The Journal of Korean
Institute of CALS/EC
Vol. 4, No. 2, September 1999

CALS체계의 정보보호 구조 연구

남길현*

A Study on the Security Architecture of CALS System

Kil-Hyun Nam

Abstract

With developing computer and communication technologies, the concept of CALS system has been popular not only to military but also to commercial industries. The security problem is one of the most critical issues to construct CALS infrastructure. The CALS system needs some security functions such that data confidentiality, integrity, authenticity, availability, and non-repudiation. This paper proposes a security architecture model in CALS. The security architecture model is composed of 5 submodels such that network security model, authentication and key management model, operation and audit model, integrated database security model, and risk analysis model.

Key Words : CALS, Security, Cryptography, Authentication, Digital Signature, Risk Analysis, Security Audit, Integrated Database

* 국방대학원 전자계산학과

1. 서 론

21세기 정보사회 진입을 눈앞에 두고 컴퓨터와 통신기술의 발전과 인터넷의 비약적인 확산에 힘입어 세계는 시분초를 다투는 단일 생활권으로 압축되고 있다. 현재 선진 각국에서는 정부기관 및 군 뿐만 아니라 일반 산업체에서도 CALS 개념을 도입하여 컴퓨터 네트워크와 통합 데이터베이스를 구축하여 정보의 공유 및 교류를 추진하고 있다. CALS체계의 환경은 통합된 공유 환경 하에서 유용한 정보를 적시에 적절히 제공받을 수 있는 분산된 통합 데이터베이스 환경이며 다양한 기능분야의 많은 사용자들이 데이터에 접근하는 체제라고 볼 수 있다. 이러한 데이터들은 개방된 공유 정보로부터 비밀을 요하는 전략 정보 및 장비 규격정보 등이 포함되어 있다. 따라서 이들 공유정보들에 대한 기밀성과 무결성을 유지하고 가용성과 인증성을 확보하기 위해서는 적절한 정보보호 체계가 구축되어야 한다. 본 논문에서는 CALS의 개념과 CALS에서의 정보보호 위협요소, 정보보호 서비스, 메커니즘, 정보보호 기술동향 등을 분석하고 안전한 CALS체계 구축을 위한 정보보호 구조 모델을 제안하고자 한다.

2. CALS 기반기술 환경과 정보보호의 위협 요소

2.1 CALS의 역사적 배경과 발전과정

CALS는 1982년 미 국방성이 막대한 국방예산의 절감방안을 강구하던 중 컴퓨터를 이용하여 군수품의 군납체제를 자동화 및 표준화시킴으로써 통일된 자료 구축을 위하여 방대한 자료를 디지털화 하는데서 비롯되었다. 초기에 CALS는 서류와의 전쟁에서 탈피하여 군수지원체계의 효율성을 증대시키고 문제점을 해결하기 위한 방안으로 시작한 프로젝트였다. 그후 CALS는 일반기업체나 산업 각 분야에서 제품의 최초 생산계획으로부터 폐기에 이르는 수명 주기 동안 관련된 모든 정보 및 활동을 통합하여 자동화시키는 개념으로 발전하게 되었다. 제품의 수명주기에 수반되는 모든 형태의 정보를 표준화된 방법으로 초고속 통신망을 통하여 상호 유통함으로써 보다 값싸고 질 좋은 제품을 소비자에게 빠른 시간내에 공급할 수 있도록 하는 것이 CALS가 지향하는 목표인 것이다[김철환, 1995]. CALS의 개념 변천과정을 살펴보면 최초에는 군의 무기체계를 지원하는 개념에서 출발했지만, 무기체계의 설계, 제작, 군수 유통체계 지원을 위해 디지털 기술의 통합과 정보 공유를 통한 신속한 자료처리 환경 구축으로 정의할 수 있다. 이제는 제품의 생산 계획으로부터 폐기에 이르는 모든 활동을 디지털 정보 기술의 통합으로 구현하는 산업화 전략이라는 표현으로 바뀌고 있다. 이에 따라 CALS의 개념도 처음 컴퓨터에 의한 군수지원(Computer -Aided Logistic Support : 85년)으로 무기에 관한 군수지원 체계의 개념에서 컴퓨터에 의한 획득 및 군수지원(Computer-Aided Acquisition & Logistic Support : 88년), 지속적인 획득 및 수명주기 지원 (Continuous Acquisition & Life-cycle Support : 90년)으로 모든 산업에 적용할 수 있는 의미로 발전하였고 최근에는 광속의 상거래(Commerce At Light Speed :

95년)로 각국의 국가정보통신망 초고속화 계획과 국제통신망인 인터넷 사용의 확산으로 인하여 광속과 같이 빠른 초고속 전자거래 환경 구축의 의미로 새롭게 바뀐 개념으로 통용되고 있다.

