通信情報保護學會論文誌
第 8 卷 第 2 號, 1998. 6

CALS 정보보호 모델설계와 적정성 분석

신 종 태*, 이 정 현***, 이 대 기***, 소 우 영**,

Design of CALS Security Model and Its Suitability Analysis

Jong-Tae Shin*, Jeong-Hyun Yi***, Dai-Ki Lee*** , Woo-Young Soh**

요 약

CALS체제의 구축에 있어 역기능으로 인한 여러 가지 문제가 대두되고 있다. 본 논문에서는 CALS 정보보호 위협 요소를 비롯한 정보보호 서비스와 메커니즘을 분석하고 CALS를 안전하게 구축하기 위한 정보보호 모델과 시뮬레이션 단계를 예시하였다. CALS 체제의 위협 요소, 보안 목적, 구현 가정 요소, 지원 보안 메커니즘을 설정하여 제안된 CALS 정보보호 모델은 4개의 서브 모델인 전송모델, 키 관리 모델, 감사 모델, 통합 데이터베이스 연계 모델로 구성하였으며 구현을 위한 모듈로 보안 관리부, 디렉토리 서비스 에이전트와 인증국을 포함하는 키관리부, 분산 환경에서의 보안 감사부, 통합 데이터베이스 관리부로 나누어 제시하였다.

Abstract

The problems of CALS system are recognized by constructing CALS system. This Paper proposed secure CALS system that information security model and simulation by analyzed the security services, mechanisms and threats against CALS system. The CALS security model consists of sub-model that key management model, audit model, intergrated database model. We proposed model is cornposed of four parts : Security management part including directory service agent and certification agency, security audit part with open system, part.

1. 서 론

최근 정보 통신 기술의 발달로 인하여 시·공을 초월한 국제 경쟁 시대로 접어들게 되었고 각 기업들을 비롯한 국가들은 제품에 대한 생산으로부터 유지보수까지 전 공정에서 경쟁력 확보의 한 방안으로 CALS를 도입하고 있는 추세다. CALS는 제품의 설계를 비롯한 개

*한국정보보호센터
**한남대학교 컴퓨터 공학과
***한국전자통신 연구원

발, 생산, 판매, 유지 보수, 폐기등 전 공정에 걸쳐 기업간에 표준화된 디지털 자료를 공유하고 교환함으로써 기업의 업무 프로세스 방식을 재구성하여 생산력 향상을 포함한 비용 절감과 품질 향상의 효과를 얻기 위한 개념으로 이해된다[1].

CALS는 1985년 미국 국방부에서 군수관리의 효율화를 위해 시작되었고 현재는 광속의 상거래라는 개념으로 통용되고 있다. 현재 미국은 정부를 중심으로, 일본은 민간부문을 중심으로, 그리고 유럽은 국가별로 진행하면서도 유럽공동체(EU)가 중심이 되어 추진 중에 있다[1]. 국내에서도 CALS의 중요성을 인식하여 산 학 연 관을 중심으로 CALS 구축을 위하여 노력하고 있다. 그러나, CALS 구축에 다양한 문제점들이 있다. 첫째, 한 기업의 모든 정보를 디지털화 하는데 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 발전에 비하여 전자문서 교환도 미진한 실정이며 CALS구축 기술과 경험이 부족한 상황이다. 다섯째, 정보보호 문제로서 기업간 교환 정보와 통합 데이터베이스 정보를 포함한 CALS체제를 내·외부로부터 안전하게 보호하는 것이 심각한 문제로 대두되고 있다. 본 논문에서는 CALS의 정보보호를 위해서 CALS 위협요소와 필요한 정보보호 서비스 및 메커니즘을 분석하여 CALS의 정보보호 모델을 제안하고자 한다. 2장에서는 CALS 정보보호 위협 요소를 비롯한 정보보호 서비스와 메커니즘을 분석한다.

3장에서는 CALS를 안전하게 구축하기 위한 정보보호 모델을 제시하고 모델설정의 적정성을 분석하며, 4장에서는 제안된 모델에서 정보의 흐름에 따라 정보보호가 이루어짐을 단순화된 가상실험을 통하여 보이고, 5장에서 결론을 맺는다.

2. CALS에서의 정보보호 환경 분석

CALS는 그 핵심요소를 EDI와 통합 데이터베이스를 포함하며 정보 교환과 공유 시에 다양한 위협요소가 존재할 수 있다. CALS는 EDI와 통합 데이터베이스를 통하여 기업간 또는 기업내 디지털 정보들이 교환 또는 공유되기 때문에 EDI의 확장된 개념으로 볼 수 있다[2]. 안전한 CALS 구축을 위하여 기밀성을 비롯한 무결성, 인증, 부인봉쇄 서비스가 요구되며 이들 서비스를 제공하기 위하여 다양한 정보보호 메커니즘들이 필요하다[3].

본 장에서는 정형화된 CALS의 위협요소, 서비스 및 메커니즘을 분석한다.

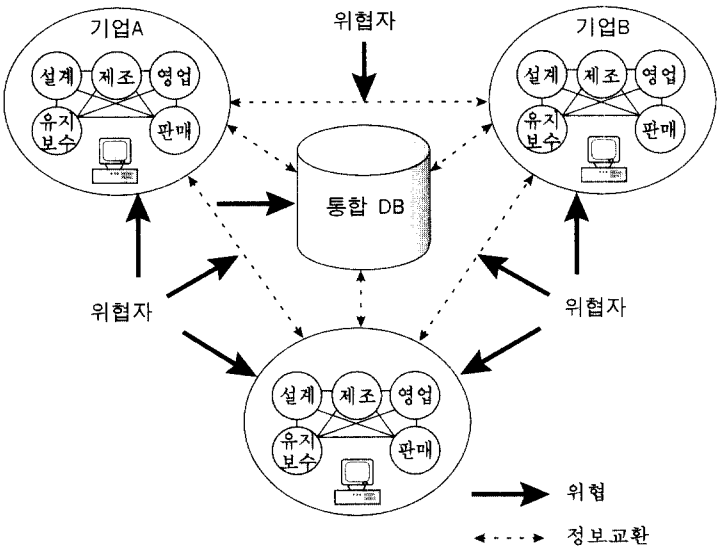
2.1 CALS 위협요소 분석

CALS체제의 기업내·외의 정보 흐름은 〈그림 1〉과 같이 나타낼 수 있다. CALS에서 교환되는 정보는 매뉴얼, 설계도, 보고서, 계약서, 및 수·발주서류 등을 포함하며, 통합 데이터베이스에 의해서 관리 및 공유하게 된다. 따라서, CALS에서는 EDI의 단순한 메시지 교환에서 일어나는 위협과 함께 통합 데이터베이스에 위협이 존재하기 때문에 정보보호의 대상 및 위협요소가 확장된다[5, 6].

CALS에서의 위협요소는 다양한 형태로 나타날 수 있으나 대부분은 정보 교환시 발생한다. 정보는 통합 데이터베이스화하여 구축 이용되며, 사용자는 정보를 송신하고 송신된 메시지는 네트워크를 통하여 다른 기업에 전달된다. 전달간 메시지는 도청, 위조, 불법 수정, 및 방해 등의 위협을 받을 수 있다[7].

