□ 기술해설 □

CALS 구현을 위한 정보기술

육군사관학교 신장균* · 나민영* · 이승희**

● 목 차 ●

1. 서 론
2. CALS 전략
2.1 CALS 개요
2.2 통합정보시스템을 위한 CALS 표준
3. 소요 정보 기술
3.1 고속 네트워크 기술
3.2 통합 데이터베이스 기술
3.3 정보보호 기술
4 결 론

1. 서 론

1980년대 중반에 탄생한 CALS(Commerce At the Light Speed) 전략은 기업이 생존을 유지하고 경쟁우위를 확보하기 위하여 컴퓨터와 통신의 신기술을 활용하는 혁신적인 정보 시스템이다. 특히 종래의 정보시스템이 컴퓨터와 데이터베이스를 수단으로 주로 기업 내부에서의 업무 합리화를 추구하는데 비해 CALS는 통합 표준에 의해 디지틀화된 데이터를 교류함으로써 기업내는 물론 기업간 컴퓨터 네트워크를 통한 정보 흐름의 고도화를 통하여 기업의 경영 혁신을 능동적으로 추구하는 것이 그 특징이다[12].

CALS 구현을 가능하게 하는 정보기술은 개방형 시스템 구조를 이루는 제반 응용 기술의 다양한 요소로 구성되는데 주요 핵심기술에는 표 1과 같이 멀티미디어 기술, 표준화 기술, 통합 데이터베이스 기술, 초고속 네트워크 기술, 정보보호기술 등이 있다.

멀티미디어 기술은 제품 수명주기에 걸쳐 생성되는 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 연구가 진행되고 있다.

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 SGML은 1986년도에 국제 표준 규격(ISO)으로 제정되었다.

네트워크 기술은 최근 광섬유 사용 및 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 연구되고 있다.

CALS 통합 데이터베이스(Integrated Database)는 각종 디지틀 정보를 통합하여 필요시 언제나 어디서나 엑세스할 수 있도록 해주는 CALS의 핵심 요소로써 이를 위해서는 먼저 공통 정보 모델을 선정하여 사용자에게 변환된 각종 정보 베이스 스키마를 제공할 수 있어야 하고 시스템은 사용자가 요청한 결과를 편집하

*종신회원
**비 회 원

표 1 CALS 구현 정보기술

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

여 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.

정보 통신망은 정보의 내용변경, 정보의 불법적 유출, 정보의 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. 보안시스템의 목표는 컴퓨터 시스템과 네트워크의 안전성, 신뢰성을 확보하여 개인의 프라이버시 문제, 자료의 신뢰성 문제, 컴퓨터 범죄 문제 등과 같은 고도의 정보화 사회가 갖는 취약점들을 극복하고 자료의 비밀성을 유지함으로써 사용자들이게 신뢰성 있는 정보를 안전하게 제공하는데 있다.

2. CALS 전략

2.1 CALS 개요

2.1.1 CALS의 개념

CALS는 1982년 미 국방성이 막대한 국방예산의 절감방안을 강구하던 중 군수지원체계의 효율성을 증대시키고, 문제점을 해결하기 위한 방안으로 시작한 프로젝트 였다. 그후 CALS는 일반기업체나 산업 각 분야에서 제품의 최초 생산계획으로부터 폐기에 이르는 수명주기 동안 관련된 모든 정보 및 활동을 통합하여 자동화시키는 개념으로 발전하게 되었다. 제품의 수명주기에 수반되는 모든 형태의 정보를 표준화된 방법으로 초고속통신망을 통하여 상호유통함으로써 보다 값싸고 질 좋은 새로운 제품을 소비자에게 빠른 시간 내에 공급할 수 있도록 하는 것이 CALS가 지향하는 목표인 것이다. 현재 CALS 개념은 미국, 캐나다, 호주, 싱가폴 등 세계 각국에서 전담부서를 설치하여 CALS 진흥활동을 전개해나가고 있는 실정이며, 과거의 CALS개념이 무기체계의 획득 및 군수지원분야에 한정되어 적용되었으나, 현재는 일반 산업분야에서 "제품의 설계로부터 제작, 정비 ,운용, 폐기에 이르는 모든 활동을 통합적인 정보기술을 통해 처리하는 산업화 전략 또는 신경영 전략" 이라는 개념으로 확장되었다[12].

현재의 CALS가 있기까지 정보기술이 발전되어온 과정을 살펴보면 다음과 같다. 먼저 수작업의 중앙집중식 전산화를 의미하는 자료처리시스템(EDPS)의 단계를 거쳐 관리자가 필요로 하는 정보를 적시에 필요한 형태로 제공해주는 관리정보시스템(MIS), 고급관리자의 의사결정을 지원하기 위한 의사결정지원시스템(DSS) 그리고 실무부서 소규모의 수작업을 분산처리하는 사무자동화(OA)단계로 발전되어 왔다. 그러나 위의 정보기술들은 기업내부에서의 업무합리화 및 효율성을 추구하는데 한정된 반면 CALS는 CALS표준에 의해 DB화된 데이터를 통신 네트워크를 통해 상호 유통시키게 됨으로서, 기업내는 물론 기업간, 또는 기업과 정부간 그리고 국가와 국가간에 정보흐름의 고도화를 이룰 수 있게 되는 것이다. CALS 구현을 위한 핵심기술로는 멀티미디어 기술, CAD/CAM 기술, 분산 DB 기술, 네트워크기술, 정보보호기술 등을 들 수 있으며, 이에 대한 통합적인 기술이 확보되어야만 CALS의 구현이

가능하게 된다. 급변하는 주변환경과 생존경쟁 체계 속에 처해 있는 현재의 기업들은 CALS가 제시하는 새로운 산업정보화 전략 또는 기업경영방법을 적극적으로 도입하여 자신의 경쟁력을 강화해야 할 것이다.

