CALS 정보보호 모델 설계

°윤여웅*, 이정현**, 이대기**, 소우영*
*한남대학교 컴퓨터 공학과, **한국전자통신연구원

The Design of CALS Security Model

°Yeo-Wung Yun*, Jeong-Hyun Yi**, Dai-Ki Lee**, Woo-Young Soh*
*Department of Computer Engineering, Hannam University, **ETRI

요 약

정보 통신 기술의 발달로 인하여 시·공간을 초월한 국제 개방화 시대로 접어들면서 각 기업과 국가에서는 국제적인 경쟁력 우위를 선점하고자 CALS를 도입하여 추진 중에 있다. 그러나 CALS 추진에 있어 다양한 문제들이 발생되고 있고 특히, 정보보호 문제는 CALS 추진의 지연 원인이 되고 있으며 안전한 CALS 구축을 위하여 CALS 정보보호에 대한 연구가 요구되고 있다. 본 논문에서는 CALS 정보보호 위협 요소를 비롯한 정보보호 서비스와 메커니즘을 분석하고 안전한 CALS를 구축하기 위한 정보보호 모델을 제시하고자 한다.

1 장. 서 론

최근 정보 통신 기술의 발달로 인하여 시·공간을 초월한 국제 개방화 시대로 접어들게 되었고 각 기업들을 비롯한 국가들은 제품에 대한 생산으로부터 유지보수까지 전 과정에서 경쟁력 우위를 선점하고자 CALS를 도입하게 되었다. CALS는 기업간에 표준화된 디지털 자료를 공유하고 신속하게 교환하는 것으로 기업 활동의 효율화를 위하여 필수적이며, 제품의 설계를 비롯한 개발, 생산, 판매, 유지 보수, 폐기 등 전반에 걸친 활동의 통합 개념이다.

CALS는 1985년 미국 국방부에서 컴퓨터 네트워크를 이용한 군수물자의 조달을 위해 시작되었고 초기에는 컴퓨터에 의한 군수지원(Computer-Aided Logistics Support)의 뜻으로 사용되었으나 현재는 광속의 상거래(Commerce At Light Speed)라는 개념으로 통용되고 있다[1,2,3,4]. CALS는 기업에 관련된 기술 정보와 제반 교역에 필요한 정보를 전자적으로 교환함으로써 기업의 업무 프로세스 방식을 재구성하므로써 기업의 생산력 향상을 포함한 비용절감과 품질 향상을 가져올 수 있다[1,2].

CALS는 세계 선진국을 중심으로 추진 중에 있으며 **미국**은 정부를 중심으로, **일본**은 민간부문을 중심으로, **유럽**은 국가별로 진행하면서도 유럽공동체(EU)가 중심이 되어 진행하고 있다. **국내**에서도 CALS의 중요성을 인식하여 산·학·연·관을 중심으로 CALS 구축을 위하여 노력하고 있다. 이러한 노력에도 불구하고 CALS를 구축함에 있어서 문제점들을 안고 있다. 첫째, 한 기업의 모든 정보를 디지털화하는데 많은 시간과 경비를 필요로 한다. 둘째, 기업내 생산, 유통, 관리 등 각 부분, 기업, 그룹, 업종들의 독자적인 추구로 인하여 변환의 문제가 있다. 셋째, 표준을 포함한 CALS 구현기술에 대한 인식과 투자가 부족한 실정이다. 넷째, 정보 통신의 급속한 발전으로 전자문서 교환도 이루어지지 않은 상태에서 CALS 기술과 경험의 부족이다. 다섯째는 정보보호 문제로서 기업간 교환 정보와 통합 데이터베이스에 저장된 정보를 포함한 CALS를 내·외부로부터 안전하게 보호하는 것이 심각한 문제로 대두되고 있다. 이러한 문제들로 인하여 CALS 구축이 지연되고 있는데 특히 분산된 개방 환경인 CALS에서는 외부로부터 정보를 보호하는 것이 중요하다. 본 논문에서는 CALS의 정보보호를 위해서 CALS 위협요소와 필요한 정보보호 서비스 및 메커니즘을 분석하여 CALS의 정보보호 모델을 제안하고자 한다. 2장에서는 CALS의 구현 기술들을 정리하고 3장에서는 CALS 정보보호 위협 요소를 비롯한 정보보호 서비스와 메커니즘을 분석한다. 4장에서는 CALS를 안전하게 구축하기 위한 정보보호 모델을 제시한다.

2 장. CALS 구현 기술

CALS는 제품의 설계로부터 개발, 조달, 운영, 유지보수에 이르기까지 다양한 구현 기술들을 이용하여 구축된 통합 정보 시스템으로써 구현 기술들은 다양하며 대표적인 기술들은 <표 1>과 같다[1,4,5].