정보보호 위협요소는 EDI와 CALS에서 전송간에 거의 동일하게 존재하나, CALS에서는 통합 데이터베이스로 인하여 이에 대한 위협

요소도 존재한다. 통합 데이터베이스에 권한 없는 기업이 권한 있는 기업으로 위장해서 정보를 요청할 수 있으며, 요청된 정보가 통합 데이터베이스로부터 전송될 때 네트워크 상에서 위조, 변조, 도청 등의 위협요소들이 존재한다. 또한 내부자에 의한 정보 노출 및 자연적인 재앙, 시스템 장애 등이 발생될 수 있다[3, 4].



〈그림 1〉 CALS 위협 환경

2.2 CALS 정보보호 서비스 분석

CALS의 위협요소를 해결하기 위해서는 각 위협요소별로 사용되고 있는 정보보호 서비스들이 통합적으로 제공되어야 한다. 네트워크 상에서 메시지의 도청, 위조, 변조 등의 위협요소로부터 안전한 메시지 전송을 위하여 기밀성 서비스, 무결성 서비스가 제공되어야 하며, 이들 서비스는 EDI에서도 제공되나, 그 목적과 강도에 있어 CALS에서와 차이가 있다. 이러한 차이의 주된 요인 중 하나는 통합 데이터 베이스에 대한 정보보호 서비스로부터 비롯된다. CALS의 통합 데이터베이스는 정보를 검색 및 저장하고, 메시지를 송·수신하는 데 있어서 많은 위협요소들이 존재하며, 또한 정보에 접근하는 사용자에 대하여 접근 권한이 있는 정보만을 제공할 수 있게 해주는 접근제어 서비스의 개념이 더욱 중요시된다.

2.3 정보보호 메커니즘 분석

본 연구에서는 정보보호 서비스를 기밀성, 무결성, 인증, 부인봉쇄, 접근제어 서비스에 대하여 CALS체제의 정보보호 메커니즘을 분석하여 CALS 정보보호 모델을 제안하였다. 제안된 CALS 모델에서의 정보보호 메커니즘과 서비스와의 관계는 다음과 같다. 키관리 메커니즘은 기밀성, 무결성, 인증, 부인봉쇄서비스를 지원하며, 암호화 메커니즘은 기밀성, 인증 서비스를 지원한다. 해쉬함수는 무결성, 인증 서비스를 지원한다. 인증 메커니즘은 무결성, 인증 서비스를 지원한다. 디지털 서명은 무결성,

부인봉쇄 서비스를 지원한다. 접근제어 메커니즘은 통합 데이타베이스의 접근제어 서비스를 지원한다. 감사추적 메커니즘은 부인봉쇄 서비스를 지원한다. EDI의 부인봉쇄 서비스는 디지털 서명과 감사추적 메커니즘에 이루어지며, CALS에서는 디지털 서명과 감사추적 메커니즘과 별도의 키 관리 메커니즘을 이용하여 이루어지기 때문에 강력한 부인봉쇄 서비스를 지원할 수 있다. 또한 EDI의 접근제어 서비스는 레이블링을 하기 위하여 제공되나, CALS의 접근제어 서비스는 통합 데이터베이스의 기밀성, 무결성을 해결할 수 있는 접근제어 메커니즘이 지원된다[4].

3. CALS 정보보호 모델

3.1 CALS 정보보호 모델 환경

CALS에서는 모든 정보가 통합적으로 운용되기 때문에 기존 EDI 정보보호에 추가되는 정보보호 요소들이있으며, EDI에서 선택적으로 제공되는 부인 봉쇄, 통합 데이터 베이스 운용상의 정보보호 요소 등이 있다.

CALS에서의 부인봉쇄는 제공되지 않을 시 제품 생산 및 판매, 유지보수에 이르는 전 공정에 영향을 미칠 수 있기 때문에 철저하게 제공되어져야 한다. 그리고 통합 데이터베이스는 정보를 검색 및 저장하고 메시지를 송·수신하는데 있어서 많은 위협요소들이 존재한다[2]. EDI에서의 정보는 전송후의 인증을 위한 저장 개념이지만 CALS에서는 정보는 운용에 영향을 미치는 저장 개념이기 때문에 통합 데이터베이스의 정보보호는 중요하다.

3.2 정보보호 목적, 위협요소, 가정

본 논문에서는 안전한 CALS 환경을 위한 정보보호 모델을 제시하였다. CALS 정보보호를 위한 보안 목적, 위협, 및 운용 가정 등을 설정한 뒤 모델을 제안하며 모델별로 각 보안 메커니즘을 제안하였다. 이들의 상관관계를 표로 작성하였다. 또한 정보보호 모델의 시뮬레이션을 통하여 적정성을 검증하였다. CALS 체제에서의 보안 목적을 다음과 같이 설정한다.

보안목적 1 (O1) : 접근통제 규칙을 통해 CALS 정보의 흐름을 제어한다.

보안목적 2 (O2) : 사용자의 식별 및 인증 기법을 통해 허가되지 않은 접근을 막는다.

보안목적 3 (O3) : 정보 접근에 대한 기록을 유지한다.

보안목적 4 (O4) : 전송되는 정보의 불법적인 변경을 막는다.

보안목적 5 (O5) : 시스템 보안 관련 정보의 불법적인 변경을 막는다.

보안목적 6 (O6) : 보안 관련 데이터는 권한을 가진 관리자에 의해서만 변경하게 한다.

보안목적 7 (O7) : 기업 고유 업무의 정보보호 서비스를 보존한다.

CALS 체제에서 발생되는 정보보호 대상이 되는 위협요소를 정보, 전송간 발생 위협, 시스템 관리시 발생하는 위협, 통합 데이터베이스에 존재하는 위협 등으로 나누어 분석하였다.

정보의 전송간에 발생할 수 있는 위협은 다음과 같다.

위협 1 (T1) : 정보의 흐름을 고의로 지연시키거나 순서를 변조하는 행위

위협 2 (T2) : 전송로 상에서 정보가 변경

(변조)되는 사건

위협 3 (T3) : 전송간에 사용자 식별 정보가 노출되는 사건

위협 4 (T4) : 정보의 송·수신 사실을 부인하는 행위

시스템 관리시 발생하는 위협은 다음과 같다.

위협 5 (T5) : 권한 없는 자가 네트워크 정보를 이용하여 정당 사용자로 가장하는 행위

위협 6 (T6) : 기업내의 사용자중 권한 없는 자가 시스템 관리자 영역에 접근하여 정보를 변경하는 행위 (보안 관련 정보의 변경 행위 포함)

위협 7 (T7) : 자기 고유 업무외에 허가되지 않은 업무 영역에 접근하는 행위.

위협 8 (T8) : 기업 내부 사용자가 외부의 사용자에게 불법적으로 정보를 제공하는 행위

통합 데이터베이스에 존재하는 위협은 다음과 같다.

위협 9 (T9) : 저장되어 있는 정보의 기밀성을 저해하는 행위

위협 10 (T10) : 정보의 실시간 접근에 따른 무결성을 유지하는 문제

위협 11 (T11) : 감사기록 데이터가 손실되는 사건

위협 12 (T12) : 감사기록 데이터의 분석을 지연시키는 행위

위협 13 (T13) : CALS체제의 특정 기억장소를 소진하는 행위

위와 같은 위협요소를 만족시킬 수 있는 CALS체제의 각 서비스별 모델을 제시하기 위하여 본 연구에서 는 다음과 같은 가정조건을 설정하였다.

가정조건 1 (A1) : 사용자가 소속된 전산망과 공중망의 정보 흐름은 단일 통로이다.

시스템 운용시 시스템의 보안관리자는 운용되고 있는 정보관리를 책임 지고 있다. 따라서 주어지는 권한 또한 크다고 할 수 있다. 보안관리자의 정보 오남용은 막을 수 없으므로 다음과 같은 가정조건이 필요하다.