2.1.2 CALS개념의 변천 및 발전과정

CALS의 개념은 시대와 상황에 따라 다음과 같이 변화, 발전되어왔다.

가. Computer - Aided Logistics Support ('82)

이 개념은 초기에 미국방성이 무기체계의 군수지원을 위해 디지틀정보의 통합과 정보의 공유를 통한 신속한 자료처리환경을 구축하고자 한 군수지원전산화의 개념이다.

나. Computer-aided Acquisition & Logistics Support('88)

이는 무기체계의 군수지원뿐만 아니라 획득과정을 포함하는 총체적인 군수지원개념이다.

다. Computer-aided Acquisition & Life-cycle Support('90)

무기체계의 군수지원대신에 산업제품의 수명주기 지원으로 바뀌었다. 이시기에 기술 데이터의 저장, 검색과 DB의 생성에 대한 표준제정이 본격적으로 시작되었다.

라. Continuous Acquisition & Life-cycle Support('92)

이 개념은 제조업의 산업정보화전략에 가장 가까운 의미로서, 제품의 전 수명주기를 관리, 지원해주며, 모든 산업에 적용할 수 있음을 의미하는 개념으로 발전된 것이다.

마. Commerce At the Light Speed('95)

각국의 국가정보통신망 초고속화 계획과 국제통신망인 인터넷 사용의 확산으로 인하여 광속과 같이 빠른 초고속 전자거래 환경구축의 의미로 새롭게 바뀐 개념이다.

2.1.3 CALS 적용시 기대효과

CALS의 적용을 통하여 서류의 감소와 업무처리시간의 단축 그리고 이를 통한 비용과 인력의 절감효과를 기대할 수가 있다. 또한 기업과 기업간의 CALS적용효과는 네트워크를 통한 정보의 교환과 통합DB를 통한 정보의 공유가 가능해져서 전세계의 기업들과의 기업통합(Enterprise Integration)이 가능해진다는 것이다

CALS의 적용을 통하여 기대할 수 있는 효과를 정리해보면 다음과 같다.

가) 신속한 정보서비스

기술정보에 대한 DB체계를 구축함으로써 업무수행상 필요한 제반정보를 신속하게 지원받을수 있다.

나) 인력과 비용의 절감

서류에 의한 업무절차를 자동화 및 통합함으로써 서류의 작성, 수정, 분배 및 유지과정상의 인력과 비용을 절감할 수 있다.

다) 품질의 향상

CALS는 CAD/CAM/CIM 절차와 DB를 직접적으로 연결함으로서 장비의 설계, 획득, 정비지원과정에서의 품질을 향상시킬 수 있다.

라) 산업 경쟁력 강화

산업정보화 전략으로서 CALS 개념을 기업경영에 종합적으로 적용함으로서 , 기업경영방법 및 절차를 획기적으로 개선할 수 있다.

2.2 통합정보시스템을 위한 CALS 표준

CALS 적용을 위해서는 디지틀화된 문서, CAD로 된 설계도면과 기술도면 등을 전산망을 통해 송수신 할 수 있어야 하기 때문에 고속 통신망 구축과 함께 표준을 정하는 일이 필수적이다. 즉 사업발주서, 설계에 관련된 데이터 등도 표준화된 코드로 작성되고, 컴퓨터에 의해 생성, 저장되며 또한 서로 다른 곳으로 송수신되어야 한다. CALS 구현을 위한 정보의 표준화 작업은 생산과 관련된 제품 데이터의 상호교환을 위한 표준, 제품기술을 디지틀자료로 생성하고 관리하는 표준, 디지틀 기술자료의 자동색인과 출판을 위한 표준, 기술설계 자료에 대한 표준, 제품의 유통, 운송과 관련된 정보의 표준 등 크게 다섯가지로 나눠볼 수 있다.

지금까지 발전시켜온 대표적인 표준에 대하

여 간략하게 살펴보면 다음과 같다.

가) AITI(기술정보 자동교환) 표준

AITI(Automated Interchange of Technical Information)는 제반 CALS표준의 상위표준으로서 앞으로 제정될 CALS표준을 포함하여 군의 모든 규격을 통일하기 위한 종합문서이다. 이는 기술정보의 자동화된 교환을 위해 관련된 규격에 대하여 자료교환 및 화일관리에 대한 사항 등을 정의하고 있다. AITI의 목적은 제품의 전수명주기에 걸쳐 필요한 기술정보를 디지틀 형식으로 교환하는데 필요한 인터페이스를 표준화하며, 그 저장을 위해 데이터화일의 포맷과 정보구조를 표준화하는데 있다.

나) SGML(표준 범용 마크업 언어)

SGML(Standard Generalized Mark-up Language)은 문서출판시스템, DBMS, 재고관리 등의 응용 프로그램에서 자료를 저장하기 위해 사용되는 데이터 저장표준 및 문서교환방법으로서, 개방형 시스템 환경하에서 널리 사용되고 있는 국제표준이다. SGML은 1960년대 IBM에서 정보시스템을 구축시 page-oriented document의 규격화와 공유를 위해 개발됐던 GML(Generalized Mark-up Language)로 부터 출발되어 그후 현재까지 발전되어 온 것이다. 현재는 인터넷상에서 SGML을 이용한 web 서버, web 브라우저들도 많이 있으며, 미국방성및 각국 특허청에서도 채택하고 있다.

다) CGM(컴퓨터 그래픽)표준

컴퓨터 그래픽 데이터의 통신을 위한 CGM (Computer Graphics Metafile)은 이의 요구사항을 정의하고 있다. CGM은 복잡한 설계도면을 위한 IGES(Initial Graphics Exchange Specification)와는 달리 기술교범 등의 간단한 그래픽에 적용하므로 취급하는 화일 크기가 비교적 작다.

라) STEP/PDES(생산 데이터) 교환 표준

STEP(Standard for the Exchange of Product Data)는 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 국제표준인 STEP을 CALS 환경에 맞게 구체화 한 것이다.

