通信情報保護學會誌
第7卷 第3號, 1997. 9

CALS 체제의 정보보호 프레임워크

CALS Security Framework

신 종 태***, 이 정 현**, 이 대 기**, 소 우 영*

요 약

현대 사회의 경제 및 사회 활동에는 필연적으로 컴퓨터, 통신과의 정보 통합이 요구되며 전송 정보의 표준화를 근간으로 하는 CALS의 도입이 필요하다.

본 논문에서는 CALS 체제의 외국 동향 분석과 CALS에서의 정보보호 위협 그리고 보안 요소들과 CALS 구현 사례 연구를 통하여 안전한 EDI 시스템을 근간으로 하는 CALS 정보보호 통합 체제의 프레임워크를 제시하였다. 이러한 작업은 국내 산업에서 도입이 되고 있는 CALS 체제의 정보보호 연구에 도움이 될 것이며 CALS 통합 체제 정보보호 모델 개발에 기반이 될 것이다.

1. CALS 체제

가. CALS 출현 배경

급속하게 변화하는 시장환경에 기동성 있고 창조적으로 대응하기 위해서는 의사 결정과 정보 확보의 신속성이 중요하다. 그러나 정보가 공유되지 않는 계층형 조직환경에서는 의사결정이 지연되거나 경영자원의 효율적 투입을 저해하고 분권적 조직의 비대화로 간접부문의 증가을 초래하여 생산성을 저하시켜 업무의 기동이 결여되는 단점이 있다. 그러므로 다양화하는 수요에 시의 적절하게 대처하며 사업의 효율적 전개와 시장 창출 및 확대를 위해 창조적인 조직이 필요하다. 그리하여 상품기획, 생산, 계획부터 생산과 출하까지의 전 업무의 프로세서를 단축할 수 있는 CALS 체제가 요구되었다[1].

CALS의 핵심은 제품의 개발, 설계, 생산, 조달, 운용, 유지보수에 이르기까지의 모든 정보를 디지털화하여 기업내의 부서간은 물론, 세계의 다른 협력기업들이 공동으로 활용하여 글로벌 시장(Global Market)을 형성하고 가상기업(Virtual Corporation/ Virtual Enterprise)을 실현하여 개별 기업과 산업 전반의 생산성을 획기적으로 높이고자 하는 것으로 이해할 수 있다. CALS의 개념은 하나의 기업, 또는 한 나라 산업의 생산성 향상과 경쟁력 확보에 엄청난 효과를 가질 수 있다는 확신에서 기인

* 한남대 컴퓨터공학과
** 한국전자통신연구원
*** 한국정보보호센터

본 논문은 한국전기통신공사의 출연금에 의하여 수행한 연구결과입니다.

한다. 그런 이유로 세계의 주요 기업들 뿐 아니라 정부 차원에서도 CALS에 대해 큰 관심을 보이고 있다.

나. CALS 개념

미국에서 태동한 CALS 개념은 정보를 다루는 각종 시스템이 산업 네트워크를 통하여 정보화 사회에서 가장 쉽고 빠르게 다양한 정보를 얻을 수 있는 기반적 도구가 된다는 것이며 이에 따라 한 국가의 시장을 전 세계에 개방하는 방향으로 발전되고 있다.

CALS는 사용자의 용도에 따라 조달정보시스템, 전자거래 지원시스템 제품통합 정보시스템으로 불리나 설계, 부품, 재료조달, 생산, 출하, 유통 등 제품의 모든 과정을 지원하는 정보시스템으로서 기업의 생산, 조달 운용지원 통합정보시스템으로 정의되어 왔다. 기술정보나 거래정보를 특정 기기나 시스템의 제약을 받음이 없이 디지털화한 상태로 주고받을 수 있는 수요자 본위의 데이터 환경을 형성하는 시스템으로 가장 간단하게는 기업활동 전반에서 종이 없는 정보시스템이라고 할 수 있는 CALS는 종래와 같은 수치데이터뿐만 아니라 설계도, 매뉴얼과 같은 화상정보나 음성을 포함한 멀티미디어 정보를 교환할 수 있는 미래형 산업 정보시스템이라 할 수 있다. 개발 설계조달에서 보수, 운용까지의 모든 부문과 각국면에서 관련되는 기업이 정보를 공유하고 활용함으로 CALS 체제는 흡사 하나의 가상기업으로 유기적으로 제휴하게 되어 개발 조달 시간을 단축하고 생산성을 향상시켜 제품의 전 과정에서 경비 절감을 위한 새로운 산업정보인프라 구조로 발전된다.

초기에는 미국에서 컴퓨터 통신을 이용한 군수지원을 위해 개발된 컴퓨터에 의한 병참지원(CALS : Computer Aided Logistic Support)라는 의미로 CALS라고 명명하였으나 현재에는 전자거래 및 결재의 광속화(CALS : Commerce At Light Speed)의 의미로 사용되고 있다[1].

표 1 CALS 확대 개념의 적용 범위

	부품소품 상거래	설계 제조 조달 품의 보급	물류	교환 자금 결재
Computer Aided Logistics Support(1985)			O	
Computer-aided Acquisition and Logistics Support(1988)		O	O	
Continuous Acquisition and Life-cycle Support(1993)	O	O	O	
Commerce At Light Speed(1994)	O	O	O	O

CALS는 궁극적으로 각종 제품 및 장비의 생산 분야, 물류지원 분야 그리고 무역 및 상거래 분야에서 국제 공동표준에 의해 정보를 상호 공유하고 교류하는 자동화 및 정보화 환경을 구축하자는 것이며 미국, 유럽 및 일본 등의 정보 선진국에서는 이미 산업 정보화 환경에 CALS개념을 적용하여 구축하고 있다.

국내에서도 CALS 체제에 의한 정보의 표준화와 경제 사회 활동에 있어 컴퓨터, 통신과의 통합이 요구되어, 최근 통상산업부에서는 국내 산업에 CALS 체제를 적극적으로 도입하기 위한 업종별 CALS 모델을 설정하기로 결정하고 이를 위해 '96년 1월 전자, 제철, 중공업, 방위

산업, 전력, 원자력, 통신, 항공 등의 8개 업종에서 10개의 시범 사업체를 선정하였다. 또한 정보통신부, 국방부, 조달청 등에서는 자체 CALS 체제 도입을 위해 활발한 활동을 보이고 있다[9].

CALS의 목표로는 첫째로 각종 기술자료를 디지털화한 후 관련 데이터를 통합 운영하는 업무환경 구축으로 종이 없는 업무수행체제를 구현하는 것과, 둘째로 요구사항 및 변경사항을 적시에 수용하여 시스템 개발기간을 단축하는 것과, 셋째로 동시공학(Concurrent Engineering)적 정보서비스를 통해 문서관리 소요비용, 행정절차, 인력 등을 절감함으로 정보화 경영혁신과 소요 비용을 절감하는 것과 마지막으로 설계제작시 발생하는 오류감소, 부적합한 분야의 운영개선, 정보의 일관성 유지 등으로 품질을 향상시킬 수 있는 것 등이며 상호적인 작용으로 많은 부가적인 효과를 기대할 수도 있다. 여기에 정보보호 서비스를 CALS에 부가 적용함으로 기업의 전자상거래 정보보호, 전자 거래 정보의 이중 사용 방지, 전송의 부인 봉쇄 등의 부가 이익을 기대할 수 있다.

CALS로의 통합 체제는 정보의 보고이자 위험의 보고라는 인터넷을 바탕으로 전개되고 있다. 인터넷은 기본적으로 개방된 네트웍이며 전산망간의 원활한 통신을 보조하는 방향으로 발전하기 때문에 이면에는 많은 정보의 노출 위험이 상존하고 있다. 최근 들어 정부기관 및 기업들의 폭발적인 인터넷 사용 증가와 상업적 인터넷 활용으로 정보보호 측면이 심각한 문제로 대두되고 있다.

내부 네트워과 외부 네트워의 모든 통신은 양자간에 오가는 모든 통신을 감시하여 불법적인 접근을 차단할 수 있어야 한다. 실제 환경에서 정보보호 기법의 적용에는 부수적인 문제가 있다. 위협에 대한 적절한 대처 방법으로 보안 메커니즘의 강도를 높이면 해킹 위험성은 감소하지만 사용자의 자유로운 활동이 제한되어 네트웍 사용 효율이 떨어지는 반면에, 보안 강도를 낮추면 해킹의 위험성은 그만큼 커지므로 체제 구축 소요 비용 문제와 함께 숙고하여 결정해야 할 중요한 요소이다. 그러므로 정보보호 기술은 CALS 통합 체제를 구축함에 있어 수반되어야 할 기반요소기술 중에 반드시 선행되어야 함을 강조함에 지나침이 없으며 가장 먼저 고려해야 할 사항 중 하나이다.

라. 동시공학

동시공학은 신제품개발 및 제품변경을 위하여 초기 제품개발 단계에서 생산 및 유지보수에 이르기까지의 관련공정을 동시적으로 통합화하기 위한 관리적, 공학적 방법을 의미하며 CALS에 있어서는 IDB(Intergrated DB)를 구축하여 CALS 환경에 필요한 여러 프로세스들 간의 상호 자료교환 및 변경이 서로 가능하세 할 수 있다.

2. CALS의 국내외 동향

가. 국외 기술 동향

1) 미국

CALS의 선두주자인 미국은 이미 '94년 10월 '연방조달효율화법'을 제정하여 연방정부와 거래를 하고자 하는 모든 기업이 의무적으로 CALS를 채택하도록 하였다. 상무부는 CSRC에서 국면에 ESRC로 개명한 공용자원센터(Shared Resource Center)를 설치하여 중소기업을 대상으로 CALS/EC 관련 교육을 시행하고 있으며, 산하기관인 NIST(표준기술원, National Institute of Standards and Technology)와 NTIS(기술정보서비스센터, National Technical Information Service)에서 CALS 연구와 대국민 교육 홍보를 수행하도록 하였다[3]. 국방부도 기

술계획청(Advanced Research Projects Agency), 방위산업협회(National Security Industry Association), 기술재투자계획(Technology Reinvestment Project) 등을 통해 CALS에 관한 연구와 산업계에의 파급 업무를 담당하도록 하였다.