2.2 CALS체계 기반기술

CALS 개념의 핵심은 정보교환 및 공유로서, CALS를 구현하기 위해서는 많은 정보 기술의 활용뿐만 아니라 표준화 및 업무의 혁신적인 재설계가 선행되어야 한다.
CALS체계 구축을 위한 필수적인 정보기술은 크게 표준화, 네트워크, 통합데이터베이스, EDI/EC, 정보보호, 경영혁신, 멀티미디어 및 객체 지향 기술 등으로 구분할 수 있다[국방부, 1997].

<표 1> CALS 기반기술

분 류	세 부 기 술
표준화 기술	데이터 표현 표준, 전송 표준 등
네트워크 기술	초고속 통신망, 인터넷 등
통합데이터베이스기술	데이터 공유, 변환, 저장, 검색 등
EDI/EC	전자문서 교환, 전자지불, 전자상거래
정보보호 기술	암호화, 디지털 서명, 인증, 키관리 등
경영혁신 기술	동시공학, 리엔지니어링, 컴퓨터 정보관리
멀티미디어 기술	하이퍼텍스트, 전송, 압축, 저장기술
객체지향 기술	객체지향 방법론, 객체 개발 지향 도구

먼저 표준화 기술은 디지털 데이터를 표준화된 포맷으로 생성, 저장하고 승인된 사용자가 활용 및 전송할 수 있는 디지털 데이터 공유를 위한 근본요소이다. CALS 표준은 각각의 표준들이 다양하고 서로 복잡하게 얽혀 있으며 분류방법도 약간씩 다르지만 크게 <표 2>와 같이 분류할 수 있다.

<표 2> CALS 표준 분야

구 분	표준 분야	내 용
가이드/절차 표준	MIL-HDBK MIL-STD CITIS IETM	데이터 구현 가이드 데이터 납기처리 사용자간의 정보 공유 절차 고장 수리절차 / 교육 가이드
데이터 파일 포맷 표준	SGML RASTER CGM MPEG JPEG	문자 래스터 그래픽 벡터 그래픽 동화상 칼라이미지(정지화상)
제품모델 표준	STEP IGES	생산데이터 CAD데이터
상거래문서 교환 표준	EDI Network Protocol	문서 교환 네트워크 접속
개방/공유 환경표준	IRDS GOSIP SQL RDA POSIX	정보자원 사전체계 정부 개방형 시스템 상호연결 프로파일 구조적 질의 언어 원격 DB 접속 호환성 OS인터페이스

네트워크 기술은 최근 광섬유 사용 및 인터넷 등의 대규모의 컴퓨터 네트워크를 통하여 정보 교환이 활성화됨으로 인하여 기존의 서비스뿐만 아니라 음성, 그래픽, 동화상 등 CALS에서 다양한 응용 서비스를 지원할 수 있는 고속 네트워크 기술을 말한다.

통합 데이터베이스 기술은 각종 디지털 정보를 통합하여 필요시 언제나 접근할 수 있도록 해주는 CALS의 핵심요소이다.
이를 위해서는 분산 데이터베이스 기술, 공통 모델 및 정보변환 기술, 정보의 저장 및 편집 기술, 이질 트랜잭션 관리 기술 등 복합적인 기술이 요구된다.

EDI(Electronic Data Interchange)는 거래 당사자들의 컴퓨터간에 네트워크를 통하여 상호거래에 필요한 표준화되고 정형화된 문서를 상호 교환하는 것을 의미하고, EC(Electronic Commerce)는 기업간 또는 기업과 개인 고객간에 가상 공간 내에서 전자정보를 통하여 거래 활동을 구현하고자 하는 기법이라고 할 수 있다. 정보보호 기술은 CALS 서비스에서 정보의 내용 변경, 정보의 불법적 유출, 정보의 파괴, 위조된 정보 유통 등의 보안 위협을 해결하기 위한 기술이다.

경영 혁신 기술은 제품의 주문으로부터 생산, 유지보수에 이르는 전 공정에서 통합관리 기능들이 요구되는데 이러한 기능을 지원하는 기술들을 말한다. 경영 혁신 기술은 조직 또는 기업 내부의 작업 방식을 변화시키며 기본적으로 프로세스를 분석, 설계, 리엔지니어링하는 전략을 제공한다.

멀티미디어 기술은 제품 수명주기에 걸쳐 생성되는 다양한 형태의 기술 데이터를 처리하는 기술로써 텍스트, 도면, 음성, 동화상 등의 데이터를 생성, 입력하기 위한 방법과 입력된 데이터의 표준화된 압축 저장 방법, 저장된 데이터의 전송 방법, 그리고 수신된 데이터를 활용하기 위한 출력 방법 등이 있다.