3. 소요 정보 기술

3.1 고속 네트워크 기술

최근 정보처리 기술이 성숙해지고, 반도체 기술의 급속한 발전과 함께 광섬유 사용 및 컴퓨터를 통한 정보 교환의 보편화로 인해 통신망 사용자들이 요구하는 서비스가 음성, 데이터, 이미지, 그래픽, 동화상 등 개별 서비스 형태에서 이들을 동시에 처리할 수 있는 복합적인 형태로 변모하고 있다. 요구 서비스의 속성 또한 고속화, 고기능화, 고품질화뿐만 아니라 시각화, 지능화, 개인화(비밀통신) 등의 양상을 보이고 있다. 따라서 이러한 요구사항을 충족시키면서 다양한 서비스를 하나로 통합하여 제공할 수 있는 새로운 통신 기술이 필요하게 되었다[1, 13].

지금까지의 통신망은 서비스 종류에 따라 회선 교환, 패킷 교환 등 서로 다른 형태의 기술로서 발전되어 왔고 이들 통신망에 사용된 전송 미디어도 전송 대역폭이 각기 다른 미디어 즉 구리선, 동축 케이블, 광섬유, 전파 등 다양했기 때문에 서로 다른 특성을 갖는 서비스들을 하나로 통합하여 제공하기는 불가능하다. 이러한 점으로부터 서비스 제공자들은 기존의 다양한 형태로 전송하던 여러 종류의 정보를 하나의 형태로 통합하여 전송, 저장하고 표현하는 멀티미디어 서비스 개발에 주력하게 되었다.

멀티미디어 응용 서비스는 개인간의 정보 교환을 위한 개인간 멀티미디어 통신, 멀티미디어 문서 처리, 멀티미디어 정보 검색, 의료 진단, 회의, 교육, 발표, 원격 합동 문서 편집 등 전 범위에 걸쳐 다양하다. 멀티미디어 서비스는 개인의 단일 서비스뿐만 아니라 다수의 사용자가 복수의 서비스를 요구하므로 복수의 사용자들 간에 복수의 서비스를 제공할 수 있는 멀티파티/멀티컨넥션 기능이 필요하다.

현재 개발되고 있는 네트워크의 전송속도는

표 2 미디어 타입에 따른 필요 전송 속도 및 지연시간, 오류 허용률

서비스 종류	최대 지연 (초)	평균 전송률 (Mbps)	오류 허용률	패킷 오류 허용률
음성	0.25	0.064	$<10^{-1}$	$<10^{-1}$
비디오 (TV화질)	0.25	100	10^{-2}	10^{-3}
압축 비디오	0.25	2−10	10^{-6}	10^{-9}
자료 (화일 전송)	1	2−100	0	0
실시간 자료	0.001−1	<10	0	0
화상	1	2−10	10^{-4}	10^{-9}

100Mbps 정도이다. 이러한 속도의 네트워크는 네트워크 응용 기반의 모든 새로운 컴퓨터 개발이 기대된다. 기존의 것과 비교되는 차이점은 음성, 비디오, 정지화상, 자료화일 등과 같이 서로 다른 정보를 통합하고 있다는 점이다. 이러한 이유 때문에 새로운 응용들은 멀티미디어 응용이라고 불린다. 비록 새로운 네트워크 기술의 효과를 예측하는 것이 불가능할지라도, 멀티미디어 응용의 영향은 충분히 알려졌다.

CCITT의 멀티미디어 응용의 서비스 클래스를 보면 다음과 같다.

- 대화 서비스 : 직접적인 인터액티브, 실시간 통신, 음성, 비디오, 정지화상, 자료화일의 혼합형 교환
- 메세징 서비스 : 간접적인 1 : 1 통신
- 배포 서비스 : 1대 다 통신 서비스, (HIFI, video, HDTV 프로그램), 사용자 조절 스킴, 사용자 개인별로 서로 다른 부분을 접근 가능
- 수집 서비스 : 다양한 자료를 모으는 센서 지국의 모니터링

각각의 미디어 타입에 따라 필요한 전송 속도 및 지연시간, 오류 허용률을 살펴보면 다음과 같다.

현재 많이 연구중인 고속 네트워크 기술을 살펴보면 표 2와 같다.

3.1.1 FDDI(Fiber Distributed Data Interface)

FDDI는 ANSI X3T9.5에서 제안한 프로토콜이다. 전송 프로토콜로 토큰링 표준 802.5에 기반을 두고 있으며 매체 접근 방법은 토큰을 사용한 TTR(Timed Token Rotation)방식이고 전송 매체로는 광섬유를 사용하며, 전송 속도는 100Mbps이다. 링의 구성은 이중링으로 되어 있어 지국의 실패나 선로의 절단에 있어서 단일링의 단점을 보완한다. 정상 동작 시에는 기본링과 보조링이 서로 반대 방향으로 진행하고 각각 100Mbps의 전송 속도를 갖는다. 최대 거리 200km내에서 최대 지국의 수가 1000개까지 가능하나 이중링 구조로 구성될 경우 최대 100km내에서 500개의 지국이 접속될 수 있다[10]. FDDI 지국의 종류에는 이중화된 링에 직접 접속될 수 있는 등급 A 지국과 그렇지 못한 등급 B 지국이 있다. 등급 A 지국은 실질적인 링을 구성하는 지국으로서 쌍 접속 지국 및 집중기가 이에 속하며, 등급 B 지국은 집중기를 통하여 링에 연결되는 단접속 지국이다. FDDI-II는 기존의 FDDI-I에서 제공되는 패킷 교환 서비스에 등시성(Isochronous) 데이터 교환 서비스(즉, 회선 교환 서비스)를 추가함으로써 단순한 데이터 전송 외에 음성 및 화상 신호등을 통합 전송이 가능하도록 설계된 프로토콜로, 기존의 FDDI-I에 HRC(Hybrid Ring Control)부분을 추가하였다. 초기 버전의 FDDI가 패킷에 중점을 둔 서비스였다면, FDDI-II는 추가로 연결-중심 서비스를 제공한다. FDDI-II 링의 대역폭은 연결-중심 서비스를 위하여 각각이 6.144 Mbps 용량을 갖는 16개의 장대역(wideband) 채널로 나누어 질 수 있다. 고정된 프레임 구조가 그러한 목적으로 사용된다. 매 125μs마다 버스 마스터에 의해 새 프레임이 삽입된다. 프레임 구조에 기반하여, FDDI-II는 4가지 형태의 트

레픽을 제공한다.

