特輯

정보보호 기술의 표준화 동향

姜 信 角
韓國電子通信研究所 情報通信標準研究센터

Ⅰ. 서론

정보통신 기술의 발전과 함께 컴퓨터등의 각종 정보통신 시스템이 널리 보급되고, 이러한 시스템간을 통신망을 이용하여 상호 접속시킴으로써 사용자들에게 다양한 형태의 정보통신 서비스를 제공하는 산업사회에서 정보화 사회로의 이행이 급속히 진전되고 있다. 그러나 이러한 정보화 사회의 편리성과 함께 각종 중요 정보의 불법유출, 개인 사생활의 침해, 컴퓨터 바이러스 및 해커에 의한 정보자원의 파괴등 정보화 사회의 역기능이 심각한 사회 문제로 대두되게 되었다. 따라서 이러한 각종 컴퓨터 범죄로 부터 정보자원을 보호하고 정보통신 서비스 이용자들에게 안전한 통신 서비스를 제공하기 위해 정보보호 기술의 연구개발이 요구되게 되었고, 이를 실제 정보통신망 및 시스템에 적용하기 위한 표준화 작업이 요구되게 되었다.

정보보호 기술의 표준화 활동은 현재 ISO, ISO/IEC JTC1, ITU-TS등의 국제표준화 기구와 IEEE, ECMA, ETSI, ANSI등 지역 및 국가레벨의 표준화 기구에 의해 이루어지고 있다. 이러한 각 표준화 기구에서 추진되고 있는 보호기술 표준화의 주요 목적은 첫째로 암호기술을 이용한 정보보호 방법과 보호 서비스를 표준화 함으로써 정보화 사회에서 요구되는 통신의 비밀보장 및 사생활 보호등과 같은 안전한 정보통신 서비스를 가능하게 하고, 둘째로 표준에 기초한 보호장치 및 소프트웨어의 양산을 통하여 정보보호에 요구되는 비용경감을 가능하게 하는것이다. 특히 정보기술 및 전기통신의 표준화가 개방시스템 개념에 따라 표준화가 이루어지면서 개방시스템 환경에서 정보보호 기술의 적용을 통하여 안전한 정보통신 서비스를 제공하고자 하는 노력이 표준화 기구를 중심으로 활발하게 이루어지고 있다. 본 고에서는 먼저 현재 세계적으로 활발하게 추진되고 있는 개방시스템 환경에서의 정보보호 기술 표준화의 개념과 대상등을 분석하였고, 다음으로 정보보호 기술의 국제표준화 동향을 살펴보았으며, 또한 국내에서 최근 이루어지기 시작한 정보보호 기술 표준화 관련 활동 현황을 살펴보았다.

Ⅱ. 개방시스템에서의 보호기술 표준화

JTC1에서는 개방시스템에서 안전한 정보통신 서비스를 제공하기 위한 보호표준의 개발을 추진하고 있다.

이러한 표준화 작업은 정보보호를 위한 일반적인 보호구조, 골격, 모델을 정의하고, 각 응용 서비스에

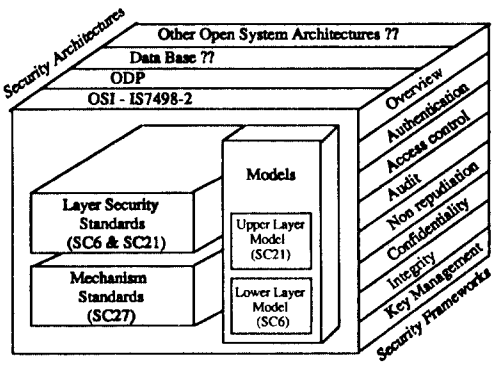

그림 1. 개방시스템 보호기술 표준화 요소

보호기능을 부가하기 위한 계층별, 응용 서비스별 표준화 작업과, 보호서비스를 실제 구현하기 위해 공통적으로 소요되는 보호메카니즘에 대한 표준화로 나누어 수행되고 있다. 개방시스템에서요구되는 이러한 각 안전요소간 상호관계는 그림.1과 같이 나타낼 수 있다.

1. 정보보호 구조

정보보호 구조는 안전한 통신이 요구되는 환경에 적용될 수 있는 일반적인 안전성에 관련된 구조적 요소에 대해 정의하고 있다. 보호구조는 일반적인 보호 관련 요소 및 서비스와 메카니즘을 추상적으로 정의하고 있으므로 정보보호에 대한 일반적인 지침이 되고 있다.

보호구조는 개방시스템 상호접속(OSI), 개방형 분산처리(ODP), 데이타베이스 및 기타 개방시스템 구조등으로 분류하고 각각에 대해 그 구조를 정의하고 있으나 현재는 OSI에 대한 보호구조만이 JTC1/SC21에 의해 ISO 7498-2로 표준화 되어 있다. ISO 7498-2는 또한 ITU-T/SG7에 의해 X.800 권고로 ITU-T 표준으로 채택되었다. ISO 7498-2에서는 OSI 환경에서 요구되는 보호서비스와 보호 메카니즘의 일반적 규정과, OSI 참조모델에 따른 각 계층별 기능과 보호서비스 및 보호 메카니즘과의 상호 관계에 대해 정의하고 있다.

2. 정보보호 골격

정보보호 골격은 특정 정보보호 서비스에 대해 이 서비스가 실제 적용될때 관련되는 모든 측면, 즉 다른 서비스와의 관계에서 부터 그 서비스를 제공하기 위한 관리적 요구사항까지를 종합적이며 일관성있게 규정한다. 현재 작성되고 있는 보호골격 표준은 OSI 보호구조에 기반을 두었으나 동일 서비스를 필요로 하는 개방시스템 어디에서나 적용될 수 있도록 하고 있다. 보호골격에서는 시스템 내부적으로 시스템과 객체의 보호수단을 정의하고 시스템간의 상호작용을 규정하나, 시스템이나 요구되는 보호 메카니즘을 구현하기 위한 방법론에 대해서는 규정하지 않는다. 현재 정의되고 있는 보호골격에는 인증, 엑세스제어, 감사, 부인봉쇄, 기밀성, 무결성, 키관리가 있으며, 이는 JTC1/SC21과 JTC1/SC27, 그리고 ITU-T/SG7에서 표준화 작업이 이루어지고 있다.

