웹서비스 용어 (Web Services Glossary)

1. 개요

1.1. 목적 본 문서는 웹서비스에서 사용되는 웹서비스 용어에 대해 설명한 용어집이다.

1.2. 개요 본 문서에는 웹서비스를 위해 사용하는 웹서비스 관련 기술 용어들에 대해 정의하고 있다. 영문의 경우 의미 있는 용어는 대문자로 표기되고 그렇지 않은 경우에는 소문자로 표시된다. 본 문서에 있는 정의의 일부는 외부 문서에서 추출된 약어를 사용하며, 출처를 [ ]와 같은 형태로 표기하였다.

2. 정의

접근 (access)

시스템 엔터티의 리소스 일부 또는 전부의 표현을 조작, 사용, 얻기, 인식 또는 가져오기 위해 시스템 엔터티와 상호 작용하는 작업. [RFC 2828]

접근 제어 (access control)

인증되지 않은 접근으로부터 리소스 보호: 리소스의 사용이 보안 정책에 따라 제한되며 해당 정책에 따라 인증된 시스템 엔터티에만 허용되는 프로세스. [RFC 2828]

접근 제어 정보 (access control information)

1. 컨텍스트 정보를 포함하여 접근 제어를 위해 사용되는 모든 정보. [X.812]

2. 컨텍스트 정보에는 소스 IP 주소, 암호화 세기, 요청된 작업의 종류, 시간 등이 포함된다. 접근 제어 정보의 일부는 요청 자체에 특정한 정보이거나, 요청이 전송된 연결과 연관된 정보이거나, "환경적"인 정보 (예를 들어 시간)일 수 있다. [RFC 2829]

접근 권한 (access rights)

대상이 리소스에 대해 가질 수 있는 인증된 상호 작용의 유형에 대한 설명. 예를 들어 읽기, 쓰기, 실행, 추가, 수정 및 삭제 등이 있다. [WSIA 용어 설명]

작업자 (actor)

1. 웹서비스의 사용을 원하거나 웹서비스를 제공하는 에이전트의 소유자일 수 있는 개인 또는 조직.

2. 작업을 수행할 수 있는 물리적 또는 개념적 존재. 예: 개인, 회사, 기계, 소프트웨어 실행. 작업자는 하나 이상의 역할을 처리하거나 구현할 수 있다. 일정 추상화 단계의 작업자는 더 낮은 추상화 단계의 역할을 하는 것으로 표시될 수 있다.

에이전트 (agent)

에이전트는 개인 또는 조직 대신 작업하는 프로그램이다. (이 정의는 [Web Arch]에 있는 정의의 제한된 정의이다. [Web Arch]의 소프트웨어 에이전트의 개념에 해당된다.)

익명성 (anonymity)

이름이나 신분이 알려지지 않거나 숨겨진 조건인 익명의 품질 또는 상태이다. [RFC 2828]

아키텍처 (architecture)

1. 프로그램이나 컴퓨팅 시스템의 소프트웨어 아키텍처는 시스템의 구조이다. 이 구조에는 소프트웨어 구성 요소, 이러한 구성 요소의 외부적으로 보이는 속성, 이들 간의 관계 및 구성 요소에 사용에 대한 제약 조건 등이 포함된다. ([Soft Arch Pract]의 아키텍처 정의에 기반)

2. 소프트웨어 아키텍처는 소프트웨어 시스템의 작동 중 일부 단계 동안의 런타임 요소의 추상화이다. 시스템은 각각에 자체적인 소프트웨어 아키텍처가 있는 여러 수준의 추상화와 여러 작동 단계로 구성될 수 있다. [필딩(Fielding)]

아티팩트 (artifact)

하나의 디지털 정보. 아티팩트의 크기는 제한이 없으며 다른 아티팩트들로 구성될 수 있다. 아티팩트의 예: 메시지, URI, XML 문서, PNG 이미지, 비트 스트림

비동기 (asynchronous)

연관된 메시지가 연대순 및 절차적으로 분리되는 경우 비동기적인 상호 작용이라고 한다. 요청-응답의 상호 작용을 예로 들면, 클라이언트 에이전트는 미래의 불확실한 시점에서 응답을 처리할 수 있다. 이렇게 하기 위한 메커니즘에는 폴링, 다른 메시지 수신의 알림 등이 있다.