가정조건 2 (A2) : 각 기업의 보안 관리자는 권한을 악용하지 않으며 신뢰된다.

시스템 운용시 시스템의 보안관리자가 운용시스템의 보안 등급을 두어 관리하며 사용자들에게도 시스템의 접근권한을 부여한다. 따라서 주어지는 권한 밖의 행위는 행사할 수 없으며, 해당 보안 관리 영역은 해당 보안관리자만이 접근할 수 있어야 한다. 따라서 다음과 같은 가정조건 3이 필요하다.

가정조건 3 (A3) : 각 기업 보안서버의 보안 관리 영역 접근은 해당 관리자만이 가능하다.

키 관리는 다른 정보와는 별개로 오프라인 상태에서 관리할 수 있어야 한다. 허가되지 않은 자외에는 키의 접근이 허용되어서는 안된다. 따라서 다음과 같은 가정조건이 필요하다.

가정조건 4 (A4) : 마스터 키는 물리적으로 안전하며 권한이 있는 자만이 접근이 가능하다.

3.3 CALS 정보보호 모델 설계

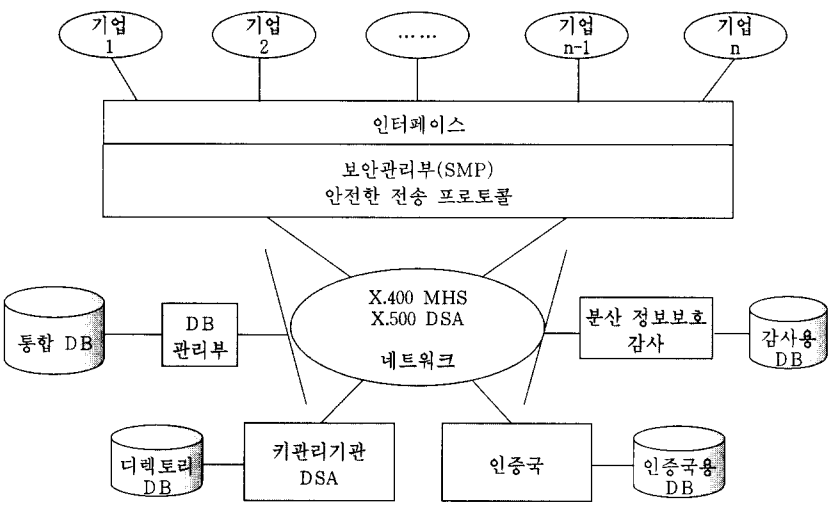
3.3.1 CALS 정보보호 모델 구조

CALS 체제는 위에서 제시한 보안 목적, 위협, 및 운용 가정요소를 바탕으로 정보에 대한 위협요소들로부터 정보를 보호하고 원활하고 효율적인 CALS 운영을 위하여 정보보호 모델이 요구된다. CALS 정보보호 모델은 CALS에서 요구되는 정보보호 서비스를 지원하며, 다양한 정보보호 메커니즘/알고리듬이 활용된다. 그러므로 안전한 CALS를 위한 개념적 정보보호 모델은 기능에 따라 〈그림 2〉와 같은 구조로 전송 모델, 키관리 모델, 보안 감사 모델, 통합 데이터베이스 연계 모델 등 4개의 서브 모델로 분리하여 구성할 수 있다.

CALS 정보보호 모델을 구현하기 위해 기존의 전송 환경에 부가하는 보안 환경으로 크게 보안 관리부, 인증국 및 키관리 기관, 디렉토리 서비스 에이전트, 통합 데이터베이스 관리부, 보안 감사(Security Audit)를 설계하여야 한다.

보안 관리부는 〈그림 3〉과 같이 구성되고 CALS 체제의 어느 한 시스템이라도 보안 관리부의 부재시에는 취약 부분이 생길 수 있으므로 모든 시스템에 제공되어야 하며 정보보호 서비스에 대한 처리 기능을 제공한다. 상위 레벨에는 정보보호 서비스를 위한 보안 관리 정보 베이스(SMIB)가 위치하게 되며 다양한 메커니즘과 연계 하에 정보보호 서비스를 제공한다. 하위 레벨에는 보안 감사, 키 관리, 데이터베이스 관리 모듈들과 각각의 인터페이스로 구성된다.

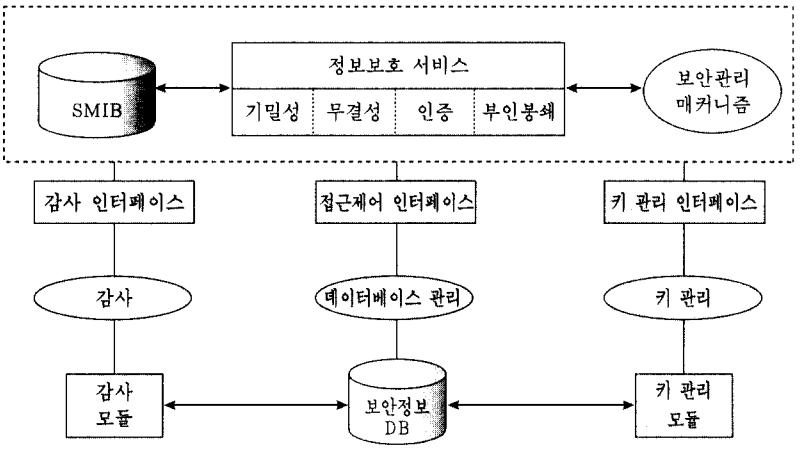
보안 감사 모듈은 정보보호 서비스를 처리하는 과정에서 발생하는 정보보호 관련 행위들을 감사 추적하기 때문에 CALS에서는 보안 감사 기능이 요구되며 데이터베이스 인터페이스를 이용하여 데이터베이스로부터 감사 자료를 이용하여 감사추적에 사용한다.



〈그림 2〉 안전한 CALS 정보보호 모델 구조

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 데이터베이스

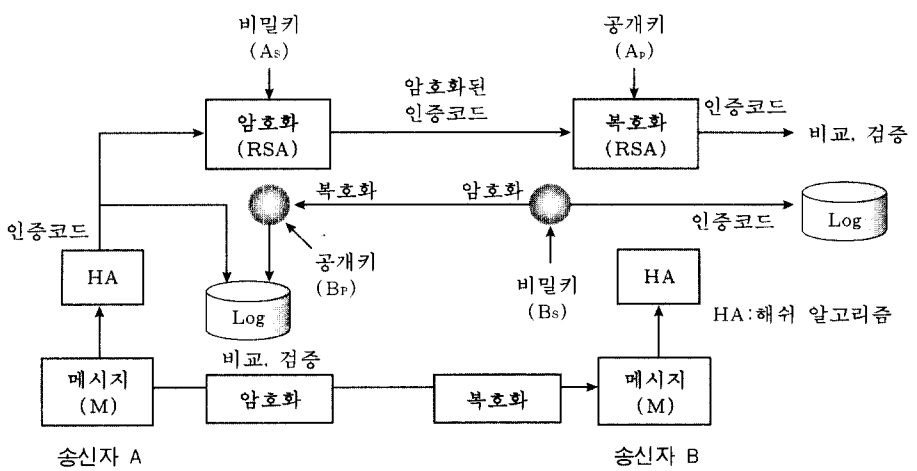
를 이용하여 키와 관련된 정보의 검색, 저장, 변경 등을 수행하게 된다. 데이터베이스 관리 모듈은 키 관리와 보안 감사를 수행하는데 필요한 정보들을 저장하고 요청에 대한 서비스를 제공한다.