미국은 94년에 연방 EC(Electronic Commerce) 시스템을 개발하여 구축하였으며 정부와 거래하는 기업간 견적서, 구매 의뢰서 등을 표준화된 형식으로 초기 EC 시스템을 구축하였다. 이에 대한 구체적인 연도별 중요사항을 살펴보면 다음과 같다. '95년에는 대금납부, 지원DB 등의 확장 EC시스템을 구축하였고 '96년에 행정업무의 전산화를 일부 마무리하였다. 전자조달 시스템을 구축하여 CALS를 가동중인 내무부는 재정시스템을 통합시켜「원-스톱」전자상거래를 구현하고 있다. 국방부도 군 표준 자동계약시스템을 가동시키고 있으며 10여 개의 부서가 EC망을 구축하여 운영중에 있다. '97년에는 연방정부는 FACNET(Federal Acquisition Computer Network) 구축할 예정이며, 2000년까지 정부의 물자조달 업무를 CALS 프로그램에 의거한 방식으로 의무화하였다. 이러한 상황 변화는 CALS의 보급여부를 떠나 글로벌한 산업정보기반인 CALS로의 정확한 대응이 필요 불가결해질 것이라는 확신하고 국제적인 거래에서 CALS 체제가 요구될 것으로 판단한 결과이다.

CALS 도입의 효과를 나타내기 위해 미국의 CALS 산업진흥회 회원 1,000명을 대상으로 제조업을 근간으로 조사한 결과를 〈표 2〉로 제시하였다.

표 2 CALS 도입의 효과

관 련 공 정		효 과
설 계 공 정	- 개발기간 단축	82%
	- 설계도면수 절감	평균 200 ⇨ 3
	- 설계변경횟수 감소	80%
	- 설계자료 열람시간 감축	수일 ⇨ 수분
	- 설계설비장치	거의 소멸
생 산 공 정	- 조립공정	6주 ⇨ 2시간
	- 공정의 축소	7 : 1
	- 불량률 제거	6배
	- 수치제어 공정	40% 축소
	- 불량검사 축소	40%
	- 제고비용 절감	30
	- 재작업 축소	80%
생 산 정 보 관리 및 전송	- 자료관리 인쇄비	70%절약
	- 자료의 착오제거	98%
	- 자료 수정시간 단축	30%
	- 설계서 작성시간 단축	70%

2) 유럽

유럽에서는 '94년 CALS International을 설치하고 미국, 영국, 프랑스, 일본의 기업인으로 구성된 IBOD(International Board Of Directors)와 미국, 영국, 프랑스, 일본, 독일, 캐나다, 호주, 대만 등 8개국 대표로 구성된 ICC(International CALS Congress)를 창설하였다[9].

한편 전자 카드 체제를 시범 운용하고 있으며 영국, 벨기에, 덴마크, 네덜란드, 핀란드 등에서는 실용화 단계에 있으며 유럽의 정보 통합을 위해 CAFE(Conditional Access for Europe) 프로젝트를 수행하고 있다.

3) 일본

경제 발전 속도에 비해 CALS에 관한 인식이 비교적 늦었지만 '91년부터 통산성이 중심이 되어 전자공업진흥협회내에 CALS 추진협의회를 조직하여 운영하고 있으며 전력부문을 대상으로 CALS 시범시스템의 구축을 근간으로 CALS의 연구개발과 조기 국내 정착에 노력하였다.

통산성에서 '95년을 CALS 구현의 원년으로 설정하여 CIF(CALS Industry Forum)을 결성하였으며 CALS 기술연구조합을 설립하였고 향후 5년간 20~30억엔을 투입하고 있다.

또한 NTT에서는 전자현금시스템을 개발하였으며 일본 대장성에서는 '98년부터 전자화폐를 실용화할 것이라고 발표하였다[3, 10].

나. 국내 기술 동향

1) CALS 추진 동향

국내의 CALS 추진을 민간에서 필요를 제기하고 정부 주도의 추진 경향을 띄고 있다.

CALS 체제 구축내용을 공개함으로써 가능한 범위에서 타사에 표본으로 제공하도록 하였고 CALS 체제 도입에 관한 주요 계획을 마련하고자 한국과학기술원, 국방대학원 등 관련 연구기관으로 하여금 국내 산업의 CALS체제 도입을 위한 기본 지침, 산업 정보망 사업 및 초고속 통신망간의 연계 및 통합방안, 산업정보화 발전프로그램 등을 검토하도록 하였다.

중소기업청에서는 CALS 도입의 가속화를 위한 CALS 표준으로 EDI(Electronic Data Interchange) 등에 대한 KS규격을 제정, 고시하였고 계속적으로 관련 표준화 작업을 추진할 계획에 있으며 산업계, 학계, 연구기관의 전문가로 구성된 CALS 표준전문위원회를 구성하여 운영하고 있다. 또한 조달청에서는 정부조달 관련 문서 교환을 위한 EDI 시스템을 개발하여 '97년부터 시행할 계획에 있으며 이를 CALS와 연계할 계획도 갖고 있다.

정보통신부는 국가 정보화 추진과 정보통신 분야의 연구개발을 지원하고 국내 기업의 CALS 도입 촉진을 뒷받침하기 위해 초고속정보통신기반 구축사업의 응용과제로 전자 교환기 관련업체들을 대상으로 한 CALS 시범사업을 추진할 예정으로 있다.

국방부는 CALS를 적극 추진하기 위해 국방정보체계연구소 내에 전담 연구실을 설치하여 국방 CALS 추진 중장기계획을 세우고 있다.

위에서 거론하지 않은 정부기관에서도 CALS의 도입을 위해 많은 노력을 하고 있으며 한국통신, 원자력 연구소, 포항제철 등과 같은 기관에서도 CALS를 응용한 시스템들을 개발하여 업무에 적용하기 시작하였고 민간부문에서 '96년 한국 CALS 위원회, 통산산업부 산하의 한국 CALS/EC 협회, 정보통신부 산하의 한국 CALS/EC 기술협회 등이 조직되었고 한국 CALS/EC 학회가 설립되어 활발한 활동을 하고 있다[9].

정부는 국가 초고속정보통신망(NII : National Information Infrastructure) 추진 정책에 CALS 개념과 구현시스템을 접목시키고 있으며, 이와 연동된 산업정보망과 산업의 정보화에 CALS 전략을 적용하며, 이를 위해 CALS 표준개발에도 적극적으로 나서고 있다.

2) 국내 구현 사례

국내 금융업계에서 최근에 활발한 움직임을 보이고 있으며 특히 개방형 클라이언트/서버 환경으로의 전환과 함께 이미지 처리 시스템, 인터네트, 그룹웨어 등을 도입하여 운영하고 있다.

SI(System Integration) 업계에서는 그룹내 계열사의 전산 시스템의 관리 및 전산화 프로젝트를 추진하고 있다. 특히 현대정보기술은 자동차, 선박, 건설, 자동화 등의 SI 사업을 중점적으로 육성하고 있으며 포스데이터는 철강, 엔지니어링 등의 주력사업 분야를 중심으로 활발하게 전개하고 있으며 철강분야의 정보시스템 구축이나 CIM 프로젝트를 적극 추진하고 있다.

LG-EDS 역시 한국통신을 비롯하여 그룹 계열사의 정보 인프라 구축 프로젝트를 수행하고 있으며 앞으로 신공항 종합전산화 프로젝트를 진행할 예정이다. 한국원자력연구소에서는 Intranet의 개념을 실용화하여 'KAERI-NET'을 통해 전자 우편, BBS, 도서 정보, 원전 설계 정보, 통합 MIS (Management Information System) 등의 주요 시스템을 운영하고 있으며 Life-cycle 동안 일관되게 유지하고 공유할 수 있는 정보 시스템의 구축을 위해 NuIDEAS(원전 종합 데이터베이스 및 설계 고도화 시스템, Nuclear Integrated Database and Design Advancement System)를 개발하고 있다.

현대중공업에서는 '95년 생산 시스템 구축을 위한 VAN 개발팀 및 TFT를 구성하고 1단계 사업으로 전자 구매 시스템, FAX 시스템 구축을 시작으로 11월에는 신물류처리 시스템, 12월에는 전자 구매 시스템 가동 및 상용 서비스를, '96년에는 거래업체를 확대하고 6월에 현대중공업 전용 EDI 중계 시스템 개발 완료 및 가동을 시작하였다[10].

또한, '95년에 동남은행과 광주은행에서 전자 카드를 개발하여 시범 운용하였으며 한국은행, 금융결재원 등을 중심으로 IC 카드 표준 제정을 완료한 바 있다.

3. EDI, CALS, EC의 관계

가. EDI와 CALS의 관계

EDI는 'Electronic Data Interchange'의 약자로 '전자 문서 교환'으로 알려져 있다. 그 의미는 '통신 회선(컴퓨터통신망)을 통해 서로 다른 기업간의 상거래를 위한 데이터(정보)를 컴퓨터로 교환하는 규약으로 당사자간에 서로 필요로 하는 각종 결정이 폭넓게 합의된 표준적인 규약'으로 교환하는 대상으로는 상품 거래 정보에 국한되지 않고 물류 및 금융도 포함한다. EDI의 대표적인 예로서는 유통업자와 상품 공급자의 네트워크를 구축하는 경우나 은행의 온라인 시스템 등을 들 수 있다.

