목적을 지원하기 위해서 설계되고 시행되는 서비스의 한 예로 본다. (그림 2)는 자원에 대한 인가 정책을 부여하는 과정을 보여주고 있다. 자원에 대한 인가 정책은 사용자 이름, 역할, 멤버십 등과 같이 관련된



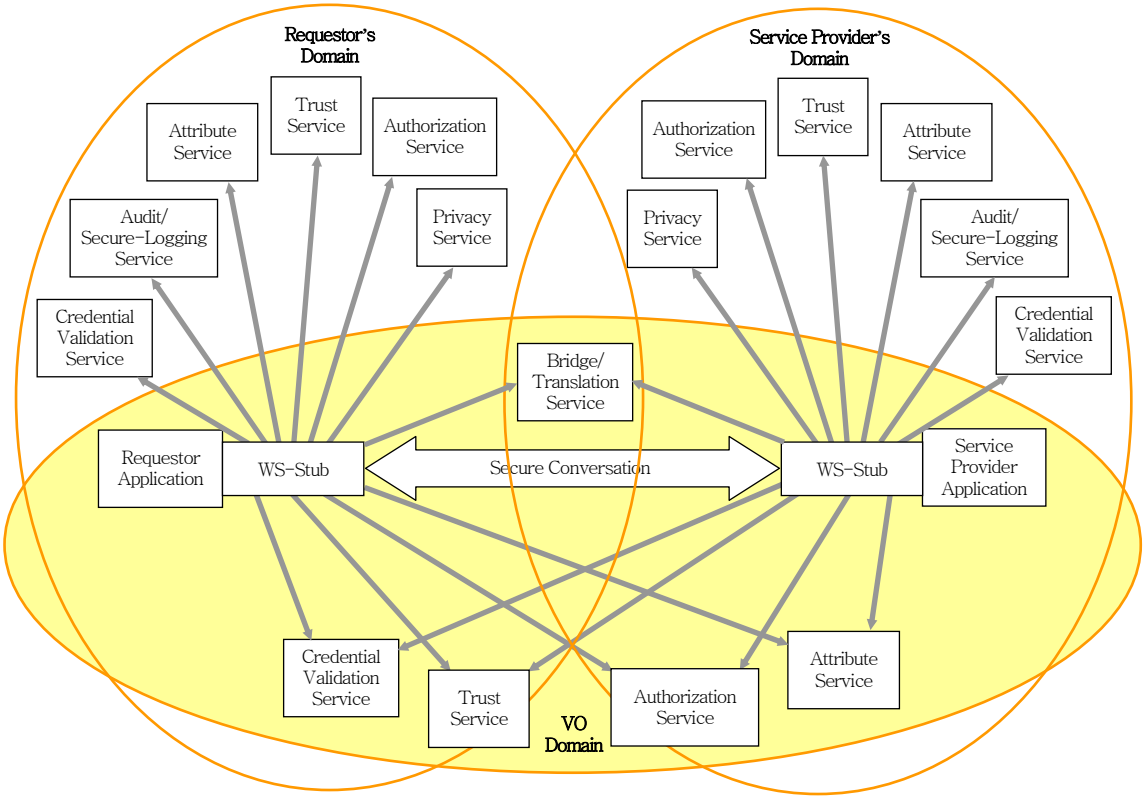
(그림 2) 보안 정책 결정과 시행 예

실체의 속성값에 대한 규칙들로 나타나게 된다. 사용자가 초기 인증과정으로 제출한 신임장(예를 들어, X.509 인증서, Kerberos 티켓 등)에서 공개키와 관련된 비밀키의 소유 여부와 반드시 요구되는 속성값을 제출 받고, 이를 검증한다. 검증이 끝난 사용자에게 적절한 인가 정책을 부여하기 위해서 정책 결정을 하게 되고, 이를 통해 사용자는 자원에 접속할 수 있는 권한을 획득하게 된다. (그림 2)와 같은 정책 결정은 [RFC2903], [Liberty] 또는 다른 기관에서 정의한 일반적인 웹서비스 보안 모델 및 분산된 컴퓨팅 구조와 다르지 않다. 다만 그리드 애플리케이션은 실체와 상호 교차하고 있는 조직과 패턴들에 대한 별도의 역할을 지정하고, 그들 사이의 상호 작용을 가능하게 하기 위해서 그리드의 특성을 고려한 보안 서비스를 추가적으로 제공하고 있다.