객체 지향 기술은 기존의 절차적인 형식의 순서화, 구조화된 형식을 크게 탈피, 실세계의 모든 개념적인 문제나 사물들을 객체(Object)로 보고 눈에 보이는 부분은 물론 보이지 않는 객체들까지 모델링하여 이를 컴퓨터로 구현하는 기술이다.

2.3 CALS에서의 정보보호 위협요소

CALS 환경은 네크워크화된 통합된 정보공유환경에서 상호 유용한 정보를 적시에 제공받을 수 있는 분산 통합데이터베이스 환경이다. 그러나 네트워크로 연결된 통합데이터베이스 환경에서는 전송자료의 불법적인 도청을 비롯하여 거짓정보를 유통시키거나 저장자료를 불법적으로 변조하고 파괴시키는 등의 여러 가지 유형의 컴퓨터 범죄와 정보화 역기능적 현상이 일어나고 있다. 이러한 CALS 체계의 위협요소는 자연적으로 발생되는 위협 요소와 고의적으로 발생될 수 있는 위협요소로 분류 할 수 있다[최용락 외, 1998].

자연적인 위협요소에는 자연적인 현상으로 화재, 홍수, 지진, 화산, 태풍, 폭풍우 등의 자연적 재앙과 사용자의 에러 및 오조작으로 인하여 발생되는 에러 및 손실, 관리자의 부주의로 발생되는 정보관리 부실, 네트워크 장애, 시스템 장애 등이 있다.

고의적인 위협요소로는 내부자 권한 남용, 산업 첩보 행위, 컴퓨터 해킹, 비인가된 이용자가 자원을 불법적으로 접근하기 위한 위장, 메시지 순서 변조, 정보 변조, 서비스 거부, 부인, 정보 누출, 신분 레이블 변조 등이 있다.

3. CALS에서의 정보보호 기반구조

CALS 체계는 통합 데이터베이스를 활용하여 정보를 검색·저장하므로 많은 위협요소가 존재할 수 있다. 안전한 CALS 체계 구축을 위하여 기밀성을 비롯한 인증, 무결성, 부인봉쇄 서비스가 제공되어야 하고 정보보호 서비스를 제공하기 위한 다양한 정보보호 메커니

즘이 활용되어야 한다. 아울러 국가, 기업 및 개인정보를 보호하기 위한 다양한 정보보호 기술들이 사용되어 정보를 안전하게 보호할 수 있다.

3.1 CALS 정보보호 서비스

CALS에서의 정보보호 서비스는 다양한 정보보호 위협요소들로부터 정보를 안전하게 보호하기 위한 것이다. 안전한 CALS 구현을 위해 제공되어야 하는 정보보호 서비스는 데이터 기밀성, 데이터 무결성, 인증, 부인봉쇄, 접근제어 등이 있다[신종태 외, 1997].

기밀성 서비스는 컴퓨터 시스템의 정보 및 전송 정보가 의도된 당사자만 읽을 수 있도록 하는 서비스를 말하며, 무결성 서비스는 사용자들간에 주고받는 메시지가 정확한지 또는 변경되지 않았는지를 확인하기 위하여 컴퓨터 시스템 및 전송 정보가 오직 인가된 당사자에 의해서만 수정될 수 있도록 통제하는 서비스를 말한다. 인증 서비스는 정보 및 시스템의 자원 사용시 자원을 사용하려는 사용자의 신원을 확인하는 것이며, 부인봉쇄 서비스는 메시지가 송신되었을 때 송신자가 송신한 내용을 부인하거나 수신자가 수신된 사실을 부인하는 것과 같은 잠재적인 위협요소를 봉쇄하기 위한 것이다. 접근 제어 서비스는 개방 시스템의 상호 연결을 통하여 비 인가된 자원의 사용에 대한 보호를 제공하는 것으로 특정 자원에 대한 여러 유형의 접근에 적용되거나 또는 모든 자원에 대한 접근에 적용될 수 있다.

3.2 CALS 정보보호 메커니즘

CALS에서 요구되는 정보보호 서비스를 제공하기 위해서 암호화 알고리즘, 디지털 서명, 해쉬 알고리즘, 인증 메커니즘, 접근제어 메커니즘, 보안감사 메커니즘 등 다양한 정보보호 메커니즘이 요구된다[신종태 외, 1997].