<표 1> CALS 구현 기술

분 류	세 부 기 술	비 고
네트워크 기술	초고속 통신망, 인터넷 등	
멀티미디어 기술	멀티미디어 데이터 압축, 전송, 저장 등	
표준화 기술	데이터 표현 표준, 전송 표준 등	
통합 데이터베이스 기술	데이터의 공유, 변환, 저장, 검색 등	
경영혁신 기술	동시공학, 리엔지니어링, 컴퓨터를 통한 정보 관리 등	
정보보호 기술	암호화, 디지털 서명, 해쉬 함수, 키 관리, 감사 등	

CALS 구현 기술들은 **첫째**, 네트워크 기술로서 기존의 텍스트 문서뿐만 아니라 도면과 그림 등의 멀티미디어 데이터까지도 전송 대상으로 하므로 기존의 통신망으로는 전송 속도나 효율을 충족시킬 수가 없기 때문에 원활한 전송을 위하여 초고속 통신 기술이 요구된다. **둘째**, 멀티미디어 기술로서 멀티미디어 데이터를 처리할 수 있는 멀티미디어 기술이 필요하며 **셋째**, 표준화 기술로서 CALS에서는 디지털 문서, CAD 설계도면, 기술도면 등을 전산망의 제약 없이 송·수신할 수 있어야 하기 때문에 국제적인 공통 표준의 지정이 필수적이고 동일 표준을 사용하는 것이 효과를 극대화시킬 수 있다. 대부분의 CALS 표준은 <표 2>에서 보는 것처럼 CALS만을 위한 전용 표준은 없으나 기존에 있는 국제 표준 및 국가표준, 산업표준을 선택하여 만든 조합된 표준이다.

<표 2> CALS 표준 현황

분 류	표준규격	내 용	표준화기구
문장(Text)	SGML	하이퍼텍스트를 비롯한 일반적인 문서 규격	ISO
도 형	CGM	그림이나 일러스트 등의 컴퓨터 도형을 다루는 규격	ISO
그 래 픽	IGES	CAD 시스템간 데이터 교환을 위한 규격	ANSI
설계, 제조	STEP	제품의 설계, 제조 데이터에 관한 규격	ISO
스캐너 정보	CCITT Group4	래스터 정보의 데이터 압축 규격	ITU
애니메이션	MPEG1,2	애니메이션 데이터 압축 규격	ISO/IEC
정지 화상	JPEG	정지화 데이터 압축 규격	ISO/IEC
음 성	G.71X,72X	음성 데이터 압축 규격	ITU
통 합	MHEG	데이터 통합화 구조의 규격	ISO/IEC
정보서비스	CITIS	통합화된 발주 정보를 계약시 사용되는 데이터 규격	미국 국방성
전자매뉴얼	IETM	매뉴얼 정보를 디지털화한 대화형 전자 매뉴얼 규격	미국 국방성
EDI	EDIFACT	상거래에서의 문서교환 사용규격	ISO/ANSI
데이터베이스	SQL	데이터베이스 질의 언어	ANSI
시스템 개발	SLCP	시스템 개발 거래 공통 언어	ISO/IEC

넷째, 통합 데이터베이스 기술로서 CALS에서는 네트워크의 발달로 데이터의 중복을 피하고 서로 정보를 공유하는 통합 데이터베이스 기술이 요구되었다. 필요시 언제 어디서나 실시간으로 접근할 수 있는 분산된 환경에서 정보의 공유를 의미한다. **다섯째**, 경영혁신 기술로서 CALS 체계는 어떤 한 제품의 주문으로부터 생산에서 사후 관리까지의 전 수명 주기 동안에 통합 관리하는 기능들이 필요한데 이를 경영 혁신 기술이라 한다. 경영 혁신 기술은 궁극적으로 조직이나 기업 내부의 작업 방식을 변화시키며 기본적으로는 프로세스를 분석, 설계, 리엔지니어링하는 전략을 제공함으로써 이들 프로세스와 연관된 조직, 정보, 데이터 구조를 움직

인다. **여섯째**, 정보보호 기술로서 정보는 전송, 저장, 접근 등의 과정에서 위협요소들에 노출될 수 있으며 공격을 받을 경우 막대한 피해를 입을 수 있다. 그러므로 정보의 위협에 대한 대책으로 정보를 안전하고 신뢰성 있게 보호하기 위해서는 정보보호 기술들이 절실히 요구된다. CALS 역시 다양한 위협요소로부터 피해를 입을 수 있기 때문에 안전한 CALS 체제에서 정보보호 서비스가 제공되어야 하며 정보보호 메커니즘들이 활용되어야 한다. 따라서 안전한 CALS를 위하여 위협요소, 정보보호 서비스, 메커니즘들이 분석되어야 한다.

3 장. CALS에서의 정보보호 요소

CALS는 EDI와 통합 데이터베이스를 사용하게 되며 정보 교환과 공유시에 다양한 위협요소가 존재할 수 있다. 안전한 CALS 구축을 위하여 기밀성을 비롯한 무결성, 인증, 부인봉쇄 서비스가 제공되어야 하며 정보보호 서비스를 제공하기 위한 다양한 정보보호 메커니즘들이 활용되어야 한다.

3.1 CALS 위협요소

CALS는 분산된 시스템 환경에서 전자문서를 교환하는데 EDI를 사용하며 데이터를 공유하는데 통합 데이터베이스를 사용하기 때문에 각각에 대한 위협요소들이 존재한다[6,7,8,9]. 이러한 위협요소들은 일반적인 요소와 기술적인 요소로 구분될 수 있다. 일반적인 위협요소는 자연적인 현상으로 발생되는 **자연적 재앙**, 사용자의 오조작으로 발생될 수 있는 **에러 및 손실**, 내부자로부터 권한의 남용으로 인하여 발생되는 위협으로 **내부의 적**, 정보 시스템의 장애로 발생되는 위협으로 **시스템 장애, 바이러스** 등이 있다. 기술적인 위협요소로는 EDI 위협요소들을 포함한 다음과 같은 위협요소들이 존재한다. **위장**은 어떤 객체가 마치 다른 객체인 것처럼 위장하는 것으로서 비인가된 이용자가 자원을 불법적으로 접근하기 위하여 제3자가 정당한 사용자인 것처럼 위장할 수 있고 **메시지 순서 변조**는 메시지의 일부 또는 전부를 지연 전달시키거나 고의로 메시지 재발급 또는 순서를 재배치할 수 있다. 수신자에게 전달되는 정보, 라우팅 정보 및 관리 정보를 손실되게 하거나 변조하는 **정보 변조**가 있다. **서비스 거부**는 객체가 자신의 기능을 수행하지 못하거나 상대방의 기능 수행을 방해하고 제공된 서비스를 거부하는 것이고 **부인**은 시스템 사용자가 메시지 전송, 제출, 배달 등의 행위를 실제로 하였음에도 불구하고 하지 않았다고 부인하는 것이다. 이 외에도 메시지 전송 감시, 시스템내의 정보에 대한 비인가적 접근, 또는 위장 등에 의해서 비인가자에게 정보를 노출시키는 **정보 노출**과 해당 자원에 접근을 제어하기 위한 신분 레이블에 관련된 요소들을 변조하는 **신분 레이블 변조** 등이 있다.