라. 보안 서비스 기능

(그림 3)은 OGSA 보안 서비스에서 제공하는 기능을 명확하게 보여주고 있으며, 요청자와 서비스 제공자 도메인이 속한 보안 서비스에서 상호간에 call-out하고, 정책의 협상과 허가를 확실하게 하기 위한 방안을 설명하고 있다. 이 그림에서 정의하고 있는 OGSA 보안 서비스 기능은 정책 시행이 이와 같이 처리될 수 있다라는 하나의 예제로 그리드 애플리케이션 개발자를 위한 보안 특정 코드 유지에 도움을 주기 위한 것이다. 또한, 그림은 그리드에서 요청자와 제공자, 가상 조직 정책에 의해 다른 조직에서 관리되는 다른 보안 서비스 인스턴스에 call-out이 만들어지는 것을 분명하게 보여준다. (그림 3)에서 제시하고 있는 OGSA 보안 서비스의 대표적인 기능은 다음과 같다.

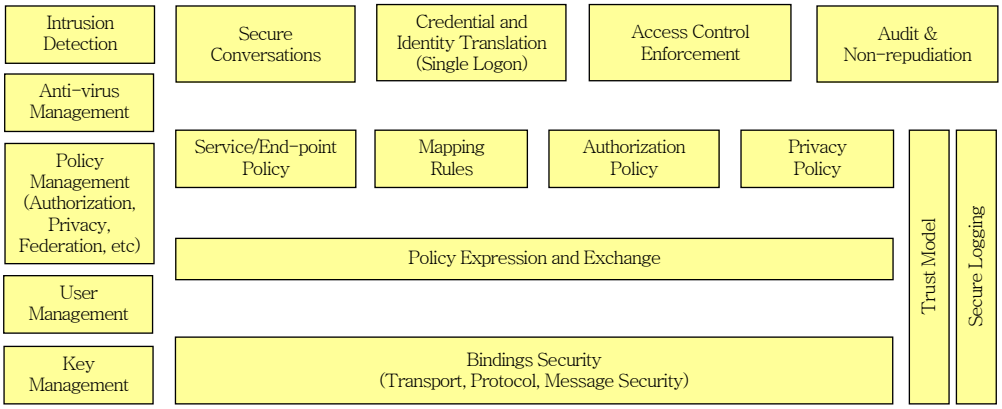
- 인증(authentication): 인증 서비스는 신원 증명을 위해서 제시된 신임장의 검증과 신뢰 서비스의 형성에 관여한다. 인증의 예는 사용자 ID와 패스워드 조합의 평가와 Kerberos 메커니즘을 이용한 서비스 요청자 인증이다.
- 신원 매핑(identity mapping): 신뢰 서비스와 브리지/변환 서비스는 서로 다른 도메인 내에서 하나의 주체 도메인(예를 들어, 요청자 또는 서비스 제공자 도메인)에 존재하는 신원 변환 기능을



(그림 3) 가상 조직에서의 보안 서비스

제공한다. 신원 매핑의 예는 X.509 인증서의 X.500 DN을 식별하는 것이다.

- 인가(authorization): 인가 서비스는 정책 기반 접근 제어 결정에 관여된다. 인가 서비스는 인증된 서비스 요청자의 신임장을 통해서 인가 정책에 의한 서비스 요청자의 자원 접근 권한을 허가해 준다. OGSA에 적합한 인가 서비스를 위해서는 호스팅 환경에서 접근 제어 기능을 제공하고, 실시되고 있는 인가 정책의 세분화를 하는 것이 적당하다.
- 신임장 변환(credential conversion): 신뢰 서비스와 브리지/변환 서비스는 신원 매핑과는 다른 형태의 신임장 또는 다른 신임장 형태로부터의 변환 기능을 제공한다. 그룹 회원, 특성, 속성과 주장을 조정하는 것은 실체(예를 들어, 서비스 요청자와 제공자)와 결합하는 신임장 변환 작업을 포함할 수 있다. 예를 들어, 신임장 변환 서비스는 Kerberos 신임장을 인증 서비스가 요구하는 다른 신임장 형태로 변환하는 것이다. 보안 정책에 의한 신임장 변환 서비스는 서로 다른 서비스의 상호운용을 용이하게 할 수 있다.
- 감사/보안 로깅(audit/secure-logging): 감사와 보안 로깅 서비스는 신원 매핑 및 인가 서비스와 유사한 정책 기반 서비스이다. 이들 서비스는 보안 서비스와 관련된 이벤트를 추적하는 기록을 생성하기 위한 서비스이다. 이의 결과로 시행중인 보안 정책을 줄이거나 고찰할 수 있다.
- 프라이버시(privacy): 프라이버시 서비스는 개인 식별 정보(PII)의 정책 기반 분류에 관여된다. 서비스 요청자와 제공자는 프라이버시 서비스를 사용하고 있는 개인 식별 정보를 저장할 수도 있다. 프라이버시 서비스는 가상 조직 내에서 프라이버시 정책을 명확하게 표현하고 적용 및 실시하기 위한 목적으로 사용될 수 있다.



