기술도면 정보를 위한 CITIS 아키텍처 연구

박정선*, 김성희**
Jeong-Sun Park, Sung-Hee Kim

Abstract

CALS에서 기술도면 관리의 중요성이 날로 커지고 있고, CITIS에 대한 관심이 고조되고 있다. CITIS는 계약자와 공급자간의 환경에 따라서 다르게 구현될 수 있는데, 본 연구에서는 CITIS에서 계약자와 공급자간의 기술도면 정보를 서비스하는 구조를 제시하고, CITIS 접근 제어에 필요한 요소 기술들을 설명하고자 한다.

CITIS는 크게 두 가지로 구성되어 있는데, 하나는 CAD 도면 같은 디지털 데이터와 그 데이터를 사용하는 어플리케이션이다. 데이터와 어플리케이션은 모두 계약자 측의 CITIS 컴퓨터에 존재하고, 사용자의 컴퓨터에는 존재하지 않는다. CITIS의 주요 목적은 권한을 갖고 있는 사용자가 업무를 수행하는 데 필요한 데이터와 어플리케이션에 온라인으로 접근할 수 있도록 서비스해 주는 데 있다. 이러한 서비스를 위해 필요한 접근 제어의 방법으로는 firewall, Unix OS, Proxy Server, 상용 데이터베이스, SSL 등을 사용한다.

* 명지대학교 산업공학과 교수

** 명지대학교 산업공학과

1. 서론

CALS는 조달, 설계, 제조와 지원에 관련된 디지털 정보의 통합을 가속화시켜 왔다. 현재 많은 기업들이 비용 감소, 품질 향상, 업무의 효율성이 명확해졌기 때문에 CALS 전략을 수용하고 있다. 그 결과로 제품 및 서비스와 관련된 정보, 그리고 설계·제조·생산 등의 엔지니어링과 관련된 정보를 디지털화하고, 관련 객체가 이와 같은 정보를 공동으로 활용한다면 조달·획득·개발 기간을 단축하고, 비용의 절감, 품질의 향상 등을 달성할 수 있을 것이다. 본 연구에서는 계약상 요구되는 데이터를 디지털화하여 정보 서비스하고 정보 통신망을 통하여 온라인 접근할 수 있도록 하는 CITIS 시스템에서 기술 도면 정보를 서비스하는 구조를 제시하고, 필요한 요소 기술들을 설명하고자 한다.

2. CITIS

가. CITIS의 정의

CITIS(Contractor Integrated Technical Information Service)는 계약상 최종 아이템(물품 및 서비스)의 계약자가 통합 데이터베이스로 조달 측의 공고, 입찰, 계약, 발주 등 계약 관계 정보를 입수하거나 조달 책임자에게 기술 정보와 지원 정보를 제공하는 데 필요한 시스템이다[11]. 즉, 조달에 관계된 정보가 모두 디지털화되어 이를 활용하는 온라인 네트워크의 역할을 하는 것이 CITIS라고 한다. 페이퍼리스로 조달업무를 한다는 당초 CALS의 목표에서 보더라도 CITIS는 CALS 전략의 실행에서 매우 중요한 시스템이다. 한편 CITIS를 통하여 어느 정도의 커뮤니케이션이 가능하다고 하더라도 조달 업무상 기밀이 조달 측과 계약자 측에도 필요하기 때문에, 양자의 정보 교환은 적절한 승인과 관리하에서 행하여야 한다. 또한 계약자 통합 기술 정보 서비스(CITIS)는 조달자가 시스템 및 제품에 관련된 기술 데이터를 필요로 할 때 분산되어 있는 각종 데이터베이스로부터 검색, 종합, 통제 가능토록 데이터를 논리적으로 통합하며, 보안 유지를 위해 인가된 사용자만이 허용되고 각각의 제품에 대한 기술 데이터베이스로써 데이터 입력, 갱신, 관리 및 통제가 가능한 통합 데이터 처리 및 운용 체계이다. 즉 CITIS는 조달자가 계약자의 데

이터베이스에 접근 가능하도록 계약자가 제공하는 서비스로, 조달자가 필요한 디지털 데이터의 사용이 가능하고 컴퓨터 소프트웨어 및 하드웨어의 제공 등을 포함하는 모든 활동과 기능을 갖는다.