- 동시성(isochronous) : 서킷 스위치 자료에 사용. FDDI-II에서만 제공된다. 동시성을 위하여 하나 이상의 FDDI-II 프레임의 장대역 채널이 사용된다. 등시성 트래픽은 일정한 지연을 갖는다.
- 동기성(synchronous) : 동기성 트래픽을 사용하여 고정된 자료를 정규화 된 시간 안에 전송할 수 있다. 그래서 이 방식은 제한된 지연에 적합하다. 이 방식은 FDDI와 FDDI-II 양쪽에서 다 사용 가능하다.
- 비동기성(asynchronous) : 등시성과 동기성에서 사용하지 않는 대역폭을 비동기성 트래픽에서 사용한다. 이 방식에서는 지연의 상한을 잡을 수 없다. FDDI에서는 두 가지 비동기성 전송을 제공한다.
  - 제한(restricted) : 모든 가능한 비동기성 대역은 제한된 토큰 방식에서만 몇몇 지국에서 사용된다.
  - 비제한(non-restricted) : 모든 지국에서 가능한 비동기성 대역폭을 사용가능하다.

3.1.2 DQDB(Distributed Queue Dual Bus)

DQDB는 IEEE에서 MAN(Metropolitan Area Network)을 염두에 두고 표준화 작업을 한 프로토콜로서, 1990년 12월에 정식으로 IEEE 802.6에서 표준으로 채택되었으며, 다음과 같이 크게 3가지의 특성을 가지고 있다[10].

첫째, 비교적 양이 적고 bursty하나 실시간 요구 특성이 약한 정보들을 전송하기 위한 비연결형 서비스와, 양이 많으면서 실시간 요구 특성이 약한 정보들을 전달하기 위한 연결형 서비스, 그리고 고정된 대역폭 및 실시간적 전달을 요구하는 등시성 서비스를 모두 제공한다.

둘째, 광섬유를 매체로 사용하는 것을 전제로 최대 전송 속도는 제한되지 않고 있으며, 현재 기본 표준안에는 전송 시스템으로서 ANSI DS3(44.736Mbps)만이 정의되어 있으나 차후에 CCITT G.703(34.368Mbps 및 139.264 Mbps) 및 CCITT G.707-709(155.520Mbps) 등을 규정할 계획에 있다.

셋째, CCITT에서 장래에 공중 광대역 서비스를 제공할 수 있도록 규정 권고 단계에 있는 광대역 종합정보통신망(BISDN)의 ATM과 같은 셀 구조를 가지고 있어서 상호 연동이 용이하도록 규정되고 있다. 이는 MAN이 사설망은 물론 공중망으로도 사용될 수 있음을 나타낸다.

DQDB는 세 개의 기능 모델을 정의하고 있는데, 비연결형 데이터 서비스를 위한 MCF(MAC Convergence Function for Connectionless service), 연결형 데이터 서비스를 위한 COCF (Connection Oriented Convergence Function) 그리고 등시성 서비스를 위한 ICF (Isochronous Convergence Function)가 있다. 이 기능 중 MCF와 COCF는 QA(Queued Arbitrated) 기능에 의해 지원되며, ICF는 PA(Pre-Arbitrated)기능에 의해 지원된다. 따라서 DQDB는 음성, 영상 등과 같이 주기적으로 생성되며 실시간 전송이 요구되는 트레픽을 전송하는 등시성 서비스와 데이터를 전송하는 비등시성 서비스를 지원하며, 이러한 두 종류의 서비스를 제공하기 위하여 두 가지 형태의 접근 제어를 하는데, 등시성 서비스를 위한 PA제어와 비등시성 서비스를 위한 QA제어가 있다. QA기능은 분산 큐잉 (Distributed Queueing) 원리에 의해 이루어지며, PA기능은 채널 할당(Channel Alloca-tion) 방식에 의해 작동되는데 이는 분산 큐잉 방식에 비해 상대적으로 간단하다. DQDB가 150Mbps의 높은 전송 속도로 데이터, 음성, 영상 등의 멀티미디어 전송 서비스를 낭비 없이 효율적으로 할 수 있지만, 각 노드들 사이에 채널 접근시 나타나게 되는 불공정성 문제를 안고 있다. 이러한 불공정성 문제는 망의 크기가 커질수록, 전송속도와 망의 부하가 높을수록 더욱 심각해진다. 이를 해소하기 위해 DQDB에서는 전송 대역폭을 각 노드에게 균등하게 분배하기 위하여 기본 분산 큐잉 알고리즘에 추가하여 BWB (Band-Width Balancing)메커니즘을 사용한다.

3.1.3 ATM(Asynchronous Transfer Mode)

ATM은 CCITT에서 B-ISDN의 전송 방식

으로 채택된 기술로서 SG11과 SG18에서 연구되고 있으며, 전송 속도는 HDTV 서비스 속도와 반도체 기술(CMOS VLSI)을 고려하여 155.520Mbps 와 622.080Mbps(4 * 155.520 Mbps)가 권고되고 있다[10]. ATM은 실시간성 서비스가 용이한 회선 교환 방식과 대역폭이 효율적인 사용이 가능한 패킷 교환 방식을 혼합한 연결성 모드(Connection-Oriented)전송방식으로서 5byte의 헤더를 포함한 53byte의 고정된 셀로 전송되며 분리된 경로를 통하여 사용자 정보와 신호 정보가 전달된다. 그러므로 ATM은 고정 속도 및 가변 속도 서비스 모두에 쉽게 적용 가능하며, 짧은 작은 지연변이 특성을 가지므로 광역망 환경 하에서 음성, 데이터, 비디오 등의 멀티미디어 정보를 통합 전송할 수 있다.