3.2 CALS 정보보호 서비스

안전한 CALS 구현을 위해 제공되어야 하는 정보보호 서비스는 데이터 기밀성, 데이터 무결성, 인증, 부인봉쇄, 접근제어가 있다. [9,10]. **데이터 기밀성 서비스**는 CALS 체제에서 송·수신하는 데이터들이 네트워크 상에서 노출되지 않게 보호하는 것으로 접속 기밀성, 비접속 기밀성, 선택적 필드 기밀성, 전송량 흐름 기밀성 등이 있다. **데이터 무결성 서비스**는 CALS에서는 메시지 노출뿐만 아니라 메시지 수정, 삭제, 변조 등의 많은 위협요소가 존재하기 때문에 메시지의 변화여부를 확인하기 위하여 메시지 무결성을 제공해야 하며 복구기능을 갖춘 접속 무결성, 복구기능이 없는 접속 무결성, 선택적 필드 접속 무결성, 비접속형 무결성 및 선택적 필드 비접속형 무결성 등이 있다. **인증 서비스**는 CALS에서 메시지를 전송한 송신자가 정당한 사용자인지에 대한 보장을 제공하는 것으로 인증 메커니즘을 통하여 수신자가 송신자를 식별할 수 있도록 제공되어야 한다. 부인봉쇄 서비스는 CALS에서 메시지가 성공적으로 송신되었을 때 송신자가 송신한 내용을 부인하거나 수신자가 수신한 사실에 대한 부인과 같은 잠재적인 위협요소가 존재하기 때문에 이러한 위협들을 봉쇄하기 위한 것이다. **부인봉쇄 서비스**는 발신지 증명을 포함하는 부인봉쇄와 수신 증명을 포함하는 부인봉쇄 중 하나의 유형으로 제공된다. 발신지 증명을 포함하는 부인봉쇄는 데이터의 수신자는 데이터의 발신지에 대한 증명을 제공받는다. 이는 송신자가 데이터 또는 내용을 보낸 사실을 거짓으로 부인하려는 시도를 방지한다. 수신 증명을 포함하는 부인봉쇄는 데이터의 송신자는 데이터 전달에 대한 증명을 제공받는다. 이는 수신자가 데이터 또는 데이터 내용을 받은 사실을 거짓으로 부인하려는 시도를 방지한다. **접근 제어 서비스**는 개방 시스템의 상호 연결을 통하여 비인가된 자원의 사용에 대한 보호를 제공하는 것으로 특정 자원에 대한 여러 유형의 접근에 적용되거나 또는 모든 자원에 대한 접근에 적용될 수 있다.

3.3 CALS 정보보호 메커니즘

CALS 정보보호 서비스는 데이터 기밀성을 비롯한 무결성, 인증, 부인봉쇄, 접근제어가 제공되어야 하며 이를 제공하기 위한 정보보호 메커니즘은 아래와 같다[9,10].

암호화 메커니즘은 데이터 또는 전송량 흐름 정보에 대한 기밀성을 제공할 수 있다. **디지털 서명 메커니즘**은 데이터의 서명과 서명된 데이터의 확인 절차를 필요로 하며 서명은 서명자의 개인적인 정보를 사용하고 확인 절차는 공개적인 절차 및 정보를 사용한다. **접근 제어 메커니즘**은 접근 객체의 인증된 신원, 객체에 대한 정보 또는 객체의 역할로 접근 권리를 결정하고 접근 정책에 사용 가능하다. **데이터 무결성 메커니즘**에서는 송신자가 데이터 자체의 해쉬값을 데이터에 첨가시키면 수신자가 해당되는 해쉬값을 생성하여 생성된 값과 수신한 값을 비교하여 데이터가 전달 과정에서의 수정 여부를 확인한다. **해쉬 함수**는 메시지의 무결성 서비스를 위하여 중요한 정보의 무결성 확인과 메시지 인증 코드(Message Authentication Code : MAC)의 구성, 디지털 서명의 효율성 증대 등을 목적으로 사용한다. 해쉬 함수는 임의 길이의 비트 스트링을 입력으로 받아 고정된 짧은 길이의 비트 스트링으로 출력하는 함수이다. 많은 양의 정보에 대한 인증을 제공하는 방법으로는 그 정보로부터 계산된 짧은 해쉬 결과에 대해 인증을 제공하는 것이다. **인증 메커니즘**은 송신자에 의해 제공되고 수신자에 의해 송신자를 확인하는 것으로 인증정보의 사용, 암호화 기법, 객체의 소유 및 특색의 사용 등이 이용된다. **공증 메커니즘**은 무결성, 발신지, 시간 및 목적지와 같은 상대와 통신되는 데이터에 대한 성질은 공증 메커니즘에 의하여 보증될 수 있으며 통신자에 의해 신뢰될 수 있고 실증될 수 있는 방법으로 제3자 공증에 의하여 제공될 수 있다. **보안 감사 메커니즘**은 정보의 불법 유출을 예방하고 불법적인 행위를 추적하기 위한 것으로 정보보호 대상 시스템의 정보보호 관련 행위를 기록하고 조사하며 분석하는 과정으로 사용자 행위를 로그 파일에 기록하므로써 상대방과의 문제 발생시 감사를 위한 자료로 이용한다.