(그림 4) 그리드 보안 모델의 구성 요소

이와 같은 보안 서비스 구성 요소들의 관계는 (그림 4)와 같이 계층화된 서비스 스택으로 표현된다. 서비스 요청자와 제공자에 의해서 사용되는 모든 보안 인터페이스는 OGSA에 적합하도록 표준화되어야 한다. OGSA에 적합한 구현은 기존 서비스 인터페이스를 이용할 수도 있고, 새롭게 구성하거나, 추가를 통해서 정책을 정의할 수도 있다. 특별히 보안 서비스와 관련된 인터페이스의 적절한 구현은 OGSA 내에서 결합되어 제공하는 대안적인 보안 서비스를 제공할 수 있다.

마. 보안 서비스 특성

일반적으로 보안 서비스의 특성은 실시되는 보안 정책의 지속적인 기술 요구사항에 의해서 결정된다. 예를 들어, 정해진 보안 정책을 실행하기 위해서 최대 대기 시간, 응답 시간, 유효성, 복구와 같은 속성 변환과 보안 서비스 계층은 정해진 보안 서비스에 의해서 적용되어야 한다. 많은 경우, 보안 서비스 구현은 다른 서비스의 이용을 통해서 적합한 특성을 구성할 수 있다. 예를 들어, 속성 정보 서비스는 디렉토리(예를 들어, LDAP) 또는 데이터베이스(예를 들어, RDBMS)에서 주장 정보에 접근하기 위한 데이터 서비스를 사용할 수 있고, 정해진 보안 정책을 시행하기 위해서 필요로 하는 적용 특성을 위해 그들 서비스 특징적인 미러링(mirroring) 데이터를 이용할 수 있다.

바. 다른 OGSA 서비스와의 상호 작용

일반적으로 OGSA 서비스 시작은 서비스와 관계된 모든 보안 정책 시행에 종속된다. 어떤 경우, 보안 정책은 묵시적으로 시행되며, 변경하지 못하게 코드화된다. 또 다른 경우, 외부 보안 서비스 구조와의 plug-in 또는 call-out이 필수적이다. 이와 같은 측면에서, 모든 OGSA 서비스는 보안 서비스 위에 계층화되고, 이를 의존하게 된다. 또한, 보안 서비스와 요구사항은 다른 OGSA 서비스의 더 상위 계층과 밀접한 관련이 있다. 예를 들어, 속성 서비스의 구현은 레지스트리 또는 데이터베이스로부터 정책을 검색하기 위해서 OGSA 데이터 서비스 사용자에게 관련된 서비스를 제공할 수 있다. 따라서 OGSA 보안 서비스는 다른 OGSA 서비스의 소비자일 수 있다.

3. OGSI와 WSRF

OGSA가 분산 컴퓨팅 환경을 만들기 위해서 그리드 기술과 웹서비스 기술을 통합한 구조라고 한다면, OGSI는 OGSA 구조가 기반으로 하고 있는 그리드 서비스에 대한 기본 인프라를 정의하기 위한 것으로, 2003년 6월에 제안되었다. OGSI에서는 그리드 서비스를 생성하고 관리하며, 정보를 교환하는 것에 대한 인터페이스와 기술적 사항을 명확히 정의하고 있다[5]. 웹서비스를 명시하는 방법으로 WSDL

을 사용하고 있는데, OGSI에서는 그리드 웹서비스를 명시하기 위해 WSDL을 확장해서 사용하고 있다. OGSI는 현재 OGF에서 폐지된 상태이며, 이의 기능은 WSRF에 의해 대신하게 되었다. OGF의 웹서비스 그룹은 WSRF을 이용하여 본래 OGSI를 이용해 기술하려던 그리드 웹서비스를 명시하고 있으며, 이를 통해서 OGF가 추구하는 웹서비스 기반으로 이양에 한층 가까워지게 되었다[6]. OGSI는 그리드를 구성하기 위해서 대표적으로 이용되는 GT3에서 구현되었으며, WSRF는 GT4에 구현되었다.

Ⅲ. 그리드 웹서비스와 보안 기술의 개발 및 적용 현황

본 장에서는 앞서 살펴본 OGSA에 적용하기 위해 연구되고 있는 대표적인 웹서비스 보안 기술에 대한 간략한 개요[7]와 이들 기술의 실제 적용 현황을 살펴본다.