속성 (attribute)

개체의 명확한 속성. 개체의 속성이 개체를 설명한다. 개체의 속성은 실제 개체의 크기, 모양, 무게 및 색 등과 같은 물리적 특징에 따라 지정되기도 한다. 사이버 공간의 개체에는 크기, 인코딩 종류, 네트워크 주소 등을 기술하는 특성이 있을 수 있다. [WSIA 용어 설명]

감사 가드 (audit guard)

감사 가드는 작업 및 에이전트를 모니터하여 책임의 이행을 검증하는 소유자 대신 사용되는 메커니즘이다.

인증 (authentication)

인증은 대화의 잠재적 파트너가 어떤 개인 또는 조직 임을 확인하는 프로세스이다. 인가 (authorization) 적용 가능한 접근 제어 정보를 평가하여 대상이 특정 리소스에 대해 지정된 유형의 접근 권한을 갖고 있는지 여부를 결정하는 프로세스이다. 일반적으로 권한 부여는 인증의 컨텍스트에서 수행된다. 대상이 인증되면 여러 종류의 접근을 수행할 수 있도록 권한이 주어진다. [STG]

바인딩 (binding)

1. 인터페이스, 구체적 프로토콜 및 데이터 형식 간의 결합이다. 바인딩은 연관된 인터페이스에 의해 정의된 메시지의 전송에 사용될 프로토콜과 데이터 형식을 지정한다. [WSD Reqs]

2. 인터페이스 및 연관된 작업을 특정 메시지 형식 및 전송 프로토콜에 매핑하는 것.

3. SOAP 바인딩 참조 능력 (capability) 능력은 에이전트가 지원하거나 요청한 것으로 선언된 기능 (특징)의 명명된 부분이다.

커리어그라피 (choreography)

1. 커리어그라피는 어떤 목적 상태를 달성하는데 필요한 작업을 수행하기 위해 공동으로 작업하는 여러 독립적 에이전트가 메시지를 교환하는 순서와 조건을 규정한다.

2. 웹서비스 커리어그라피는 서비스와 사용자 간의 상호 작용에 관련된다. 자동화 여부에 관계없이 웹서비스의 모든 사용자는 해당 서비스의 클라이언트이다. 이러한 사용자는 다시 다른 웹서비스, 응용 프로그램 또는 인간의 사용자일 수 있다. 웹서비스와 해당 웹서비스의 클라이언트 간의 트랜잭션은 실행 시 명확하게 정의되어야 하며 완전한 트랜잭션을 구성하는 구조를 가진 별도의 여러 상호 작용들로 구성될 수 있다. 이러한 구성, 메시지 프로토콜, 인터페이스, 순서 및 연관된 로직을 커리어그라피로 가정한다. [WSC Reqs]

컴포넌트 (component)

1. 컴포넌트는 특정 기능 또는 기능 집합을 캡슐화하여 다른 구성 요소와 상호 작용하기 위한 소프트웨어 개체이다. 구성 요소에는 명확하게 정의된 인터페이스가 있고 아키텍처 내의 모든 구성 요소에 공통으로 미리 기술된 동작을 준수한다. [CCA T&D]

2. 컴포넌트는 소프트웨어 명령의 추상적 단위이며 인터페이스를 통해 데이터의 전환을 제공하는 내부 상태이다. [필딩(Fielding)]

3. 컴포넌트는 경계가 정의된 아키텍처의 단위이다.

기밀성 (confidentiality)

접근를 적절한 사람에게로만 제한하여 정보의 비밀을 유지한다. [NSA 용어 설명]

구성 (configuration)

변경될 수 있는 속성의 집합. 속성은 엔터티의 동작에 영향을 줄 수 있다.

연결 (connection)

통신을 위해 두 프로그램 간에 설정된 전송 계층 가상 회로이다. [RFC 2616]

제어 (control)

상태에 원하는 변경을 가한다. 관리 시스템은 관리 가능한 웹서비스 또는 메시지와 같은 정보 흐름의 주기를 제어할 수 있다.

대화 (conversation)

웹서비스 대화의 경우 여러 메시지 및 참가자가 관여하는 상호 작용 도중 몇 가지 상태를 유지해야 한다.

자격 증명 (credentials)

신분을 증명하기 위해 전송되는 데이터. [X.800]

전송 정책 (delivery policy)

전송 정책은 메시지 전송에 의해 메시지가 전송되는 방법을 제한하는 정책이다.