암호화 알고리즘은 데이터 혹은 전송 메시지 정보에 대한 기밀성을 제공할 수 있는 메커니즘으로 관용 암호 시스템과 공개키 암호 시스템으로 구분할 수 있다. 디지털 서명은 데이터의 서명과 서명된 데이터의 확인 절차를 말하는 것으로 서명은 서명자의 개인적인 정보를 사용하고 확인 절차는 공개적인 절차 및 정보를 사용한다. 해쉬 알고리즘은 임의 비트 스트링을 입력받아 고정된 짧은 길이의 비트 스트링으로 출력하는 함수로서 메시지의 무결성 확인과 메시지 인증 코드의 구성, 디지털 서명의 효율성 증대 등을 목적으로 사용한다. 인증 메커니즘은 송신 객체에 의해 제공되고 수신 객체에 의해 인증되는 패스워드와 같은 인증 정보의 사용, 암호화 기법, 객체의 소유 및 특색의 사용 등이 이용된다. 접근제어 메커니즘은 객체에 접근을 원하는 사용자가 자신의 신원을 제시하고 인증 시스템으로부터 접근을 위한 신원 인증을 받은 후 객체에 대한 접근 권한을 획득하는 과정이다. 기타 정보보호 레이블 메커니즘, 보안 감사 메커니즘, 키관리 메커니즘, 경로설정 제어 메커니즘, 공증 메커니즘 등이 있다.

3.3 CALS체계에서의 정보보호 기술

CALS체계에서 국가, 기업 및 개인정보를 보호하기 위한 정보보호 기술은 시스템 정보보호기술, 네트워크 정보보호 기술, 암호화 기

술, 데이터베이스 정보보호 기술 등으로 분류할 수 있다.

시스템 정보보호 기술은 시스템의 약점을 이용하여 공격하는 해킹이나 바이러스 등 각종 시스템에 불법적인 접속을 통한 자료의 노출, 파괴, 변조, 유출 등의 보안 위협 요소들에 대한 대처기술로서 기존의 운영체제 내에 보안 기능을 갖는 보안 커널(Security Kernel)을 추가로 이식한 보안 운영체제를 운영하는 방법 등이 있다.

네트워크 정보보호 기술로서 네트워크에 제공되는 기본적인 정보보호 서비스로는 인증,접근통제, 비밀보장, 무결성, 부인봉쇄 등이 있고 이를 위한 정보보호 메커니즘으로 암호화, 인증, 데이터 무결성, 트래픽 패딩, 경로제어 등이 있다.

암호화 기술은 키관리기술, 전자서명기술, 메시지 다이제스트, 인증 기술로 분류할 수 있는데 이 세분화된 기술들에 의해 기밀성, 인증, 무결성, 부인봉쇄 등의 정보보호 서비스를 제공한다. 암호화 방법에는 관용키 암호기술을 사용한 DES, IDEA 등이 있고, 공개키 암호기술은 RSA, 타원곡선(Elliptic Curve)이론 등이 있으며 관용키 암호기술의 키 공유 문제를 해결할 수 있으나 속도가 느린 단점이 있다.

데이터베이스 정보보호 기술은 사용자와 데이터에 등급을 두어 기밀 정보의 보안을 유지하는 다단계 보안 시스템(Multilevel Secure System, MLS)이 제시되었고 가장 널리 사용되고 있다. 이 시스템은 사용자를 위한 하나 이상의 보안인가 등급과 시스템 내의 데이터를 위한 하나 이상의 분류 등급을 가진 시스템을 말하며 이러한 등급을 이용하여 기밀 정보의 노출을 제어하는 기법들을 제공한다.

4. CALS체계의 정보보호 구조 모델 제안

4.1 CALS 정보보호 구조 모델 개요

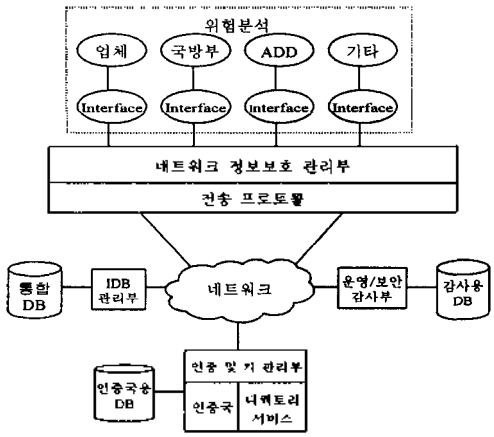
CALS 체계는 통합 데이터베이스의 정보를 검색 및 저장하고 메시지를 송·수신하는데 있어서 많은 위협요소들이 존재하며 이러한 위협요소로부터 정보를 보호하고 CALS의 원활하고 효율적인 운영을 위하여 적절한 정보보호 체계가 구축되어야 한다. CALS 정보보호 구조 모델은 CALS에서 요구되는 정보보호 서비스를 지원해야 하며 서비스를 지원하기 위하여 다양한 정보보호 메커니즘들을 활용하여야 한다. 따라서 제안된 모델은 개념적인 모델로서 각 응용별로 개발된 정보보호 기술들을 CALS 환경에서 통합된 형태로 모델화 하였다. 안전한 CALS 정보보호 구조 모델은 기능에 따라 <그림 1>과 같이 네트워크 정보보호 모델, 인증 및 키관리 모델, 운영 및 보안감사 모델, 통합 데이터베이스 모델, 위험분석 모델 등으로 분리하여 구성할 수 있다.