〈그림 3〉 보안 관리부 내부 구조

인증국 및 키관리 기관은 키와 관련된 생성 및 분배, 인증서 발급 등을 수행하며 키 관련 정보들을 저장, 검색, 변경의 기능까지도 요구된다 [8]. 기업들의 디렉토리 서비스 에이전트(DSA)에는 CALS 사용자들에 대한 정보들을 저장하고 있으며 서비스 요청시에 실시간으로 수행하며 디렉토리 사용자에 대한 인증기능도 제공한다.

통합 데이터베이스 관리부는 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 4〉 CALS 전송 정보보호 환경

3.3.2 전송 모델

CALS의 메시지들은 외부 노출시 피해를 입을 수 있기 때문에 송신자가 수신자 사이에는 안전한 메시지전송이 요구된다. 이를 위해 다양한 정보보호 서비스 제공하에 전송하게 되는데 전송 모델에서는 기밀성, 무결성, 인증, 부인봉쇄 서비스가 제공되어야 하며 CALS 전송 정보보호 환경에서는 〈그림 4〉와 같은 정보보호 메커니즘들의 지원이 요구된다.

보안 메커니즘 1 (M1) : 송신자가 데이터를 노출시키지 않고 수신자에게 전송하기 위한 기밀성 메커니즘

보안 메커니즘 2 (M2) : 수신자에게 전송된 데이터가 아무런 변화없이 전송되었다는 무결성 커니즘

보안 메커니즘 3 (M3) : 데이터 송신자가 정당한 사용자라는 것을 식별하기 위한 인증 메커니즘

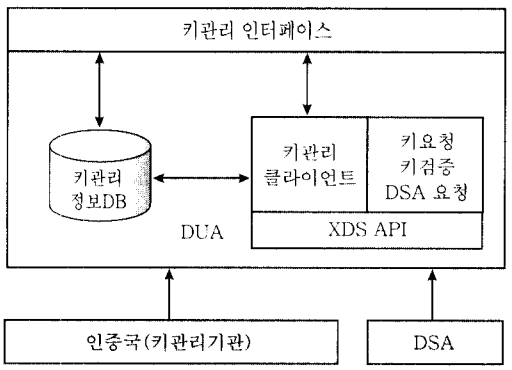
보안 메커니즘 4 (M4) : 송신자와 수신자의 데이터 송·수신에 대한 부인을 봉쇄하기 위한 부인 봉쇄 메커니즘

3.3.3 키 관리 모델

키 관리에서는 사용자 비밀키를 당사자만이 알아야 하며 정보보호를 위하여 키의 생성에서 폐기까지 보호가 절실히 요구된다[8]. 키는 인증국으로부터 생성되며 인증국은 키의 관리를 위하여 인증서를 생성하여 오프 라인으로 발행하게 된다. 인증서에는 유효기간과 관련된 기한이 포함되어야 하고 인증서의 재사용을 위하여 인증국은 만기된 인증서를 대체하는 인증서 교체를 정확히 제공해야 한다. 그리고 유효기간이 지난 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, 신원 정보의 인증을 위한 검증 및 디렉토리 서버에 접속 등을 포함한 기능을 수행하고 인증국 키 관리 모듈은 사용자 인터페이스, 키 생성, 키 분배, 키 파기 기능을 수행한다.

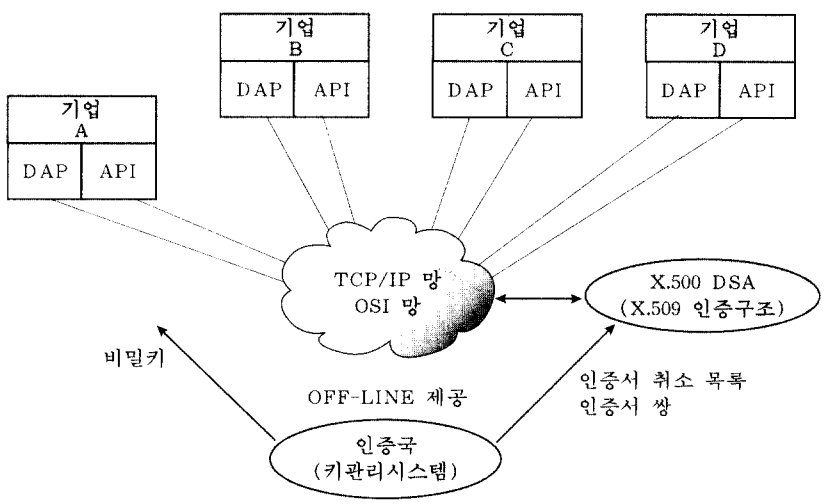
보안 메커니즘 5 (M5) : 사용자 키 관리와 인증 관련 키 관리를 위해 인터페이스를 통하여처리되는 키의 요청, 생성, 분배, 파기 등을 수행하는 키 관리 메커니즘.

사용자 키 관리 모듈은 〈그림 5〉와 같이 디렉토리 사용자 에이전트와 키 관리 인터페이스로 구성되며 인증국 및 DSA가 요구된다[5, 9]. 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 5〉 CALS 키관리 모듈

인증국 키관리 모듈은 사용자 인터페이스, 키 생성, 키 분배, 키 관리 모듈별로 기능을 수행한다. 사용자의 공개키가 포함된 인증서는 디렉토리의 서비스 에이전트와 완전히 분리된 오프 라인으로 인증국에 의해서 생성되며 사용자의 개인 식별 정보와 함께 디렉토리에 저장된다[4]. 사용자의 디렉토리 인증을 위하여 X.509 디렉토리 인증 서비스가 사용되고 비밀키는 그 사용자에게 전달하고 공개키는 인증서 형태로 디렉토리에 저장한다[10]. 사용자의 비밀키가 노출되거나 사용자의 공개키를 더 이상 인증할 필요가 없는 경우 그러한 인증서들에 대한 취소목록을 만들어 디렉토리에 저장하는 기능까지도 수행하며 〈그림 6〉은 인증국으로부터 생성된 비밀키와 인증서의 분배를 나타낸 것이다.



〈그림 6〉 인증국의 키 분배 모듈

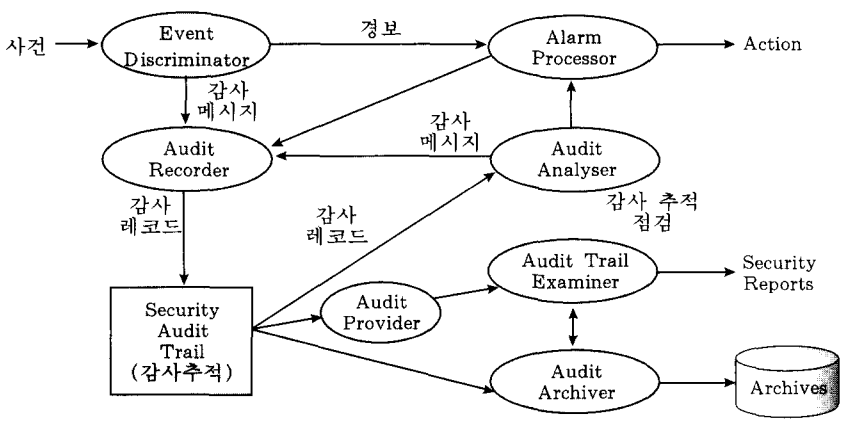
3.3.4 보안 감사 모델

보안 감사 모델은 부인 봉쇄를 위해 사용되는 모델로써 정보의 불법 유출을 방지, 불법적인 행위를 추적하기 위한 것으로 정보보호 관련 행위들을 기록하여 조사 및 분석하는 것이다. 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[11]. 보안 감사에 필요한 정보는 보안 감사 메시지, 보안 감사 레코드, 정보보호 경보, 정보보호 보고등이 사용된다.