디지털 서명 (digital signature)

데이터의 모든 수신자가 서명을 사용하여 데이터의 출처와 무결성을 확인할 수 있도록 암호화 알고리즘으로 계산되어 데이터에 첨부되는 값이다. (참조: 데이터 출처 인증 서비스, 데이터 무결성 서비스, 디지털화된 서명, 전자 서명, 서명자) [RFC 2828]

발견 (discovery)

이전에 알려진 바 없고, 특정한 기능적 조건에 일치하는 웹서비스 관련 리소스의 기계가 처리 가능한 설명을 찾는 작업. 여기에는 기능 집합 및 조건을 리소스 설명 집합과 일치시키는 작업이 포함된다. 목표는 적절한 웹서비스 관련 리소스를 찾는 것이다.

발견 서비스 (discovery service)

발견 서비스는 에이전트가 웹서비스 관련 리소스 설명을 검색할 수 있도록 하는 서비스이다.

문서 (document)

디지털 형식으로 나타낼 수 있는 모든 데이터. [UeB 용어 설명]

전자 데이터 교환 (EDI) (Electronic Data Interchange)

둘 이상 조직의 정보 시스템 간의 업무를 위해 미리 정의되고 구조화된 데이터의 자동화된 교환. [ISO/IEC 14662]

도메인 (domain)

도메인은 하나 이상의 정책의 제약 조건을 따르는 에이전트 및 리소스의 식별된 집합이다.

암호화 (encryption)

데이터가 알려지거나 사용되는 것을 방지하기 위해 데이터의 원본을 숨기는 형식(“암호화 텍스트”)으로 데이터를(“일반 텍스트”)로 암호화 전환. 전환을 되짚을 수 있는 경우 해당 반전 프로세스를 “암호 해독”이라고 한다. 이 프로세스는 암호화된 데이터를 원래 상태로 복원하는 전환이다. [RFC 2828]

종점 (end point)

URI 로 지정된 바인딩 및 네트워크 주소 간의 연관으로 서비스의 인스턴스와 통신하는 데 사용될 수 있다. 종점은 특정 프로토콜 및 데이터 형식을 사용하여 서비스에 접근하기 위한 특정 위치를 가리킨다. [WSD Reqs]

게이트웨이 (gateway)

메시지를 아웃바운드 인터페이스를 통해 새 메시지로 나타내기 위해 인바운드 인터페이스의 메시지를 종료시키는 에이전트. 게이트웨이는 프록시와 달리 메시지의 최종 수신자인 것처럼 메시지를 수신한다. 인바운드 및 아웃바운드 인터페이스 간의 가능한 불일치 때문에 변환 프로세스 도중 메시지가 수정되어 의미의 일부 또는 전부가 손실될 수 있다. 예를 들어 HTTP PUT는 SMTP 에 해당하는 것이 없다.

주: 게이트웨이는 SOAP 노드이거나 아닐 수 있다. 하지만 게이트웨이는 메시지를 종료하는 반면 SOAP 는 메시지를 중간에서 중개하기 때문에 게이트웨이는 SOAP중개가 아니다. 게이트웨이는 영구적 역할인 반면 SOAP 중개는 메시지별 역할이다.

등멱원 (idempotent)

수행 회수에 관계 없이 결과 및 부작용이 같은 상호 작용의 속성. [RFC 2616]

안전 상호 작용은 본질적인 등멱원 (idempotent)이다.

식별자 (identifier)

식별자는 리소스에 대한 분명한 이름이다.

초기 SOAP 전송자 (initial SOAP sender)

SOAP 메시지 경로의 메시지 지점에서 SOAP 메시지를 전송하는 SOAP 전송자이다.

무결성 (integrity)

정보가 실수로 또는 악의적으로 변경되거나 파괴되지 않았음을 보증하는 것. [NSA 용어 설명]

느슨한 커플링 (loose coupling)

커플링은 상호 작용 시스템 간의 종속성이다. 이 종속성은 실제 종속성 및 인위적 종속성으로 분리될 수 있다.

1. 실제 종속성은 시스템이 다른 시스템으로부터 소비하는 기능 또는 서비스의 집합이다. 실제 종속성은 항상 존재하며 축소될 수가 없다.

2. 인위적 종속성은 다른 시스템이 제공하는 기능이나 서비스를 소비하기 위해 준수해야 하는 요소의 집합이다. 일반적인 인위적 종속성 요소는 언어 종속성, 플랫폼 종속성, API 종속성 등이 있다. 인위적 종속성은 항상 존재하지만 인위적 종속성 또는 그 비용은 줄어 들 수 있다. 느슨한 커플링은 인위적 종속성이 최소로 축소된 구성을 말한다.