1. 웹서비스 보안 기술

가. SAML

SAML은 OASIS에 참여한 많은 업체들의 상호 협력적인 노력에 의해 작성되었으며, SAML v1.0과 v1.1을 거쳐 2005년 3월에 SAML 2.0이 표준으로 승인되었다. SAML의 초기 버전은 브라우저 기반의 SSO을 제공하는 데 목적이 있었으나, 점차 통합 identity 관리와 웹서비스 보안 토큰으로서의 역할이 가능하도록 범위가 확장되었으며, 그리드, healthcare, e-비즈니스 등 대부분의 웹서비스 보안 프레임워크에 수용되고 있다[8].

나. XACML

XACML은 2003년에 v1.0이, 2005년 2월에 v2.0이 표준으로 승인되었다. XACML은 초기 접근 제어를 위한 표준으로서의 역할을 수행하였지만, v2.0에 와서는 다양한 응용 프로파일(RBAC, 다중 자원, 개인 보안 정책, XML 전자서명 등)을 위한 접근 제어를 수행할 수 있도록 다양한 문서를 제공하고 있고, SAML v2.0과의 연동을 통해서 인증, 인가, 위임, 접근 제어 등의 웹서비스 보안을 제공하기 위한 응용으로 확장되었다. 현재는 v3.0에 대한 표준화 작업을 진행하고 있다[9].

다. WS-Security

WS-Security는 OASIS에서 표준화를 진행하고 있으며, 단일 표준 문서라기 보다는 SOAP, Kerberos, X.509 인증서 등의 다양한 보안 프로토콜을 웹서비스에 적용하는 데 있어서 고려되는 보안 사항들에 대한 문서 집합이라고 할 수 있다. WS-Security 문서의 핵심은 2004년에 표준으로 승인된 'Web Services Security v1.0'이며, SOAP 메시지에 대한 보안을 제공하기 위한 SOAP 확장들의 정의와 이들에 대한 구문 및 처리 방법을 규정하고 있다. 현재는 'Web Service Security v1.1' 제정을 위한 표준화를 진행하고 있다[10].

라. WS-SecurityPolicy

WS-SecurityPolicy는 IBM, MS 등의 상용 업체가 공동으로 표준화 작업을 수행하고 있다. WS-SecurityPolicy는 SOAP 메시지 보안, WS-Trust, WS-SecureConversation의 웹서비스 보안에서 일반적인 보안 정책을 정의하고 주장하기 위한 목적으로 WS-Policy의 부록으로 사용되며, 2005년에 v1.1을 공개하였다[11].

마. WS-SecureConversation

WS-SecureConversation은 보안 문맥 설정과 공유, 세션키(session key) 파생을 가능하게 하는 확장 기능을 제공하기 위해서 IBM, MS 등의 상용 업체가 공동으로 표준화 작업을 수행하고 있으며, 통신 보안 측면에서 메시지 인증 모델에 중점을 두고 있다. 2004년에 v1.0이, 2005년 2월에 기존 문서를 업데이트한 버전이 공개되었다[11].

바. WS-Trust

WS-Trust는 IBM, MS 등의 상용 업체가 공동으로 표준화 작업을 수행하고 있다. WS-Trust는 WS-Security에서 제공되는 보안 메시지를 위한 기본 메커니즘을 기반으로 구현되어 다양한 신뢰 도메인 내에서 보안 토큰의 발행 및 교환 방법과 신뢰 관계의 존재 설정 및 접근 방법에 대한 확장을 정의하고 있다. 2004년에 v1.0이, 2005년 2월에 기존 문서를 업데이트한 버전이 공개되었다[11].

2. 보안 기술의 개발 및 적용 현황

가. OGF

OGF는 그리드 컴퓨팅을 위한 환경 조성과 제공, 전개와 그리드 기술과 애플리케이션의 개발 및 기술 분석서, 사용자 경험서, 개발 지침서 등의 문서를 작성하기 위한 목적으로 설립된 포럼으로 그리드 관련 표준안 제정과 공표, OGF 회의 개최, 그리드 관련 기술의 개발 및 운영에 대한 주요 역할을 수행하고 있다. OGF에서 본 고의 내용과 관련한 표준화를 진행하고 있는 작업그룹은 'Open Grid Services Architecture (ogsa-wg)', 'OGSA Authorization (ogsa-authz-wg)' 등이며, 이외에도 다수의 작업 그룹과 연구 그룹이 그리드 웹서비스에 대한 연구를 진행하고 있거나, 성공적인 활동을 종료하였다.

ogsa-wg는 OGSA 서비스들을 위한 기능, 통합, 우선 순위, 상세 명세 등에 관한 문서를 개발하는 표준화 기술 작업그룹으로, 그리드 웹서비스의 통합을 달성하기 위하여 상세화된 문서를 개발하고, 각종 서비스에 대한 기능과 인터페이스 등을 표준화하고 있다. ogsa-authz-wg는 OGSA 프레임워크에서 인가 컴포넌트를 위한 기본적인 상호운용성과 기능 확장에 필요한 명세를 정의하기 위한 표준화를 진행하고 있다[12].