보안 메커니즘 6 (M6) : 불법적인 행위 추적을 위해 정보보호 관련 행위를 기록하고 조사하며 분석하는 보안 감사 메커니즘.

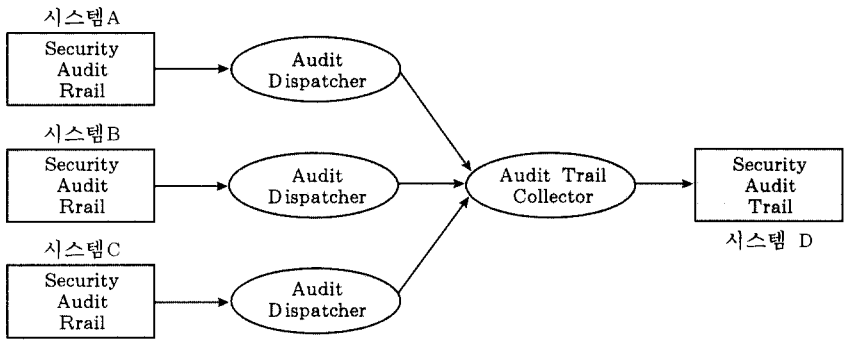
보안 감사 모델은 여러 개의 프로세스로 구성되며 감사 절차는 감지 단계, 결정 단계, 경보 절차 단계, 분석 단계, 수집 단계, 보고 발생 단계, 기록 단계별로 수행되며 〈그림 7〉과 같다.

각 프로세스의 기능은 사건식별자가 보안 감사 메시지 또는 정보보호 경보 메시지를 생성하여야 하는지를 결정하기 위해서 사건을 초기 분석한다. 보안 감사 메시지들은 양식화되어 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.



〈그림 7〉 보안 감사 모델 구조

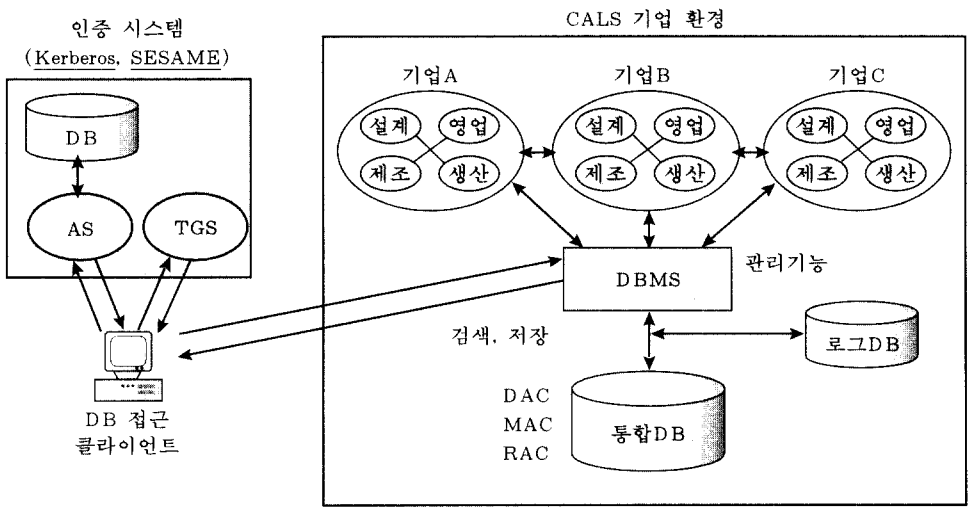
감사추적 수집자는 감사 송부자로부터 감사 메시지를 수집하여 보안 감사가 수행되어야 하며 감사 기록자를 지원해야 하며 〈그림 8〉과 같다.



〈그림 8〉 분산된 감사 추적 구조

3.3.5 통합 데이터베이스 정보보호 연계 모델

CALS에서의 통합 데이터베이스는 정보 저장 및 수정시 발생하는 위협, 접근제어, 및 관리적인 위협 등이 존재할 수 있으므로 다양한 정보보호 메커니즘을 이용한 정보보호가 절실히 요구된다[2]. 본 연구에서 제안한 통합 데이터베이스가 연계된 정보보호 모델은 〈그림 9〉와 같으며 인증 메커니즘, 접근통제, 암호화 기술, 감사가 제공된다.



〈그림 9〉 통합 데이터베이스 정보보호 연계 모델

통합 데이터베이스에 클라이언트들의 임의 접근시 권한 없는 클라이언트가 접근할 수 있

으므로 접근하려는 클라이언트가 정당한지를 확인할 필요가 있으며 인증 절차로 Kerberos 또는 SESAME 인증 시스템을 이용하여 신분을 확인한다. 또한 권한이 부여되지 않은 사용자에게 데이터베이스에 저장된 정보를 노출시키지 않기 위한 방법으로 접근제어를 실시한다. 접근 제어에는 임의적 접근통제(DAC : Discretionary Access Control), 강제적 접근통제(MAC : Mandatory Access Control), 역할기반 접근통제(RAC : Role-based Access Control) 등이 있다.

보안 메커니즘 7 (M7) : 비권한 사용자에게 정보의 접근을 제한하는 접근통제 메커니즘

본 연구에서는 통합 데이터베이스에서 데이터 저장 또는 검색된 데이터를 전송할 때 암호화 기술을 사용하여 데이터의 기밀성을 제공할 수 있도록 연계 모델을 제시하였다. 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.

3.3.5 통합적 보안 관리

CALS체제는 각 정보보호 모듈이 통합적으로 관리하는 환경이 제공되어야 한다. 각 기업에서 시스템을 관리하는 자에게 부여되는 관리자 환경이 CALS체제로 확장되어 적용되어야 하기 때문에 접근 통제를 위하여 적용되는 규칙을 설정하고 변경하는 업무, CALS체제의 공통적 감사기록 대상사건을 설정하고 변경하는 업무, 공통적 감사기록 파일을 관리하는 업무등을 비롯한 보안 관리 기능을 수행하는 메커니즘이 요구된다.

보안 메커니즘 8 (M8) : CALS 체제에서 요구되는 공통적 보안 지원 방법을 관리하고 접근 규칙을 관리하는 보안 관리 메커니즘.

3.4 모델 설정의 적절성 분석

위에서 제시한 모델의 적절성을 검증하기 위해 CALS 체제에서 발생 가능한 위협요소와 제안 모델을 바탕으로 시스템 설계를 위한 보안 목적, 가정 조건, 메커니즘과의 연관관계를 도출하여 모든 위협에 대한 대응 방법을 제시할 수 있음을 보이고자 한다.

〈표 1〉 CALS체제의 보안 목적과 보안 메커니즘과의 관계

	O1	O2	O3	O4	O5	O6	O7
M1				◎	O		O
M2				O	O		O
M3	O	O		O		O	O

M4						○	○
M5		○		◎			○
M6			◎			○	
M7	◎					○	
M8	○		○			○	○

◎ : 아주 밀접한 연관성, ○: 일반적인 연관성

〈표 1〉과 〈표 2〉에서는 CALS체제의 정보보호 모델에 따라 안전성 설계를 위해 설정한 보안 목적이 요구되는 보안 메커니즘과의 연관 관계에 의해 충분히 만족됨으로 CALS 환경의 모든 위협요소가 적정하게 설계될 수 있으며 〈표 3〉에서는 앞에서 제시한 네 가지 가정조건과 보안 메커니즘의 조합으로 기본적으로 설정한 위협요소에 대한 대응 방법을 제시할 수 있다.