관리 가능 서비스 (manageable service)

웹서비스는 서비스 관리 용도의 추가적인 시매틱, 정책문 및 모니터링과 제어 (또는 관리) 기능 (관리 인터페이스를 통해 노출됨)을 통해 관리 가능한 서비스가 된다.

관리 (management)

안정적인 동작 환경을 만들고 유지하기 위해 값 모니터링, 상태 추적 및 엔터티의 제어를 수행하기 위한 관리 시스템의 관리 기능 활용.

관리 기능 (management capability)

서비스를 제어하거나 모니터링하기 위해 웹서비스가 갖고 있는 기능으로 서비스의 관리만을 목적으로 관리 시스템에 노출될 수 있는 기능.

관리 인터페이스 (management interface)

서비스의 관리 기능이 노출되는 인터페이스.

관리 정책 (management policy)

서비스의 관리 책임 및 권한을 설명하기 위한 용도만으로 웹 서버와 연관된 정책.

관리 시맨틱 (management semantics)

관리별 시맨틱으로 서비스의 시맨틱을 증가시키는 서비스의 관리 시맨틱. 이러한 관리 시맨틱은 서비스의 관리 및 관리 정책에 관련된 효과와 요구 사항을 표현하는 제공자 엔터티와 요청자 엔터티 간의 계약을 형성한다.

메시지 (message)

1. 메시지는 한 웹서비스 에이전트에서 웹서비스의 다른 컨텍스트로 전송되는 데이터의 기본 단위이다.

2. 웹서비스와 요청자 간의 통신의 기본 단위: 하나의 논리적 전송으로 웹서비스 안팎으로 통신할 데이터 [WSD Reqs]

3. 참조: SOAP 메시지

메시지 상호 관계 (message correlation)

메시지 상호 관계는 메시지와 컨텍스트의 연관성을 말한다. 메시지 상호 관계는 요청자 에이전트가 응답을 요청과 일치시킬 수 있도록 한다. (특히 응답이 여러 개일 때)

메시지 교환 패턴 (MEP) (message exchange pattern)

1. 메시지 교환 패턴 (MEP: Message Exchanage Pattern)은 에이전트 간의 메시지 교환을 위한 일반적인 패턴을 설명하는 응용 프로그램 시맨틱의 템플릿이다. 이것은 패턴을 따르는 모든 메시지 교환의 정상적 및 비정상적 종료와 패턴에 따라 교환되는 여러 메시지의 관계 (예: 임시, 원인, 결과 등)를 기술한다.

2. 참조: SOAP 메시지 교환 패턴(MEP).

메시지 수신자 (message receiver)

메시지 수신자는 메시지를 수신하는 에이전트이다.

메시지 신뢰성 (message reliability)

메시지 신뢰성은 메시지가 전송되고 전송자와 수신자가 전송 상태에 대해 동일하게 알고 있는 확실성의 정도를 말한다.

메시지 전송자 (message sender)

메시지 전송자는 메시지를 전송하는 에이전트이다.

메시지 전송 (message transport)

메시지 전송은 에이전트가 메시지를 배달하기 위해 사용할 수 있는 메커니즘이다.

부인 방지 (non-repudiation)

데이터 전송자에게 데이터가 배달되었음을 알리고 데이터 수신자가 전송자의 신분을 확인할 수 있도록 하여 둘 모두 데이터 처리를 거부할 수 없도록 하는 방법. [INFOSEC 용어 설명]

책임 (obligation)

책임은 에이전트 및 리소스의 작업 및 상태를 지정하는 정책의 한 종류이다.

오퍼레이션 (operation)

단일 웹서비스 작업에 관련된 메시지 집합. [WSD Reqs]

오케스트레이션 (orchestration)

오케스트레이션(orchestration)은 일부 유용한 기능을 구현하기 위해 한 웹서비스가 다른 웹서비스를 호출하는 순서와 조건을 정의한다. 즉, 오케스트레이션은 웹서비스 에이전트가 그 목적을 달성하기 위해 따라야 하는 상호 작용의 패턴이다.

사용 권한 (permission)

사용 권한은 에이전트 및 리소스의 허용된 작업과 상태를 지정하는 정책의 한 종류이다.