3.2 통합 데이터베이스 기술

본 절에서는 CALS 시스템에서 핵심적 역할을 담당하는 통합 데이터베이스의 개념 및 기능을 살펴보고 그 소요 기술을 분석한다.

3.2.1 CALS와 IDB

통합 데이터베이스(Integrated Data Bases : IDB)는 그림 1에서 보는 바와 같이 CALS 시스템의 핵심 요소로서 기존의 시스템과 제품 개발자의 데이터를 통합한 다른 형태의 데이터베이스이며 실제적으로 분배가능한 데이터베이스이다[12]. 여기서 통합이란 표현은 논리적 통합으로 이는 즉 다양한 형태와 성질의 정보를 어디에서나 투명하게 실시간에 액세스할 수 있다는 의미이지 물리적으로 하나의 컴퓨터나 한 장소에 모아 둔다는 것은 아니다. CALS의 목표 달성은 궁극적으로 처리 및 액세스가 가능한 데이터를 한번 생산하여 여러번 사용할 수 있는 통합 데이터베이스에 달려 있다. 다시 말하면 CALS 전략의 1단계 목표는 디지틀의 흐름이고 최종 목표는 정부와 업체가 통합된 데이터베이스를 구축하고 이를 공유하면서 제품의 전 수명 주기에 활용한다는 것이다.

IDB에 포함되는 정보의 형태는 참고도서 데이터베이스, 사전/법령 데이터베이스, 제품 기술정보, 사건 기록 및 추적체계 데이터베이스,

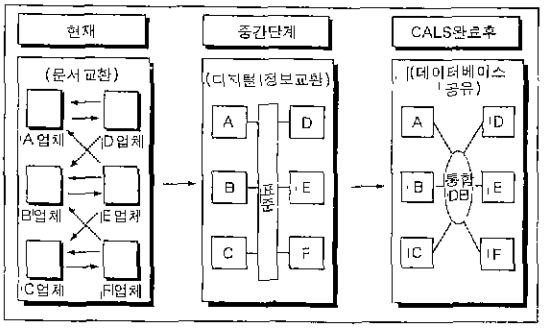


그림 1 CALS의 단계별 구축개념

기술도면 데이터베이스 및 다양한 통계 데이터 등이 있으며 이들 각각의 구성 요소들은 서로 다른 데이터베이스의 데이터를 받아 결합하여 새로운 데이터를 구성할 수 있다. 물론 이때 각각의 데이터베이스들은 서로 독립적이어야 한다. 이러한 IDB 개념이 회사에 적용하면 IPDB(Integrated Product Data Base)라 불리고 군수 분야에 적용되면 IWSDB(Integrated Weapon System Data Base)로 불린다.

IDB가 구축되면 구축된 IDB는 다음과 같이 단계별로 활용될 수 있다[12].

가) 획득단계

IDB는 새로운 시스템의 획득과 현존 시스템의 현대화의 개선에 중대한 역할을 수행한다. 통합 디지틀 데이터의 저장, 전자 네트워크, 조회의 자동화 그리고 주석 능력은 시스템을 획득하는데 질적인 개선을 가져올 것이다.

나) 설계단계

CALS IDB는 동시공학 다양하고 강력한 기법, 논리적인 데이터베이스 표준을 이용한 데이터를 지원하기 위해 컴퓨터를 이용한 설계 절차를 가능하게 할 것이며 복잡한 제품이 효과적으로 설계될 것이다.

다) 생산단계

선박, 비행기, 탱크, 그리고 다양한 시스템과 장비의 수리를 위한 부품이나 구성품의 신속한 생산은 필수적이다. IDB로부터의 정확한 기술데이터의 신속한 가용도는 이와 같은 신속한

생산을 가능하게 해준다.

라) 정비단계

정비활동은 훌륭한 진단과 수리 데이터베이스에서 특별한 수리를 위한 모든 절차를 통합하여 지원받게 될 것이다. 통합생산 데이터베이스는 정비 속도를 증대시킬 것이고 변경과 평가 설계 그리고 통합을 철저하게 할 것이다. 관계된 그래픽, 데이터, 본문, 표를 연결시키고 상호운용 전자 기술교범을 이용한 진단 결과 그리고 과업을 간략하게 통합시키는 패키지는 일반적인 활동으로 만들 것이다.

마) 후속지원단계

IDB는 서류 없는 환경하에서 후속 지원 요소의 획득을 지원한다. 이는 수리 진단, 피드백 데이터, 엔지니어링 데이터, 그리고 후속 지원성 데이터를 통합한다.

바) 물자 및 획득단계

IDB는 향상된 후속 지원 데이터의 정확성을 유지하며 재고를 관리한다. 예를 들면, 고장 및 정비를 위하여 획득되어진 데이터를 분석하여 개략적인 요소로 설명하는데 사용되어질 것이다.

사) 교육단계

제품이 더욱 복잡해지고 운용 교리는 조화에 강조를 두게 되어 상호 운용성 및 높은 수준의 성능을 갖게 됨에 따라 중단 없는 인력 양성 교육의 필요성이 대두되었다. IDB는 개선된 교육의 개발과 운용을 지원하기 위한 통합되고 정확한 정보를 제공하게 될 것이다.