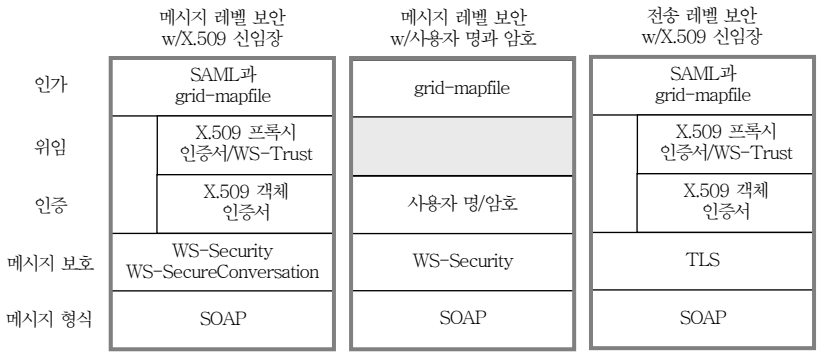
현재 OGF에서 그리드 웹서비스 보안 기술에 대해서 중점적인 연구를 수행하고 있는 부분은 그리드에서 제공하는 인가 서비스에 대한 분야이다. 이를 담당하는 ogsa-authz-wg에서는 SAML을 인가 서비스 제공을 위한 주요 기술로 결정하고, 이에 대한 속성, 인가서비스 시나리오, 정책 및 요구 사항 등에 대한 표준화를 진행하고 있다. OGF에서 도입한 SAML은 클라이언트가 요청하는 서비스에 인가 결정을 위한 통신을 허용하는 OGSI 인가 서비스로부터의 인가 주장과 결정을 요청하고 표현하기 위한 목적으로 사용되며, 현재 SAML v1.1을 기반으로 그리드에서 요구하는 기능을 추가하기 위해서 기존의 버전에 새로운 확장을 추가하여 표준화 되었다. 한편 XACML을 포함한 새로운 SAML 인가 기능을 포함한 버전은 SAML v2.0의 도입과 함께 연구될 예정이다. <표 1>은 OGF에서 현재까지 제정된 그리드 웹서비스 및 웹서비스 보안 기술 중에서 본 고에서 인용한 주요 표준 문서 목록이다.

〈표 1〉 그리드 웹서비스 보안 기술 관련 주요 표준안

번호	제목	형태
GFD.81	Open Grid Services Architecture Glossary of Terms Version 1.5	INFO
GFD.80	The Open Grid Services Architecture, Version 1.5	INFO
GFD.72	OGSA™ WSRF Basic Profile 1.0	REC
GFD.67	OGSI Authorization Requirements	INFO
GFD.66	Use of SAML for OGSI Authorization	EXP
GFD.59	OGSA Profile Definition Version 1.0	INFO
GFD.57	Attributes Used in OGSI Authorization	EXP
GFD.31	Open Grid Service Infrastructure Primer	INFO

나. 글로버스 프로젝트

글로버스는 OGF에서 제정한 표준을 바탕으로 그리드를 구성하기 위해 필요한 미들웨어를 개발하고, 이를 배포하기 위한 프로젝트로 글로버스에서 배포하는 글로버스 툴킷(globus toolkit)은 현재 그리드를 구성하기 위한 미들웨어로 가장 널리 활용되고 있다. 글로버스에서 현재 제공하고 있는 GT4에서는 웹서비스와 관련한 다수의 컴포넌트를 제공하고 있다. GT4에서 제공하고 있는 그리드 웹서비스



(그림 5) 웹서비스 기반의 GSI 계층 구조

보안 기술은 (그림 5)와 같이 메시지 레벨, 전송 레벨과 SAML을 이용한 인가 프레임워크 등으로 구성된다[13].

1) 메시지 보안

GT4에서는 그리드 웹서비스간 통신을 위해서 SOAP 메시지 프로토콜을 사용한다. 메시지 보안은 TLS 상에서 SOAP 메시지를 전달하는 방법과 WS-Security 규격을 사용하여 SOAP 메시지 부분에 대한 암/복호화를 통해서 제공하는 방법이 있다.