〈표 2〉 CALS 체제의 위협 요소와 보안 메커니즘과의 관계

	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13
M1	○	○	○		○		○		○	○		○	
M2		○			○		○		○	○	○		
M3			○		○	○	○						
M4				○									
M5		○	○		○		○					○	
M6	○			○	○	○		○	○	○			
M7						○		○	○	○	○	○	
M8	○			○								○	○

〈표 3〉 보안 위협과 대응책

위 협		대 응 책
T1	정보의 흐름을 고의로 지연시키거나 순서를 변조하는 행위	M1, M6, M8, A1
T2	전송로 상에서 정보가 변경(변조)되는 사건	M1, M2, M5, A41
T3	전송간에 사용자 식별 정보가 노출되는 사건	M1, M3, M5, A11
T4	정보의 송·수신 사실을 부인하는 행위	M4, M6, M8, A4
T5	권한 없는 자가 네트워크 정보를 이용하여 정당 사용자 로 가장하는 행위	M1, M2, M3, M5, M6, A1

T6	기업내의 사용자중 권한 없는 자가 시스템 관리자 영역에 접근하여 정보를 변경하는 행위 (보안 관련 정보의 변경 행위 포함)	M4, M6, M8, A2
T7	자기 고유 업무외에 허가되지 않은 업무 영역에 접근하는 행위	M1, M2, M3, M5, A2
T8	기업 내부 사용자가 외부의 사용자에게 불법적으로 정보를 제공하는 행위	M6, M7, A2, A3
T9	저장되어 있는 정보의 기밀성을 저해하는 행위	M1, M2, M6, M7, A4
T10	정보의 실시간 접근에 따른 무결성을 유지하는 문제	M2, M7
T11	감사기록 데이터가 손실되는 사건	M1, M5, M7, M8, A2
T12	감사기록 데이터의 분석을 지연시키는 행위	M1, M2, M6, M7, A2
T13	CALS체제의 특정 기억장소를 소진하는 행위	M8, A3

4. 모델의 적정성 검토를 위한 예

제안된 CALS 정보보호 모델은 전산망을 통한 기존 전송환경을 기반으로 설계된 개념 모델로서 전송되는 환경의 메시지 흐름에 따라 순차적인 단계별로 검토함으로써 모델 설정의 적정성을 나타내고자 한다. CALS에서 전송되고 공유되는 정보들은 문서뿐만 아니라, 관리정보나 멀티미디어 정보가 포함되며 통합 데이터 베이스에 총괄적으로 저장되어 필요시에 정해진 규칙에 따라 저장 정보를 사용할 수 있는 환경으로 가정하여 설명하였다.

4.1 시뮬레이션 환경

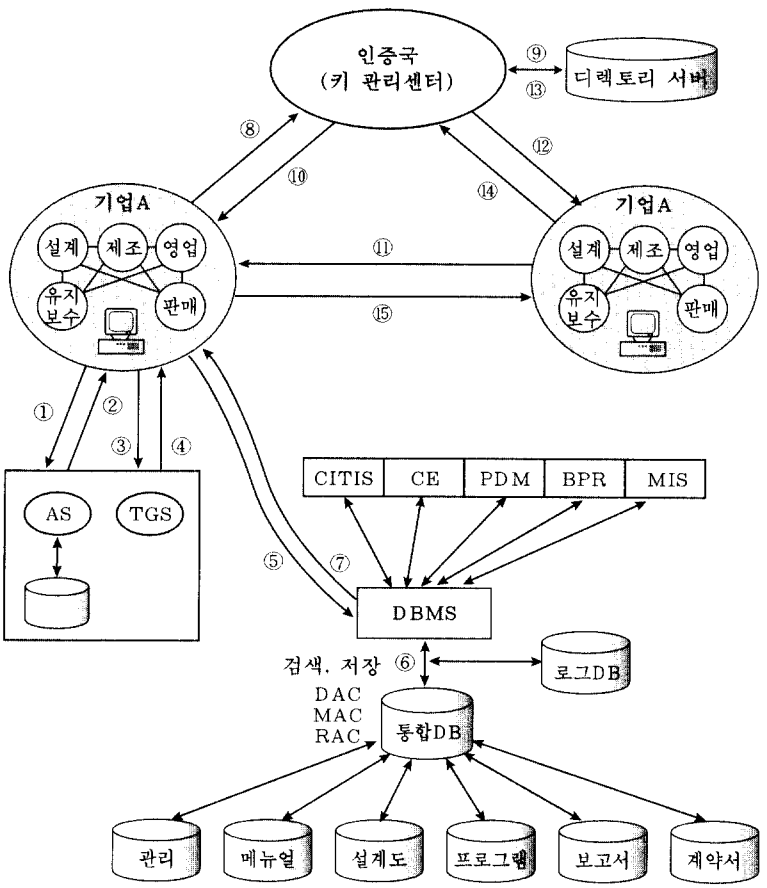
시뮬레이션을 위한 CALS 환경은 기업내 또는 기업간에 다양한 정보를 송·수신하고 통합 데이터베이스 접근 및 공유할 수 있는 통합된 환경이다. 이러한 CALS 환경에서 정보보호를 요하는 대상은 데이터베이스와 전송되는 메시지로 집약될 수 있다.

CALS 환경에서 메시지 흐름에 따른 시뮬레이션 환경은 〈그림 10〉과 같다. 기업A와 기업B 사이에서 제품의 전 공정에 관련된 정보를 통합 데이터베이스로부터 획득하여 송·수신하며 정보보호를 위한 인증서 관리는 인증국과 DSA가 담당한다. 통합 데이터베이스내의 정보들은 기업에서 요구되는 관리정보, 설계도, 계약서, 매뉴얼 등에 관한 정보들이며 저장되어 필요시에 서비스 요청에 따라 접근하여 메시지를 획득하여 전송한다. 개방형 네트워크 환경에서는 모든 클라이언트들이 원하는 서비스를 요구할 수 있기 때문에 보안상 통합 데이터베이스에 접근시 제약사항이 요구되며 특히 정당한 사용자로 위장한 침입자는 허가받은 사용자가 갖는 권한을 모두 가질 수 있기 때문에 중요시된다. 따라서 통합 데이터베이스 서버는 서비스를 제공하기 전에 서비스를 요청하는 클라이언트의 신원을 확인해야 하며 이를 위해 인증 메커니즘이 제공되어야 한다. 인증 서버로부터 승인을 받은 후에 통합 데이터베이스에 필요한 메시지를 요청하게 되

고 통합 데이터베이스 서버는 클라이언트로부터 서비스를 요청 받고 클라이언트의 신원을 확인한다. 인증을 통한 신원확인 후 요청된 정보를 기업 A로 전송한다. 통합 데이터베이스로부터 전송된 메시지를 기업 B에 안전하게 전송하기 위하여 암호화, 해쉬 함수, 디지털 서명등의 메커니즘이 사용될 수 있다. 또한 이러한 메커니즘과 연계될 기업 B의 공개키 확보가 선행되어야 한다. 기업 B의 공개키를 얻고자 할 때 인증국에 공개키가 포함된 인증서를 요청한다. 요청된 인증서는 인증국과 DSA로부터 제공되며 전송된 인증서를 통하여 기업 B가 공개키를 획득한다. 메시지 전송시 상대방의 공개키를 이용하여 기밀성을 비롯한 무결성, 인증, 부인봉쇄 서비스가 제공된 보호된 메시지를 전송한다. 기업 A로부터 메시지를 수신한 기업 B에서는 기업A의 공개키를 동일한 방법으로 획득한 후, 전송된 메시지에 대한 결과를 송신자에게 전송한다.