3. 정보보호 모델

정보보호 모델은 보호구조와 보호골격에서 정의된 보호 개념을 개방형 시스템 구조의 특정 분야에 어떻게 적용할지에 대해 규정하고 있다. 현재 OSI 참조모델에 적용하기 위한 보호모델이 상위계층 보호모델과 하위계층 보호모델로 나뉘어 표준화되고 있으며, 개방형 분산처리, 데이타베이스, 분산사무응용에 적용되기 위한 보호모델의 표준화가 현재 진행되고 있다. 보호모델에 대한 표준화는 현재 JTC1/SC6, JTC1/SC18, JTC1/SC21과 ITU-T/SG7에 의해 이루어지고 있다.

4. 보호 서비스 및 메카니즘

ISO 7498-2로 표준화된 보호구조에서는 개방시스템 환경에 적용되기 위한 보호 서비스 및 메카니즘에 대해 정의하고 있으나, 이는 OSI 뿐만 아니라 통신망, 정보처리 시스템등 정보통신 환경에 포괄적으로 적용될 수 있다. 현재 정의되어 있는 보호 서비스로는 인증, 엑세스 제어, 데이타 무결성, 기밀성, 부인봉쇄가 있다. 또한 이러한 보호 서비스를 실제 구현하기 위한 기술을 보호 메카니즘으로 정의하고 있으며, 현재 정의되어 있는 메카니즘에는 암호화, 디지탈 서명, 엑세스 제어, 데이타 무결성, 인증교환, 트래픽 패딩, 경로제어, 공증이 있다. 보호 서비스와 메카니즘과의 상관관계는 표1과 같다.

표 1. 보호 서비스와 메카니즘과의 상관관계

서비스 \ 메카니즘	암호화	디지털서명	엑세스제어	데이타무결성	인증교환	트래픽패딩	경로제어	공증
대등실체 인증	Y	Y	•	•	Y	•	•	•
발신처 인증	Y	Y	•	•	•	•	•	•
엑세스 제어	•	•	Y	•	•	•	•	•
접속 기밀성	Y	•	•	•	•	•	Y	•
비접속 기밀성	Y	•	•	•	•	•	Y	•
선택영역 기밀성	Y	•	•	•	•	•	•	•
트래픽 흐름 기밀성	Y	•	•	•	•	Y	Y	•
복구기능을 갖는 접속 무결성	Y	•	•	Y	•	•	•	•
복구기능없는 접속 무결성	Y	•	•	Y	•	•	•	•
선택영역 접속 무결성	Y	•	•	Y	•	•	•	•
비접속 무결성	Y	Y	•	Y	•	•	•	•
선택영역 비접속 무결성	Y	Y	•	Y	•	•	•	•
발신 부인봉쇄	•	Y	•	Y	•	•	•	Y
수신 부인봉쇄	•	Y	•	Y	•	•	•	Y

현재 보호 서비스 및 보호 메카니즘의 표준화 작업은 주로 JTC1/SC27에 의해 이루어지고 있으며, 응

용서비스 별로 해당 표준화 위원회에서 일부 수행되기도 한다.

5. 응용 서비스별 보호기능의 추가

메세지처리 시스템(MHS), 데렉토리(DIR), 화일전송, 접근제어 및 관리(FTAM), 전자데이타 교환(EDI)등의 각 응용 서비스와 수송계층, 망계층 규약등과 같은 각 계층별 통신규약에 사용자가 요구하는 보호서비스를 제공하기 위해 기존 통신 규약에 보호기능을 추가하는 작업이 계층별, 응용 서비스별로 진행되고 있다. 이러한 표준화 작업은 응용 서비스의 속성에 따라 요구되는 서비스를 정의하고, 이를 지원하기 위한 통신절차 및 기능등을 규정하는 형태로 작업이 진행되고 있으며, JTC1/SC6, SC17, SC18, SC21, SC22, ISO/TC68, ITU-T/SG7, SG8등에 의해 표준화 작업이 이루어지고 있다.

Ⅲ. 국제표준화 동향

정보보호 기술의 표준화를 가장 적극적으로 추진하고 있는 국제표준화 기구는 정보기술 전반의 표준화 업무를 담당하는 ISO/IEC JTC1과, 은행 및 금융업무의 표준화를 추진하는 ISO/TC68이다. 그리고 전기통신의 국제표준화 업무를 수행하는 ITU-TSS(구 CCITT와 CCIR의 표준화 관련 작업반이 통합된 새로운 전기통신 표준화 위원회)에서도 JTC1과 협력하에 정보보호 기술에 대한 표준화 작업이 진행되고 있다. 또한 IEEE 802 위원회에서는 근거리망에서의 정보보호를 위한 보호규약의 표준화 작업이 진행되고 있다. 이밖에 유럽의 컴퓨터 제조회사들로 구성된 ECMA와, 과거 CEPT의 업무를 이어받아 전기통신 분야의 유럽표준을 개발하는 ETSI 같은 지역 표준화 기구에서도 정보보호 기술에 대한 표준화 작업이 진행되고 있으며, 국가별로도 표준화 단체 및 관련 기관에 의해 표준화 작업이 이루어지고 있다.