사용 권한 가드 (permission guard)

사용 권한 가드는 사용 권한 정책을 강화하기 위해 소유자 대신 배포되는 메커니즘이다.

개인 또는 조직 (person or organization)

개인 또는 조직은 웹서비스를 제공하거나 요청하는 에이전트의 소유자가 될 수 있다.

정책 (policy)

정책은 에이전트나 개인 또는 조직의 동작에 대한 제약 조건이다.

정책 가드 (policy guard)

정책 가드는 하나 이상의 정책을 적용하는 메커니즘이다. 소유자를 대신하여 배치된다.

주 사용자 (principal) (principal)

신분이 인증될 수 있는 시스템 엔터티. [X.811]

개인 정보 보호 정책 (privacy policy)

개인 또는 조직이 상호 작용의 결과로 상대방의 개인 데이터를 수집, 처리 (사용) 및 공개하는 방식을 지정하거나 규제하는 규칙 집합.

제공자 에이전트 (provider agent)

소유자 (제공자 엔터티) 대신 서비스와 연관된 작업을 수행할 기능을 갖춘 에이전트.

제공자 엔터티 (provider entity)

웹서비스를 제공하는 개인 또는 조직.

프로토콜 (protocol)

데이터가 전송되는 방식 (특히 네트워크를 통해)을 설명하는 공식화된 규칙의 집합. 저수준 프로토콜은 준수해야 할 전자적, 물리적 표준, 비트 및 바이트 순서, 전송과 오류 검출 및 비트 스트림의 수정을 말한다. 고수준 프로토콜은 메시지의 구문, 컴퓨터 대화 상자에 대한 터미널, 문자 집합, 메시지의 시퀀싱 등을 포함한 데이터 서식을 처리한다. [FOLDOC]

프록시 (proxy)

요청자 에이전트 및 제공자 에이전트 간에 메시지를 전달하는 에이전트로 요청자에게는 웹서비스로 나타난다.

서비스 품질 (quality of service)

서비스 품질은 제공자 엔터티가 서비스 사용자에게 광고하고 받아들이기로 한 책임이다.

참조 아키텍처 (reference architecture)

참조 아키텍처는 하나 이상의 공통 도메인을 공유하는 여러 최종 시스템의 정규화된 아키텍처이다. 참조 아키텍처는 최종 시스템에 공통적인 인프라와 최종 시스템에 포함될 구성 요소의 인터페이스를 정의한다. 그런 다음 참조 아키텍처는 인스턴스화되어 특정 시스템의 소프트웨어 아키텍처를 생성한다. 참조 아키텍처를 정의하면 시스템 클래스에 대한 새로운 소프트웨어 아키텍처를 추출하고 확장하는 데 도움이 된다. 따라서 참조 아키텍처는 특정 대상 소프트웨어 아키텍처와 관련하여 이중의 역할을 수행한다. 먼저 공통 기능 및 구성을 일반화하고 추출한다. 두 번째로 더 안정적이고 비용 효율적으로 사용하는 대상 시스템의 인스턴스화에 대한 기반을 제공한다. [Ref Arch]

레지스트리 (registry)

권한이 있고 중앙 집중식으로 제어되는 정보 저장소.

요청 에이전트 (requester agent)

자신 대신 수행될 작업을 요청하기 위해 제공자 에이전트와 상호 작용하고자 하는 소프트웨어 에이전트.

요청자 엔터티 (requester entity)

제공자 엔터티의 웹서비스를 사용하고자 하는 개인 또는 조직. 안전 (safe) 정보 검색 이외에는 다른 작업 수행에 중요성을 두지 않는 상호 작용의 속성. [RFC 2616]

보안 관리 (security administration)

보안 도메인을 가능하게 하도록 시스템이나 응용 프로그램을 구성, 보안 및 배포하는 작업.