EDI는 산업계의 기반구조로 정보 교환의 범용성을 중시한 개념이며 정보 교환의 통일된 수준을 정해 경제 활동에서 전반적으로 이용할 수 있는 네트워크 환경을 구성하고자 한다. EDI가 지향하는 전자 거래의 표준화는 CALS가 기업 계열이나 국가 사이의 정보 교환을 수행하려는 개념과 유사하며 EDI가 타 기업과 수주·발주 데이터를 교환할 수 있도록 구성한다면 CALS와 동일하게 된다.

표 3 EDI/CALS

EDI	CALS
국내 대상	국내외 대상
전용 OnLine Network	Open Network(Internet)
기업대 기업/정부/소비자	기업대 기업 대상(기본)
업계내의 EDI	무국경(국제화)
text data	multimedia data
Close System	Open System/Network
DB의 공유화 안됨	DB의 공유/통합화 가능

CALS와 EDI의 가장 큰 차이점은 수용하는 정보의 종류에 대한 문제이다. EDI가 수주·발주 등 특정 거래 데이터를 대상으로 함에 비해 CALS는 '모든 기업 정보의 디지털화'를 지향하고 있다.

또한 'EDI는 CALS의 중요한 구성 요소 중 하나'라는 표현으로 CALS 개념의 폭이 EDI 개념보다 넓음을 나타낼 수 있다. EDI는 거래에 관련되는 비즈니스 문서 데이터를 대상으로 하지만 CALS는 기술적인 정보가 중요한 부분을 차지하고 있다. 〈표 3〉과 〈표 4〉에서는 EDI를 중심으로 EDI와 CALS, EDI와 EC의 관계를 나타내고 있다.

나. EDI 와 EC의 관계

EDI 시스템은 정보교환의 신속성, 데이터 입력의 정확성, 데이터 재입력 비용의 절감, 우편 및 전화비의 감소, 서류처리에 관련된 비용감소 등의 효과를 제공한다. EDI 활용은 불필요한 인적, 물적 자원의 낭비를 줄이고 신속한 업무처리를 통해 개별기업은 물론 국가 전체의 경쟁력을 강화시킬 수 있다. 미국에서는 현재 10여만개 이상의 업체들이 EDI시스템을 도입하여 사용하고 있으며 특히 자동차, 식품, 운송 등의 산업에서는 EDI를 사용하지 않는 업체는 경쟁적인 불이익을 받을 정도로 활발하게 이용되고 있다.

'90년대 초반부터 EDI에 더하여 기업간의 거래를 위해 발생되는 정보의 교환수단으로 전자우편을 함께 사용하면서 EC의 개념이 사용되기 시작했다. EC란 특정 제품 및 서비스가 생산되어 고객에 전달되기까지의 전 과정을 정보통신 기술에 기반을 둔 새로운 형태의 상거래 시스템으로 재 구축하는 것으로 소비자와 생산자간, 생산자와 생산자간, 국가와 국가간 등 모든 거래 관계에 적용할 수 있다. 특히 여러 기업들이 사업을 추진하면서 발생하는 제반 업무를 기업 상호간을 연결해 주는 일련의 기술적 도구(tool)를 활용해 처리하는 것을 의미한다. 결국 EC는 기업내의 모든 업무프로세스와 전략을 포함하고 있다고 할 수 있다.

즉 EC는 단지 하나의 기술 및 도구가 아니라 기술, 애플리케이션, 프로세스, 비즈니스 전략을 결합한 것으로 한 기업에서 독자적으로 수행하기 어려운 통합적인 개념이다. 정보통신의 발전으로 국가간의 경계와 거리가 허물어져 세계 각국의 정보화를 촉진하여 WTO 체제의 출범을 가져왔다면 EC는 이같은 정보화 사회의 경제 기반을 떠받치는 경제 인프라 내지는 이념으로까지 확대되고 있으며 EC는 경영혁신의 일환으로 80년대 이후부터 기업체들로부터 관심을 끌기 시작하였고 기업의 세계화 및 정보화가 확산되고 고객 만족이 제일의 가치로 떠오르면서 급부상하였다.

특히 외부적으로 국내 기업은 물론 해외 기업과 대규모 상거래를 추진하고 있는 대기업의 경우 '기업 경영의 세계화' 혹은 '세계 수준의 고객만족'을 실현하기 위해 내부 업무 내용과 처리 방법 등에 대한 표준화가 필수적인데 표준화된 EC시스템이 바로 이같은 요구를 충족시켜준다고 할 수 있다. 실제로 미국의

국방부에서 CALS/EDI 프로젝트를 추진하면서 EC에 대한 관심이 높아졌다. 당초 군수품 조달을 위해 추진됐던 CALS가 현재는 미국을 중심으로 한 태평양 주변국 및 NATO(North Atlantic Treaty Organization)를 비롯한 유럽의 모든 국가로 확산되고 있으며 민간기업들이 산업개혁의 일환으로 이에 관심을 가지면서 EC가 상거래수단으로 계속 관심을 끌고 있다. 전자문서교환 수준에 불과했던 EDI가 전자적 상거래를 의미하는 EC개념으로 확대된 것이다.

EC는 상용 온라인 서비스와 인터네트 검색 도구의 성장에 힘입어 산업계뿐만 아니라 일반 소비자들에게도 굉장한 관심사항이 되고 있다. 현재 많은 업체가 웹과 온라인 서비스를 이용해 자사의 제품과 서비스를 홍보하거나 주문처리하고 있으며 고객 지원 및 설문조사 업무도 수행하고 있다.

EDI를 위한 전자데이터교환에 관한 규약 작성은 세계 각국에서 수행되고 있다. 미국은 ANSI 및 각종 산업계가 중심이 되어 업계 횡적인 규격 작성에 추진하여 ANSI X.12를 제정하였다. 유럽은 UN의 유럽 경제위원회(UN/ECE/WP4)가 개발을 담당한 UN/EDIFACT라고 하는 규약에 기인하여 EDI화가 진행되고 있다.

표 4 EDI/EC

EDI	EC
전자 거래	전자 상거래
정보를 주고받음	상업적인 거래
기업대 기업	기업대 소비자(가정))
특정한 상대 기초	불특정다수 대상
국내 한정	국내/해외 대상
업계 내	기업내외
Close System	Open System

한편, 일본에서는 '92년에 EDI의 보급·계몽을 위한 업종 횡적인 조직으로서 EDI 추진협의회(JECIC)가 설립되어 40여개 이상의 업계단체·관계기관이 참가하여 활동이 진행되어 왔다. 또한 일본 정보처리 개발 협회, 산업정보화 추진센터(JIPDEC-CII : Center for the Informatization of Industry)가 중심이 되어 개발된 CII표준(신텍스 룰)을 10여 개 이상의 업계에서 채용하고 있어 일본의 실질적인 표준으로 되고 있다.

UN/EDIFACT는 '85년에 ISO-9735로서 제1판이 등록되었다. 미국 및 일본은 자국 개발의 규약과 UN/EDIFACT에 관한 대응을 검토하고 있다. 일본에서는 지금까지 국내 거래량이 많은 제조업을 중심으로 한 움직임과 해외 직접 거래량이 많은 유통업을 중심으로 한 움직임이 있었지만, 여기에 대금지불 및 결제 등의 금융업에 도입된 새로운 EDI 파일롯트 사업이 시동되기 시작하였다.

다. CALS/EC/EDI의 관계

CALS는 제품의 수명주기, 즉 제품의 기획, 설계, 생산, 유통등의 공정에 필요한 동시공학, 컴퓨터공학, 데이터 공유등 정보기술에 의한 합리화를 통해 품질 및 생산성 극대화 전략을 목적으로 한다.

EDI는 표준 전자정보를 이용한 문서거래의 전자화는 전자 수주, 발주, 자금결재 등에서 필요한 정형화된 형태의 자료교환을 의미한다.

CALS는 EDI의 정형화된 디지털 정보뿐만 아니라 각종도면, 음성, 영상등의 멀티미디어 정보를 교환할 수 있어야 한다. 상거래 자료를 주된 대상으로 하는 EDI와 기술 자료를 주된 대상으로 하는 CALS는 전자적인 정보교환을 실행함으로서 리엔지니어링을 수행한다는 의미에서는 공통의 무대에 있으며, 이들 두 개념은 현재 소위 EC라고 하는 새로운 개념으로

정리되어 가고 있다.

CALS/EDI/EC와의 관계를 다음 (그림 1)에서 도식화하여 보았다. CALS/EDI는 제품 개발 공정에서의 일정단계까지 디지털 정보를 공유하며 EDI/EC간은 기업간 정보교환을 통한 상거래 활동을 성립하는 데 도움을 준다. CALS/EDI/EC의 통합된 형태는 제품의 Life-cycle과 상거래 활동 모두를 만족시키고 있다.

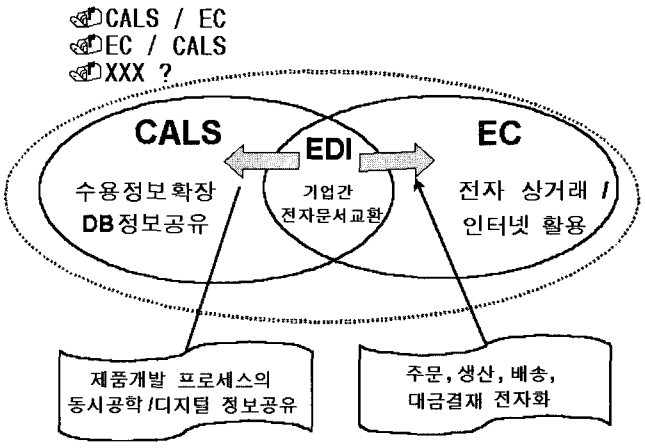


그림 1 CALS/EC/EDI 관계

4. CALS 구현 기술

CALS 구현을 가능하게 하는 정보기술은 개방형 시스템 구조를 이루는 제반 응용 기술의 다양한 요소로 구성되는데 주요 핵심기술에는 다음 표와 같이 멀티미디어 기술, 표준화 기술, 초고속 네트워크 기술, 통합 DB 기술, 정보보호 기술등이 있다[4].