1. JTC1에서의 보호기술 표준화

JTC1내에서 보안기술 표준화를 추진하고 있는 관련 주요 표준화위원회로는 SC6, SC17, SC18, SC21, SC22, SC27이 있다. SC21에서는 OSI 환경 전반에 적용되는 보호구조, 보호골격과 상위계층 보호모델 및 보호관리에 대한 표준화를 추진하며, 화일전송, 접근 및 관리(FTAM), 디렉토리등 특정 응용 규약별로 보호 서비스를 추가하기 위한 표준화 작업이 이루어지고 있다. 또한 SC21에서는 개방형 분산처리(ODP)에서의 보호 서비스 제공을 위한 보호구조 및 보호기능에 대한 표준화 작업이 진행되고 있다. SC6에서는 OSI 환경에서의 하위계층 정보보호 모델과 망계층 및 수송계층의 보호규약 표준화가 현재 추진되고 있으며, SC18에서는 분산 사무환경에서의 보호 요구사항과 ODA/ODIF와 같은 사무응용 규약에 보호서비스를 추가하기 위한 표준화 작업이 진행되고 있다.

SC27에서는 정보기술 전반에 대한 보호기술 표준화를 수행하며, 특히 보호기술을 실제 적용하기 위해 소요되는 암호기술과 관련하여 보호 서비스의 정의, 각종 보호 알고리즘 표준의 개발 및 안전평가기준 등에 대한 표준화 작업이 진행되고 있다. 그리고 IC-카드 기술에 대한 국제표준화 작업을 수행하고 있는 SC17에서는 IC-카드를 보호기술과 결합하여 응용하기 위한 작업이 진행되고 있으며, SC22에서는 POSIX 보호에 대한 표준화 작업이 진행되고 있다. JTC1에서는 이러한 관련 위원회 간에 표준화 작업의 중복성을 피하고 작업효율을 높이기 위해 공동워크샵을 개최하는등 각 위원회간 상호협력과 조정을 위해 노력하고 있다. 여기에서는 JTC1 내에서 정보보호 표준 개발과 밀접한 관련이 있는 위원회에서 이루어지고 있는 작업현황을 살펴본다.

1) ISO/IEC JTC1/SC6

시스템간 통신 및 상호접속에 관련된 국제표준화를 추진하는 SC6에서는 정보보호 기술과 관련하여 OSI 하위 4계층에 대한 국제표준을 개발하고 있다. 현재 SC6에서 진행되고 있는 정보보호 기술 표준화 현황에 대해 살펴보면 먼저, "OSI 하위계층 정보보호 모델"에 대한 표준(안)이 작성되어 검토중에 있다. 또한 수송계층에서의 정보보호 서비스를 제공하기 위한 "수송계층 보호규약(TLSP: Transport Layer Security Protocol)" 표준이 개발 완료되었고, TLSP의 동작을 위해 사전에 요구되는 "보호연계 설정 규약(SAP: Security Association Protocol)"에 대한 표준(안)이 최종 검토단계에 있다. 그리고 망계층에서 정보보호 서비스를 제공하기 위한 "망계층 보호규약(NLSP: Network Layer Security Protocol)" 표준(안)이 역시 최종 검토단계에 있다.

또한 IEEE 802 위원회에서 표준화 한 안전한 근거리망 통신을 위한 보호규약 표준인 SDE(Secure Data Exchange)가 SC6에 제안되었으나, 표준화의 필요성에 대한 합의가 이루어지지 않아 아직 정식 표준화 항목으로는 채택되지 않고 있다. 특히 영국에서는 SDE가 지원하는 보호 기능을 NLSP로 충분히 커버할 수 있다고 주장하였으나, NLSP가 LAN 프로토콜 스택위에 올라가지 않고 MAC과 LLC위에 바로 응용이 올라가는 형태의 근거리망 환경에서는 SILS가 필요한 것으로 의견이 모아지고 있는 상태이다.

2) ISO/IEC JTC1/SC21

개방형 시스템의 상호접속을 위한 정보검색, 전달 및 관리에 대한 국제표준화를 추진하는 SC21에서는 OSI 참조모델을 개발하고 이에따른 각종 응용 서비스등 OSI 상위 3계층에 대한 국제표준을 개발하고 있다. 정보보호 기술과 관련하여서는 개방형 시스템에서의 정보보호를 위한 일반적 개념 및 구조체계를 규정하는 표준인 ISO 7498-2(보호구조)를 표준화 하였다. 그리고 인증, 접근제어, 부인봉쇄, 기밀성, 무결성, 보호감사 추적에 대한 보호골격 표준(안)이 개발 완료단계에 있다. 이밖에도 OSI 상위계층에서의 정보보호 모델 표준(안)이 최종 검토단계에 있고, 연계제어서비스(ACSE)에서의 인증표준이 개발되었으며, 표현계층에 기밀성 및 무결성 서비스를 지원하기 위한 작업이 진행되고 있다. 또한 FTAM, 거래처리(Transaction Processing), 디렉토리등 응용 서비스별로 보호기능을 부가하기 위한 표준화 작업이 진행되고 있다. 특히 디렉토리 시스템에서는 정보보호를 위해 공개키 암호화 기법을 이용한 인증골격을 정의하였으며, 디렉토리 접근제어에 대해서도 규정하고 있다.

SC21에서는 또한 데이타베이스와 관련하여 정보보호 표준화 작업을 추진하고 있는데 데이타관리 참조모델에서는 접근제어에 대한 구조적 모델을 정의하고 있다. 그리고 정보자원 사전 시스템(IRDS:Information Resource Dictionary System) 골격과 원격 데이타베이스 접근(RDA: Remote Database Access) 규약에서도 접근제어와 관련된 사항을 규정하고 있다.

SC21에서 이루어지는 보호기술 표준화 작업중 중요한 사항으로써 보호관리를 들 수 있다. OSI 보호관리와 관련하여 보호 경보보고(Alarm report) 기능, 보호 감사추적(Audit trail) 기능, 접근제어를 위한 객체 및 속성에 대한 표준이 제정되었거나, 완료단계에 있다.

