JTC1/SC27의 정보통신 보호기술 표준화 현황

이용준, 강신각, 진병문, 김영회
한국전자통신연구소 표준연구2실

Standardization Activity of JTC1/SC27 for IT Security Techniques

Y.J. Lee, S.G. Kang, B.M. Chin, Y.H. Kim
Standardization Research Section 2, PEC, ETRI

요 약

정보통신 보호기술은 컴퓨터와 컴퓨터 통신망의 이용시에 발생할수 있는 정보의 불법적인 사용 및 파괴를 방지하는 기술이다. 최근 컴퓨터범죄가 빈번하게 발생함에 따라 보안기술에 관한 관심 및 연구, 개발이 크게 증대되고 있으며 이에따라 정보기술의 국제표준화 작업을 수행하는 ISO/IEC JTC1내에 정보기술 관련 보안기술 표준화를 담당하는 SC27을 새로이 발족하였다. 본 고에서는 SC27의 설립 배경, 설립 목적, 조직 구성, 표준화 분야, 주요 표준화 활동현황등에 대해 최근에 개최되었던 세차례의 SC27 총회결과를 중심으로 정보통신 보호기술 표준화에 대한 전반적인 현황을 살펴보았다.

1. 개 요

보안기술의 표준화 활동은 현재 ISO, CCITT, ANSI, ECMA등의 표준화 기구에서 적극적으로 수행되고 있다. 보안기술 표준화의 주요 목적은 첫째로, 암호를 이용한 보안 방법과 보안 서비스를 표준화 함으로써 공중망에서 기밀통신 서비스를 가능케 하고 둘째로, 표준에 기초한 암호장치 및 통신용 보안장비의 양산을 통하여 비용경감을 가능케하는것이다.

이러한 표준화 활동중 가장 적극적으로 보안 관련 기술의 표준화를 추진하고 있는 기관은 ISO내 JTC1(정보처리)과 TC68(은행 및 금융업무)이다. 기존의 JTC1/SC20에서는 보안 기술의 핵심인 데이타 암호화기술 표준화를 수행하고 있었으나, 보안기술 표준화 작업이 JTC1내에서 중복되어 일어나고, 암호화기술 이외에 감사기술등 타 보안기술에 대한 표준화가 요청되게 되자, 1989년 6월에 개최되었던 JTC1 총회에서 SC20을 해산시키고 정보기술 전반에 관한 보안기술 표준화를 수행하는 새로운 위원회를 설립하기로 결정한 결의안 28에 의해 SC27이 설립되었다. SC27은 JTC1 총회의 결의안에 따라 1990년 4월에 스웨덴 스톡홀름에서 제1차 총회를 갖고 위원회의 명칭, 작업범위 및 작업영역, 조직구성등을 결정한 이래로 1991년 4월 동경에서 제2차 총회를, 그리고 10월 브뤼셀에서 제3차 총회를 개최하였다.

JTC1내의 그룹중 보안기술 표준화를 추진하는 관련 위원회로는 SC6, SC17, SC18, SC21, SC27이 있다. 이중 SC6에서는 OSI 환경에서의 하위계층 보안모델과 망계층 및 수송계층의 보안규약을, SC17에서는 IC-카드를, SC18에서는 분산 사무환경에서의 보안요구사항과 ODA/ODIF 보안 표준화 작업을 수행하고 있다. 또한 SC21에서는 OSI 환경 전반에 적용되는 보안구조, 체계 및 상위계층 보안모델과 보안관리에 대해, 그리고 SC27에서는 정보기술 전반의 보안기술 표준화를 추진하고 있다. JTC1에서는 이러한 관련 위원회간에 표준화 작업의 중복을 피하고 작업효율을 높이기 위해 공동 워크샵을 개최하는등 각 위원회간 상호협력과 조정을 위해 노력하고 있다.

본 고에서는 이러한 보안기술의 표준화를 수행하는 상기 위원회중 정보기술 전반에 걸친 보안문제를 다루고 있는 JTC1/SC27의 조직, 작업범위 및 주요 표준화 활동현황등을 살펴보았다.

2. 조직현황 및 작업범위

SC27은 정보기술의 안전 및 보호기술에 대한 국제표준을 작성하는 위원회로 JTC1의 시스템 지원 그룹에 속해있으며 정식명칭은 "IT Security Techniques"이다. 여기서 IT란 정보기술(Information Technology)을 의미한다. SC27에는 작업내용에 따라 세개의 작업그룹(WG: Working Group)이 조직되어 있다. WG1은 보안 요구사항과 서비스 및 지침을, WG2는 보안기술과 메카니즘을, 그리고 WG3는 보안평가 기준을 다루고 있다. SC27의 임원을 보면 SC27 의장은 독일이, WG1은 영국이, WG2는 프랑스가, 그리고 WG3는 노르웨이가 각각 의장 및 간사를 맡아 활동하고 있다.