표 5 CALS 구현 정보기술

기 술 분 야	주 요 내 용
멀티미디어 기술	멀티미디어 데이터의 입출력, 저장, 압축, 전송 등
표준화 기술	멀티미디어 문서의 표현, 데이터 교환 양식 등
네트워크 기술	대용량, 실시간 전송을 위한 초고속 통신망
통합 DB 기술	분산 DB, 정보의 변환, 저장 및 공유
정보보호 기술	신분 인증, 암호화 알고리즘, 디지탈 서명 등

가. 멀티미디어 기술

다양한 형태의 기술 데이터를 처리하는 기술로써 텍스트, 도면, 삽화, 음성, 동화상 등의 데이터를 생성·입력하기 위한 방법과 입력된 데이터의 표준화된 압축 저장방법, 저장된 데이터의 전송방법, 그리고 수신된 데이터를 활용하기 위한 출력 방법 등에 관한 연구개발이 필요하다.

나. 표준화 기술

CALS 표준화 체계는 크게 기능 표준, 기술 표준, 데이터 관리 표준으로 구성되는데 개방형 시스템 응용과 통합 데이터베이스 환경을 구현하기 위한 표준 규격들이 포함된다. 특히 문서의 구성요소인 문장을 세분화하고 각각에 인식을 붙여 전체 구조를 명시할 수 있는 SGML (Standard Generalized Mark-up Language)은 '86년도에 국제 표준 규격(ISO)으로 제정되었다.

다. 고속 네트워크 기술

컴퓨터를 통한 정보 교환이 활성화됨으로 인하여 기존의 서비스뿐만 아니라 음성, 그래픽, 동화상 등의 다양한 응용 서비스를 지원할 수 있는 고속 네트워크 기술이 필요하게 되었다. 고속 네트워크 기술에는 FDDI, DQDB, ATM 등의 기술이 요구된다.

라. IDB 기술

각종 디지털 정보를 통합하여 필요시 언제 어디서나 액세스할 수 있도록 하는 CALS의 핵심 요소로써 이를 위해서는 먼저 공통 정보 모델을 선정하여 사용자에게 변환된 각종 정보 베이스 스키마를 제공할 수 있어야 하고 시스템은 사용자가 요청한 결과를 편집하여 제공해 줄 수 있어야 한다. 이러한 CALS IDB 구축을 위해서는 분산 데이터베이스 기술, 공통 모델 및 정보변환 기술, 정보의 저장 및 편집 기술, 이질 트랜잭션 관리 기술 등 복합적인 기술이 요구된다.

마. 정보보호 기술

정보 통신망은 정보의 내용변경, 불법적 유출, 파괴, 위조된 정보 유통 등의 보안 위협을 내포하고 있다. 그러므로 정보 통신망의 보안 위협에 대하여 정보를 안전하고 신뢰성 있게 보호하기 위해서는 정보 보호 서비스를 제공하는 보안 시스템이 절실히 필요하다. 보안 시스템의 목표는 컴퓨터 시스템과 네트워크의 안정성, 신뢰성을 확보하여 개인 프라이버시 침해 문제, 자료 신뢰성 문제, 컴퓨터 범죄 문제 등과 같은 고도의 정보화 사회가 갖는 취약점들을 극복하고 자료의 비밀성을 유지함으로써 신뢰성 있는 정보를 안전하게 제공하는데 있다.

5. CALS의 표준

CALS는 디지털화된 문서, CAD(Computer Aided Design)로 설계된 도면등을 전산망을 통해 송수신할 수 있어야 하기 때문에 고속 통신망 구축과 함께 표준화 된 양식을 정하는 일이 필수적이며, 사업발주서, 설계에 관련된 데이터 등도 표준화된 코드로 작성되고, 컴퓨터에 의해 생성, 저장되며 또한 서로 다른 곳으로 송수신되어야 한다. 대부분의 CALS 표준은 CALS를 위해서 새로 만들어진 것이 아니며, 기존에 있는 산업계 및 국제 표준에서 선택하여 조합된 표준이다. 미국방성은 국방성내의 시스템 개발 프로그램에 CALS를 구현하기 위해 구조적 접근 방법을 정하여 이를 군용 핸드북(Military Handbook) 59B로 제공하고 있다[5].

CALS 표준은 자료 접근과 자료 교환으로 나뉠 수 있다. 세부적으로 정보의 표준화 작업은 생산과 관련된 제품 데이터의 상호교환을 위한 표준, 제품 기술을 디지털 자료로 생성하고 관리하는 표준, 디지털 기술자료로 생성하고 관리하는 표준, 기술설계 자료에 대한 표준, 제품의 유통, 운수와 관련된 정보의 표준 등으로 나눌 수 있다.

가. 자료 교환 표준

MIL-STD-1140은 전자 자료 파일을 CALS 표준 포맷으로 교환하는 구조를 정하고 있으며 표준 파일 포맷과 자료의 표현, 파일 이름 규칙 등과 같은 전자자료의 전송을 위한 전반적 접근 방법을 설명하고 있으며, STEP (Standard for the Exchange of Product Data)과 음성/영상/사진/하이퍼미디어에 대한 조항 등을 포함하기 위해 개정이 계획되고 있다. 미국방성은 2000년에 국제표준화한다는 목표를 세우고 있다. 현재 개정판인 1140A와 1140B가 유효하다. 1140B는 기술 자료의 팩키지를 한 조직에서 다른 조직으로 전송할 때 사용된다.

자료 팩키지는 문서들로 구성되어 있으며 문서는 하나 또는 그 이상의 파일로 구성된다. 각 파일은 제목, 저자, 송신자, 수신자, 보안등급 등과 같은 파일에 대한 색인 자료를 제공하는 메타자료가 첨가되어 있다. 또한 1140C가 현재 작성되고 있으며, 이 개정판은 1140자료를 인터넷트 전자우편 방법인 MIME(Multipurpose Internet Mail Extension)전송을 정의하고 있다.

- SGML(표준 범용 마크업 언어)
  ISO 8897로 국제표준으로 채택되었으며, CALS에서도 문서관리 및 교환을 위한 표준인 MIL-D-28001로 채택되고 있는 SGML은 문서출판 시스템, DBMS, 재고관리 등의 응용 프로그램에서 자료를 저장하기 위해 사용되는 데이터 저장표준 및 문서교환방식으로서, 개방형 시스템 환경하에서 널리 사용되고 있는 국제표준이다.
  SGML은 '60년대 IBM에서 정보 시스템을 구축시 page-oriented document의 규격화와 공유를 위해 개발됐던 GML (Generalized Mark-up Language)로부터 출발되어 그후 현재까지 발전되어 온 것이다. 현재는 인터넷 상에서 SGML을 이용한 web 서버, web 브라우저들도 많이 있으며, 미국 국방부 및 각국 특허청에서도 채택하고 있다.
- CGM(컴퓨터 그래픽) 표준
  CALS에서 그래픽 표준으로는 CGM (Computer Graphics Metafile), 주사선 그래픽, IGES(Initial Graphics Exchange Specification)가 사용되고 있다. CGM은 2-D 그림이나 도해를 표현하는데 사용되는 일반적 표준이다.
  CGM은 ISO에 의하여 ISO 8632로 채택되었으며 미국은 ANSI X3.122, FIPS 128로 채택되어 있다. 미국 국방부는 FIP PUB 128의 구현으로 MIL-D-28003을 채택하고 있다.
- AITI(기술정보 자동교환) 표준
  AITI(Automated Interchange of Technical Information)는 제반 CALS 표준의 상위표준으로서 앞으로 제정될 CALS표준을 포함하여 군의 모든 규격을 통일하기 위한 종합문서이며, 기술정보의 자동화된 교환을 위해 관련된 규격에 대하여 자료교환 및 파일관리에 대한 사항 등을 정의하고 있다.
  AITI의 목적은 제품의 전수명주기에 걸쳐 필요한 기술정보를 디지털 형식으로 교환하는데 필요한 인터페이스를 표준화하여, 그 저장을 위해 데이터화일의 포맷과 정보구조를 표준화하는데 있다.
- STEP/PDES(생산 데이터 교환) 표준
  STEP은 제품의 생산을 위한 설계 및 제조에 필요한 데이터의 표준을 정의한 것이며 PDES(Product Data Exchange using STEP)는 생산 데이터의 보다 완벽한 표현 및 공유를 위하여 국제 표준

인 STEP을 CALS 환경에 맞게 구체화 한 것이다.

- 기타 자료교환 표준

  MIL-HDBK-59B는 위에서 설명한 표준 이외에도 다양한 표준들을 전자 자료교환을 위하여 사용하고 있다. VHDL, EDIF, IPC-D-350등이 상호협의하에 사용될 수 있다.

  VHDL은 전자 시스템의 제작시 모든 단계에서 사용되는 공식표현방법을 기술하고 있으며, 기계와 사람 모두가 읽을 수 있는 형태이므로 하드웨어의 개발, 검증, 시험, 설계자료의 통신, 유지보수, 수정 및 구매에 이르는 모든 측면을 지원할 수 있다.

  EDIF은 EIA에 의해 개발되었으며 다양한 CAD 하드웨어와 소프트웨어간의 전자 제품 자료 교환을 원활히 할 목적으로 작성되었다.

  IPC-D-350은 IPC(Institute for Interconnecting and Packaging Electronic Circuits)에서 개발된 산업 표준으로 printed-circuit board 제품을 기술하는데 사용되는 80자의 고정된 레코드 포맷을 제시하고 있다.