3) ISO/IEC JTC1/SC27

과거 JTC1/SC20에서는 정보보호 기술의 핵심인 데이타 암호화기술 표준화를 수행하고 있었으나, 보호기술 표준화 작업이 JTC1내에서 중복되어 일어나고 암호화기술 이외에 안전평가 및 감사 기술등과 같은 타 보호기술에 대한 표준화가 요청되게 되자 1989년 6월 JTC1 총회에서 SC20을 해산시키고 정보기술 전반에 대한 보호기술 표준화를 수행하는 새로운 위원회를 설립하기로 결정한 결의안 28에 의해 SC27이 설립되었다. SC27은 JTC1 총회의 결의안에 따라 1990년 4월 스웨덴 스톡홀름에서 제1차 총회를 갖고 위원회의 명칭, 작업범위 및 영역, 조직구성등을 결정한 이래로 1991년 4월 동경에서 제2차 총회를, 그리고 10월 브뤼셀에서 제3차 총회를 개최하였다. 현재는 매년 4월경 작업반 회의가, 그리고 10월경 총회가 개최되고 있다. SC27에서 다루고 있는 작업영역 및 범위는 정보기술 보호를 위한 포괄적인 방법과 기술의 표준화로써, 구체적인 작업 내용으로는 정보시스템의 보호 서비스를 위한 요구사항 검증과 보호기술 및 메카니즘의 개발, 그리고 위험분석등과 관련한 보호지침의 개발이 있으며, 또한 용어와 보호평가기준등 지원기술의 개발을 수행한다. 단 암호화 알고리즘 자체의 표준화나 보호 메카니즘을 특정 응용에 적용하는 일등은 SC27의 작업범위를 벗어나는 것으로 다루지 않고 있다.

SC27의 조직을 보면 3개의 작업반으로 구성되어 있다. WG1에서는 보호 요구사항, 서비스 및 지침을 다루며, WG2에서는 보호기술 및 기법에 대해, 그리고 WG3에서는 보호기술 평가기준과 관련된 사항을 다루고 있다. WG1에서 수행되는 주요 작업항목으로는 첫째로 응용과 시스템 구성요소의 요구사항 검증이 있고, 둘째로 WG2에 의해 개발되는 보호기술 및 메카니즘을 이용하여 인증, 접근제어, 무결성, 기밀성, 키관리 및 감사등과 같은 보호 서비스 표준을 개발한다. 세째로 보호지침, 위험분석등 정보보호 기술에 대한 설명이나 해석을 위한 지원문서를 작성하는 일을 수행하고 있으나, WG1의 작업영역이 다양한 사용자와 밀접한 관련이 있는 부분이고, 현재 정보통신 환경이 확장되고 있는 추세이므로 작업범위는 점차 확대될 전망이다. WG2에서는 정보기술 분야에 적용될 보호기술 및 메카니즘의 표준화를 수행하며,

표 2. SC27에서의 표준화작업현황

과 제 명	표준화상태 및 관련문서	담당 WG	표준화 예상시기
64비트 블럭암호 운영모드	IS 8372:1987	WG2	
n비트 블럭암호운영모드	IS 10116:191	WG2	
실체인증, 제1부 : 일반모델	IS 9798-1:1991	WG1	
실체인증, 제2부 : 대칭형기술을 이용한 인증	IS 9798-2:1994	WG2	
실체인증, 제3부 : 공개키암고리즘을 이용한 인증	IS 9798-3 :1993	WG2	
실체인증, 제4부 : 암호학적 검사함수를 이용한 인증	DIS 9798-4	WG2	'95
실체인증, 제5부 : 영지식기술을 이용한 인증	WG2 / N297	WG2	'96
블럭암호 알고리즘을 사용한 데이타 무결성기법	DIS 9797	WG2	
부인봉쇄기법, 제 1부 : 일반모델	WD (WG2 / N298)	WG2	'96
부인봉쇄기법, 제2부 : 대칭형 암호알고리즘을 사용한 기법	CD 13888-2 (WG2 / N299)	WG2	'96
부인봉쇄기법, 제3부 : 비대칭형 암호알고리즘을 사용한 기법	WG2 / N300	WG2	'96
메세지 복원을 주는 디지탈서명 방식	IS 9796:1991	WG2	
부가형 디지탈 서명	WG2 / N221	WG2	'97
해쉬함수, 제1부: 일반모델	IS 10118-1:1994	WG2	
해쉬함수, 제2부 : 대칭형 블럭 암호알고리즘을 사용한 해쉬방식	IS 10118-2:1994	WG2	
해쉬함수, 제3부 : 전용해쉬방식	WG2 / N301	WG2	'96
해쉬함수, 제4부 : 모듈라산술법을 사용한 해쉬방식	WD 10118-4 (WG2 / N302)	WG2	'96
암호알고리즘의 등록절차	IS 9979:1991	WG1	
보안정보객체	SC27 / N872	WG1	'96
IT 보호관리지침, 제1부 : 기본방침과 모델	PDTR 13335-1 (SC27 / N873)	WG1	'95
IT 보호관리지침, 제2부 : 보호관리와 계획	WD13335-2 (SC27 / N874)	WG1	'96
IT 보호관리지침, 제3부 : 보호관리를 위한 기법	WD 13335-3 (SC27 / N875)	WG1	'96
정보보호평가기준을 위한 요구사항 수집 및 분석	WG3 / N83	WG3	
정보보호평가기준, 제1부 : 일반모델	WD (SC27 / N805)	WG3	'96
정보보호평가기준, 제2부 : IT 시스템의 기능등급	WD (SC27 / N806)	WG3	'96
정보보호평가기준, 제3부 : IT 시스템의 보증	WD (SC27 / N807)	WG3	'96
키관리, 제1부 : 골격	WD 11770-1 (SC27 / N871)	WG1	'96
키관리, 제2부 : 대칭형 암호기술을 사용한 키관리 기법	CD 11770-2	WG2	'95
키관리, 제3부 : 비대칭형 암호기술을 사용한 키관리 기법	CD 11770-3	WG2	'95
키관리, 제4부 : 암호적 논리	SC27 / N522 N628	WG2	'97
IT 보호기술 용어	SC27 / N697	WG1	계속
IT 보호의 평가, 검증, 인정 관련 용어	SC27 / N439	WG3	계속
밝힐 수 있는 제3자의 사용과 관리지침	NP (SC27 / N786)	WG1	
해쉬함수 등록절차	NP (SC27 / N761)	WG1	
IT시스템을 위한 보호서비스와 기법의 사용 및 선택 지침	SP (SC27 / N614)	WG1	
안전사고의 보고	NP (WG1 / N457)	WG1	
정보보호 등급	NP (WG1 / N448)	WG1	