4 장. 안전한 CALS 정보보호 모델

4.1 안전한 CALS 정보보호 모델 구성

CALS 체제는 통합 데이터베이스의 정보를 검색 및 저장하고 메시지를 송·수신하는데 있어서 많은 위협요소들이 존재하며 이러한 위협요소들로부터 보호하고 CALS를 원활하고 효율적인 운영을 위하여 정보보호 모델이 요구된다. CALS 정보보호 모델은 CALS에서 요구되는 정보보호 서비스를 지원해야 하며 서비스를 지원하기 위한 다양한 정보보호 메커니즘들의 활용이 불가피하다. 따라서 **안전한 CALS를 위한 정보보호 모델은 기능에 따라 4개의 서브 모델로 구성되는데 전송 모델, 키관리 모델, 보안 감사 모델, 통합 데이터베이스 연계 모델**이며 <그림 1>과 같은 구조를 갖는다.

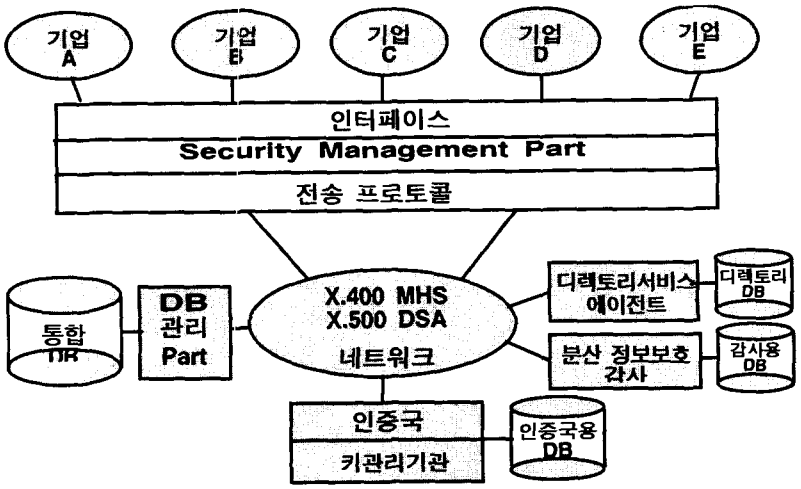
CALS 정보보호 모델 구조는 크게 **정보보호 관리부(Security Management Part), 인증국 및 키관리 기관, 디렉토리 서비스 에이전트, 통합 데이터베이스 관리부, 보안 감사(Security Audit)**로 구성된다.

정보보호 관리부는 <그림 2>와 같이 구성되고 CALS 체제의 어느 한 시스템이라도 정보보호 관리부의 부재시에는 취약 부분이 생길 수 있으므로 모든 시스템에 제공되어야 하며 정보보호 서비스에 대한 처리 기능을 제공한다. 상위 레벨에는 정보보호 서비스를 위한 정보보호 관리 정보 베이스(SMIB)가 위치하게 되며 다양한 메커니즘과 연계하에 정보보호 서비스를 제공한다. 하위 레벨에는 보안 감사, 키 관리, 데이터베이스 관리 모듈들과 각각의 인터페이스로 구성된다. 보안 감사 모듈은 정보보호 서비스를 처리하는 과정에서 발생하는 정보보호 관련 행위들을 감사 추적 하기 때문에 CALS에서는 보안 감사 기능이 요구되며 데이터베이스 인터페이스를 이용하여 데이터베이스로부터 감사 자료를 이용하여 감사추적에 사용한다. 키 관리 모듈은 키 관련 요청들을 처리하기 위한 것으로 발신자의 비밀키 및 공개키의 요청, 수신자의 공개키 요청, 신원 정보의 검증 및 디렉토리 시스템 접속 등을 수행하고 데이터베이스를 이용하여 키와 관련된 정보의 검색, 저장, 변경 등을 수행하게 된다. 데이터베이스 관리 모듈은 키 관리와 보안 감사를 수행하는데 필요한 정보들을 저장하고 요청에 대한 서비스를 제공한다.

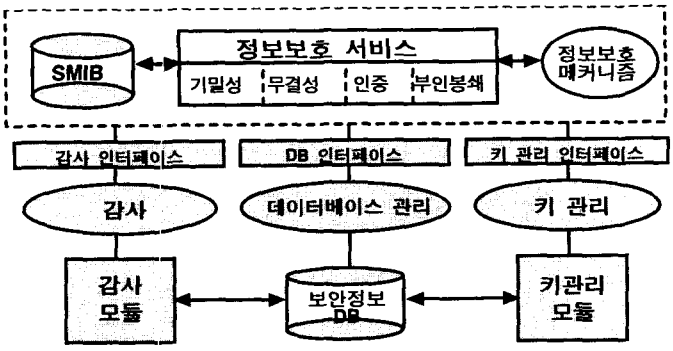
인증국 및 키관리 기관은 키와 관련된 생성 및 분배, 인증서 발급 등을 수행하며 키 관련 정보들을 저장, 검색, 변경의 기능까지도 요구된다.