나. 자료 접근 표준

MIL-STD-974는 구매자가 온라인 접근 또는 기술정보의 전달을 요구할 경우 계약자가 제공해야 할 핵심기능과 선택기능들을 정의하고 있다. 계약자가 제공하는 온라인 서비스는 CITIS (Contractor Integrated Technical Information Service)로 불리운다. 974는 인식, 승인/거부, 접수, 검색, 저장, 보기를 핵심기능으로, 응용, 결합, 수정 등을 선택기능으로 정하고 있다. 본 문건은 '99년에 미국 연방정부 표준인 FIPS (Federal Information Processing Standard)로 제정될 예정이다.

다. 제품, 과정, 자료 통합 표준

CALS의 구현은 공유된 자료를 사용하여 기능적으로 통합된 팀들이 통합된 설계, 개발, 제조 환경을 만들 것을 요구한다. 이러한 통합환경의 구축을 위하여 미국 국방부는 공학 관리, 업무분장구조, 구성관리 및 통합환경을 위한 데이터베이스 스키마에 대한 표준을 제공하고 있다.

- MIL-STD-499(Engineering Management)

  공학관리에 대한 표준은 MIL-STD-499로 작성되어 있다. 본 문건은 국방 시스템 구매 및 기술개발에 있어서 시스템 공학적 노력의 정의, 관리 및 평가에 대한 기준을 제공한다. 이 표준은 동시공학의 기술적 체계를 제시하고 시스템 공학의 방법론을 기술하고 있다.

- MIL-STD-881(Work Breakdown Structure for Defense Material Items)

  업무 분장 구조에 대한 표준은 MIL-STD-881로 작성되어 있다. 이 표준은 구매시 사용되는 업무분장 구조의 준비와 고용에 대한 기준을 제공한다. 통일된 정의와 접근방법을 정의하므로서 다양한 자료 요구사항들의 호환성을 증진시킨다.

- MIL-STD-973(Configuration Management)

  미국방성 환경하에 적합한 구성관리를 정의하고 있다. 구성항목의 생명주기상에서 적용되는 기술적 및 관리적 지침을 제공하고 있으며 제품 개발이나 목적 달성을 위해 필요한 기준 및 계획된 하드웨어나 소프트웨어의 기능적 물리적 특성을 기술한다.

■ MIL-STD-1388(Logistic Support Analysis) MIL-STD-1388-2는 LSAR(Logistic Support Analysis Record)에 대한 자료 요소 정의, 자료 필드 길이, 포맷을 정의한다. 이 표준은 제품의 생명주기상에서 제품에 관한 자료를 관리하는 제품자료 관리 및 구성관리 데이터베이스에 대한 관계형 데이터베이스 스키마를 정의한다. LSAR 스키마는 논리적 및 물리적 구조를 모두 정의하고 있다.

표 6 주요 CALS 사용 표준

	일반호칭	국방성 규격병	대 상	내 용
기술계데이터	SGML(Standard Generalized Markup Language)	MIL-M-28001	문 장	문장을 세분화하여, 각각에 인식표를 붙여서 전체구조를 명시하기 위한 표준규정, 1986년에 제정된 ISO 규격
	CGM(Computer Graphics Metafile)	MIL-D-28003	간이도, 일러스트	책이나 챠트에 일반적으로 사용되는 그림이나 일러스트 등의 그래프의 축적, 교환을 위한 표준규정
	IGES (Initial Graphics Exchange Specification)	MIL-D-28000	CAD DATA	CAD/CAM 시스템간의 DATA 교환을 위한 표준 규정
	STEP (Standard for the Exchange of Product Model Data)		설계/제조 DATA	IGES의 DATA를 포함하여 사양, 기능, 구성, 구조해석등 설계, 제조에 필요한 모든 DATA 교환을 위한 표준규정
	CCITT Group 4	MIL-R-28002	도형의 Raster DATA	그래픽 DATA 교환의 효율화를 위한 DATA 압축 기술의 표준규정
	CITIS (Contractor Integrated Technical Information Service)	MIL-STD-974	발주 정보	국방성이 계약 발주 정보를 제공할 때의 DATA 규정
	IETM (Interactive Electronic Technical Manual)	MIL-M-87268	기술 메뉴얼	Computer를 사용하는 대화형 매뉴얼(ITEM)의 개발 및 화면 사양 등에 관한 규정
		MIL-D-87269	상기 납입사양	IETM의 정부 기관에의 납입에 있어서 제품 사양에 관한 규정
		MIL-Q-87270	상기 품질보증	IETM의 Contract 품질보증 규정
일반상거래데이터	EDI (Electronic Data Interchange)		일반 상거래와 관련한 서류	수발주, 견적, 재고확인, 운송의뢰, 집하확인, 청구서등 일반 상거래에 있어서의 모든 서류의 전자화와 페이퍼레스 환경을 위한 규정

라. CALS와 표준화

CALS의 성공을 위해서는 표준화가 필수적이다. CALS의 표준을 처음으로 발기를 한 미국방부의 표준에서부터 국제 표준까지의 단계를 살펴보면 다음 〈표 7〉과 같다.

ISO는 범위가 매우 넓으며 반면에 미국방부 표준은 그 범위가 좁다. 표준을 그 적용범위로 구분하여 볼 때, 표준은 국제표준, 국가표준, 정보표준, 부처표준으로 구분할 수 있다.

CALS표준은 미국방부에서 먼저 제정되고 추후에 정부 및 국가 표준이 되는 경로를 따르고 있다. 즉 기술개발과 동시에 표준화를 하였고 국방부 표준은 좀더 일반화되어서 정부부처 모두가 같이 쓸 수 있는 표준인 정부 표준으로 제정되고 나아가서는 국가 및 국제표준으로 제정되는 길을 밟고 있다.

표 7 CALS 표준화 단계

표 준	국제 표준	국가 표준	정부 표준	발 기
	ISO/IEC		FIPS	CALS
SGML	ISO 8879	EIA-538-1988 AIIM-M553- (199X) Type 2	FIPS 152	MIL-M-28001
RASTER	CCITT, Group 4 ISO 8613-7 Type 2	ISO 8632.1-4	FIPS 1062 FIPS 150 Draft FIPS Tpye 2	MIL-D-28002
CGM	ISO 8632.1-4	Y14.26M	FIPS 128-1	MIL-D-28003
IGES			FIPS 177	
STEP	ISO 10303			
IETM				MIL-M-87268 MIL-Q-87280 MIL-D-87269
SQL	ISO 9075	X3.135-1992	FIPS 127-2	MIL-STD-1388
CITIS				MIL-STD-974
Data Delivery Procedure				MIL-STD-1840B
LSAR				MIL-STD-1338
EDI	EDIFACT	ANSI X112		AECMA 2000M (Europe)

마. 국내 CALS 표준화 방향

CALS의 도입시 우선적으로 필요한 부분이 표준화이다. 정확한 표준이 없을 경우 제품이나 시스템의 개발과 시험시 사용할 수 있는 기준이 없는 것이며 CALS 구현이 원래의 목적을 달성할 수 없다.

CALS 표준은 미국과 국제 표준화기구에 의해서 많은 부분이 제정되었으며 새로운 부분들이 표준화되고 있다. 따라서 국내에서는 현재 나와있는 CALS의 기본표준이나 구문표준을 외국의 사례를 검토하여 우리나라의 상황에 맞게 구현표준을 만드는 것이 필요하다[6].

구현 표준을 만들기 위해서는 개발자의 적극적인 참여가 필요하다. 기본적으로 기술개발 없이 표준화가 없다는 것이 인식되어야 하며 기술개발 과정이 시간적으로 너무 길고 비용이 많이 들 경우 외국적으로부터 기술도입 또는 제품구매등이 고려될 수 있을 것이다.

이 경우 기술개발과는 다른 표준화 체계가 필요할 것으로 보인다. 즉 기술개발에는 공급자 입장에서 기존의 산업표준에 근거한 기능 프로파일의 국내 표준화가 시급할 것이나 외국으로부터의 기술 구매시에는 사용자 입장에 더욱 가까운 시스템 프로파일의 개발이 조속히 요구될 것이다.

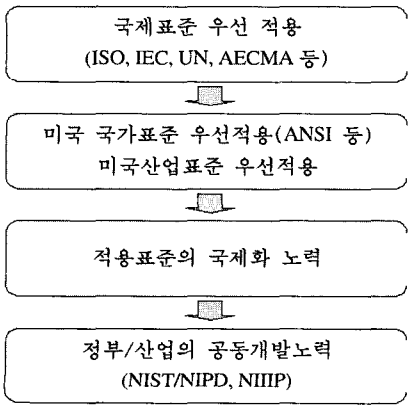


그림 2 국내 CALS 표준화 방향

따라서 CALS의 표준화는 우선 핵심기술중 우리나라에서 개발될 필요성이 제기되는 기술들은 기술 개발과 동시에 기능 프로파일의 국내 표준화가 추진되어야 할 것이며 기타 분야는 사용자가 사용할 수 있는 시스템 프로파일의 표준화가 추진되어야 할 것이다.

6. CALS 정보보호 기술

CALS의 정보보호는 EDI에서의 정보보호의 확장이라고 볼 수 있으며 다음 (그림 3)에서는 연결통신과 비연결통신으로 구분하여 다음과 같은 정보보호 표준 및 모델을 제안하였다.

4계층으로 분류하여 비연결통신의 Step1에서는 비정형화된 문서교환 방식으로 X.400 표준을 적용할 수 있으며, Step2의 EDI의 비정형화된 문서 교환에서는 UN/EDIFACT, ANSI X.12, Pedi 등을 적용시킬 수 있다.

연결통신에서는 Step3의 분산개방형 정보교환 체제에서는 X.500, X.25등의 표준을 적용시킬 수 있다. Step 4의 인터넷을 이용한 통합 DB의 정보공유는 TCP/IP를 이용한 표준이 이루어져야 한다.

본 논문에서는 위의 4단계의 구분지어 정보보호 표준들을 나누어 보았으며 하나의 단일화된 형태의 모델로 제안하여 보았다.