기존의 프로세스에서는 계약자 혹은 부계약자가 조달자의 요구에 따라 계약에 관련된 기술 정보를 문서화하여 조달자에게 제공하면, 조달자는 다시 이를 복사하여 여러 검토자가 검토를 함으로써 프로세스의 시간과 비용을 낭비하는 비합리적인 방식이었다. 그러나, CITIS 환경에서의 CITIS를 통하여 모든 처리를 온라인화하여 검토시간을 최소화하고 종이로 된 문서의 복사, 작성, 운송 비용을 획기적으로 절감할 수 있으며, 실질적인 CALS 구현 목표중의 하나인 정보의 공유와 페이퍼리스를 실현할 수 있게 되었다.

나. CITIS의 기능

계약자 통합기술정보 서비스(CITIS) 규격은 계약상 요구되는 디지털 정보의 전달 및 전자적 접근 서비스를 구성하는 일반 요구사항, 그리고 조정이 가능한 상세 요구사항들을 정의하여 계약상 구현 가능한 수단이 되도록 작성되었다. 현재 한국 산업 규격으로 심의 중인 CITIS 초안에 의하면, CITIS는 일반 요구사항과 상세 요구사항으로 나눌 수 있다[1][7][11].

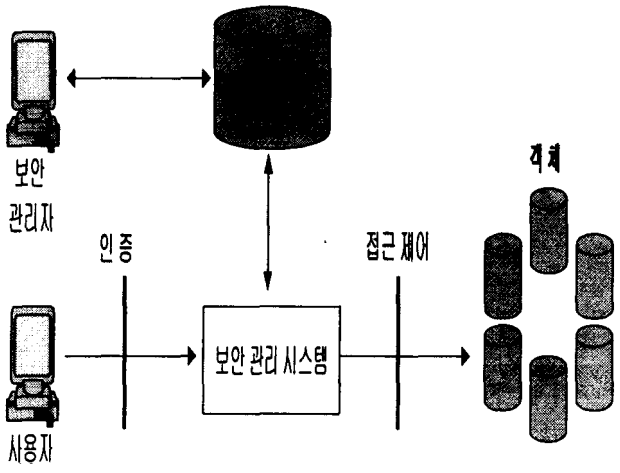
일반 요구사항에는 정보 서비스, 데이터 구성관리, CITIS 보안 기능, 데이터 항목 색인, 데이터 교환 표준 등을 포함하고 있다. 또한, CITIS는 상세 요구사항으로 수신확인, 어플리케이션, 승인과 거부, 보관, 조합, 주석, 다운로드, 편집, 발송, 전달공고, 패키지, 질의, 수신, 검색, 분류, 저장, 사용자 그룹, 열람 등의 수정 가능한 기능들을 포함한다.

3. CITIS를 위한 접근 제어 기술

3.1 데이터베이스 접근 제어

CITIS에서는 보안과 관련하여 데이터베이스의 접근 제어 기능을 사용할 수 있다. 데이터베이스 접근 제어 방법은 사용자가 데이터베이스에 직접적인 경로를 통해서 접근할 때, 이를 통제하여 데이터의 보안성을 달성하는 방법이다. 접근 제어는 그림 1에서 처럼 여러 가지 보안 서비스들과 상호 의존적인 관계에 있으며 시스템 내에 공존한다. 접근 제어는 합법적인 사용자들의 활동을 제한하는 것과 밀접한 관련이 있다. 접근 제어와 관련된 정보는 원칙적으로 보안 관리자에 의하여 관리되며, 몇몇 경우에는 사용자에 의하여 변경도 가능하다.

그림 1에서 인증과 접근 제어는 분명히 구별되어야 한다. 인증은 사용자의 신원을 확인하기 위하여 필요하고, 접근 제어는 인증이 확실하게 수행되었다는 가정하에서 합법적인 사용자들에 대하여 관리 정보의 접근을 제한하기 위하여 필요하다. 따라서 접근 제어의 효율성은 사용자의 신원 확인을 위한 인증이 얼마나 잘 수행되었느냐와 각각의 사용자에게 얼마나 적절히 권한 부여가 이루어졌는가에 달려 있다.