디렉토리 서비스 에이전트는 CALS 사용자들에 대한 정보들을 저장하고 있으며 서비스 요청시에 실시간으로 수행하며 디렉토리 사용자에 대한 인증기능도 제공한다.

통합 데이터베이스 관리부는 기업들의 정보가 통합된 형태로 정보가 어느 곳에 위치하든지 요청시에는 즉시 서비스를 제공해야 되며 분산된 환경에서 보안 감사를 수행하므로써 정보보호를 위반하는 사건 발생시 경보를 울리거나 추적하는 기능을 필요로 한다.



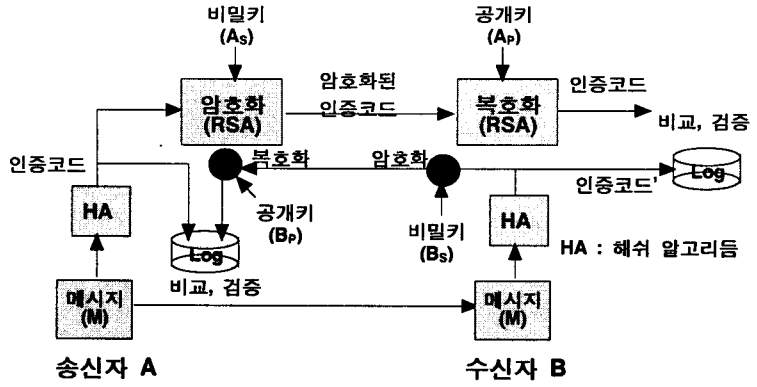
<그림 1> 안전한 CALS 정보보호 모델 구조



<그림 2> Security Management Part 구조

4.2 전송 모델

CALS 메시지들은 외부 노출시 막대한 피해를 입을 수 있기 때문에 송신자가 수신자 사이에는 안전한 메시지 전송이 요구된다. 이를 위해 다양한 정보보호 서비스의 제공하에 전송하게 되는데 CALS에서는 데이터 기밀성, 데이터 무결성, 인증, 부인봉쇄 서비스가 제공되어야 한다. 이러한 서비스는 송신자가 데이터를 노출되지 않고 수신자에게 전송하기 위한 기밀성, 수신자에게 전송된 데이터가 아무런 변화 없이 전송되었다는 무결성, 데이터 송신자가 정당한 사용자라는 것을 식별하기 위한 위한 인증, 그리고 송신자와 수신자의 데이터 송·수신에 대한 부인을 봉쇄하기 위한 부인 봉쇄이다. CALS에서는 이러한 서비스들은 앞에서 분석된 정보보호 메커니즘들의 지원하에서 제공될 수 있으며 이러한 메커니즘들의 지원하에서 제공되는 CALS 전송 모델 중 예로서 부인봉쇄 서비스를 <그림 3>에서 제시했다.



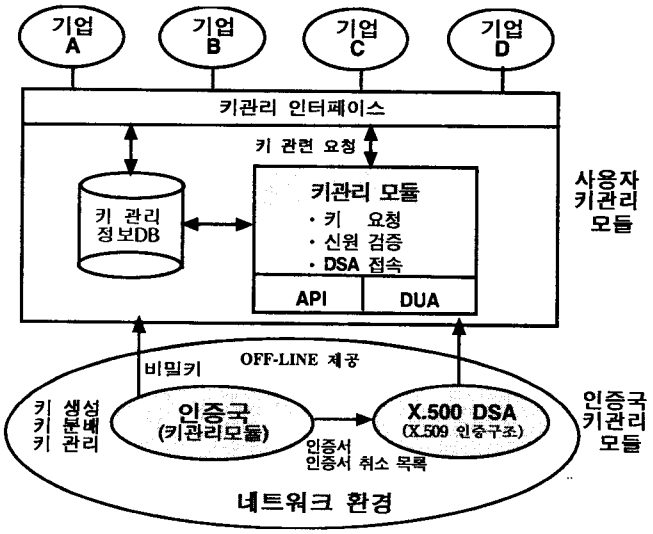
<그림 3> 부인봉쇄 모델

4.3 키 관리 모델

키 관리에서는 사용자 비밀키를 당사자만이 알아야 하며 정보보호를 위하여 키의 생성으로부터 키의 폐기까지 키에 대한 보호가 절실히 요구된다. 키는 인증국으로부터 생성되며 인증국은 키의 관리를 위하여 인증서를 생성하여 오프 라인으로 발행하게 된다. 인증서에는 만기일에 관련된 기한이 포함되어야 하고 인증서의 재사용을 위하여 인증국은 만기된 인증서를 대체하는 인증서 교체를 정확히 제공해야 한다. 그리고 만기된 인증서는 디렉토리로부터 제거된다.

CALS에서의 키 관리는 각각의 사용자를 지원하는 키 관리 모듈과 이러한 각각의 키 관리 모듈들을 전체적으로 관리하는 인증국 키 관리 모듈로 구분할 수 있다. CALS 키 관리 모듈은 주로 키 관리 인터페이스를 통하여 키 관련 요청들을 처리하게 되는데 발신자의 비밀키 및 공개키의 요청, 수신자의 공개키 요청, 신원정보의 인증을 위한 검증 및 디렉토리 서버에 접속 등을 포함한 기능을 수행하고 인증국 키 관리 모듈은 사용자 인터페이스, 키 생성, 키 분배, 키 관리 기능을 수행한다.