4.2. 단계별 시뮬레이션

앞서 살펴본 CALS 환경에서의 메시지 흐름에 따른 시뮬레이션 단계는 크게 15단계로 구성된다. 각 단계별 분석을 위하여 사용된 표기법들은 〈표 4〉와 같으며 세부적인 분석 내용은 아래와 같다.



〈그림 10〉 CALS 체제에서의 메시지 흐름에 따른 정보보호

〈표 4〉 사용된 표기법

A, B	: CALS 사용자	$Ticket_{tgs}$	: TGS에 접근을 위한 티켓
AS	: 인증 서버	$Ticket_v$	: 서버 V에 접근을 위한 티켓
V	: 서버	TS	: 시간을 확인할 수 있는 Time Stamp
M	: 전송 메시지	Lifetime	: 티켓의 유효시간
H	: 해쉬 함수	Ver	: 인증서 버전
E	: 암호화	SN	: 인증서 일련번호
ID_a, ID_b	: CALS 사용자 A, B의 식별자	AI	: 서명에 사용된 알고리듬 식별자
K_a, K_b	: A, B의 패스워드	CA	: 인증국
ID_{tgs}	: TGS의 식별자	A_k	: 메시지 암호화를 위한 사용자키
ID_v	: V의 식별자	K_a, K_{tgs}, K_v	: A, TGS, V의 패스워드
AD_a	: A의 네트워크 주소	K_{Ap}, K_{As}	: A의 공개키, 비밀키
$K_{a,tgs}$	: 사용자 A와 TGS간 공유 세션키	K_{Bp}, K_{Bs}	: B의 공개키, 비밀키
$K_{a,v}$	: 사용자 A와 서버 V의 공유 세션키	K_{CAp}, K_{CAs}	: 인증국의 공개키, 비밀키
$Auth_a$	: 사용자에 의해 생성된 인증자	T^A, T^B	: 인증서의 유효기간

[1] 단계 : 인증 서버에 티켓-승인 티켓 요청

$ID_a \| \| ID_{tgs} \| \| TS_1$

기업A가 인증 서버(AS)에 티켓 승인 서버에 접근하기 위한 티켓-승인 티켓을 요청하는 단계이다. 기업A는 IDB에 접근 권한이 있는 정당한 사용자임을 인증서버가 식별할 수 있도록 기업A의 ID와 티켓 승인 서버의 ID를 보낸다.

[2] 단계 : 기업A와 티켓 승인 서버가 공유할 세션키와 티켓-승인 티켓 전송

$E_{Ka}[K_{a,tgs} \| \| ID_{tgs} \| \| TS_2 \| \| Lifetime_2 \| \| Ticket_{tgs}]$

$Ticket_{tgs}=E_{Ktgs}[K_{a,tgs} \| \| ID_a \| \| AD_a \| \| ID_{tgs} \| \| TS_2 \| \| Lifetime_2]$

인증서버가 기업A에게 티켓-승인 티켓과 티켓 승인 서버와 공유할 수 있는 세션키를 전송하는 단계이다. 인증 서버는 정당한 사용자 확인한 후 전송된 기업A의 패스워드를 이용하여 생성된 키와 티켓-승인 티켓을 암호화한 후 전송한다.

[3] 단계 : 접근하려는 DB 서버 관련 정보와 인증자 전송

$ID_v \| \| Ticket_{tgs} \| \| Auth_a$

$Ticket_{tgs} = E_{Ktgs}[K_{a,tgs} \| \| ID_a \| \| AD_a \| \| ID_{tgs} \| \| TS_2 \| \| Lifetime_2]$

$Auth_a = E_{Ka,tgs}[ID_a \| \| AD_a \| \| TS_3]$

기업A가 티켓 승인 서버에게 자신의 ID와 접근하려는 IDB 정보를 전송하는 계이다. IDB에 접근하기 위하여 접근하려는 IDB의 ID, 티켓-승인 티켓, 그리고 기업A임을 확인시켜줄 수 있는 사용자 ID, 네트워크 주소, 타임 스탬프를 포함한 인증자를 암호화하여 전송한다.

[4] 단계 : IDB 서버에 접근을 승인하는 서비스-승인 티켓 전송

$E_{Ka,tgs}[K_{a,v} \| \| ID_a \| \| AD_a \| \| ID_{tgs} \| \| Ticket_v]$

$Ticket_v=E_{Kv}[K_{a,v} \| \| ID_a \| \| AD_a \| \| ID_v \|$

$|TS_4||Lifetime_4]$

티켓 승인 서버가 기업A에게 IDB 접근을 승인하는 서비스-승인 티켓을 전송하는 단계이다. 티켓 승인 서버는 IDB로부터 서비스를 받을 수 있는 서비스-승인 티켓과 기업A와 IDB 서버가 공유할 수 있는 세션키를 암호화한 후 전송한다.

[5]단계 : IDB에 서비스를 요청

$Ticket_v||Auth_a, Request_5||TS_5$

$Ticket_v = EK_v[K_{a,v}||ID_a||AD_a|$
$|ID_v||TS_4||Lifetime_4]$

$Auth_a = E_{Ka,v}[ID_a||AD_a||TS_5]$

$Request_5$: 기업A가 IDB에게 원하는 메시지를 요청

5단계는 IDB에 서비스를 요청하는 단계이다. 기업A는 티켓 승인 서버로부터 전송된 IDB 서비스-승인 티켓과 인증자를 전송한 후에 IDB에 원하는 메시지를 요청한다.

[6]단계 : 검증 및 요청에 대한 서비스 제공

$Request_6||TS_6, M||TS_6$

요청된 정보 : M을 검색 및 획득

IDB 서버가 기업A로부터 요청된 서비스를 처리하는 단계로서 요청된 정보를 검색하고 획득하여 전송한다.

[7]단계 : IDB의 정보 전송

$E_{Ka,v}[M||H(M)||TS_7]$

획득한 IDB 정보를 기업A에게 전송하는 단계로서 전송시 해쉬함수를 이용한 인증코드를 생성하고 기업A와 IDB가 공유하는 세션키를 이용하여 메시지와 함께 암호화하여 전송한다. 기업A로부터 요청된 정보가 검색되었을 때 검색된 정보를 기업A에게 전송하고 요청된 정보가 검색되지 않았을 때도 검색된 정보의 없음에 대한 결과를 기업A에게 전송한다.

[8]단계 : 인증국에게 기업B의 인증서 발급 요청

$Request_8||TS_8$

$Request_8$: 기업A가 인증국에 기업B의 인증서를 요청

정보보호 메커니즘과 연계될 B의 공개키를 얻기 위하여 인증국에 기업B의 인증서를 요청하는 단계이다.