CALS의 정보보호는 각 단계의 표준이 이용되며 본 논문에서 여러 가지 정보보호시에 필요한 위협요소, 보안 서비스, 보안 메카니즘, 대상보안성 등으로 나누어 살펴보도록 하겠다.

가. 위협요소

1) 위장(Masquerade)

어떤 실체가 마치 다른 실체인 것처럼 위장하는 것으로서 비인가된 이용자가 자원을 불법적으로 액세스하기 위하여 제3자가 정당한

사용자인 것처럼 위장할 수 있으며 사용자의 위장, 거짓 수신 확인, 메시지 발신의 거짓 주장 등을 포함하고 있다.

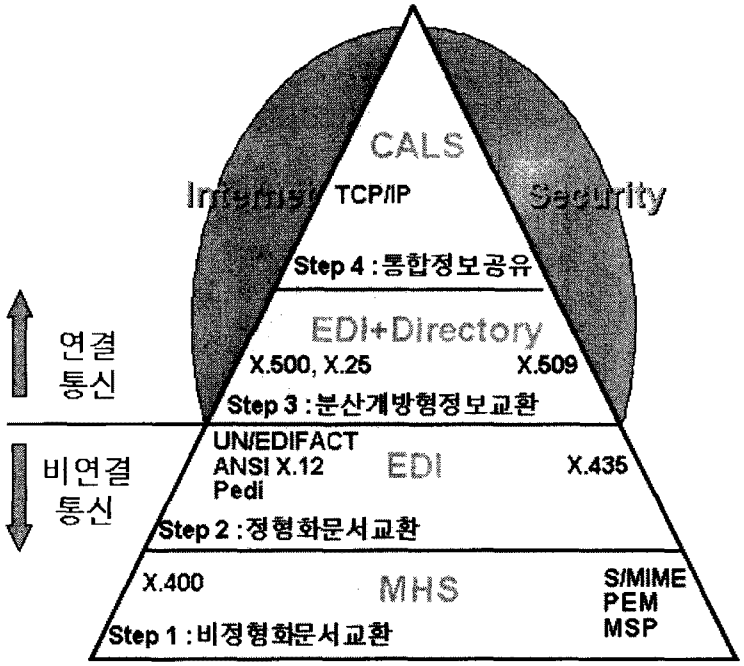


그림 3 CALS 구현단계에서의 정보보호

2) 메시지 순번 변조(Modification of Message Sequence)

메시지의 일부 혹은 전부를 지연 전달시키거나 고의로 메시지의 재발급 혹은 순번을 재배치하는 것으로서 메시지 되풀이 공격, 메시지 reordering, 메시지 지연 등이 있다.

3) 정보 변조(Modification of Information)

수신자에게 전달되는 정보, 라우팅 정보 및 관리 정보를 손실되게 하거나 변조하는 것으로서 메시지 변조, 메시지 파괴, 라우팅 및 관리 데이터 파괴 등을 포함하고 있다.

4) 서비스 거부(Denial of Service)

앤티티가 자신의 기능을 수행하지 못하거나 상대방으로 하여금 기능 수행을 방해하는 것으로서 액세스 거부, 통신거부, 메시지 수신 금지, 과잉 트래픽 조작 등이 있으며 데이터 overflow, 시스템 고장 등으로 나타난다.

5) 부인(Repudiation)

시스템 사용자가 메시지 전송, 제출, 배달 등의 행위를 실제로 하고서도 하지 않았다고 부인하는 것으로서 발신 부인, 제출 부인, 배달 부인 등이 있다.

6) 정보 노출(Leakage of Information)

메시지 전송 감시, 시스템 내의 정보에 대한 비인가적 액세스, 혹은 위장 등에 의해서 비인가자에게 정보를 노출시키는 것으로서 기밀성 손실, 익명성 손실, 메시지 남용, 트래픽 분석 등이 유발된다.

7) 신분 레이블 변조

해당 자원에 접근을 제어하기 위한 신분 레이블에 관련한 위협으로 발신자의 불명확한 메시지 레이블 사용, 시스템 사용자의 불명확한 context 사용 등과 같은 사항을 포함하고 있다.

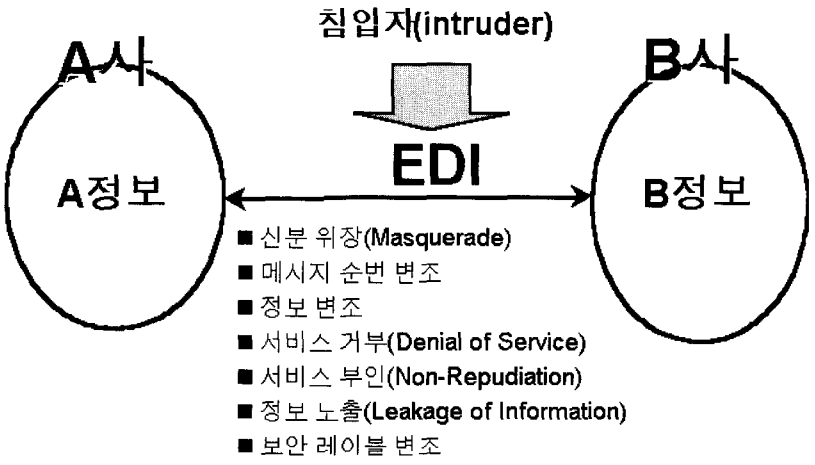


그림 4 CALS 정보보호 : 위협요소

나. 보안 서비스

1) 인증(Authentication)

- 메시지 발신 인증(Message Origin Authentication)
  메시지 발신 인증 서비스는 수신자에게 메시지가 정당한 발신자로부터 왔음을 인증해 주는 서비스이며 라우팅, 효율적인 발신처 확인와 무결성 점검을 위해 메시지 보안 레이블과 함께 사용될 수 있다[7].
- Probe 발신 인증(Probe Origin Authentication)
  probe가 정당한 발신자로부터 발신되었음을 인증해 주는 서비스로서 메시지 발신 인증 서비스와 밀접한 관계를 갖고 있다. probe는 content-less 메시지이고 수신자에게는 배달되지 않는다.
- 제출 증명(Proof of Submission)
  발신자가 메시지 제출자에게 메시지는 요구된 수신자에게 전달하기 위해서 수신하였음을 증명해주는 서비스이다.
- 배달증명(Proof of Delivery)
  메시지 발신자에게 메시지는 변조없이 정당한 수신자에게 배달되었음을 증명해 주는 서비스이다.
- 통지 증명(Proof of Notification)
  메시지 발신자에게 메시지가 수신되었고, 수락/거부/회송되었음을 알리는 통지의 발신처를 증명해 주는 서비스이다.
- 검색 증명(Proof of Retrieval)
  메시지가 수신 사용자에 의해 검색되었음

을 운영자에게 증명해 주는 서비스이다.

- 상대 실체 인증(Peer Entity Authentication) 기능 구성요소 간에 상대방의 ID를 인증해 주는 서비스를 말한다.

2) 데이터 기밀성(Data Confidentiality)

- 접속 구간 기밀성(Connection Confidentiality)
  통신 요소 간의 데이터 기밀성을 보호해 주는 것으로 주로 TLSP(Transport Layer Security Protocol), NLSP(Network Layer Security Protocol) 등 lower layer에서 제공되며 보안 모델에서는 잠정적으로 요구하고 있으나 프로토콜 지원은 없다.
- 내용 기밀성(Content Confidentiality)
  발신자와 수신자 사이에서 메시지 내용의 기밀성을 보호해주는 서비스이다.
- 메시지 흐름 기밀성(Message Flow Confidentiality)
  메시지 흐름 관찰에 의한 정보 누출 방지를 위하여 double-enveloping 기술에 의해 서비스를 제공할 수 있다.

3) 데이터 무결성(Data Integrity)

- 접속구간 무결성(Connection Integrity)
  통신 요소 간의 전송메시지에 대한 데이터 무결성을 보호해주는 것으로 TLSP, NLSP등 lower layer에서 제공될 수 있으며 보안 모델에서는 잠정적으로 요구하고 있으나 프로토콜 지원이 없다.
- 내용 무결성(Content Integrity)
  발신자와 수신자 사이에서 전송 메시지 내용에 대한 무결성을 유지해 주는 것
- 메시지 순번 무결성(Message Sequence Integrity)
  신자와 수신자 사이에서 순서적인 메시지의 reordering, replay, deletion을 방지하기 위해 메시지 순번에 대한 무결성을 제공해 주는 것

4) 부인봉쇄(Non-repudiation)

- 통지 부인봉쇄(Non-repudiation of Notification)
  메시지 발신자에게 메시지가 수신되었고 수락/거부/회송되었음을 알리는 통지 기능의 발신처를 메시지 수신자가 부인할 수 없도록 하는 증명을 제공해주는 것
- 검색 부인봉쇄(Non-repudiation of Retrieval)
  시스템 운영자에게 특정 메시지가 사용자에 의해 검색되었음을 사용자가 부인할 수 없게 증명을 제공해 주는 서비스이다.
- 내용 부인봉쇄(Non-repudiation of Content)
  메시지 수신자에게 수신한 메시지 내용은 발신자가 보낸 메시지 내용과 같음을 발신자가 부인할 수 없도록 하는 증명을 제공해 주는 서비스이다.
- 발신 부인봉쇄(Non-repudiation of Origin)
  수신자에게 메시지의 발신자, 발신내용, 보안 레이블에 대해서 발신자가 부인하지 못하도록 하는 서비스이다.
- 배달 부인봉쇄(Non-repudiation of Delivery)
  발신자에게 메시지는 변조없이 정당한 수신자에게 배달되었음을 부인봉쇄하는 서비스이다.

5) 보안 레이블링(Security Labelling)

- 메시지 보안 레이블(Message Security Labelling)
  기능 구성요소 상호 간에 주고받는 메시지에 허용되는 보안 레이블들을 설정하는 서비스이며 메시지에 보안 레이블을

첨부하여 요소 간에 보안 환경을 설정하도록 해준다. 이 서비스는 보안 정책(액세스 제어)을 지원해 준다.