* NP: New work item Proposal, SP: Study Period

이러한 작업 내용으로써 암호화, 인증, 무결성, 부인봉쇄, 디지탈 서명, 해쉬함수, 키관리 기법등이 있다. WG3에서는 컴퓨터망, 분산 시스템 및 관련 응용서비스등을 고려하여 정보기술의 보호 평가기준을 개발하며, 정보시스템과 그 구성요소 및 제품의 인증표준을 개발한다. WG3의 이러한 작업은 평가기준 자체의 개발과 평가기준 적용방법의 개발, 그리고 평가, 인증 및 보증기법의 관리절차 개발등 크게 3가지로 구분할 수 있다. 현재 SC27에서 이루어지고 있는 표준화 작업항목과 표준화 현황 및 수행되고 있는 작업반 할당현황등은 표.2와 같다.

4) JTC1내에서의 기타 표준화 활동

JTC1/SC18에서는 사무 및 문서응용과 관련된 국제표준을 개발하는 위원회로 정보보호 기술과 관련하여 분산 사무응용에서 요구되는 정보보호 서비스를 제공하기 위한 내용이 분산 사무응용 모델(DOAM:Distributed Office Application Model) 표준에 규정되어 있으며, 개방형 문서구조 및 상호교환(ODA/ODIF) 표준에 보호기능을 추가하는 작업이 이루어졌다. 또한 ITU-T/SG7의 MHS와 동일한 표준인 MOTIS에 보호기능을 추가하는 작업이 ITU-T와 협력하에 이루어지고 있다. 그리고 JTC1/SC17은 IC-카드에 관한 국제표준을 개발하는 위원회로 IC 카드에서의 인증 및 메세지 암호화등을 위한 서비스, 규약, 기법을 표준화하고 있으며, SC22에서는 POSIX 보호에 대한 표준화 작업이 이루어지고 있다.

2. ITU-TS에서의 보호기술 표준화

ITU-TS에서는 정보보호 기술을 전기통신에 적용하기 위하여 JTC1과 협력하에 표준화 작업을 추진하고 있으며, 주로 데이타통신 및 텔리마틱 응용과 관련하여 ITU-T/SG7과 ITU-T/SG8에서 표준화 작업이 이루어지고 있다. 이밖에도 ISDN에서의 보호 서비스 제공을 위한 방안이 검토되고 있으며, UPT, FPLMTS등과 같은 무선통신 서비스에서의 정보보호를 위한 표준화 작업이 최근 제안되어 표준화 추진을 검토중에 있다.

ITU-T/SG7에서는 데이타통신 전반에 대한 ITU-T 권고를 개발하고 있으며, ITU내에서 OSI에 대한 표준화 작업을 수행하고 있다. ITU-T/SG7에서의 정보보호 기술 표준화와 관련하여서는 JTC1/SC6, SC21, SC27과 협력하에 표준화 작업을 추진중에 있다. ISO 7498과 동일한 내용을 X.800(정보보호 구조) 권고로 채택하였으며, 현재 JTC1/SC6와 SC21에서 표준화가 완료되었거나 완료단계에 다다른 OSI 하위계층 및 상위계층 정보보호 모델과, 보호골격, 보호관리에 대한 표준(안)을 ITU-T 권고로 채택하기 위해 공동작업을 추진하고 있다. 이러한 표준화 작업은 금번회기('93~'96)동안 Q.20(연구과제 20:

ITU-T 적용을 위한 정보보호 서비스, 메카니즘 및 프로토콜)으로 채택되어 수행되고 있다. ITU-T/SG7에서는 또한 MHS, Directory에 보호기능 부가를 위한 표준화 작업을 JTC1/SC18 및 SC21과 협력하에 공동으로 추진하고 있다.

ITU-T/SG8에서는 표준화 대상인 텔리마틱 응용에 정보보호 기능을 부가하기 위한 작업을 추진중에 있으며, 이러한 활동은 JTC1/SC18과 협력하에 이루어지고 있다. 현재 ODA/ODIF에 정보보호 서비스를 추가하기 위한 표준화 작업이 추진되고 있다.

3. ISO/TC68에서의 보호기술 표준화

TC68은 은행 및 금융업무 관련 표준화 업무를 수행하는 기술위원회로 JTC1과는 독립적으로 은행, 금융업무의 관점에서 필요한 보호기술의 표준화를 추진중이다. TC68에서 보호기술 관련 표준화는 SC2에서 메세지 인증에 대해, SC4에서는 메세지 보호에 대해, SC5에서는 EDI와 전기통신에 대해, SC6/WG6에서는 Retail bank에 관한 정보보호 문제를, 그리고 SC6/WG7에서는 IC-카드를 사용하는 은행의 보호구조에 대한 표준화를 다루고 있다.

SC2에서는 메세지 인증과 키 관리, 메세지 암호화 절차, 금융 응용을 위한 데이타 보호골격등의 표준화 작업이 진행되고 있다. SC6/WG6에서는 메세지 인증, 개인식별번호 관리와 보호, 키 관리에 대한 표준화 작업이 이루어지고 있으며, SC6/WG7에서는 금융거래 카드에 정보보호 기능 부가를 위해 암호키 관계, 보호 응용 모듈, 카드 소지자의 확인, 키 관리에 관한 사항을 표준화하고 있다.