<그림 1> 접근 제어 및 기타 보안 서비스

접근제어 정책은 크게 자율적 접근 제어(DAC: Discretionary Access Control) 정책, 강제적 접근 제어(MAC: Mandatory Access Control) 정책, 그리고 역할기반 접근 제어(RAC: Role-based Access Control) 정책 등이 있다. 이 중에서 어느 접근 제어 정책을 선택할 것인가는 관리되어야 할 환경의 특성과 그 응용에 따라 달라질 수 있다[2].

3.1.1 자율적 접근 제어

자율적 접근 제어는 접근을 요청한 사용자의 신원(identification)에 근거를 두고 있다. '자율적'이라고 하는 말은 사용자가 사용하려는 객체에 대한 접근 권한을 자율적으로 부여하거나 철회할 수 있다는 것을 의미한다. 이것은 접근 권한의 통제가 사용하려는 객체의 각 소유자에 의하여 분산화되어 수행됨을 의미하지만, 이러한 통제는 보안 관리자에 의하여 중앙 집중적으로 수행될 수도 있다.

3.1.2 강제적 접근 제어

강제적 접근 제어는 자율적 접근 제어와는 달리 사용자와 사용하려는 객체에 부여된 보안 등급을 기반으로 접근을 제어하는 방법이다. 각각의 사용자와 사용하려는 객체에게는 보안 등급이 부여되며, 특히 사용자의 보안 등급을 인가 등급(clearance level)이라고도 한다.

사용하려는 객체와 관련된 보안 등급은 객체에 포함된 정보가 불법적으로 누출되었을 때 입게 되는 손해의 정도, 즉 그 정보의 중요도를 나타낸다. 그리고, 사용자와 관련된 보안 등급은 중요한 정보를 인가되지 않은 사용자에게 어느 정도로 누설하지 않을 것인가 하는 사용자의 신뢰도를 나타낸다.

자율적 접근 제어와는 달리 강제적 접근제어는 새로운 객체가 생성될 때 특정한 보안등급 부여 메카니즘에 의하여 객체에 보안등급이 부여되어야 한다. 강제적 제어정책은 모든 사용자 및 객체에 대하여 일정하며 어느 하나의 사용자/객체 단위로는 접근 제한을 설정할 수 없다. 즉 한 사용자가 어느 한 객체를 접근하지 못하면 이때에 그 사용자는 그 객체와 동일한 보안등급을 갖는 모든 객체에 접근이 허락되지 않는다.

3.1.3 역할기반 접근 제어

강제적 접근 제어 정책이 군대와 같은 엄격한 보안 통제를 필요로 하는 환경

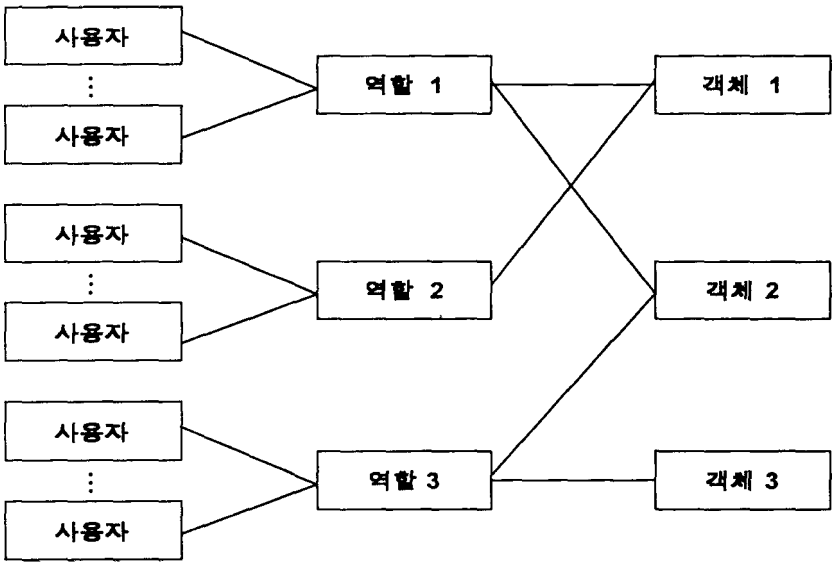
에서 개발되었고, 자율적 접근 제어는 학술 연구 단체와 같은 자율적이고 협동적인 환경에서 개발되었기 때문에, 두 보안 정책이 모두 상업적인 분야에 적용하기에는 다소 부적합한 면이 있다. 따라서 전통적인 자율적 접근 제어에서처럼 사용자나 사용자의 그룹에게 객체에 대한 접근 권한을 부여하고, 강제적 접근 제어에서처럼 접근 권한을 부여하는데 제한을 가할 수 있는 접근 제어 방법에 대한 연구가 진행되었다. 그 결과로서 역할기반 접근 제어 정책이 만들어지게 되었다.