보안 아키텍처 (security architecture)

관리 도메인과 사용자의 필요를 충족시키기 위해 시스템이 제공해야 하는 보안 서비스, 서비스를 구현하기 위해 필요한 시스템 요소 및 위협 환경을 처리하기 위해 요소에 필요한 성능 수준을 설명하는 보안 도메인에 대한 계획 및 원칙 집합. 시스템 주소 관리 보안, 통신 보안, 컴퓨터 보안, 방출 보안, 인적 보안 및 물리적 보안과 각각에 대한 보안 정책을 지정하는 완전한 보안 아키텍처. 완전 보안 아키텍처는 의도적, 지능적 위협과 우발적 위협을 모두 처리해야 한다. 보안 아키텍처는 관리 도메인 진화의 통합된 일부로 시간에 따라 명시적으로 전개되어야 한다. [RFC 2828]

보안 감사 (security auditing)

이벤트 시퀀스의 재현 및 검사를 가능하게 하는 감사 추적을 생성하는 보안 관련 이벤트를 안정적이고 안전하게 기록하는 서비스. 보안 이벤트에는 인증 이벤트, 정책 적용 결정 등이 포함될 수 있다. 결과로 생성되는 감사 추적은 공격 감지, 정책 준수 확인, 악용 차단 또는 기타 용도로 사용할 수 있다.

보안 도메인 (security domain)

리소스에 접근할 수 있도록 권한 부여된 리소스와 시스템 엔터티 집합이 포함된 보안 아키텍처와 보안 모델에 의해 정의된 환경 또는 컨텍스트. 하나의 관리 도메인에 하나 이상의 보안 도메인이 있을 수 있다. 특정 보안 도메인을 정의하는 특색은 일반적으로 시간에 따라 발전한다. [RFC 2828]

보안 메커니즘 (security mechanism)

시스템에서 또는 시스템 내에서 제공되는 보안 서비스를 구현하는 데 사용될 수 있는 프로세스 (또는 이러한 프로세스가 통합된 장치).

보안 모델 (security model)

시스템에서 또는 시스템 내에서 제공되는 지정된 보안 서비스 집합의 엔터티 및 관계에 대한 구조적 설명. [RFC 2828]

보안 정책 (security policy)

시스템이나 조직이 리소스를 보호하기 위해 보안 서비스를 제공하는 방식을 지정하거나 규제하는 규칙 및 원칙의 집합. 보안 정책은 보안 아키텍처의 구성 요소이다. 보안 정책의 중요한 부분은 보안 정책 표현식을 사용하여 보안 서비스를 통해 구현된다. [RFC 2828]

보안 정책 표현식 (security policy expression)

원칙 신분 및 특성과 허용 가능한 작업의 매핑. 보안 정책 표현식은 접근 제어 목록인 경우가 많다. [STG]

보안 서비스 (security service)

리소스에 특별한 종류의 보호를 제공하기 위해 시스템이 제공하는 프로세스 또는 통신 서비스로, 리소스가 현재 시스템에 있는지 또는 인증 서비스나 PKI 기반 문서 특성 및 인증 서비스 등의 다른 시스템에 있는지 알린다. 보안 서비스는 AAA 서비스의 상위 집합이다. 보안 서비스는 일반적으로 보안 정책의 일부를 구현하며 보안 메커니즘을 통해 구현된다. [RFC 2828]

서비스 (service)

1. 서비스는 제공자 엔터티 및 요청자 엔터티의 관점에서 기능을 형성하는 작업을 수행하는 기능을 나타내는 추상 리소스이다. 서비스를 사용하려면 구체적 제공자 에이전트에 의해 구체화되어야 한다.

2. WSDL 서비스: 종단점의 컬렉션. [WSD Reqs]

3. 참조: 웹서비스

서비스 설명 (service description)

서비스 설명은 서비스의 인터페이스 및 시맨틱을 설명하는 문서 집합이다.

서비스 인터페이스 (service interface)

1. 서비스 인터페이스는 서비스가 나타나는 추상적 경계이다. 메시지 및 해당 메시지가 암시하는 조건과 함께 서비스와의 상호 작용에 관여하는 메시지 교환 패턴의 종류를 정의한다.

2. 작업의 논리적 그룹화. 인터페이스는 추상 서비스 유형, 전송 프로토콜의 독립성 및 데이터 형식을 나타낸다. [WSD Reqs]

서비스 중개 (service intermediary)

1. 서비스 중개는 기본 역할이 부가 가치적 방식으로 메시지를 전송하는 것인 웹서비스이다. (메시징의 관점에서 보면 중개는 메시지를 중간에서 한 에이전트에서 다른 에이전트로 처리하는 것이다.) 특히 서비스 중개는 일부 응용 프로그램 정의 관점에서 볼 때, 나가는 메시지가 들어오는 메시지와 동등한 서비스이다.

2. 참조: SOAP 중개

서비스 제공자 (service provider)

제공자 에이전트 및 제공자 엔터티를 참조한다. [WS Arch]의 서비스 제공자에 대해를 참조한다.