① 전송 레벨 보안

전송 레벨 보안은 TLS에 의해서 보호되는 네트워크 상에서 SOAP 메시지를 전달하며, SOAP 메시지에 대한 무결성과 프라이버시 보호를 암호화를 통해서 제공한다. 전송 레벨 보안은 메시지 레벨 보안에 비해서 향상된 성능을 제공한다. 전송 레벨 보안에서는 인증을 위해서 X.509 인증서와 관련된 보안 토큰을 일반적으로 사용하지만, 인증 없이 메시지를 보호하기 위한 목적으로 사용하는 경우도 있으며, 이를 '익명 전송 레벨 보안(anonymous transport-level security)'이라고 부른다. 익명 전송 레벨 보안에서는 SOAP 메시지 또는 통신이 신뢰받기 위해서 ID/PW와 같은 다른 인증 수단을 필요로 한다.

② 메시지 레벨 보안

SOAP 특수화는 전자서명, 무결성 보호, 암호화와 같은 다른 보안 페이로드를 애플리케이션 특화 부분의 페이로드로 추상화하는 것을 허용한다. 또한, 다른 웹서비스를 위해 SOAP 메시지를 통한 일관된 방법으로의 GSI 보안 서비스 적용이 가능하다. GT4에서는 SOAP 메시지에 대한 보안을 제공하기 위해서 WS-Security와 WS-SecureConversation을 적용한다. WS-Security는 OASIS에서 표준화 되었으며, 개개의 SOAP 메시지에 보안을 적용하기 위한 보안 프레임워크이다. WS-SecureConversation은 IBM, MS 등이 상용 업체에서 제안한 규격으로 초기 메시지 교환 이후에 메시지를 보호하기 위해 사용될 수 있는 보안 컨텍스트를 확립하기 위한 보안 프레임워크이다. WS-Security와 WS-SecureConversation에서 보안 서비스를 제공하기 위해서 사용되는 인증서는 특수한 형태로 구성되어 있다. GT4에서는 ID/PW와 X.509 인증서를 사용하여 WS-Security 표준에 정의되어 있는 인증을 수행한다. X.509 인증서가 사용될 경우에 GT4는 다음과 같은 사항을 위해 추가적인 보호 메커니즘을 사용하거나, WS-Security 또는 WS-SecureConversation과 결합하여 사용한다.

- 무결성 보호(integrity protection): 수신자가 전송자로부터 전달되어온 메시지가 변경되지 않았다는 사실을 검증할 수 있다.
- 암호화(encryption): 메시지는 비밀성을 제공하기 위해서 보호될 수 있다.
- 재생 방지(non-replay): 수신자가 이전에 같은 메시지를 받지 않았다는 것을 검증할 수 있다.

이와 같은 보호를 위한 방법은 WS-Security와 WS-SecureConversation 사이에 변화를 주는 것이다. WS-Security의 경우에서 전송자와 수신자의 X.509 인증서와 함께 키가 구성되어 사용된다. WS-SecureConversation의 경우에는 X.509 인증서는 메시지 보호를 위해 제공되는 세션키를 확립하기 위해서 사용된다.

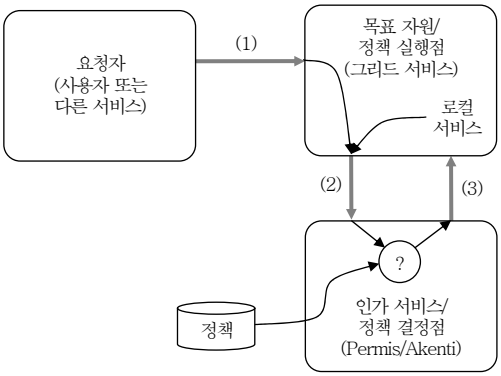
2) 인가 서비스

GT4의 웹서비스 기반 인가 프레임워크는 컨테이너 레벨 인가를 위한 프레임워크를 제공한다. 이 프레임워크는 인가 모듈과 서비스와 같은 컨테이너에 속한 여러 객체들과의 연계를 위한 인터페이스를 제공하며, SAML 프로토콜을 이용하여 다른 서비스와의 인가 결정을 위한 모듈의 구현을 지원한다. GT4의 인가 프레임워크는 다음과 같은 특징을 가지고 있다.

- 그리드 맵 파일(gird-mapfile)과 다른 ACL 기반의 인가 서비스 제공
- 주문형(사용자 및 서비스가 요구하는) 인가 모듈 구현 방안 제공

① SAML 인가 모델

GT4의 SAML 인가 모델은 (그림 6)과 같이 PEP와 PDP 사이의 메시지 교환으로 이루어진다. 이 사이에서 교환되는 메시지는 인가 결정을 위한 구문인 AuthorizationDecisionStatement이다. (그림 6)에서 인가를 위한 메시지 흐름은 다음과 같은 순서로 이루어진다.