CALS 키 관리 모델은 <그림 4>에서와 같이 디렉토리 사용자 에이전트와 키 관리 인터페이스로 구성되며 인증국 및 디렉토리 서비스 에이전트가 요구된다[9,11,15]. 디렉토리 사용자 에이전트는 X.500 디렉토리 서버에 접속하여 사용자 인증서, 인증국 인증서, 취소목록 등을 조회하는 역할을 하며 키 관리 인터페이스는 수신된 공개키가 정당한가를 확인하고 상위레벨로 키의 정보를 전달하는 역할을 수행하며 키 관리 정보 데이터베이스에 키 관련 정보들을 저장하므로써 필요시 접근 가능하도록 구성된다.



<그림 4> CALS 키관리 모델

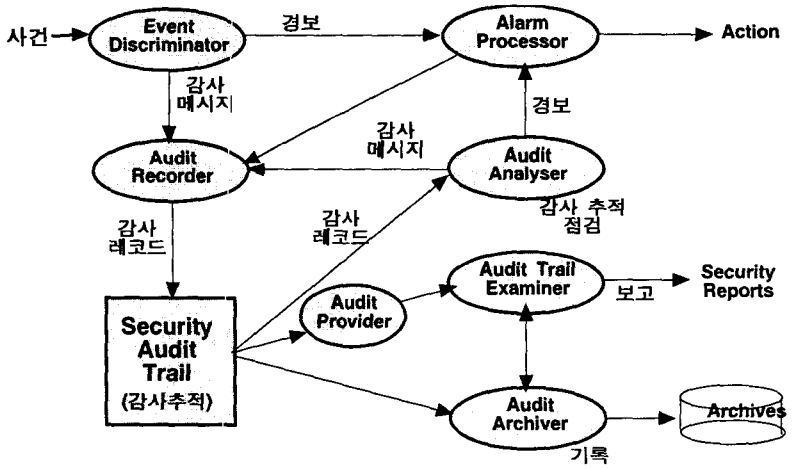
인증국 키관리 모듈은 사용자 인터페이스, 키 생성, 키 분배, 키 관리 모듈을 포함하고 있으며 모듈별로 기능을 수행한다. 사용자의 공개키가 포함된 인증서는 디렉토리의 디렉토리 서비스 에이전트와 완전히 분리된 오프 라인으로 인증국에 의해서 생성되며 사용자의 개인 식별 정보와 함께 디렉토리에 저장된다. CALS 사용자의 디렉토리 인증을 위하여 X.509 디렉토리 인증 서비스가 사용되고 인증국들은 계층구조를 가지며 오프 라인으로 생성된 비밀키는 그 사용자에게 전달하고 공개키는 인증서 형태로 디렉토리에 저장한다. 사용자의 비밀키가 노출되거나 사용자의 공개키를 더 이상 인증할 필요가 없는 경우 그러한 인증서들에 대한 취소 목록을 만들어 디렉토리에 저장하는 기능까지도 수행한다.

4.4 보안 감사 모델

CALS 체제는 다른 어떤 체제보다도 많은 거래들을 포함하고 있으며 거래자들 사이에서 정보의 불법적인 유출을 비롯한 불법적인 행위들이 발생할 수 있으며 이러한 문제들을 해결해 줄 수 기능이 요구된다. CALS는 개방형 환경에서 시스템들이 분산되어 있기 때문에 정보보호를 위하여 분산된 보안 감사가 필요하며 필요시에는 정보보호 경보를 울리므로써 시스템들을 비롯한 CALS의 자산들은 보호되어야 한다.

보안 감사는 정보의 불법 유출을 방지하고 불법적인 행위를 추적하기 위한 것으로 정보보호 대상 시스템의 정보보호 관련 행위들을 기록하고 조사하며 분석하는 과정이라 말할 수 있다. 감사 대상은 시스템의 사용자 및 프로세스 등의 주체, 단말기 및 통신 메시지 등의 객체와 인증 및 부인 봉쇄 등의 정보보호 서비스 수행을 위한 해쉬, 인증 알고리듬 및 키 교환 알고리듬 등을 대상으로 한다[14]. CALS 보안 감사 정보는 보안 감사 메시지, 보안 감사 레코드, 정보보호 경보, 정보보호 보고가 사용된다. 보안 감사는 정보보호 정책의 적절성을 평가하고 정보보호를 위반하는 사건들을 감지하게 된다. 개개인이 적절한 행동을 취할 수 있어야 하며 자원의 오용에 대한 감지까지도 지원해야 하며 정보보호 위반에 대한 보호를 직접적으로 포함하지는 않으나 정보보호 위반 사항들에 대한 사건들을 감지, 기록, 분석할 수 있다. 정보보호 경보는 경보 상태의 정보보호 정책에 의해 정의된 정보보호 관련 사건의 감지에 따라서 생성된다.

보안 감사 모델은 alarm processor, audit analyser, audit archiver, audit dispatcher, audit trail examiner, audit recorder, audit provider, audit trail collector, event discriminator의 프로세스로 구성되며 감사 절차는 감지 단계, 결정 단계, 경보 절차 단계, 분석 단계, 수집 단계, 보고 발생 단계, 기록 단계별로 수행되며 <그림 5>와 같다.