서비스 요청자 (service requester)

요청자 에이전트 및 요청자 엔터티를 참조한다. [WS Arch]의 서비스 요청자에 대해를 참조한다.

서비스 역할 (service role)

서비스를 제공하는 개인 또는 조직에 관련된 것으로 식별된 추상적 작업 집합. 서비스 역할은 서비스와 교환되는 메시지의 특정 측면과도 연관된다.

서비스 시맨틱 (service semantics)

서비스의 시맨틱은 서비스와 상호 작용할 때 필요한 과정으로써, 제공자 엔터티와 요청자 엔터티 사이의 계약 (반드시 법적 계약일 필요는 없음)을 표현한다. 즉, 요청 서비스의 효력을 나타내는 것이다. 서비스 시맨틱은 확인되었지만 공식적으로 규정되지 않은, 또는 제공자와 요청자 엔터티 사이의 계약을 통해 비공식적으로 규정된 기계 판독 양식으로 공식 기술될 수 있다.

서비스 지향 아키텍처 (service-oriented architecture)

호출이 가능하고 인터페이스 설명을 게시하고 발견할 수 있는 구성 요소 집합.

세션 (session)

시스템 엔터티 사이의 상호 작용으로, 사용자가 관여하기도 하고 상호 작용 기간 동안 상호 작용의 몇 가지 상태로 규정된다. [WSIA 용어 설명] 이러한 상호 작용은 시스템 엔터티 간의 단일 연결로 제한되지 않을 수도 있다.

SOAP

SOAP 메시지의 형식 및 프로세싱을 규정하는 공식적인 규약 집합. 이러한 규약에는 SOAP 메시지 경로를 따라 정보를 교환할 목적으로 SOAP 메시지를 생성하고 수용하는 SOAP 노드 간의 상호 작용이 포함된다.

SOAP 응용 프로그램 (SOAP application)

SOAP 프로세싱 모델에 따라 SOAP 메시지에 특정 작업을 수행하거나, 생산, 사용하는 소프트웨어 엔터티.

SOAP 바인딩 (SOAP binding)

교환의 목적으로 다른 프로토콜 (기본 프로토콜) 내에서 또는 위에서 SOAP 메시지를 전달하기 위한 공식적 규칙 집합. SOAP 바인딩의 예에는 HTTP 엔터티 본문 내에서 또는 TCP 스트림을 통한 SOAP 메시지 전송이 포함된다.

SOAP 본문 (SOAP body)

SOAP 메시지 경로에서 최종 SOAP 수신자를 대상으로 하는 0 개 또는 그 이상의 요소 정보 항목의 집합.

SOAP 봉투 (SOAP envelope)

SOAP 메시지의 가장 외부의 요소 정보 항목.

SOAP 장애 (SOAP fault)

SOAP 노드가 생성한 장애 정보가 포함된 SOAP 요소 정보 항목.

SOAP 특징 (SOAP feature)

일반적으로 통신 중인 SOAP 노드 사이의 메시지 교환관 연관된 SOAP 메시징 프레임워크의 확장. 기능의 예에는 "안정성", "보안", "상호 관계", "라우팅" 및 메시지 교환 패턴의 개념이 포함된다.

SOAP 헤더 (SOAP header)

SOAP 메시지 경로 내에서 SOAP 수신자를 대상으로 할 수 있는 0 개 또는 그 이상의 SOAP 헤더 블록의 집합. S

OAP 헤더 블록 (SOAP header block)

SOAP 헤더 내에서 논리적으로 하나의 계산 가능한 단위를 구성하는 데이터의 한계 지정에 사용되는 요소 정보 항목. SOAP 헤더 블록의 유형은 헤더 블록 요소 정보 항목의 정규화된 이름으로 식별된다.

SOAP 중개 (SOAP intermediary)

SOAP 중개는 SOAP 수신자 및 SOAP 전송자이며 SOAP 메시지 내에서 대상으로 지정될 수 있다. 해당 블록을 대상으로 하는 SOAP 헤더 블록을 처리하고 SOAP 메시지를 최종 SOAP 수신자로 전달한다.

SOAP 메시지 (SOAP message)

SOAP 노드 간 통신의 기본 단위.