(그림 6) GT4에서의 SAML 흐름

1. 요청자가 자원에 접속한다.
2. 서비스를 생성하고, 인가 서비스에 SAML AuthorizationDecisionQuery를 전달한다.
3. 인가 서비스는 요청에 대한 정책을 평가하고, 하나 이상의 AuthorizationDecisionStatement로 SAML 주장을 인코드하여 응답한다.
4. AuthorizationDecisionStatements에 정의된 정책에 따라 요청자에게 권한을 허가한다.

② SAML 인가 요소

SAML 인가 서비스를 위해 새롭게 정의된 요소는 큰 범주로 보았을 때 다음과 같이 AuthorizationDecisionQuery와 Assertion 요소로 나누어진다.

- AuthorizationDecisionQuery: 인가 서비스에 권한을 획득하기 위한 주장을 요청하기 위해 사용
- Assertion: 한 개체의 다른 권한을 주장하기 위해서 사용되며, GSI에서는 Assertion 요소에 포함되는 AuthorizationDecisionStatements 요소를 추가하였다.

다. EGEE

EGEE의 그리드 보안 기반 구조는 웹서비스 보안 기술을 적용하기 위해서 크게 두 가지 메커니즘을 도입하고 있다. 하나는 Apache Axis와 Tomcat과 같은 컨테이너와 애플리케이션 서버에서 호스트되는 웹서비스의 도입으로, EGEE의 미들웨어 구조에서 큰 부분을 차지하고 있다. EGEE는 메시지 전송을 위한 웹서비스 기반 구조를 위해 XML 기반의 더 나은 수준의 전송레벨 보안(예를 들어, SOAP, HTTPS)을 적용하고 있으며, 실제 종단-대-종단(end-to-end) 보안 요구사항을 대체하고 있다. 하지만, 기존의 소프트웨어와 표준들이 그리드에서 요구하는 보안 수준보다 더욱 발전되었기 때문에 웹서비스 보안 기술의 적용을 통해서 확실한 보안을 제공할 수 있다. WS-Security 메시지 레벨 보안은

EGEE에서 전달되는 정보에 대한 상호운용성의 보장과 안전을 책임진다. 또 다른 하나는 GridFTP와 같이 웹서비스에 기반을 두지 않는 다른 프로토콜에 의한 보안 제공으로 기존의 프로토콜에 그리드를 위한 확장 또는 수정을 가하여 적용하고 있다[14], [15]. 현재 EGEE에서는 2007년까지 메시지레벨의 보안 서비스의 제공과 동적인 신뢰, 보안 컨텍스트의 관리, 가상 조직에 대한 보안 주장을 위한 연구를 수행하고 있으며, 이를 위해 WS-Security, WS-ReliableMessaging, WS-SecureConversation 등의 웹서비스 보안 기술을 인증 및 인가 절차에 적용하고 있다.

라. IBM

IBM은 웹서비스 보안 기술의 개발과 표준화에 선도적인 업체로 그리드를 비즈니스적 관점에서 새로운 수익을 창출할 수 있는 커다란 시장으로 인식하고, 이에 대한 상업화를 적극적으로 추진하고 있으며, IBM Grid and Grow™을 그리드를 도입하는 기업들을 위한 통합 솔루션으로 제공하고 있다. IBM에서는 그리드를 '서비스 지향적인' 독립적인 산업으로 보고, 웹서비스를 분산 처리와 그리드를 지원하는 기능들을 구성하기 위한 가장 적합한 기술로 간주하고 있다. 웹서비스는 그리드가 가지는 유연하고 동적인 시스템 특성을 잘 반영할 수 있는 이상적인 기술로, IBM은 그리드에 웹서비스 도입하기 위해 WSRF, WS-Notification을 제안하였으며, 이를 통해서 '상태 기반'의 그리드 웹서비스 환경을 제공하고 있다[16]. 또한, 최근에는 MS, Intel, HP 등과 컨버전스 계획을 진행하고 있으며, 보안을 위한 WS-Security, 서비스 레벨 관리를 위한 WS-Agreement, 보안 정책 표현을 위한 WS-Security-Policy와 같은 중요한 기능을 추가하기 위한 표준화를 진행하고 있다.