3.2.2 CALS IDB 구축방안 및 소요기술

먼저 정보베이스의 가장 기본인 데이터베이스를 통합하는 기법부터 살펴보자. 이질 데이터베이스를 통합하는 방법에는 크게 tightly coupled 방법과 loosely coupled 방법의 두가지로 나누어 생각해 볼 수 있다[8].

이질 데이터베이스 통합을 이루는 한 가지 방법은 tightly coupled 방법이라 하여 전역스키마(통합스키마, global schema, universal schema)를 사용하는 것이다. 전역스키마를 사용하는 시스템에서는 스키마 변환 및 스키마 통합을 통해 전역스키마를 구성한 다음 이 전역스키마에 해당되는 데이터 조작언어를 이용하여 질의어를 표현한다. 이러한 연구의 대표적인 예로서는 CCA의 MULTIBASE [2], UNISYS 의 Mermaid[11] 등이 있다. Mermaid는 미 국방성의 요구에 의거 1982년부터 1987년까지 SDC사가 개발한 시스템으로 그 구조는 사용자 인터페이스, 데이터 사전, 서버, DBMS 인터페이스 등 4부분으로 구성된다. 이 시스템은 데이터베이스 시스템이라기 보다는 지역 DBMS에 의해 유지되는 데이터를 통합해 주는 일종의 front-end로 볼 수 있다. 사용자는 하나의 단일 언어 즉 SQL을 사용하여 여러 데이터베이스로부터 데이터를 액세스하고 통합할 수 있다. 통합을 위해서는 데이터를 먼저 표준 데이터 타입으로 변환해주어야 한다. 이러한 tightly coupled 기법을 이용하면 여러 데이터베이스 스키마를 통합하여 단일의 인터페이스를 제공하게 되므로 위치 투명(Location Transparency)을 얻을 수 있으나 스키마를 통합해야하는 어려움이 있다.

이질적인 데이터베이스들을 통합하는 또 하나의 다른 방법은 loosely coupled 방법이라 하여 전역스키마를 사용하지 않는 대신 강력한 DB 조작 언어를 이용하는 것이다. 이 언어를 Litwin은 multidatabase language라 불렀다. 대표적인 예로서는 휴스톤 대학의 Omnibase [7], DIRECT[3] 등이 있다. DIRECT는 관계대수에 기초를 둔 이질 데이터베이스를 위한 질의어로서 서로 다른 데이터베이스의 데이터를 검색하는데 유니폼한 인터페이스를 제공한다. 시맨틱 상으로 동등한 데이터 요소들은 조인이나 유니온 같은 질의 기능을 통해 간접적으로 정의될 수 있다. DIRECT 질의어는 데이터를 합병하고 조인하는 연산, 서브질의어로 나누는 연산 및 대부분의 질의어에서 제공되는 연산 등을 제공한다.

일반적으로 이러한 멀티 데이터베이스 언어는 일반 데이터베이스 언어의 능력도 가지고 있어야 함은 물론 관련된 데이터베이스들이 상호작용(interoperable)할 수 있도록 지원해야

만 한다. 여기서 상호작용이란 전역스키마의 부재와 자치성의 제약에도 불구하고 비절차적 오퍼레이션을 통해서 데이터베이스들을 사용할 수 있음을 의미한다. 이 기법을 이용하면 스키마 통합을 하지 않아도 되는 편리함이 있는 반면 위치 투명이 제공되지는 않는다.

CALS IDB는 다양한 데이터베이스들이 그 입력이 될 수 있으므로 이 두가지 접근 방법 중 스키마를 통합하는 기법은 다양한 형태의 많은 스키마를 통합하는 일이 쉽지 않고 더우기 계속 변화하는 스키마를 통합에 반영하는 것이 어렵기 때문에 loosely-coupled 방법을 사용하여 IDB를 구축하는 것이 바람직할 것이다.

이러한 CALS IDB를 구축하기 위한 소요 기술에는 공통 모델의 선정 및 변환 기술, 언어 번역 기술, 정보 필터링 기술, 제약조건 명세 기술, 분산 트랜잭션 기술 등 여러 가지 복합적인 기술이 요구되고 있으며 이들은 상호 유기적인 관계에서 연구되어야 할 것이다. 따라서 CALS IDB를 구축하기 위해서는 우선 이질 분산 데이터베이스 시스템을 구축한 후 초고속 정보통신망이 구축되어 가동되면 이 때 이질 분산 다매체 정보베이스 시스템으로 확장하는 방안이 좋을 것으로 생각된다.

3.3 정보보호 기술

컴퓨터 네트워크는 정보의 내용변경, 정보의 불법적 유출, 정보의 파괴, 위조된 정보의 유통 등의 보안 위협을 내포하고 있다. 이 절에서는 다양한 보안 위협에 대해서 정보를 안전하고 신뢰성 있게 보호할 수 있는 보안 서비스의 종류와 이를 구현할 수 있는 보안 메커니즘을 분석한다.

3.3.1 보안 서비스

컴퓨터 네트워크가 제공해야 하는 보안 서비스에는 비밀성(confidentiality), 인증성(authenticity), 무결성(integrity), 가용성(availability)이 있다[9].

가) 비밀성 서비스

컴퓨터 네트워크는 컴퓨터 시스템에 대한 비인가자 및 불법 침입자의 액세스를 제어하고, 전송되는 정보의 비밀 내용이 노출되지 않도록 인가된 자에게만 읽기 접근이 가능하도록 하여야한다. 이러한 비밀성을 보장하기 위한 메커니즘으로는 액세스 제어와 화일 암호화를 들 수 있다.

나) 인증성 서비스

컴퓨터 네트워크의 사용에서는 다양한 실체들을 확인할 필요가 있다. 이에 해당하는 실체에는 물리적 실체(예, 컴퓨터 시스템), 논리적 실체(예, 통신계층의 각 실체 또는 응용 프로그램) 그리고 사용자 자체이다. 인증이란 이러한 실체를 가장하여 컴퓨터 네트워크에 침입하는 경우를 대비하여 정확하게 실체를 확인하는 작업을 의미한다. 이러한 인증성을 보장하기 위한 메커니즘으로는 디지틀 서명이 있다.