SOAP 메시지 교환 패턴 (SOAP message exchange pattern )(MEP)

하나 이상의 기본 SOAP 프로토콜 바인딩에 의해 활성화된 SOAP 노드 간의 SOAP 메시지 교환을 위한 템플릿. SOAP MEP 는 SOAP 기능의 한 예이다.

SOAP 메시지 경로 (SOAP message path)

하나의 SOAP 메시지가 통과하는 SOAP 노드 집합. 여기에는 초기 SOAP 전송자, 0 개 이상의 SOAP 중개 및 최종 SOAP 수신자가 포함된다.

SOAP 노드 (SOAP node)

이 권장안에 의해 정의된 규약 집합에 따라 SOAP 메시지를 전송, 수신, 처리 및 릴레이하기 위해 필요한 처리 로직의 구체화. SOAP 노드는 SOAP 메시지의 교환을 구성하는 규칙을 적용하는 역할을 한다. 하나 이상의 SOAP 바인딩을 통해 기본 프로토콜이 제공하는 서비스에 접근한다.

SOAP 수신자 (SOAP receiver)

SOAP 메시지를 받는 SOAP 노드.

SOAP 역할 (SOAP role)

메시지 처리에서 SOAP 노드의 필요한 기능. SOAP 노드는 여러 역할을 수행할 수 있다.

SOAP 전송자 (SOAP sender)

SOAP 메시지를 전송하는 SOAP 노드.

상태 (state)

특정 시점에서 구성 요소의 속성을 나타내는 특성 집합.

동기화 (synchronous)

참여 에이전트들이 상호 작용이 시작된 때부터 모든 메시지가 실제로 수신되거나 실패 조건이 결정될 때까지 연관된 메시지를 수신하고 처리할 수 있어야 하는 경우 상호 작용이 동기화 된다고 표현한다. "메시지를 수신할 수 있음"의 정확한 의미는 참여 에이전트 (에이전트가 사용하는 전송 프로토콜 포함)의 특성에 따라 다르다. 하지만 정확한 시간 동기, 위협 차단 등을 의미하지는 않는다.

시스템 엔터티 (system entity)

컴퓨터/네트워크 시스템의 활성 요소. 자동화된 프로세스 또는 프로세스 집합, 하위 시스템, 여러 기능 집합이 통합된 개인 또는 개인 그룹을 예로 들 수 있다. [RFC 2828]

트랜잭션 (transaction)

트랜잭션은 조화 또는 다단계 상호 작용에서 결과 또는 작업의 조화를 지원하는 아키텍처의 기능이다. 트랜잭션의 근본적 특성은 여러 작업을 같은 작업 단위로 결합시켜 해당 작업들이 한 단위로 성공하거나 실패하도록 하는 기능이다.

최종 SOAP 수신자 (ultimate SOAP receiver)

SOAP 메시지의 최종 목적지인 SOAP 수신자. SOAP 본문 및 대상 SOAP 헤더 블록의 내용을 처리할 책임이 있다. 일부 환경에서는 SOAP 메시지가 SOAP 중개의 문제 등과 같은 이유로 최종 SOAP 수신자에 도달하지 못할 수 있다. 궁극적 SOAP 수신자는 같은 SOAP 메시지의 SOAP 중개가 될 수 없다.

사용 감사 (usage auditing)

이벤트 시퀀스의 재현 및 검사를 가능하게 하는 감사 추적을 생성하는 사용 관련 이벤트를 안정적이고 안전하게 기록하는 서비스. 사용 이벤트에는 리소스 할당 이벤트와 리소스 해제 이벤트가 포함될 수 있다.

웹서비스 (Web service)

크게 보면 "웹서비스"로 명명할 수 있는 것들이 매우 많다. 하지만 본 프로젝트 그룹의 목적과 다른 정의에의 침해를 배제하면 다음과 같은 정의를 사용할 수 있다. 웹서비스는 네트워크를 통한 상호 연동 가능한 시스템 대 시스템 상호 작용을 지원하도록 설계된 소프트웨어 시스템이다. 시스템이 처리 가능한 형식 (구체적으로 WSDL)으로 기술된 인터페이스를 갖고 있다. 다른 시스템은 SOAP 메시지를 사용하여 설명으로 지정된 방식으로 웹서비스와 상호 작용하며, 일반적으로 다른 웹 관련 표준과 함께 XML 직렬화를 적용한 HTTP 를 사용하여 전송된다.

자료 : 정보통신단체표준(국문표준) TTAS.KO-10.0179 웹서비스 용어