4. 기타 표준화 현황

미국의 IEEE에서 이루어지는 표준화 작업 내용중 정보보호 기술과 관련하여 관심을 갖고 추진되고 있는 위원회로는 근거리망의 표준화 작업을 수행하는 IEEE 802위원회와 POSIX 표준을 개발하는 P1003 위원회, 그리고 의료데이타 상호교환 표준을 개발하는 P1157 위원회를 들 수 있다. 이중 특히 IEEE 802 위원회에서는 근거리망에서의 정보보호 서비스 제공을 위해 802.10 작업그룹에서 SILS(Standard for Interoperable LAN Security)라는 이름으로 표준화를 추진중에 있다. IEEE 802.10 위원회에서는 SILS 모델, 데이타의 안전한 교환규약(SDE), 키 관리, 시스템 및 보호관리로 나누어 표준화 작업을 진행중에 있으며, 이중 SDE는 표준화가 완료되어 JTC1/SC6에 국제표준(안)으로 제출된 상태이고, 다른 표준은 현재 802.10 작업그룹에서 검토되고 있는 중이다. OSI 참조모델에 따른 완전한 SILS 모델은 그림 2와 같다.

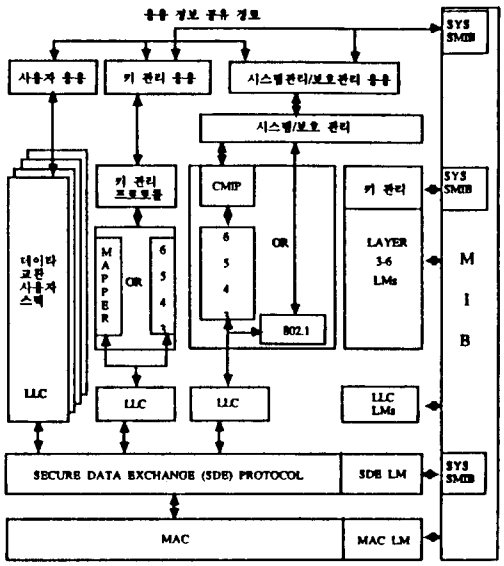

그림 2. 완전한 SILS 모델

유럽 단체중 ECMA는 개방시스템에서의 정보보호 문제를 중요하게 고려하여 개방시스템에서의 보호문제를 다룬 기술문서 TR46을 발표했다. TR46은 종단시스템에서의 보호 개념 및 보호 기능에 대한 많은 견해를 통일시키는데 중요한 역할을 하였다. TR46 이후 ECMA는 "데이타 요소와 서비스 정의"라는 표준 STD138을 개발했다. 이 표준은 OSI 모델의 응용계층에서 사용하기 위한 일련의 보호 서비스와 보호 정보를 정의한다. ECMA에서는 또한 보호 서비스와 보호 서비스에 접근하기 위한 규약을 정의하는 작업을 하며, ISO, ITU-TSS와 협력하에 개방시스템에서의 보호 표준 개발을 위해 노력하고 있다. ECMA에서의 보호기술 표준화 관련 활동은 TC22, TC29, TC32 및 TC36에서 이루어지고 있다. TC22에서는 데이타베이스 시스템의 보호에 대해, TC29에서는 개방형 문서구조(ODA) 보호에 대해, 그리고 TC32/TG6에서는 OSI 하위계층 보호와 ISDN 보호에 대한 표준화 작업을 진행하고 있다. 또한 TC32/TG9에서는

개방시스템 보호에 대한 표준화를 수행하며, 주요 표준화 항목으로는 개방시스템을 위한 보호골격, 보호규약, 데이타 요소와 서비스, 인증과 보호속성, 보호연계 관리등이 있다.

5. 개방시스템 보호기술의 국제기능표준화

현재 국제 표준화 기구를 통해 이루어지고 있는 표준화 작업의 형태는 크게 기본표준화 작업과 기능표준화 작업으로 구분되어 수행되고 있다. ISO, JTC1, ITU-TSS등의 국제표준기구에서 제정하는 표준은 표준화 활동에 참여하는 각 국가의 지역적, 문화적 특성과 기술적 요구사항을 반영하여야 하므로 다양한 환경에서 시스템간 상호접속을 위한 일반적인 절차를 기본표준으로 정의하고, 표준 사용자가 환경과 특성에 따라 기본표준에 존재하는 기능이나 매개변수값을 적절히 선택하여 사용할 수 있도록 허용하고 있다. 따라서 같은 기본표준을 채택한 시스템 사이에도 구현시 선택한 내용에 따라 시스템간 상호접속이 보장될 수 없는 경우가 발생할 수 있게 되었다. 이러한 표준에 따른 구현 제품간의 상호호환성을 높이기 위해 기본표준에 존재하는 선택사항들에 대해 좀 더 구체적으로 규정하여 제품개발자, 구매자, 사용자등 표준의 이용 당사자간에 상호합의한 표준이 기능표준이다. 이러한 기능표준화 작업은 현재 세계적으로 AOW(아시아 대양주 기능표준 워크샵), EWOS(유럽지역 기능표준 워크샵), OIW(미주지역 기능표준 워크샵)라는 3개 지역별 워크샵을 조직하여 수행되며, 각 워크샵을 통해 이견수렴이 완료된 기능표준(안)은 기능표준 활동을 총괄하는 JTC1/SGFS에 제출되어 국제표준으로 제정되는 절차를 거친다.