6) 보안 관리(Security Management)

- 보안 정보 변경(Change Credentials)
  접속되어 있는 다른 사용자에게 자신의 보안정보(패스웨드, 공개키등)를 변경하는 서비스이다.
- 등록(Register)
  사용자가 자신이 사용할 보안 레이블을 등록하는 서비스이다.

다. 보안 메카니즘

1) 암호화 알고리듬

암호화 알고리듬이란 평문을 암호문으로 바꾸어 출력하며, 암호문을 본래의 평문으로 복원하는 알고리듬이다. 암호시스템은 관용 암호시스템과 공개키 암호시스템으로 나눌 수 있다[2]. 관용 암호시스템은 암·복호화 키가 동일하거나 혹은 동일하지 않더라도 하나의 키에서 다른 키를 쉽게 계산하여 얻을 수 있는 시스템으로 블록 암호시스템과 스트림 암호시스템으로 분류될 수 있으며 사용이 편리하고, 속도가 빠르다는 장점이 있다. 그러나 암호키가 제 3자에게 노출되면 암호문의 기밀이 노출될 수 있으므로 컴퓨터 네트워크 상에서 송신자와 수신자간에 안전하게 보호된 채널을 이용하여 키 분배를 할 수 있는 환경에서 사용해야 한다. 대표적인 관용 암호시스템에는 DES(Data Encryption Standard), IDEA (International Data Encryption Algorithm) 등이 있다[2, 8].

공개키 암호시스템은 비밀키와 공개키로 구성된 키쌍을 사용하는데 공개키는 암호화에 사용하고 비밀키는 복호화에 사용한다. 복호화 키는 특수한 비밀정보를 알고 있을 때만 공개된 암호키를 이용하여 계산할 수 있다. 따라서 암호키를 일반 채널로 분배하거나 키 디렉토리에 공개하여도 암호문의 비밀성을 유지할 수 있다. 공개키 암호시스템은 키관리 문제를 해결하는 장점이 있으나 아직은 대부분이 복잡하고 많은 계산 시간을 필요로 한다. 대표적인 공개키 암호시스템에는 RSA 알고리듬이 있다.

- 국제 데이터 암호 알고리듬(IDEA)
  IDEA는 스위스 연방 기술 기관이 Xuejia Lai와 James Massey가 개발한 새로운 블록 지향 암호 알고리듬이다. IDEA는 DES를 대체하기 위해 최근 몇 년에 걸쳐 제안된 관용 암호 알고리듬 중의 하나이다.
- SKIPJACK 알고리듬
  '93년 4월 클린턴 정부에서 제안된 암호화 기술의 발표이후에 '93년 6월에 공식적인 발표가 제안된 암호화 알고리듬으로 블록 암호알고리듬의 일종이며 칩 형태로 공급되며 세부의 암호화 과정은 밝히지 않았지만 대략적인 구조는 연방 정보 처리 표준의 코멘트에 대한 요청으로 연방 정부 간행물에 설명되었다.
- Diffie-Hellman 공개키 암호 방식
  '76년에 Diffie와 Hellman이 제안한 공개키 암호 방식 알고리듬이다. 키 교환용으로 잘 사용되는 DH 알고리듬은 두 사용자가 안전하게 키를 교환하고, 메시지를 암호화하는데 사용할 수 있도록 한다. DH 알고리듬의 효용성은 이산 대수 계산의 어려움에 의존하고 있다.

2) 디지털 서명

디지털 서명은 서명자의 문서적 행위를 제3자에게 간접적으로 증명할 수 있는 수단으로

서명자의 비밀키를 이용하여 서명하고자 하는 메시지의 함수로써 서명하는 서명 생성과정과 서명자의 공개키를 이용하여 서명을 확인하는 서명확인 과정으로 구성된다.

공개키 암호시스템에서 서명자가 소유한 비밀키로 메시지를 암호화하면 그 결과가 서명이 되며 이 서명은 누구나 서명자의 공개키로 복호화하여 그 결과가 일정한 규칙을 만족하는 의미 있는 메시지인가를 확인할 수 있다. 이와 같이 서명의 확인 과정에서 원래의 메시지가 복원되는 서명방법을 메시지 복원형 디지털 서명이라고 한다.

서명할 메시지가 긴 경우 메시지 복원형 디지털 서명에서는 메시지를 일정한 길이로 분할하여 각 블록마다 서명 및 확인 과정을 반복해야 하므로 많은 수의 연산이 필요하며 서명 생성이나 확인과정에 많은 시간이 소요된다. 따라서 메시지에 해쉬 함수를 작용시켜 임의 길이의 해쉬결과에 대해서만 서명을 하고 수신된 메시지의 해쉬 함수 결과와 서명을 복원하여 얻은 결과가 일치하는지를 확인함으로써 서명을 확인할 수 있다. 이러한 서명 방법은 부가형 디지털 서명이라고 하며 대표적인 방법에는 DSS(Digital Signature Standard)이 있다.

- ID를 이용한 디지털 서명 방식

  '84년 Shamir는 주소, 성명 등 각 개인이 식별할 수 있는 ID(Identification)을 이용한 암호시스템을 제안하였다. 이러한 암호시스템은 송수신자간에 공개키나 비밀키를 교환할 필요가 없고 키의 리스트나 제 3자에 대한 서비스도 필요없는 방법으로서, 임의의 통신자 간에 안전한 통신이 가능하고 서로 서명을 인증할 수 있는 암호시스템이다. 즉 ID를 공개키로 사용하기 때문에 공개키를 인증할 필요성이 없어진다. 일반적으로 ID를 이용한 암호시스템에서는 공개키에 해당하는 ID와 ID에 대응되는 비밀키가 있으며 비밀키를 만드는 신뢰할 수 있는 키 관리 센타가 요구된다.

- RSA 디지털 서명 방식

  RSA 디지털 서명 방식은 '78년 R. Rivest, A. Shamir, L. Adleman에 의해 제안된 RSA 공개키 암호시스템을 이용한 디지털 서명 방식이다. 이 방식은 두 개의 큰 소수의 곱으로 이루어진 합성수의 소인수분해가 매우 어려운 점에 안전성을 근거를 두고 있다. RSA 디지털 서명 방식은 현재 가장 널리 사용되고 있는 디지털 서명 방식으로 IBM, MS, DEC, Apple, GE, Unisys 등 유수의 기업들이 사용하고 있다. 하지만 모듈러 승산 회수가 많아서 그 이후에 나온 많은 디지털 서명 방식보다 효율면에서 약간 떨어진다고 볼 수 있다.

- DSS 디지털 서명 방식

  DSS(Digital Signature Standard)는 NIST가 '91년 8월에 정부용 디지털 서명 알고리듬으로 DSA(Digital Signature Algorithm)를 발표한 후, 이를 미국내 디지털 서명 표준안으로 제안한 방식이다. 이 DSS는 특허권 저촉 문제를 고려하여 이미 특허 출원된 RSA방식이나 Schnorr 방식 등의 특허권을 피하기 위해 Schnorr 방식의 변형형으로 제안되었다. 이 DSS 방식의 안전성은 이산대수(discrete logarithm) 문제의 어려움에 근거한다.

3) 해쉬 알고리듬

- MD5 메시지 다이제스트 알고리듬

  MD5 알고리듬은 MIT의 Ron Rivest에 의해 개발되었다. 임의의 길이의 메시지를 입력으로 취하고, 128bit 메시지 다이

제스트를 출력으로 제시한다. 입력은 512 bit 블록으로 처리한다.

- SHA(Secure Hash Algorithm) 알고리듬
  NIST에서 개발하여 '93년 FIPS PUB 110(Federal Information Processing Standard)로 미국 표준으로 공포된 SHA는 해쉬함수 MD4 알고리듬에 기반을 두고 모델화하여 설계되었다.

4) 인증 메카니즘

- Kerberos
  MIT에서 Athena프로젝트의 일환으로 개발된 Kerberos는 인증서비스를 제공하는 보안패키지이다. 분산된 클라이언트/서버 구조를 가정하고 인증서비스를 제공하기 위해 하나 이상의 Kerberos 서버를 사용하였고 공개키 암호방식을 전혀 사용하지 않았으며 관용 암호방식에 의존하였다.
- SESAME
  SESAME는 유럽에서 분산 환경의 자원을 보호하기 위해서 제안되었고 SESAME 프로젝트는 CEC (Commission of the European Communities)에 의해 ECMA에서 작업이 시작되었다. SESAME는 응용 계층에 많은 비중을 두고 개방 시스템에서 정보보호를 위한 어플리케이션의 정보보호 프레임워크이며 상업적 제품이 아닌 개발자들이 제품을 만드는데 보안의 핵심 기능을 제공할 뿐이다.
  뿐만 아니라 개방 분산 시스템 정보보호에서 GSS-API이다. 이 인터페이스는 사용자로부터 인증, 접근제어 메카니즘의 상세한 부분을 숨기고 보다 다른 어플리케이션과의 호환성과 이식성을 제공한다.

라. 대상보안성

CALS의 정보보호 대상은 인증문제로서의 RSA, Kerberos가 있으며, 신뢰성 있는 키 생성 및 분배를 통한비밀성을 지키는 문제와 MD5, SHA와 같은 해쉬 함수를 사용하여 자료의 무결성을 보호하는 것이 있을 수 있으며, 이와 같은 보호 대상은 현재 EDI에서도 적용되고 있으며 CALS에서는 확대 적용시킬 수 있다. 또 다른 보호대상은 분산 접근제어 및, Role-Based 접근 제어를 통한 접근제어가 있으며, 통합DB 구축시에 발생할 수 있는 DB의 가용성의 확보문제 등이 대두된다. 이들 두가지 대상은 CALS의 구현시에 통합DB를 구축하여 생기는 여러 가지 요소중에 하나이다. IDB의 가용성 확보는 DB의 동시처리문제(Concurrency control)가 해결되어야 한다. 이 문제가 가장 시급한 문제가 될 수 있다.