역할기반 접근 제어 정책에서는 데이터 또는 객체를 몇 개의 범주로 나누었으며, 여러 명의 사용자는 역할이라고 하는 클래스들로 그룹화되어진다. 역할은 어떤 조직체의 사용자들의 임무를 여러 개의 영역으로 분할해 놓은 것으로서 역할 이름과 범주에 접근할 수 있는 권한으로 구성되어 있다. 즉, 사용자가 시스템에 대한 접근은 사용자 개인별로 권한이 주어지는 것이 아니고 공통적인 기능들에 기반을 둔 그룹들의 역할에 권한을 부여한다. 이는 사용자들을 클래스 단위로 취급하여 시스템 내에서의 사용자들을 관리하기 쉽게 하는 데 그 목적이 있다.

본 연구에서 CITIS의 데이터베이스 접근 제어 방식으로 역할 기반 접근 제어 정책을 고려하고 있다. 그 이유는 자율적 접근 제어보다는 안전한 정보의 흐름을 보장하고, 강제적 접근 제어보다는 융통성 있는 접근제어를 제공하기 때문이다. 사용자들은 그들이 수행하는 공통적인 기능들에 기반을 둔 그룹들의 역할로 구성된다. 그래서 사용자들은 시스템에 대해 접근할 때 개인별로 접근권한을 부여받는 것이 아니라 그들의 임무에 근거하여 사용자들을 그룹화한 역할에 접근 특권을 부여한다. 이렇게 하는 목적은 개개의 사용자 단위로 처리하는 대신에, 그러한 사용자들을 클래스 단위로 취급하여 개개의 사용자에 대한 권한 부여 횟수를 줄이는 것이다. 시스템 권한은 역할과 관련이 있고, 사용자도 역할과 관련이 있다. 그러므로 사용자의 접근 권한은 사용자가 어느 그룹에 속해 있느냐와 그룹이 어떠한 접근 권한을 갖고 있느냐에 달려 있다.

즉, 개개의 역할은 그 역할이 접근할 수 있는 객체 및 그 객체에 대한 접근 형태가 능력 리스트의 형태로 정의되어 있어서 실질적으로 그 역할이 수행할 수 있는 사용 범위가 능력 리스트에 의하여 제한이 된다. 각각의 사용자에게는 이렇게

정의된 역할이 적절히 배정이 되며, 이 역할에 할당된 접근 권한에 따라 사용자의 사용하려는 객체에 대한 접근 범위가 결정된다. 역할 기반 접근 제어의 예는 그림 2와 같다.



<그림 2> 역할 기반 접근 제어

역할기반 접근 제어는 역할을 중심으로 접근을 통제하는데, 각각의 사용자는 자신에게 할당된 적절한 역할들을 가지고 있다. 역할에는 그 역할에 할당된 사용자 리스트와 역할이 접근 가능한 사용 객체 및 그들에 대하여 수행 가능한 연산들에 대한 정보를 포함하고 있다.

역할기반 접근 제어 정책은 자율적 접근 제어와 강제적 접근 제어의 장점을 모두 가지고 있으며, 개개의 사용자가 아닌 역할 단위로 접근을 통제함으로써 사용자의 역할 변화에 따른 접근 권한의 감독 및 관리를 용이하게 할 수 있는 장점을 가지고 있다.

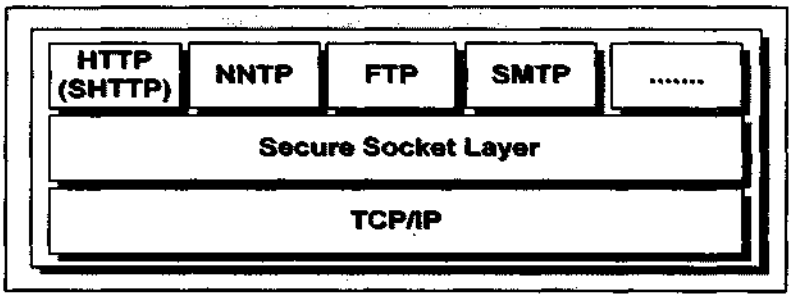
역할기반 접근 제어 정책은 아래와 같은 과정으로 수행되는데, 먼저 사용자가 속한 역할을 찾아내어 그 역할 내에 사용자가 접근을 원하는 객체와 수행 가능한 연산이 정의되어 있는지를 검사함으로써 접근 허용 여부를 결정하게 된다.