CALS체계의 정보보호 구조 모델을 구현하기 위해 기존의 전송환경에 부가하는 정보보호 환경으로 크게 네트워크 정보보호 관리부, 인증 및 키관리부, 통합 데이터베이스 관리부, 운영 및 보안 감사부 등으로 설계하였다.

4.2 네트워크 정보보호 모델

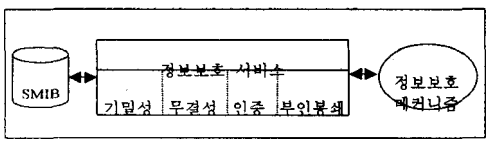
네트워크는 컴퓨터 시스템간의 상호 접속 및 정보 교환의 편리한 창구 역할을 하는 반면에 시스템에 대한 불특정 다수의 접근을 가

능하게 하여 시스템 침입자에 의한 보안 사고의 위험을 내포하고 있다. 특히 CALS 체계에서는 조직이나 업체의 이익과 관련되는 자료를 전송하는 경우가 있기 때문에 메시지를 안전하게 전송하기 위해서는 다양한 정보보호 서비스가 제공되어야 한다.



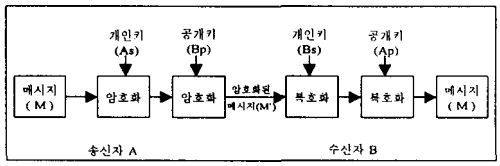
<그림 1> CALS체계의 정보보호구조 모델

네트워크 정보보호 모델은 <그림 2>와 같이 구성되며, 정보보호 서비스를 제공하기 위하여 다양한 메커니즘이 활용되며, 서비스 제공시 필요한 관련 정보들은 정보보호 관리 정보 베이스(SMIB)에서 유지한다. 정보보호 관리 정보 베이스는 암호 알고리즘, 초기벡터, 암호화키 등의 정보를 유지하는데 사용된다.



<그림 2> 네트워크 정보보호 모델

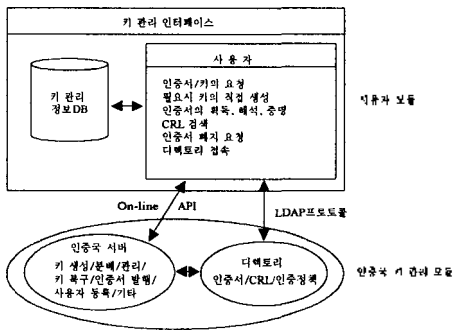
네트워크 정보보호 모델에서는 기밀성, 무결성, 인증, 부인봉쇄 서비스가 제공되어야 한다. CALS 체계에서는 이러한 서비스들은 앞장에서 설명된 정보보호 메커니즘들의 지원하에 제공될 수 있으며 그중 인증 서비스에 대한 예는 아래 <그림 3>과 같다.



<그림 3> 인증 서비스

4.3 인증 및 키관리 모델

인증 및 키관리 모델은 <그림 4>에서와 같이 사용자를 지원하는 사용자 모듈과 각각의 모듈들을 전체적으로 관리하는 인증국 키 관리 모듈로 구분할 수 있으며 다수의 사용자 키를 효과적으로 관리할 수 있어야 한다.



<그림 4> 인증 및 키관리 모델

사용자 모듈은 네트워크 정보보호 관리부에서 정보보호 서비스를 제공하기 위하여 필요한 사용자의 개인키와 공개키를 키관리 인터페이스를 통하여 키 관련 정보를 제공한다[강창구 외, 1997].

사용자 모듈에는 디렉토리 사용자와 키관리 인터페이스, 키관리 정보 데이터베이스가 위치한다. 디렉토리 사용자는 X.500 디렉토리 서버에 접속하여 인증서, 취소목록 등을 조회하는 역할을 하며, 키관리 인터페이스는 수신된 공개키가 정당한가를 확인하기 위하여 네트워크 정보보호 관리부로 키의 정보를 전달하는 역할을 수행하고 키관리 정보 데이터베이스에 키 관련 정보들을 저장함으로써 필요시 접근 가능하도록 구성된다.