● 용 어 해 설 ●

웹서비스 보안 기술(Web Services Security Technology): 다수 응용들 간의 안전한 문서 전송, 접근 제어와 인가, 인증 등의 보안 서비스를 제공하기 위해 웹서비스 기술표준을 적용한 표준 보안 기술. 기술 특성에 따라 XML 정보보호 기술, 웹서비스 보안 프레임워크 기술, 웹서비스 응용 보안 기술 등으로 구분된다. 본 고에서 언급된 웹서비스 보안 기술 중 SAML, XACML은 XML 정보보호 기술, WS-*는 웹서비스 보안 프레임워크 기술의 범주에 속한다.

Ⅳ. 결론

본 고에서는 지금까지 OGF에서 제정한 표준 문서와 실제 그리드를 구축하고 운영하고 있는 기관에서 제공하는 백서를 중심으로 한 그리드 웹서비스 보안 서비스에 대한 기술 동향에 대해 살펴보았다. 이를 통해 그리드에서 웹서비스와 웹서비스 보안 기술을 적극적으로 도입하는 이유와 앞으로의 연구 방향을 파악할 수 있었다. 현재 그리드 기술 개발은 웹서비스와 기존 그리드 기술을 결합하는 방향으로 급격히 전환되고 있으며, EGEE, 글로버스를 비롯한 그리드 프로젝트, IBM을 비롯한 상용 그리드 구축에 적극적으로 도입되고 있다. 웹서비스 보안 기술은 그리드 웹서비스에 대한 안정성과 신뢰성을 높이기 위해서 반드시 도입되어야 하는 기술이다. 현재 그리드에서 도입하고 있는 다양한 웹서비스 보안 기술을 설명하였지만, 그리드 웹서비스 보안 서비스에서 가장 큰 문제는 도입하려는 웹서비스 보안 기술의 발전이 매우 빠르며, 새로운 기술이 지속적으로 등장하고 있다는 점이고 그리드에 적합한 표준의 부재로 인하여 기존 웹서비스 보안 기술에 대한 수정 및 확장이 요구된다는 점이다. 이로 인하여 그리드에 웹서비스 보안 기술을 도입하려는 시도는 상대적으로 늦어질 수밖에 없다. 하지만, 현재의 표준화 및 기술 발전 속도를 보았을 때, 그리 멀지 않은 시점에 그리드 웹서비스 보안 서비스의 안정적인 제공이 가능해질 것으로 판단된다.

약 어 정 리

DN Distinguished Name

EGEE	Enabling Grids for E-sciencE
GGF	Global Grid Forum
GSI	Grid Security Infrastructure
GT4	Globus Toolkit version 4
OGF	Open Grid Forum
OGSA	Open Grid Service Architecture
OGSI	Open Grid Service Infrastructure
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PII	Personally Identifiable Information
SAML	Security Assertion Markup Language
SOAP	Simple Object Access Protocol
WS-Security	Web Services Security
WS	Web Services
WSDL	Web Services Description Language
WSRF	Web Services Resource Framework
XACML	eXtensible Access Control Markup Language

참 고 문 헌

[1] 허의남, "글로벌 신경망, 그리드(GRID) 기술," 오라클 매거진, 2004.

[2] 윤훈주, "유비쿼터스와 그리드컴퓨팅," 유비유넷 리포트, 제2호, 2006. 2.

[3] 함재균외 3명, "웹 서비스를 통한 그리드의 진화," GFK (Grid Forum Korea) 기술 동향, 2006.

[4] I. Foster 외 11명, "The Open Grid Services Architecture, Version 1.5," GGF Standard, July 2006.

[5] S. Tuecke, "Open Grid Services Infrastructure (OGSI) Version 1.0," GGF Standard, June 2003.

[6] TTA, "개방형 그리드 서비스 하부구조에서 WS-RF로의 변환," TTA Standard, Dec. 2005.

[7] 김주한 외 7명, "웹서비스 보안 기술의 표준화 및 시장 동향," 전자통신동향분석, 제20권 제1호, 2005. 2., pp.43-53.

[8] OASIS Security Service TC, http://www.oasis-open.org

[9] OASIS eXtensible Access Control Markup Language (XACML) TC, http://www. oasis-open.org

[10] OASIS Web Services Security (WSS) TC, http://www.oasis-open.org

[11] IBM, http://www-128.ibm.com/developerworks/library/specification/ws-polfram/

[12] http://www.ogf.org

[13] http://www.globus.org/toolkit/security/

[14] EGEE, "Global Security Architecture," EGEE Document, Aug. 2004.

[15] Yuri Demchenko 외 3명, "Security Architecture for Open Collaborative Environment," LNCS 3470, Feb. 2005.

[16] IBM, "Grid Computing: Past, Present and Future, an Innovation Perspective," IBM Whitepaper, June 2006.