지금까지 지역별 기능표준 워크샵을 통해 주로 OSI 관련 규약의 기능표준화 작업이 수행되어 왔으며, 정보보호 기술과 관련하여 특히 개방시스템에서의 정보보호 서비스를 제공하기 위한 작업이 진행되고 있다. 이러한 보호기술의 기능표준화 작업은 MHS, 디렉토리, 거래처리등 응용 서비스별로 보호기능을 추가하기 위한 작업과 관리통신에서 보호관리 기능을 지원하기 위한 내용 및 하위계층에서의 보호서비스 제공을 위한 내용으로 나누어 진행되고 있다. 이를 위해 EWOS와 OIW에는 각각 보호기술 위원회가 조직되어 기능표준화 작업을 추진하고 있으며, AOW에서는 응용 서비스별로 보호기술에 대한 기능표준화 작업이 진행되고 있다. 현재 기능표준 워크샵에서 중점 논의되고 있는 개방시스템 보호규약의 기능표준화 항목은 MHS와 디렉토리 및 OSI 관리에서의 보호기능 부가이며, 특히 '93년 말부터 JTC1/SC6에서 기본표준화가 완료되었거나 최종 단계에 다다른 수송계층 및 망계층 보호규약에 대한 기능표준화 작업이 새로운 작업항목으로 채택되어 현재 검토되고 있다. 망계층 보호규약의 기능표준화는 EWOS가 에디터를 맡았으며, 수송계층 보호규약 기능표준화는 OIW가 에디터를 맡았다. 아직까지는 기능표준화 작업이 크게 진전된 것이 없으나 하위계층 보호규약 기능표준화 작업의 지침서 역할을 하게될 "OSI Lower Layer Security Profile Options(Ver.6)"가 EWOS에 의해 작성되어 검토중에 있고, 유럽의 활동이 활발하여 망계층 보호규약 기능표준화 작업은 상당히 빠르게 진행될 것이 예상된다. 우리나라의 경우 AOW에 참가하고 있으나 AOW에는 아직 개방시스템 보호규약 전문가가 부족한 상황이어서 적극적인 표준화 작업이 이루어지지 못하고 있는 상황이다.

Ⅳ. 국내 표준화 활동현황

국내의 경우 정보보호 기술에 대한 연구는 일부 관련 기관에 의해 제한적으로 수행되어 선진국에 비해 상당히 저조한 실정이나, 80년대 부터 통신망의 안전문제에 대해 관심을 갖고 암호화 알고리즘 및 이의 실용화 기술개발 연구가 한국전자통신연구소등에 의해 수행되어 왔다. 1990년 말에는 산,학,연의 정보보호 및 암호화 기술에 대한 정보교류와 연구의 활성화를 위해 한국통신정보보호학회가 설립되어 국내 정보보호 기술 발전에 기여하고 있다. 이와 함께 과학기술처의 지원으로 "데이타보호 기반기술 워크샵"이 매년 개최되어 국내 학계의 정보보호 기술 연구 활성화에 크게 기여하였으며, 체신부에 의해 계속 지원될 전망이다.

한국통신정보보호학회는 국내 정보보호 기술에 대한 연구의 활성화 방안으로 산하에 7개 연구분과위원회를 구성중에 있으므로, 앞으로 더욱 이 분야의 연구가 체계적으로 수행될 수 있을 것으로 기대된다. 현재 학회내에 구성중인 연구분과위원회는 정보보호 표준 연구회, 통신망 보호기술 위원회, 암호이론 연

구회, 컴퓨터시스템 보호 연구회, 컴퓨터바이러스 및 해커 대책위원회, 통신정보보호 정책 연구회, 전산감사 연구회가 있다.

국제표준화 활동과 대응한 국내 표준화 활동의 현황을 보면, 먼저 ISO 및 ISO/IEC JTC1 조직에 대응한 국내 전문위원회가 공진청 산하에 조직되어 있고, 산업표준원이 간사기관 역할을 하고 있다. 즉, JTC1/SC6, SC21, SC17, SC18등 정보보호 기술과 관련있는 국제표준화 조직에 대응되는 국내 표준화 전문위원회가 조직되어 있으나 정보보호 기술에 대한 활동은 거의 이루어지지 않고 있고, 다만 JTC1/SC27 국내 전문위원회를 통해 활발한 표준화 활동이 이루어지고 있다. 그러나 JTC1/SC27의 표준화 대상이 정보보호 기술중 암호화 기술, 보호 메카니즘, 보호 평가기준등에 대한 것으로 제한되어 있으므로, 실제 컴퓨터 시스템이나 통신망 환경에 정보보호 기술을 적용하여 사용자들에게 최종적으로 보호 서비스를 제공 해 주는 분야에 대한 표준화 활동도 강화되어야 할 것이다.

국제표준화 기구중 정보보호 기술과 밀접한 관련이 있는 조직으로 ITU-TSS(구 CCITT)가 있다. 우리나라의 경우 전기통신 표준화와 관련해서는 체신부가 ITU에 통신주관청으로 가입되어 있고, 체신부 산하에 한국통신기술협회(TTA: Telecommunications Technology Association)가 조직되어 ITU의 표준화 조직에 대응되는 국내 표준화 연구위원회를 운영하고 있다. 정보보호 기술과 관련이 있는 ITU-T/SG7 연구위원회등이 운영되고 있으나, 아직 정보보호 기술에 대한 표준화 연구는 미진한 상태이다. 최근 한국통신기술협회는 조직개편을 통해 ITU의 표준화 활동뿐만 아니라 전기통신과 밀접한 관련이 있는 JTC1 표준화 활동에 적극 대응하기 위하여 협회내에 관련 표준화 연구위원회를 구성하였다. 정보보호 기술과 관련이 있는 JTC1/SC6, SC21, SC27에 대응되는 국내위원회가 조직되었으나 이제 시작 단계이므로 앞으로 그 활동이 주목된다. 한국통신기술협회내에 JTC1 관련 연구위원회가 구성됨으로써 ITU와 JTC1에서 이루어지는 표준화 활동이 상호보완적으로 수행될 수 있을것으로 예상되나, 현재 조직되어 있는 공진청 산하 관련 전문위원회와의 관계 및 역할이 검토되어야 할것이다.