인증국 키관리 모듈은 사용자 인터페이스, 키 생성, 키 분배, 키관리 모듈을 포함하고 있으며 모듈별로 기능을 수행한다. 키 생성 모듈은 사용자 개인키 및 공개키를 생성하며 또한 공개키에 대한 인증서를 생성한다. 키관리 모듈은 유효기간이 만료되거나 신뢰성에 문제가 발생한 인증서를 관리하며, 생성된 키, 인증서, 취소목록 등의 분배는 키 분배 모듈이 수행한다. 모든 키의 생성, 관리, 분배 상황은 보안 감사를 위하여 기록되어야 하며 사용자 인터페이스 모듈은 GUI를 통하여 쉽게 사용하도록 구성되어야 한다. 인증국은 사용자의 공개키를 포함한 인증서 관리를 위해 신뢰할수 있는 망을 통하여 온라인으로 인증서를 발급한다. 인증서는 사용자의 개인 식별 정보와 함께 디렉토리에 저장되며 CALS 사용자의 다양한 정보를 보호하기 위하여 X.509 디렉토리 인증 서비스에서 정의된 강한 인증 방법을 사용한다. X.509 디렉토리 인증 서비스는 공개키 암호 시스템에 기반을 두고 있으며 사용자의 공개키는 인증서 형태로 디렉토리에 저장된다[CCITT,1993].

CALS에서 정보보호를 위한 인증 및 키관리 모델은 CALS사용자들이 상호 인증을 효율적으로 하기 위하여 인증국들은 계층구조를 가져야 하며 각 인증국은 상호간 보증하지 않는다. 사용자의 개인키가 노출되거나 사용자의 공개키를 더 이상 인증 할 필요가 없는 경우 인증서들에 대한 취소목록을 만들어 디렉토리에 저장한다.

4.4 운영 및 보안감사 모델

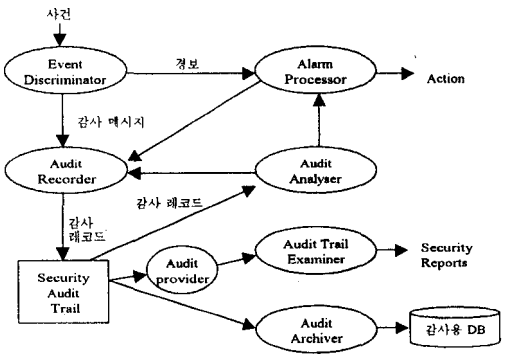
CALS 환경은 정부를 비롯한 기업, 관공서 등을 대상으로 하며 그 범위도 광범위하기 때문에 거래자들 사이에서 정보의 불법적인 유출을 비롯한 불법적인 행위들이 많이 발생할 수 있다. CALS에서는 이러한 문제들을 해결해 줄 수 있는 메커니즘이 요구되며 이를 지원하기 위하여 보안 감사가 제공된다. 보안 감사 정책은 정보보호 관련 사건들을 정의하고 다양한 정보보호 관련 사건의 수집, 기록, 분석에 대한 적용 가능한 규칙들을 식별한다.
보안 감사는 정보보호 정책의 적절성을 평가하고 정보보호를 위반하는 사건을 감지, 기록, 분석뿐만 아니라 자원의 오용에 대한 감지까지도 지원하여야 한다.

<그림 5>의 CALS 운영 및 보안 감사 모델은 ISO/IEC 표준에 따라 여러 단계로 구성하였으며 사건의 감지를 통한 보안 감사 결정은 사건이 정보보호와 관계가 있는지에 따라 결정된다[ISO/IEC, 1996].

보안 감사 절차는 감지단계, 결정단계, 경

보단계, 분석단계, 수집단계, 보고 발생단계, 기록단계로 구분할 수 있으며 이러한 절차들은 시간에 따라 분리된 것이 아니라 중첩되어야 한다.

감지 단계는 정보보호 관련 사건들의 발생을 결정하는 것이다. 사건의 응답으로 발생된 행동은 정보보호 정책에 의해 결정되거나 Event Discriminator에 의해 발생 즉시 경보를 발생시킨다.



<그림 5> 보안감사 모델

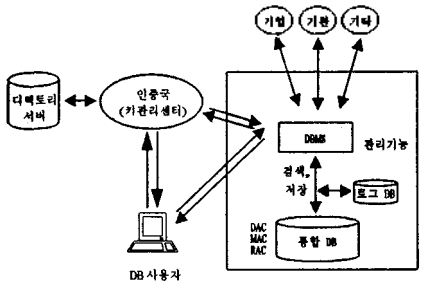
결정 단계는 정보보호 관련 사건이 감지되었을 때 Event Discriminator는 행동의 적절한 초기 과정을 결정한다. 각 사건에 따라 취해진 행동에 대한 결정은 운영상 정보보호 정책에 의존하게 된다. 경보 단계는 Alarm Processor가 행동의 정확한 과정을 결정하기 위하여 경보를 분석한다. 각 사건에 따라 취해진 행동은 운영상 정보보호 정책에 따라 결정된다. 분석 단계는 Alarm Analyser가 정보보호 관련 사건에 따른 행동을 결정하기 위해 사건을 처리·분석하고, 분석시에는 이전의 정보보호 관련 사건들에 대한 정보를 이용한다. 수집 단계는 audit trail collector와 audit dispatcher 기능을 포함한 과정을 수집이라 하는데 분산된 보안 감사 추적으로부터 각각의 보안 감사 레코드들은 주기적으로 단일 감사 추적에 수집된다. 보고 발생 단계는 시스템의 정보보호를 위반하는 행위에 대한 보안 감사 추적을 통하여 보안 보고를 발생하고 위반시 정보보호 회복 행동의 시작을 의미하며 이때 보안 감사 추적 분석은공격의 범위를 평가하고 적절한 손실 제어 절차를 결정하는데 사용된다. 마지막으로 기록 단계는 보안 감사 추적의 긴 주기 동안에 유지되어야 하기 때문에 보안 감사 추적의 일부분이 저장소로 이동하여 저장된다. 기록에 사용된 저장소는 원 레코드와 무결성을 유지해야 한다.