역할기반 접근 제어의 수행 방법은 자율적 접근 제어의 경우와 유사하지만,

먼저 접근하고자 하는 사용자가 자신에게 할당된 역할에 해당하는 역할기반 접근 제어 객체에 정의되어 있는 가를 검사하여야 한다. 그리고 나서 그 역할 객체에 수행하고자 하는 연산이 정의된 경우에만 참을 반환하고, 그렇지 않은 경우에는 거짓을 반환하여 접근을 허용하지 않는다.

3.2 SSL(Secure Socket Layer)

SSL은 Netscape Communications사에서 인터넷 보안을 위하여 설계한 프로토콜이다. 이것은 그림 3에서처럼 응용 계층과 TCP/IP 계층 사이에 위치하며 데이터의 암호화, 서버 인증 기능, 데이터 무결성, 그리고 클라이언트 인증 기능을 수행하기 위한 프로토콜이다[5]. 응용 계층의 아래에 위치하기 때문에 각종 응용 계층 프로토콜(HTTP, NNTP, FTP 등)에서 사용이 가능하고 메시지 단위의 암호화가 아닌 서비스 단위의 암호화가 이루어진다. 여기서 서비스 단위의 암호화라는 것은 다른 말로는 "end-to-end" 암호화라고도 표현할 수 있는데 서비스의 시작부터 끝까지 주고받는 모든 데이터를 암호화하는 기법을 의미한다. 이 방식은 Firewall이 갖는 단점을 보완하는 CITIS에서 가장 효율적인 방법으로 사용될 수 있는 암호화 방식이라 할 수 있다.



<그림 3> SSL 프로토콜 Spec.

SSL은 "handshake" 방법을 사용하여 TCP/IP 커넥션을 초기화하는데 이 결과로 인해서 클라이언트와 서버는 서로 주고 받는 데이터를 암호화하는데 사용할 암호화 기법, 암호화의 정도, 그리고 상호 인증에 필요한 모든 데이터를 주고 받는다. 사실 이러한 모든 사전 작업이 끝난 후에 비로소 SSL에 의해 모든 데이터들(URL, 사용자 ID, 카드번호, 패스워드 등)이 암호화가 되어 클라이언트와 서버간에 교환되는 것이다.

3.2.1 Handshake

SSL이 작동하기 위하여 필요한 사전작업들이 바로 이 handshake 과정에서 수행된다. 이 작업들을 정리하면 다음과 같다.

· 클라이언트와 서버가 서로 자신의 인증서(Certificate)를 교환한다. 그리고 각각은 자신이 받은 인증서에 기록되어 있는 유효기간, 서명을 확인한다.
· 클라이언트는 이후에 수행될 암호화와 메세지 인증 코드(MAC : Message Authentication Code)의 생성에 필요한 난수(비밀키)를 생성하여 이것을 서버의 공개키로 암호화하여 서버에게 전송한다.
· 서비스를 받는 동안 사용할 암호화 알고리즘과 해쉬함수의 종류를 결정한다.

이 과정에서는 클라이언트는 자신이 제공할 수 있는 암호화 알고리즘의 리스트를 서버에게 제시하고 이들 중에서 하나를 서버가 선택한다. 인증서(Certificate)란 일상생활에서 볼 수 있는 인증서의 개념과 똑같이 생각하면 된다. 우리가 흔히 볼 수 있는 "** 인증서"에는 그 인증서를 발급한 기관이나 사람의 도장(서명)이 찍혀 있고 인증하는 내용이 있으며 인증서를 수령한 사람의 이름이 적혀 있다. 이와 마찬가지로 온라인으로 사용하기 위한 인증서도 비슷한 구조로 되어 있다. Netscape에서는 ITU(International Telecommunication Union)에서 제정한 X.509의 양식 또는 RSA Data Security 사에서 제정한 PKCS-6의 양식을 따르는 인증서를 사용한다.