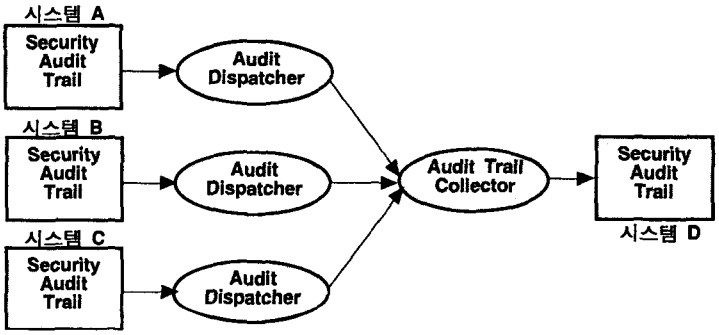
<그림 5> 보안 감사 모델 구조

event discriminator는 보안 감사 메시지 또는 정보보호 경보 메시지가 생성되어야 하는지를 결정하기 위해서 사건을 초기분석한다. 보안 감사 메시지는 audit recorder로 전송되고 정보보호 경보는 평가 및 추가 행동을 위하여 alarm processor로 전송된다. 보안 감사 메시지들은 형식화(format)되어 보안 감사 추적을 위한

보안 감사 레코드로 변환된다. 보안 감사 추적에 이미 존재하던 부분들은 기록되고 보안 감사 추적과 보안 감사 추적 레코드들은 특정화된 기준에 따라서 특정 보안 감사 레코드를 선택하므로써 정보보호 보고를 수행한다. 즉, 보안 감사 추적에서 생성된 보안 감사보고 그리고(또는) 정보보호 경보가 분석된다.

CALS에서는 한 시스템만의 보안 감사뿐만 아니라 분산된 환경에서의 모든 시스템들의 총괄적인 보안 감사가 요구된다. <그림 6>의 기능들은 시스템 중 하나의 구성요소에 배치되며 특히 동일한 보안 감사 추적에서 작동되는 audit recorder, audit dispatcher, audit provider, 그리고 audit analyser는 포함되지 않는 종 시스템의 일부분을 형성할 수도 있다. 다른 그룹화는 audit trail examiner일 수 있으며 보안 감사자를 위한 유용한 audit analyser일 수 있다.

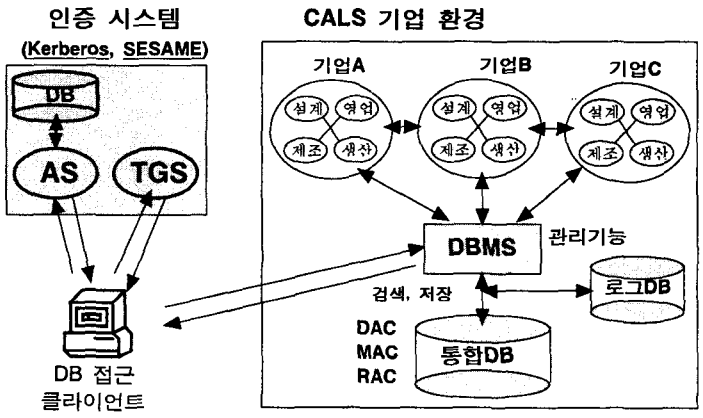
특히 분산된 보안 감사 추적에서 계층적 의미로는 정렬된 기능이다. 하나의 구성요소인 audit trail collector는 audit dispatcher로부터 감사 메시지를 수집하며 어떤 구성요소로부터 audit dispatcher가 지원되지 않을 때 종료한다. 이 경우에서 보안 감사 추적을 성취시킬 수 있는 audit archiver를 지원해야 한다.



<그림 6> 분산된 감사 추적 구조

4.5 통합 데이터베이스 정보보호 연계 모델

CALS에서의 통합 데이터베이스는 기업간의 정보공유를 비롯하여 정형·비정형 정보의 관리, 문서 검색 기능, 데이터 분석 기능, 외부정보 수집 기능 등이 제공된다. 많은 유용한 정보를 소유하고 있는 통합 데이터베이스는 많은 위협들이 존재할 수 있으므로 다양한 정보보호 메커니즘을 이용한 정보보호가 절실히 요구된다[4]. CALS에서 통합 데이터베이스가 연계된 정보보호 모델은 <그림 7>과 같으며 통합 데이터베이스의 정보보호를 위하여 인증 메커니즘, 접근제어, 암호화 기술, 감사가 제공된다.



<그림 7> 통합 데이터베이스 정보보호 연계 모델

통합 데이터베이스의 서버로부터 서비스를 받기 위하여 임의 클라이언트들은 접근을 시도할 수 있다. 권한 없는 클라이언트가 접근할 수 있으므로 접근하려는 사용자가 정당한 사용자인지를 확인할 필요가 있으며 인

증 절차로 Kerberos 또는 SESAME 인증 시스템을 이용하여 신분을 확인한다[12,14]. CALS에서는 비밀성을 유지하기 위하여 권한이 부여되지 않은 사용자에게 데이터베이스에 저장된 정보를 노출시키지 않기 위한 방법으로 접근을 제어한다. 접근 제어에는 임의적 접근제어(DAC : Discretionary Access Control), 강제적 접근제어(MAC : Mandatory Access Control), 역할기반 접근제어(RAC : Role-based Access Control) 등이 있다. 통합 데이터베이스의 정보보호를 위한 또 다른 기법으로는 통합 데이터베이스에 접근하여 데이터를 저장하거나 검색된 데이터를 전송할 때 암호화 기술을 사용하여 데이터의 기밀성을 제공할 수 있다. 데이터베이스의 정보를 암호화하여 저장하고 암호화된 상태로 전송하므로 데이터를 좀더 안전하게 유지할 수 있으며 통합 데이터베이스 서버는 정보를 저장시에 암호화한 후에 저장한다. 통합 데이터베이스의 DBMS가 데이터들을 저장하고 데이터를 변경하고 검색하는 등에 대한 행위들을 로그 화일에 기록·저장하여 유지하므로써 정보보호 문제 발생시 보안 감사의 자료로 제공될 수 있으며 보다 향상된 정보보호를 기할 수 있다.