다) 무결성 서비스

무결성 유지는 인가된 사용자에 의해서만 화일 자료를 변경할 수 있도록 하여 비인가자 및 불법 사용자의 화일에 대한 기록, 삭제, 생성, 변경등의 액세스로부터 정보를 보호할 수 있어야 한다. 무결성 유지를 위한 메커니즘으로는 물리적 통제와 액세스 제어를 들 수 있으며 또한 이미 변경되었거나 변경 위험이 있을 때 이를 탐지하여 복구할 수 있는 메커니즘도 필요하다.

라) 가용성 서비스

시스템이나 시스템내의 자료는 허가된 사람에게는 효율적으로 사용할 수 있도록 하여야 한다. 즉 정보가 손상되지 않고 사용하고자 할 때는 항상 획득이 가능하도록 데이터의 백업, 중복성(redundancy)유지, 물리적 위협 요소로부터의 보호를 유지함으로써 이러한 가용성을 높일 수 있다. 그러나 시스템 사용을 완전히 배제하는 완벽한 보안성과 가용성은 상호 이율배반적인 면이 있으므로 컴퓨터 네트워크 보안의 균형을 이루도록 절충하는 것이 바람직하다.

3.3.2 보안 메커니즘

보안 공격을 탐지하고, 예방하며, 복구할 수

있는 보안 메커니즘은 하나 또는 여러 개의 메커니즘으로 구성되어 보안 서비스를 제공한다.

가) 액세스 제어

객체의 액세스를 원하는 이용자가 자신의 신원을 제시하고 인증 시스템으로부터 액세스를 위한 신원 인증을 받은 후, 확인된 이용자가 객체에 대한 액세스 권한을 확인하는 과정을 액세스 제어라고 한다. 액세스 제어는 임의적 액세스 제어(DAC; Discretionary Access Control)와 강제적 액세스 제어(MAC; Mandatory Access Control)로 구분된다. 임의적 액세스 제어는 주체의 식별(identification)에 근거하여 객체에 대한 액세스 요구를 통제하는 방법으로 한 주체가 다른 주체에게 자신이 갖고 있는 액세스 권한을 넘겨주는 것을 허용하는 것으로 가장 일반적인 모델로는 액세스 행렬 모델이 있다. 강제적 액세스 제어는 객체에 포함된 정보의 기밀성(sensitivity)과 주체에 부여된 보안인가(clearance)에 근거하여 수학적 보안 모델에 의한 보안 정책을 적용함으로써 주체의 객체에 대한 액세스를 강제로 통제하는 방법으로 일반적인 모델로는 BLP모델, Lattice모델 등이 있다.

나) 암호화 알고리즘

암호화 알고리즘이란 평문(plaintext)을 암호문(ciphertext)으로 바꾸어 주며, 암호문을 본래의 평문으로 복원하는 알고리즘이다. 대부분의 암호시스템은 암.복호화 과정에서 특정한 키(key)를 사용하여 키를 알고 있는 자만이 암호문을 생성할 수 있고 특정 암호문을 평문으로 복호화 할 수 있도록 하고 있다. 따라서 자료를 암호화시켜 보호하는 데는 알고리즘뿐만 아니라 키 관리를 어떻게 하느냐가 매우 중요하다.

일반적으로 암호 시스템은 관용 암호 시스템(conventional cryptosystems)과 공개키 암호 시스템(public-key cryptosystems)으로 분리하고 있다. 관용 암호 시스템은 암.복호화 키가 동일하거나 혹은 동일하지 않더라도 하나의 키에서 다른 키를 쉽게 계산하여 얻을 수 있는 시스템으로 사용이 편리하고, 속도가 빠르다는 장점이 있다. 그러나 암호키가 제3자에게 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)가 있다[4].

공개키 암호 시스템은 비밀키와 공개키의 두 개의 키를 사용하는데, 공개키는 암호화할 때 사용하고 비밀키는 복호화 할 때 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 암호 시스템에는 RSA알고리즘이 있다[6].

다) 디지틀 서명

디지틀 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.

즉 공개키 암호 시스템에서 서명자가 소유한 비밀키로 메시지를 암호화하면 그 결과가 서명이 되며 이 서명은 누구나 서명자의 공개키로 복호화 하여 그 결과가 일정한 규칙을 만족하는 의미 있는 메시지인가를 확인할 수 있다. 이와 같이 서명의 확인과정에서 원래의 메시지가 복원되는 서명방법을 메시지 복원형 디지틀 서명이라고 한다. 메시지 복원형 디지틀 서명은 서명할 메시지가 긴 경우 이를 일정한 길이로 분할하여 각 블록마다 서명 및 확인 과정을 반복해야 하므로 많은 수의 연산이 필요하며 서명 생성이나 확인과정에 많은 시간이 소요된다. 따라서 임의 길이의 메시지에 해쉬 결과에 대해서만 복원형 서명을 생성하고, 수신된 메시지를 해쉬 한 결과와 서명을 복원하여 얻은 결과가 일치하는지를 확인함으로써 서명을 확

인할 수 있다. 이러한 서명 방법은 부가형 디지를 서명이라고 하며 대표적인 방법에는 DSS (Digital Signature Standard)[5]이 있다.