다. CITIS의 접근 제어 방안

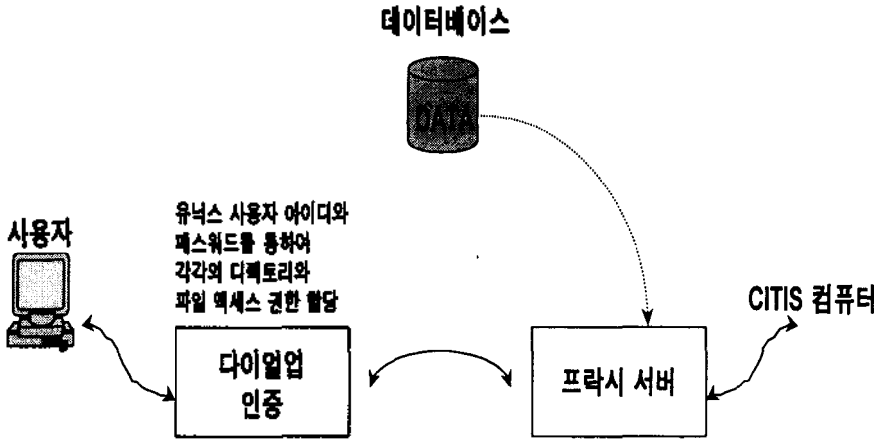
CITIS는 두 가지 부분으로 구성되어 있는데, CAD 도면같은 디지털 데이터와 그 데이터를 사용하는 어플리케이션이다. CITIS의 주요 목적은 권한을 갖는 사용자가 계약자를 위하여 업무를 수행하는데 필요한 데이터와 어플리케이션에 접근하도록 하는 것이다.

정보 교환을 효율적으로 하기 위한 것이 CITIS의 주요 목적이지만, 오직 허가 받은 자원만을 액세스할 수 있게 제한해야하는 문제들이 있다. CITIS는

Firewall 뿐만 아니라 좀 더 확실한 보안을 위하여 다른 보안 방법을 겸용하여야 한다.

CITIS에 의하여 사용되는 보안의 첫 번째 단계는 유닉스 운영 시스템에서 사용되고 있는 보안 시스템이다. 이것은 시스템 관리자가 디렉토리와 파일에 접근 권한을 사용자에게 할당해주는 Unix의 일반적인 기능을 말한다. 사용자에게 컴퓨터에 로그온 하기 위한 ID와 패스워드를 할당해준다.

두 번째 단계로 데이터베이스를 사용하여 사용자 리스트와 그들이 사용할 수 있도록 허가 받은 CITIS 디렉토리와 파일들을 연결한다. 그리고 어플리케이션과 데이터 억세스를 위한 프락시(Proxy)를 사용한다. 다시 말하자면 CITIS에 연결되어 있는 사용자의 모든 활동을 체크하는 것이다. 사용자가 접근 권한을 갖고 있지 않는 활동을 하게 되면 그것을 막게 하는 역할을 하는 것이다.

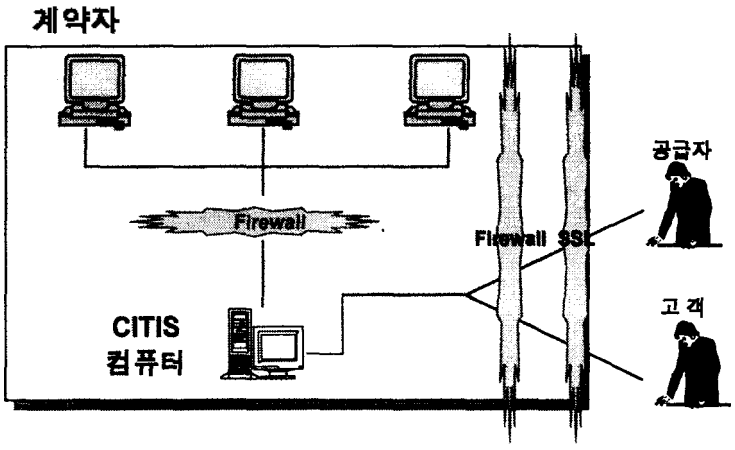


<그림 4> CITIS의 접근 및 보안 방법의 구조

CITIS에 웹 접근을 제어하기 위하여 또 다른 보안 계층이 추가되었는데, 앞에서 언급한 SSL(Secure Sockets Layer)이다. SSL 프로토콜을 사용하여 서버와 브라우저간에 교환되는 데이터를 암호화하고, 권한을 갖지 않는 사용자가 데이터를 검색하고 가로채는 것을 막는다.