5 장. 결 론

CALS 도입으로 네트워크를 통한 데이터 교환 및 공유가 가능해졌다. 그러나 이러한 장점에도 불구하고 정보보호 문제라는 역기능으로 인하여 군을 비롯한 민간부문과 정부에서 CALS를 구축하여 운영하는데 문제시되고 있다. 따라서 본 논문에서는 CALS 정보보호 위협 요소를 비롯한 정보보호 서비스와 메커니즘을 분석하고 CALS를 안전하게 구축하기 위한 정보보호 모델을 제시하였다.

본 논문에서 제안된 CALS 정보보호 모델은 4개의 서브 모델인 전송모델, 키관리 모델, 감사 모델, 통합 데이터베이스 연계 모델로 구성된다. 전체적인 구조는 정보보호 관리부, 디렉토리 서비스 에이전트, 인증국과 키관리 기관, 분산 환경에서의 보안 감사, 통합 데이터베이스 관리부로 구성된다. 정보보호 관리부는 키관리, 감사, 데이터베이스 관리부로 구성된다. 인증국과 키관리 기관은 키 생성부터 폐기까지의 모든 정보들을 관리하는 기능을 수행하고 디렉토리 서비스 에이전트는 각 사용자를 지원하는 디렉토리 사용자 에이전트와의 통신을 통하여 사용자들의 정보들을 저장하고 정보 요청시 실시간으로 제공하는 기능을 수행하며 디렉토리 서비스 인증은 X.509의 정의를 따르고 있다. 보안 감사는 정보의 불법 유출을 예방하고 불법적인 행위를 추적하므로서 향상된 정보보호를 제공한다. 통합 데이터베이스 관리부는 접근하는 사용자의 권한을 검증하여 요청된 정보를 제공하는 기능을 수행하게 되는데 인증 메커니즘, 접근 제어, 암호화기술, 감사 등을 통하여 통합 데이터베이스의 보호를 제공하므로서 안전한 CALS 환경을 구축할 수 있을 것이다.

본 논문에서는 분산 개방형 환경인 CALS 체계의 안전한 구축을 위하여 정보보호 메커니즘들을 활용한 정보보호 모델을 제시하였다. 지금까지 CALS에 대한 정보보호 연구가 활발히 진행되지 못하였고 모델이 제시된 바도 없었다. 제안된 CALS 정보보호 모델은 CALS를 안전하게 구축하는데 도움이 되리라 생각된다. 앞으로도 CALS에서 정보보호에 대한 연구는 계속될 필요가 있으며 이러한 정보보호 연구외에도 CALS의 원활한 운영을 위하여 다양한 기술들이 연구되어야 할 것이며 예로서 통합 데이터베이스에서 실시간 처리 및 병행제어 연구가 요구된다.

참 고 문 헌

[1] 김철환, 김규수, "21세기 정보화 산업 혁명 CALS", 도서 출판 문원, 1995, pp.13-18.

[2] 김규수, 김철환, 김유일, 윤용석, 김문호, "산업 정보화와 CALS", 한국 CALS/EC 기술협회 세미나, 1996.6.

[3] 정기원, "국내기업의 CALS 관련 정보화 실태 및 SI업체 동향 조사", 한국 CALS/EC 학회, 1993.7.

[4] 김덕현, "CALS 개념의 통합 데이터베이스", 한국 정보처리 학회지, Vol.4 No.1, 1997.1.

[5] 신장균, 나민영, 이승희, "CALS 구현을 위한 정보기술", 한국 정보과학회지 Vol.13. No.11, 1995.11.

[6] Fred Cohen, "Large Information System Attack Methods : A Preliminary classification Scheme", Computer & Security, Vol.16 No.1, 1997.

[7] 강창구, "EDI 정보보호 서비스 분석", 제2차 안전한 EDI 관련기술 심포지움, 1996.3.

[8] Chang Goo Kang, E Joong Yoon, Dae Ho Kim, Dai Ki Lee, "A Design of Secure EDI Systems", 8th CCSS '96, 29 April-3 May, 1996.

[9] 이임영, 이재광, 소우영, 최용락, "통신망 정보보호", 도서출판 그린, 1996.2, pp.342-356, pp.394-439.

[10] CCITT X.800, "Security Architecture for Open System Interconnection for CCITT Applications".

[11] 최용락, 강창구, 김대호, "디렉토리 모델과 정보보호 서비스", 한국통신정보보호 학회지, Vol.5 No.3, 1995.9.

[12] 강창구, 최용락, "개방형 분산 시스템 환경의 인증 메커니즘 분석", 한국통신정보보호 학회지 Vol.7 No.2, 1997.6.

[13] 김영균, 서재현, 노봉남, "객체지향 데이터베이스 보안", 한국통신정보보호 학회지 Vol.4 No.4, 1994.12.

[14] ISO/IEC 10181-7, "Information technology - OSI - Security frameworks for open systems : Security audit and alarms framework", 1996.

[15] Tom Carty, GTE, Security Eletronic Commerce, Certificate Management Systems", 9th CITSS '97, 12-16 May, 1997.