라) 신원 확인

안전한 통신 환경을 유지하기 위해서는 원거리 신원확인 즉 통신 상대자가 적법한 상대인가를 알아야 하고, 상대방에게도 자신이 적법한 통신 상대자라는 것을 인식시켜 주어야 한다. 신원확인에는 그 형태에 따라 일방향 신원확인과 양방향 신원확인으로 구분된다. 일방향 신원확인은 메시지를 전송하는 측에서 일방적으로 송신자가 정당함을 증명하고, 수신자로 하여금 메시지 전송자를 확인하고 신뢰할 수 있도록 하기위하여 무연결 지향(connentionless oriented) 통신에서 사용하는 것으로 송신자의 신원을 수신자에게 확인시켜 주는 과정이므로 발신처 신분확인(data origin authentication)이라고도 한다. 한편 양방향 신원확인은 연결지향(connection oriented) 통신에서 서로를 확인하기 위하여 사용되는데 양 당사자간에 서로를 확인하기 때문에 쌍방 신원 확인(peer entity authentication)이라고도 한다. 이와 같은 원거리 신원확인에서는 서로의 특정정보가 능동적인 도청 등의 보안 위협에 의해 변조되지 않았음을 서로가 확인할 수 있어야 하는데 이를 구현할 수 있는 방법에는 암호화 프로토콜에 의한 신원확인과 영지식 증명을 이용한 신원 확인 프로토콜이 있다.

4. 결 론

국방 군수 산업을 중심으로 시작된 CALS는 이제 군수분야뿐만 아니라 각종 제조업 중심의 전 산업에 걸친 산업 정보화로 발전해가고 있다. 각종 제품의 전 수명주기와 관련된 정보는 점점 더 복잡해져 많은 도면과 문서, 그림 등 복합적인 정보로 변해가고 있다. 이와 같은 다양한 성질의 정보는 최초 생성 후 저장 유통 단계가 종합적으로 관리되어야 한다. 본 고에서는 이러한 산업정보화 전략인 CALS가 무엇인가 그 개념을 살펴보고, 이를 근거로 대략적이나마 주요 소요기술을 살펴보았다. CALS의 구현을 위해서는 여러 정보 기술이 복합되어야 하며 이는 개방형 시스템 구조를 이루는 제반 응용 기술의 다양한 요소로 구성되는데 이를 위한 주요 핵심 기술에는 표준화 기술, 고속 네트워크 기술, 통합 데이터베이스 기술, 그리고 이러한 정보 및 시스템을 보호하는 정보보호 기술 등이 있다.

국제 경쟁력 있는 산업 정보화를 위해서는 위에서 언급한 CALS 관련 기술들이 인프라스트럭쳐인 초고속 정보통신망과 연계되어 심도 깊게 연구되어야 할 것이다.

참고문헌

[1] Dietmar B. Hehmann, Michael G. Salmony, Heinrich J. Stuttgen. 'Protocols for High-speed Networks", IFIP. pp. 303-312. 1989.

[2] Katz, R., Goodman, N., Landers, T., Smith, J. M., and Yedwab, L., "MULTIBASE-A System for Integrating Heterogeneous, Distributed databases," Computer Corporation of America, Technical Report 81-06, May 1981.

[3] Merz, V. and King, R., "DIRECT : A Query Facility for Multiple Databases," ACM Transactions on Information Systems, Vol. 12, No. 4, 1994.

[4] NIST. Data Encryption Standard, FIPS PUB, 46, 1977.

[5] NIST, Digital Signature Standard, FIPS PUB 186, 1994.

[6] Rivest, R., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public Key Crytosystems", Comm. ACM, Feb, 1978.

[7] Rusinkiewicz, M., Czejdo, B., Elmasri. R., Georakopoulos, D., Jamoussi, A., Karabatis, G., Li, Y., Loa, K., Gilbert, J., and Musgrove, R., "Query Processing in OMNIBASE - A Loosely Coupled Multidatabase System," Technical Report UH-CS-88-05, University of Houston, February 1988.

[8] Sheth, A., and Larson, J.. "Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases," ACM Computing Surveys, 22(3), September 1990.

[9] Stalling, W, Network and Internet Security, P-H, 1995.

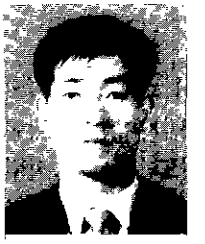
[10] Stalling,W., Networking Standards, Addison-Wesley, 1993.

[11] Templeton, M., Brill, D., Dao, S. K., Lund, E., Ward, P., Chen, A. L. P., and Macgregor, R., 'Mermaid-A Front-end to Distributed Heterogeneous Databases," *Proceedings of the IEEE*, Vol. 75, No. 5, May 1987.

[12] 김철환, 김규수, 21세기 정보화 산업혁명 CALS, 문원, 1995.

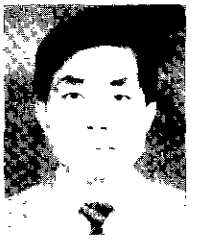
[13] 송덕영, 임만엽, 김대영, "멀티미디어 통신 프로토콜 구조에 관한 연구," 동계 컴퓨터 통신 Workshop 논문집, 1992.

신 장 균



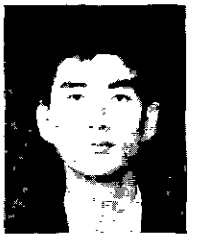
1974 육군사관학교 졸업
1979 서울대학교 산업공학과 (학사)
1983 미국 위스콘신 대학교 전산학 석사
1989 고려대학교 전산학 박사
1979～현재 육군사관학교 전산학과 교수
관심분야 : 컴퓨터 네트워크 보안, 암호학 응용

나 민 영



1978 육군사관학교 졸업
1983 서울대학교 전자계산기 공학과 (학사)
1986 서울대학교 전자계산기 공학과 (석사)
1990 University of Florida 전산학 박사
1986～현재 육군사관학교 전산학과 부교수
관심분야 : 데이터베이스 설계, 분산 및 연합 데이타베이스, 정보공학

이 승 희



1982 육군사관학교 졸업
1988 미국 해군대학원 전산학 석사
1989～1995.9 육군본부/교육사령부 전산실 근무
1995.9～현재 육군사관학교 전산학과 전임강사
관심분야 : 컴퓨터 네트워크, 지형정보 시스템