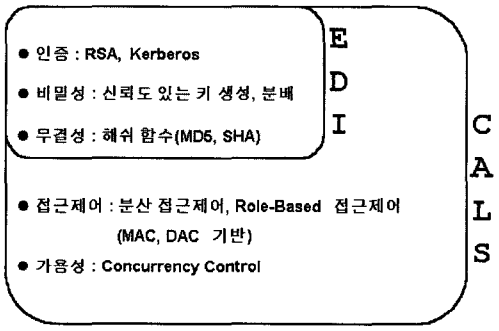


그림 5 CALS 대상에 따른 보안성

7. 맺는 말

가. CALS 정보보호 모델의 의미

CALS 시스템이 안전하게 적용되기 위해서는 연관되는 기관들의 역할과 상호 연관성이 명확히 정의되어 분담하는 총괄적인 CALS 정보보호 모델이 필요된다.

정보보호 기술의 실제 환경으로의 적용 가능성을 바탕으로 제안되는 CALS 정보보호 모델은 국내 CALS 시스템 대부분이 외국에서 수입한 것이므로 국내 제품 개발을 위해 많은 의미를 가지고 있다고 할 수 있으며 국내 개발 가능성을 검토함에 도움을 줄 수 있다.

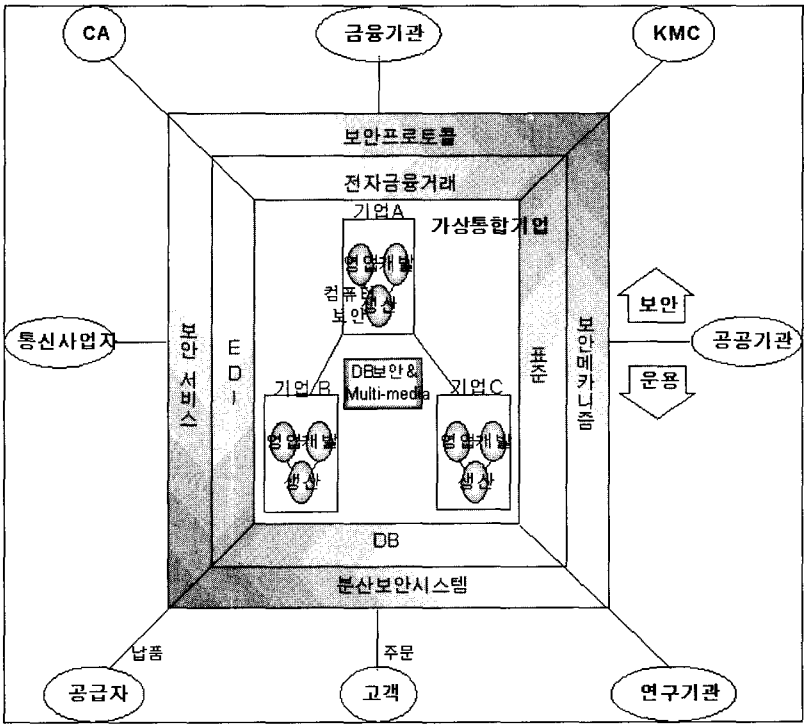


그림 6 CALS 정보보호 연관도

나. 관련 기관의 역할

- 기 업 : 기업은 자신의 상품과 고객의 전자 화폐를 교환하는 역할을 수행한다. 고객으로부터 받은 전자화폐를 해당 은행에 조회함으로써 고객의 주문과 지불에 대한 검증을 거친 후 자신의 상품을 고객에게 전달한다. 이때, 거래처는 고객의 전자 화폐를 고객이 거래하는 은행의 공개키를 사용하여 인증 요청을 한다.
- 통신사업자 : 기반이 되는 빠른 속도의 통신 인프라를 구축하여 제공한다.
- CA(Certification Authority) : 가입자의 신분을 인증하는 업무를 담당한다.
- KMC(Key Management Center) : CALS 체제에서 적용되는 모든 키의 생

성부터 파기에 이르는 일련의 과정을 담당한다.

- 연구기관 : 정보보호 메카니즘/알고리듬을 개발하여 공급한다.
- 정부기관 : 법과 제도를 통하여 CALS 체제를 제정하고 감독한다. CALS 관련 규격을 표준으로 제정하여 보급하며, 위험부담이 큰 기술개발분야에 대한 연구비를 지원하고, 특히 민간분야의 정보화 추진을 위한 환경을 정비하여 산업전반의 경쟁력과 생산성을 향상시킨다.
- 금융기관 : 가상의 은행 역할을 수행하는 부분으로 화폐 발행, 화폐 보증 및 교환 기능을 수행하며 화폐 발행시 고객의 전자 화폐에 은행의 비밀키로 디지털 서명 메카니즘을 이용하여 서명한다.
- 고객 : 전자상거래 시스템에서 구매를 요청하는 실체로서 은행에 계좌를 소유하고, 자신의 계좌에서 입출금이 가능하다. 고객은 자신의 은행 구좌에 서명하고 자신의 비밀키로 서명함으로써 전자 화폐를 인출하며, 은행은 출금 시 고객의 공개키를 사용하여 고객의 서명을 확인한다.

다. 앞으로의 연구 방향

다가오는 21세기에는 모든 분야에서 CALS와의 만남은 우리의 선택이 아니라 모두에게 외부로부터 불어오는 필연적인 피할 길 없는 숙명과도 같을 것이다. 따라서, 관련 전문가는 CALS를 보다 체계적으로 이해하고, 엔지니어링의 관점에서 해결책을 제시하여야 한다.

진행 속도가 가속화되고 있는 정보화는 빠른 진행 속도에 비례하여 정보화의 역기능 또한 다양한 형태로 나타나고 있다. 앞으로 정보화가 급진될수록 정보보호의 중요성은 날로 부각될 것이며 정보보호 분야가 정보기술산업을 주도할 것이다. 미래의 유망 서비스가 될 CALS 체제에 대한 정보보호는 필수적이므로 정보보호 분야에 대한 산업의 관심이 강조된다. 정보사회의 빠른 도래 및 정보화의 가속화와 더불어 정보보호에 대한 관심과 필요성이 증가하고 있으며 정보보호 기술의 적용이 급증할 전망이다. 안전하고 신뢰성 있는 CALS 체제로의 전환을 위해 우선적으로 안전한 CALS 정보보호 모델이 설정되어야 한다. 앞으로 본 연구팀은 CALS 체제에서의 정보보호 전반에 대한 정보보호 환경을 바탕으로 구체적으로 안전한 CALS 정보보호 모델을 제시하고자 한다.

참 고 문 헌

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

[2] 이임영, 이재광, 소우영, 최용락, "통신망 정보보호", 도서출판 그린, 1996. 2.

[3] 한태인, "세계 주요국의 CALS 정책", 정보처리 학회지, 1991, Vol. 4. No. 1.

[4] 정석찬, "일본의 CALS 정책과 NCALS 프로젝트", CALS/EC Journal, 1996. 9.

[5] 신장균, 나민영, 이승희, "CALS 구현을 위한 정보기술", 정보과학회지 제13권 11호, 1995. 11.

[6] 신동익, "CALS와 표준화", 정보과학회지 제13권 11호, 1995. 11.

[7] 강창구, "EDI 정보보호 서비스 분석", 제2차 안전한 EDI 관련기술 심포지움, 1996. 3.

[8] 김중인, 김석우, "CALS의 단계별 구현을 위한 보안기술", 정보보호와 암호에 관한 학술대회 자료집, pp.311-342, 1996.

[9] 한국 CALS/EC학회, "충청지부 CALS/EC 학회", 1996. 6.

[10] CALS/EC Journal, 1996. 9.

□ 著者紹介

신 종 태

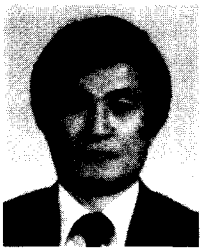
1978년 ~ 1982년 서울대학교 수학교육과(이학사)
1982년 ~ 1987년 숭실대학교 대학원 전자계산학과(공학석사)
1996년 ~ 현재 한남대학교 대학원 전자계산학과 박사과정
1984년 ~ 1996년 한국전자통신연구원 선임연구원
1996년 ~ 현재 한국정보보호센터 책임연구원, 시험평가팀장

※ 주관심분야 : 정보보호시스템 평가, 암호학, IDS, 컴퓨터/네트워크 보안, CALS/ES 보안

이 정 현

1993년 숭실대학교 전자계산학과(공학사)
1995년 숭실대학교 대학원 전자계산학과(공학석사)
1995년 ~ 현재 한국전자통신연구원

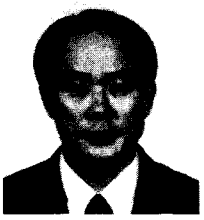
※ 주관심분야 : 컴퓨터/네트워크 보안



이 대 기

1966년 한양대학교 전자공학과(공학사)
1987년 한양대학교 산업대학원 전자공학과(공학석사)
1980년 ~ 현재 한국전자통신연구원 책임기술원

※ 주관심분야 : 정보시스템 감사, 통제 및 보안



소 우 영

1979년 2월 중앙대학교 전자계산학과 학사
1981년 2월 서울대학교 대학원 계산통계학과 전자계산학 석사
1991년 1월 매릴랜드대학교 대학원 전자계산학과 박사
1981년 3월 ~ 1985년 3월 공군사관학교 수학과 전자계산학과 전임강사
1991년 9월 ~ 현재 한남대학교 전자계산학과 부교수

※ 주관심분야 : 인공지능, 신경회로망, 통신망 정보보호