4.5 통합 데이터베이스 정보보호 모델

통합 데이터베이스는 지리적으로 분산되어 있고 이질적인 데이터들을 논리적으로 연결한 정보 저장소(Information Repository)를 가리키는 사용자 관점의 용어로서, 기술 관점에서는 분산 데이터베이스의 한 형태라 할 수 있다. 다만, 종래의 분산 데이터베이스가 지리적으로 분산된 자료들을 단일 데이터베이스 관리체계(DBMS : Database Management System)에 의해 연계시킨 것이었다면 CALS에서 제기된 통합 데이터베이스는 이종의 자료관리 시스템들을 연동시킨 것이라는 점에서 차이가 있다[김덕현 외, 1998]. CALS 체계에서의 통합 데이터베이스는 업무나 제품의 전 공정에서 요구되는 모든 정보들을 저장하고 있는 통합된 개념으로 대부분 유용한 정보들이 저장되어 있기 때문에 많은 위협들이 존재할 수 있으며

정당한 사용자들에게 요청된 통합 정보를 안전하게 제공하기 위하여 여러 정보보호 메커니즘을 이용한 정보보호가 요구된다.

통합 데이터베이스의 정보보호를 위하여 제공될 수 있는 메커니즘으로는 인증 메커니즘, 접근제어 메커니즘, 암호 알고리즘, 보안 감사 등이 활용될 수 있으며 통합 데이터베이스의 정보보호 모델은 <그림 6>과 같다.



<그림 6> 통합 데이터베이스 정보보호모델

통합 데이터베이스로부터 서비스를 받기 위한 접근 절차는 다음과 같다.

첫째, 임의의 사용자가 통합 데이터베이스 서버로부터 원하는 서비스를 제공받기 위하여 인증 및 키관리 모델로부터 신분을 확인 받고 정당한 사용자인지를 확인한다.

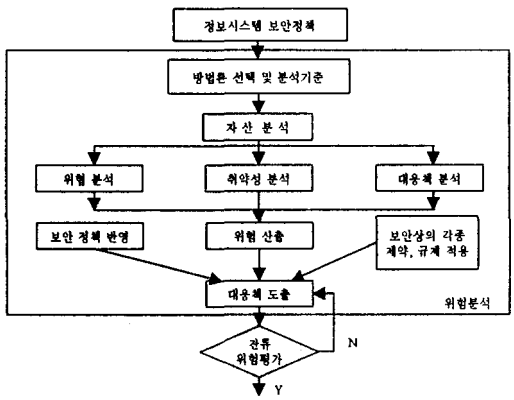
둘째, 사용자 인증을 마친 후에 통합 데이터베이스에 있는 객체에 접근하기 위해서는 다시 데이터베이스 관리 시스템에 의해 접근 제어를 받게 된다. 이러한 접근 제어로는 임의적 접근제어(DAC), 강제적 접근제어(MAC), 역할 기반 접근제어(RAC) 등이 있다.

셋째, 통합 데이터베이스의 정보보호를 위한 다른 기법으로는 통합 데이터베이스에 접근하여 데이터를 저장하거나 검색된 데이터를 전송할 때 암호화 기술을 사용하여 데이터의 기밀성을 제공할 수 있다. 통합 데이터베이스의 정보를 암호화하여 저장하고 암호화된 상태로 전송하므로 데이터를 보다 안전하게 유지할 수 있다.

넷째, 데이터의 저장, 변경, 검색 등에 대한 사항을 로그 파일에 기록·저장하여 유지함으로써 정보보호 문제 발생시 보안 감사의 자료로 제공될 수 있다.

4.6 위험분석 모델

위험분석 모델의 목적은 대상 조직의 정보시스템을 비롯하여 이와 관련된 모든 자산의 전반적인 위험 수준을 측정하여 비용 효과적인 측면에서 최선의 대응책을 제시하는 것이다. 세계적으로 여러 위험분석 방법론이 있으나 여기에서는 <그림 7>과 같은 국내 표준으로 제정된 위험분석 모델을 바탕으로 위험분석을 실시할 수 있다[이병만 외, 1998].