국내에서 이루어지고 있는 또 다른 표준화 활동으로 개방형컴퓨터통신연구회(OSIA: Open System Interconnection Association)를 중심으로 한 개방시스템 표준화 활동이 있다. OSIA는 OSI 참조모델에 근거한 개방시스템 관련 연구 활동을 수행하는 조직으로, 응용 서비스의 형태 및 표준화 기술별로 기술위원회를 조직하여 산,학,연의 전문가가 참여하는 가운데 표준화연구 및 기술교류 활동을 수행하고 있으며, 한국전자통신연구소 정보통신표준연구센터의 지원으로 개방시스템 관련 국내표준(안) 개발연구를 수행하고 있다. OSIA 산하에 조직되어 있는 보안기술위원회에서는 컴퓨터 시스템 및 전산망 환경에서 요구되는 정보보호 표준의 연구와 국내 관련 전문가간의 정보교류 및 국내 표준(안) 개발 작업을 추진한다. 금년부터 한국전자통신연구소 정보통신표준연구센터의 지원으로 디지탈서명 국내 표준(안) 개발 작업에 착수하였다.

이러한 국내의 정보보호 기술 표준화 활동은 이제 시작 단계로써 아직 활성화되어 있지는 못하지만, 국가기간전산망 사업등의 국책사업을 통해 정보통신 설비 및 전산망의 보급이 급속히 확대되면서 정보보호 기술의 적용 필요성이 증대되어 체신부에서는 "정보통신 설비에 관한 안전신뢰성 기준"과 "전산망 안전신뢰성 기준"을 고시하였다. 체신부에서 고시한 안전신뢰성 기준은 안전한 통신 서비스를 제공할 수 있도록 통신설비 및 전산망에 대해 기본적인 정보보호 요구사항만을 규정하고 있으나, 정부 차원에서 정보보호의 중요성을 인식하고 대책을 수립하고 있다는 측면에서 중요한 의미가 있다 하겠다.

Ⅴ. 결론 및 향후전망

종래의 산업사회로 부터 정보화 사회로의 이행과 함께 등장한 컴퓨터 범죄등의 각종 위협으로 부터 정보통신망 및 시스템을 안전하게 보호하고, 이용자들에게 안전하고 편리한 정보통신 서비스를 보장하기 위해서는 정보보호 기술의 연구개발이 필수적이며 표준화를 통하여 구체적으로 적용이 가능하다. 본 고에서 고찰한 바와 같이 정보보호 기술의 실용화를 위한 노력이 세계적으로 표준화 활동을 통하여 적극적으로 이루어지고 있음을 알 수 있다. 우리나라의 경우도 정부 주도로 5대 기간전산망 사업등과 같은 대형 프로젝트를 통하여 정보통신망이 구축, 보급되면서 정

보보호의 필요성이 점차 증대되고 있으나 그에 상응하는 연구개발에의 투자가 저조한 실정이다. 특히 이러한 정보보호 기술의 적용 및 실용화를 위해서는 정보보호 기술에 대한 연구개발과 함께 국내 실정에 적합한 정보보호 표준의 개발이 요구되나 아직 본격적인 표준화 연구가 이루어지지 못하고 있는 단계이다. 다행히 한국통신정보보호학회가 설립되어 산학연의 정보보호 기술에 대한 연구활동이 활성화 되어가고 있고, 한국전자통신연구소등의 연구기관에서는 정보보호기술의 실용화를 위한 연구와 함께 표준화 연구가 수행되고 있으며, 한국전산원에서는 행정전산망등 국가기간전산망에 정보보호 기술을 적용하기 위한 연구를 추진하고 있는등 국내에서도 많은 관련 기관에서 정보보호 기술에 대한 연구개발이 이루어지고 있다. 또한 최근 표준화의 중요성이 인식되면서 산업표준원, 개방형컴퓨터통신연구회, 한국통신기술협회등의 표준화 관련 단체에서 정보보호 기술에 대한 표준화 활동이 강화되고 있으므로 앞으로 정보통신 환경에서 요구되는 국내 보호기술 표준이 수립될 것으로 예상된다. 그러나 국내 표준화 연구의 활성화를 위해서는 위와 같이 여러 기관에서 이루어지고 있는 정보보호 기술 관련 연구개발 및 표준화 활동이 서로 밀접한 관련을 가지고 이루어질 수 있도록 추진해야 하며, 각 기관별 적절한 역할분담을 통하여 유사한 활동이 중복되어 일어나지 않도록 해야 할 것이다.

參 考 文 獻

[1] 이용준, 강신각, 진병문, 김영희, "JTC1/SC27의 정보통신 보호기술 표준화 현황", 한국통신정보보호학회 학술발표회, 1991.11.

[2] 이필중, "정보보안기술 '93 국제표준화 총회 참석보고", 한국통신정보보호학회 종합학술발표회, 1993. 11.

[3] 강신각,진병문, "LAN에서의 정보보호모델 분석", 전자통신동향분석, 한국전자통신연구소, 1992.1.

[4] 김영희, 강신각, "OSI 환경에서의 정보보호 모델 분석", TM91-4320-125, 한국전자통신연구소, 1991.12.

[5] 장청룡, "개방형통신 안전기술의 국내외 표준화 동향", 전자공학회지, 제20권 2호, 1993. 2.

[6] ITAEGV, "Memorandum M-IT-06(Draft 2.0): Taxonomy and Directory of European Standardization Requirements for Information Systems Security", ITSTC, October, 1992.

[7] JTC1/SC27/WG1, "WG1 Resolutions", JTC1/SC27/N880, March, 1994.

[8] JTC1/SC27/WG2, "WG2 Resolutions of the 8th Meeting in Trondheim", JTC1/SC27/WG2/N303, March, 1994 .

[9] JTC1/SC27/WG3, "Resolutions of WG3 Meeting", JTC1/SC27/WG3/N195, March, 1994.

[10] JTC1/SGFS, "RWS-CC Program of Work", JTC1/SGFS N1072, December, 1993.

筆 者 紹 介

姜 信 角

1961年 10月 15日生

1984年 2月 충남대학교 전자공학과 졸업(학사)

1987年 8月 충남대학교 대학원 전자공학과(석사)

1984年 3月 ~ 현재 한국전자통신 연구소 정보통신표준연구센터 선임연구원

주관심 분야 : 컴퓨터 네트워크(OSI, 고속통신), 멀티미디어, 통신망 보호