4. 기술 도면 정보를 위한 CITIS 구조

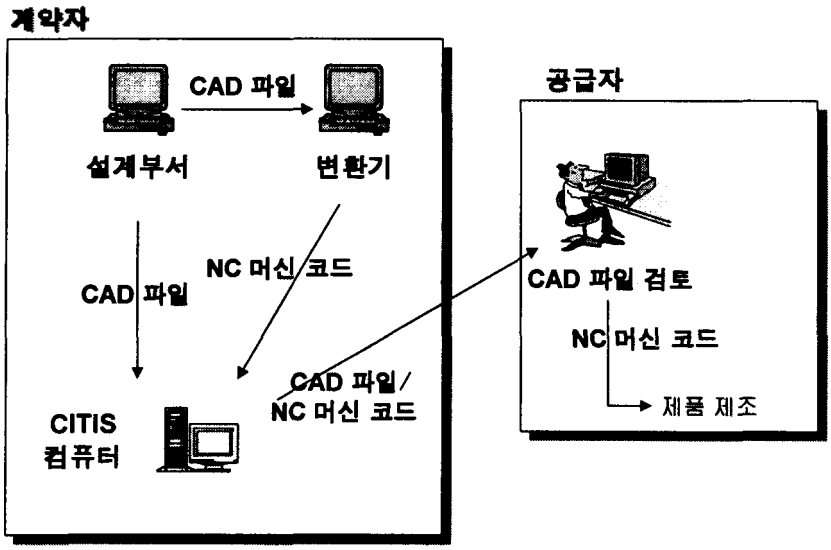
CAD도면 데이터와 어플리케이션 모두 CITIS 컴퓨터에만 존재한다. CITIS의 주요 목적은 권한을 갖는 사용자가 그들이 계약자를 위하여 임무를 수행하는데 필요한 데이터와 어플리케이션에 접근하도록 하는 것이다. 이를 그림으로 나타내면 다음과 같다. 그림 5는 공급자와 고객이 초기 인증과정을 거쳐 CITIS 컴퓨터에 접근하는 CITIS의 단순화된 구조이다.



<그림 5> CITIS의 단순화된 구조

가. 기술 도면 정보 교환

계약자는 변경된 CAD 도면을 공급자에게 온라인으로 보내길 원하는 경우라도, 공급자가 직접 CITIS 컴퓨터에 액세스하는 것을 보안상의 문제로 원하지 않을 수 있다. 이런 경우 계약자의 설계팀에서 설계한 CAD 도면을 공급자의 기계를 사용하기 위하여 NC 머신 코드로 변환하고, 이를 CITIS 컴퓨터에 저장한다. 이는 모뎀을 통하여 공급자에게 보내지고, 공급자는 이 CAD 파일을 검토한 후, 제조 부서로 NC 코드를 보낸다. 그러면 이 코드를 사용하여 제품 혹은 부품을 제조한다. 이 경우 기존의 마그네틱 테이프를 사용하여 전달하던 비용을 획기적으로 줄일 수 있다. CAD 파일이 변경될 때마다 드는 배달 비용을 획기적으로 절감할 수 있는 것이다. 그림 6은 계약자와 공급자 사이의 기술 도면 정보 교환의 예이다.