<그림 7> 위험 분석 모델

위험분석 모델의 위험분석 절차는 다음과 같다. 첫째, 정보 시스템 보안 정책에서 요구하는 보안 수준을 파악하여 분석기준을 만들고 요구 수준에 따라 적절한 위험분석 방법론을 선택해야 한다. 둘째, 방법론과 분석기준이 마련되면 자산분석을 수행해야 한다. 자산분석은 위험분석 대상 정보시스템과 관련 있는 모든 자산을 조사하고 이들 자산들의 가치를 산정하는 과정이다. 자산 분석 방법은 화폐가치를 이용한 정량적 분석방법과 기술변수 등으로 나타내는 정성적 방법이 있다. 셋째, 위협분석으로 조직 내에서 발생했거나 앞으로 발생할 가능성이 있는 위협을 조사하고 이들 위협이 자산에 미칠 영향을 분석한다. 넷째, 취약성 분석으로 특정 취약성에 대하여 어떠한 위협이 존재하는지를 조사한다. 다섯째, 대응책 분석으로 운영중인 대응책들을 파악하고 이들 대응책들이 기본기능을 적절히 수행하고 있는지를 파악해야 한다. 여섯째, 위험 산출은 정보시스템 관련 자산이 노출되어 있는 위험을 파악하고 알맞은 대응책 도출을 돕기 위한 것이다. 위험산출 단계에서는 이미 분석된 결과를 바탕으로 위험수준을 결정하게 된다. 일곱째, 대응책 도출 단계로 위험수준을 적정수준으로 낮추기 위하여 필요한 대응책들을 조사하고 도출하는 단계이다. 여덟째, 잔류위험 평가로서 잔류 위험을 평가하여 위험수준이 받아들일 수 있는지 여부를 검증하는 단계이다.

5. 결 론

CALS는 미 국방성에서 최초 "무기체계 획득에 대한 군수지원 전산화"개념으로 출발하여 현재는 "광속의 상거래"와 전자상거래(EC)를 의미하는 CALS/EC로 확대하여 사용되고 있으며, 그 적용 범위가 급격히 증가하고 있다.

이러한 CALS는 통합 데이터베이스를 통한 정보 공유와 네트워크에서의 데이터 교환을 기본 개념으로 하고 있기 때문에 유통·저장된 정보보호가 매우 중요한 선결과제로 인식되고 있다.

본 논문에서는 현재 CALS 체계에서 발생하기 쉬운 정보보호 위협요소와 CALS 정보보호 서비스, 메커니즘 등을 통하여 정보보호의 기본적인 개념과 정보보호 기술동향을 분석하고 안전한 CALS체계 구축을 위한 정보보호 구조 모델을 제시하였다.

제안된 CALS 정보보호 구조 모델은 개념적인 모델로서 각 응용별로 개발된 정보보호 기술들을 통합하여 CALS 환경에 적용 가능한 통합 정보보호 기술로 모델화 하였다. 이러한 모델은 CALS체계에서의 정보를 안전하게 보호하는데 도움이 될 것이라 생각하고 제시된 모델을 토대로 상세 설계 및 구현을 위한 더 많은 연구가 수행되어야 할 것이다.

참고문헌

[강창구, 1997] 강창구 외 2명, "디렉토리 모델과 정보보호서비스," 한국통신정보보호 학회지, Vol.7 No.2, 1997.6.

[국방부, 1997] 국방부, 국방 CALS 종합 계획서, 국방부, 1997.

[김덕현 외, 1998] 김덕현 외 5명, 무기체계 통합 DB 기본 설계, 국방 과학 연구소, 1998.6.

[김철환, 1995] 김철환 외 1명, 21세기의 정보화 산업혁명 CALS, 문원, 1995.9.

[신종태, 1997] 신종태 외 3명, "CALS 체제 정보보호 프레임워크," 한국통신정보보호 학회지, Vol.7 No.3, 1997.9.

[이병만 외, 1998] 이병만 외 2명, 정보시스템 위험분석 모델 에 관한 연구, 한국전산원, 1998.

[최용락 외, 1998] 최용락 외 5명, CALS/EC 정보보호 기술 표준화에 관한 연구, 한국정보보호센터, 1998. 6.

[CCITT, 1993] CCITT Recommendation X.509, The Directory-Authentication Framework, 1993

[ISO/IEC, 1996] ISO/IEC 10181-7, "Security audit and alarms framework ," 1996.9.

저 자 소 개

남길현(khnam@kndu.ac.kr)

육군사관학교(이학사)
서울대학교 공과대학(공학사)
미해군 대학원(전산학 석사)
미 위스콘신주립대(전산학 석사)
미 남서루이지아나 주립대(전산학 박사)
관심분야 : 암호학, 정보보호체계, 데이터베이스 시스템, 알고리즘