[9]단계: 인증국으로부터 인증서 요청 및 DSA로부터의 인증서 전송

$Request_9||TS_9, E_{KCAp}[Ver||SN|$
$|AI||CA||ID_b||B_P||T_B]$

$Request_9$: 인증국이 DSA에 기업B의 인증서를 요청

인증서 발급을 요청 받은 인증국이 인증서를 DSA에게 요청하고 전송받는 단계이다. 기업A로부터 기업B의 인증서 발급을 요청 받은 인증국은 인증서가 저장되어 있는 DSA에게 기업B의 인증서를 요청하고 DSA는 요청된 인증서를 획득한 후에 인증국에게 전송한다.

[10]단계: 인증국으로부터 기업B 인증서 발급

$E_{KAp}[E_{KCAs}[Ver||SN||AI||CA|$
$|ID_b||B_P||T_B], TS10]$

기업A가 인증국으로부터 기업B의 인증서를 발급 받는 단계이다.

[11]단계: 보호된 메시지 전송

$E_{KAk}[M||H(M)]||E_{KBp}[E_{KAs}[Ak]|$
$|TS_{11}]$

기업A가 IDB로부터 얻은 메시지를 기업B로 안전하게 전송하는

단계이다. 기업A는 공개키를 획득하여 정보보호 메커니즘의 연계하에 정보보호 서비스를 제공한다. 해쉬함수를 이용하여 무결성을 제공하고 메시지 암호화를 통하여 기밀성을 제공한다. 메시지 암호화에 사용된 키를 자신의 사용자키(Ak)를 이용하여 암호화함으로써 인증을 제공한다. 또한 전송하려는 보호된 메시지를 로그화일에 저장하고 송신함으로써 메시지 수신에 대한 부인봉쇄 서비스를 제공한다.

[12]단계: 인증국에게 기업A의 인증서 발급 요청

$Request_{12}||TS_{12}$

$Request_{12}$: 기업B가 인증국에 기업A의 인증서를 요청

전송된 메시지의 복호화를 위한 기업A의 공개키를 획득하기 위하여 인증국에 기업A의 인증서를 요청하는 단계로서 세부사항은 8단계와 동일하다.

[13]단계: 인증국으로부터 인증서 요청 및 DSA로부터 인증서 전송

$Request_{13}||TS_{13},E_{KCA_P}[Ver||SN||AI||CA||ID_a||A_P||T^A]$

$Request_{13}$: 인증국이 DSA에 A의 인증서를 요청

인증서 발급을 요청 받은 인증국이 인증서의 발급을 위하여 DSA에 인증서를 요청하고 DSA로부터 인증서를 받는 단계로서 세부사항은 9단계와 동일하다.

[14]단계: 인증국으로부터 기업A 인증서 발급

$E_{KB_P}[E_{KCA_S}[Ver||SN||AI||CA||ID_a||A_P||T^A], TS_{14}]$

기업B가 인증국으로부터 기업A의 인증서를 발급 받는 단계로서 세부사항은 10단계와 동일하다.

[15]단계: 전송된 메시지 수신에 대한 결과 전송

$E_{KA_P}[E_{KB_S}[TS_{11'}]$

기업A로부터 전송된 메시지 수신에 대한 결과를 기업A에게 전송하는 단계로서 11단계에서 전송된 정보를 활용한다. 전송된 메시지에 대한 결과를 생성하고 로그화일에 저장함으로써 송신에 대한 부인봉쇄 서비스를 제공한다.

5. 결 론

CALS 도입으로 네트워크를 통한 데이터 교환 및 공유가 가능해졌다. 그러나 이러한 장점에도 불구하고 정보보호 문제라는 역기능으로 인하여 민간부문과 군, 정부 등에서 CALS를 구축하여 운영하는데 많은 우려가 되고 있다. 따라서 본 논문에서는 CALS 정보보호 위협 요소를 비롯한 정보보호 서비스와 메커니즘을 분석하고 CALS를 안전하게 구축하기 위한 정보보호 모델과 시뮬레이션 단계를 제시하였다.

본 논문에서는 CALS 체제의 위협요소 13개, 보안 목적 7개, 가정요소 4개, 8개의 보안 메커니즘을 설정하여 제안된 CALS 정보보호 모델은 4개의 서브 모델인 전송모델, 키관리 모델, 감사 모델, 통합 데이터베이스 연계 모델로 구성하였으며 구현을 위한 모듈로 보안 관리부, DSA와 인증국을 포함하는 키관리부, 분산 환경 보안 감사부, 통합 데이터베이스 관리부로 나누어 제시하였다. 보안 관리부는 키관리, 감사, 데이터베이스 관리부로 구성된다. 인증국과 키관리 기관은 키 생성부터 폐기까지의 모든 정보들을 관리하는 기능을 수행하고 DSA는 각 사용자를 지원하는 DUA와의 통신을 통하여 사용자들의 정보들을 저장하고 정보 요청시 실시간으로 제공하는 기능을 수행한다. 보안 감사부는 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. 제안된 CALS 정보보호 모델은 안전한 CALS 모델 구축의 기초가 될 것이며 지속적인 CALS 정보보호에 대한 연구와 통합 데이터베이스에서 실시간 처리 및 병행 제어를 비롯한 CALS의 원활한 운영을 위한 다양한 기술 연구가 추진되어야 할 것이다.

참 고 문 헌

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

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

[3] 신종태, 이정현, 이대기, 소우영, "CALS 체제의 정보보호 프레임워크" 통신정보보호 학회지, 제7권, 제3호, 1997. 9.

[4] 윤여웅, 이정현, 이대기, 소우영, "CALS 정보보호 모델 설계" 97 한국통신정보보호학회 종합학술대회 논문집, 1997. 9.

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

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

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

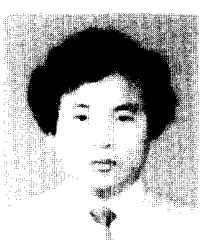
[8] 한국전자통신연구원, "정보보호 서비스 제공을 위한 안정성 서버 개발" 1995. 12.

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

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

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

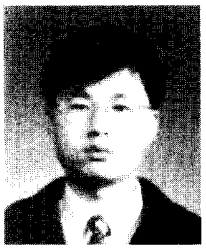
□ 著者紹介



신 종 태

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

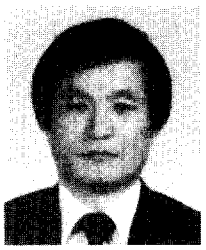
※ 주관심분야 : 정보보호시스템 평가, 암호학, IDS, 컴퓨터/네트워크보안, CALS/EC 보안



이 정 현

1993년 숭실대학교 전자계산학과 (공학사)
1995년 숭실대학교 대학원 전자계산학과(공학석사)
1995년 ~ 현 재 한국전자통신 연구원

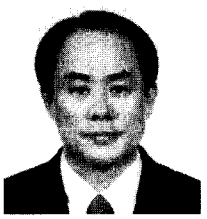
※ 주관심분야 : 컴퓨터/네트워크보안



이 대 기

1966년 한양대학교 전자공학과(공학사)
1987년 한양대학교 산업대학원 잔자공학과(공학석사)
1980년 ~ 현 재 한국전자통신연구원 책임기술원

※ 주관심분야 : 정보시스템 감사, 통제 및 보안



소 우 영

1979년 2월 중앙대학교 전자계산학과(학사)
1982년 2월 서울대학교 대학원 계산통계학과 전자계산학 석사
1991년 1월 메릴랜드대학교 대학원 전자계산학과 박사
1981년 3월 ~ 1985년 3월 공군사관학교 수학과 전자계산학과 전임강사
1991년 ~ 현 재 한남대학교 전자계산학과 부교수

※ 주관심분야 : 인공지능, 신경회로망, 통신망 정보보호