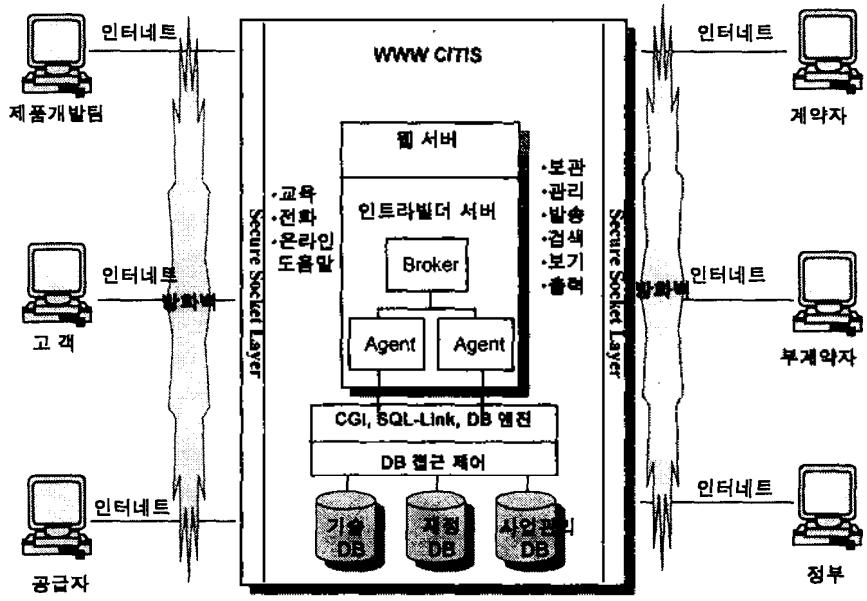


<그림 6> 기술도면 정보 교환의 예

나. 인트라빌더를 이용한 기술 도면 정보 CITIS 구조

본 연구에서는 웹 어플리케이션 개발 툴 중 인트라빌더를 예로 들어 기술 도면 정보를 위한 CITIS 모형을 제시하고자 한다. 인트라빌더는 자바스크립트를 근간으로 하여 RAD (Rapid Application Development) 특징을 갖는 웹 어플리케이션 개발 도구이다. DB의 자료를 웹에서 볼 수 있는 어플리케이션을 쉽게 개발할 수 있고, 확장된 자바스크립트를 사용하여 서버와 클라이언트 측에서 각각 동작하는 코드를 작성해 낼 수 있다.

인트라빌더를 이용하여 기술 도면 정보를 위한 CITIS 개발 모형은 다음과 같다. 각 사용자는 웹 브라우저를 통하여 WWW CITIS에 접근할 수 있고, 이때 CITIS 접근 제어방식으로 Firewall과 SSL 그리고 역할기반 DB 접근 제어를 사용하였다.



<그림 7> 기술도면 정보를 위한 CITIS 모형

6. 결론

본 연구에서는 기술 도면 정보 서비스를 위한 CITIS의 구조를 제시하였고, 권한을 갖고 있는 사용자가 업무를 수행하는 데 필요한 데이터와 어플리케이션에 온라인으로 접근할 수 있도록 서비스해 주는 CITIS를 위해 필요한 접근 제어의 방법을 제시하였다.

참고문헌

[1]국방체계연구소, "계약자 통합 기술정보 서비스 한국 산업 규격 심의 초안", 국방정보체계연구소, 1997.

[2]김종덕, 정철윤, 노봉남, "망관리정보베이스에 대한 접근 제어 정책",정보처리 제4권 제2호, 1997, pp44-51

[3]이원희, "한국형 CITIS 개발 방안", 한국 CALS/EC학회 96종합학술대회발표 논문집, 1996, pp.55-81.

[4]정석찬, 우훈식, 백종명, 주경준, "CITIS(Contractor Integrated Technical Information Services) 구현에 관한 고찰", 한국경영과학회/대한산업공학회 '97 춘계공동학술대회, 1997, pp.637-640.

[5]"암호를 이용한 정보보호 기법", http://www.posdata.co.kr/k-pc/in1.htm.

[6]"CITIS Solution Enables On-line Access to Contractually Required Information", FORMTEK Journal, Fall, 1995, Issue 26.

[7]CALS Industry Steering Group, "Commercial Standard Contractor Integrated Technical Information Services(CITIS)", CALS Industry Steering Group, 1995.

[8]Borland, IntraBuilder Developer's Guide, Borland International, 1996.

[9]David Kosiur, Understanding Electronic Commerce, Microsoft Press, 1997.

[10]DoD, MIL-HDBK-59B : Continuous Acquisition and Life-Cycle Support Implementation Guide, Department of Defense, USA, 1994.

[11]DoD, MIL-STD-974 : Contractor Integrated Technical Information Services (CITIS), Department of Defense, USA, 1993.

[12]DoD, Program Manager Desktop Guide for Continuous Acquisition and Life-cycle Support (CALS) Implementation, Department of Defense, USA, 1995.

[13]Mark Galigher, Christine Ford, Contracting for CALS, Department of Defense, USA, 1996.