SC27의 회원에는 정식 투표권을 행사할 수 있는 P-회원국과 투표권이 없는 O-회원국, 그리고 협력회원(Liaisons)이 있다. P-회원국에는 벨기에, 브라질, 캐나다, 중국, 덴마아크, 핀란드, 프랑스, 독일, 이탈리아, 일본, 네덜란드, 노르웨이, 스페인, 스웨덴, 스위스, 영국, 미국, 소련 18개국이 등록되어 있고, O-회원국에는 호주, 오스트리아, 체코, 아일랜드, 이스라엘, 폴란드, 포르투칼, 남아프리카공화국, 대만 9개국이 등록되어 있다. 그리고 협력회원은 JTC1 및 ISO내 타 위원회와 기타 외부기관들로 이루어지며, 현재 SC27에 등록된 협력회원은 <표.1>과 같다.

SC27에서 다루고 있는 작업영역 및 범위는 정보기술 보안을 위한 포괄적인 방법과 기술의 표준화로써, 구체적인 작업 내용으로는 정보시스템의 보안 서비스를 위한 포괄적 요구사항 검증과 보안기술 및 메카니즘의 개발, 그리고 위험분석등과 관련한 보안지침의 개발이 있으며, 또한 용어와 보안평가기준등 지원기술의 개발을 수행한다. 단 암호화 알고리즘 자체의 표준화나 보안 메카니즘을 특정 응용에 적용하는 일등은 SC27의 작업범위를 벗어나는것으로 다루지 않는다.

WG1에서 수행되는 주요 작업항목으로는 첫째로 응용과 시스템 구성요소의 요구사항 검증이 있고, 둘째로는 WG2에 의해 개발되는 보안기술 및 메카니즘을 이용하여 인증, 엑세스 제어, 데이타 무결성 보장, 비밀보장, 관리와 감사등 보안 서비스 표준의 개발이 있으며, 세

째로는 보안 지침, 위험분석등 설명이나 해석을 위한 지원 문서의 작성이 있다. 그러나 WG1의 작업영역이 다양한 분야의 사용자들과 밀접한 관련이 있는 부분이고, 현재 정보통신 환경이 개방 시스템으로 확장되고 있으므로 추후에 더욱 그 범위가 확장될 수 있다.

WG2는 정보기술 분야의 보안기술 및 메카니즘 표준화를 수행하며, 이러한 작업 내용으로써 신분확인, 엑세스제어, 비밀보장, 부인봉쇄, 데이타 정확성 보장 메카니즘의 개발등이 있다. WG2의 작업영역은 WG1이나 기타 표준단체의 요청이 있을때 SC27의 승인하에 결정된다.

WG3는 보안평가기준을 개발하는 실무위원회로 컴퓨터망, 분산시스템 및 관련 응용 서비스등을 고려하여 정보기술의 보안평가표준을 개발하며, 정보 시스템과 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.

JTC1/SC1	용어 및 어휘
JTC1/SC6	시스템간 통신과 정보교환
JTC1/SC17	개인식별과 신용카드
JTC1/SC18	텍스트 및 사무시스템
JTC1/SC21	OSI를 위한 정보검색, 전송 및 관리
JTC1/SC22	WG15 : POSIX
JTC1/SC25	정보기술 장비
JTC1/SWG-EDI	전자 자료교환
TC68/SC2	은행업무 절차 및 조작
TC68/SC6	금융관련 카드, 매체
CCITT/SG VII	Q.19 : 분산응용체계 보안
ECMA/TC32	TG6 : ISDN에서의 암호화 TG9 : 개방시스템에서의 보안

<표. 1> JTC1/SC27 협력회원

3. 주요 작업내용 및 활동현황

3.1 WG 1 (보안 요구사항, 보안 서비스 및 지침)

WG1에서 다루고 있는 주요 표준화 항목으로는 개체인증 메카니즘 모델과 암호화 알고리즘 등록, 보안정보객체, 키 관리체계, 보안 관리지침등이 있으며, 이밖에도 EDI 보안, POSIX 보안등에 대해 타 협력기관과 공동으로 표준화 작업을 수행하고 있다.

개체인증 메카니즘 모델은 JTC1/SC21의 CD 10118-2(인증체계) 문서와의 호환성 검토를 거친후 1991년 4월 총회에서 IS 9798-1로 승인되었다. SC27에서는 암호화 알고리즘을 어떤 특정 방식으로 표준화하지 않고 다양한 알고리즘을 표준화하여 이를 등록시킴으로써 필요에따라 선택사용할 수 있도록 하는 개념을 채택하고 있다. WG1에서는 이러한 암호화 알고리즘을 등록하는 일을 맡고있으며, 등록절차는 현재 DIS 9979로 제정되어 있고 1992년 완료될 예정이다.

현재 WG1에서 중점적으로 논의되고 있는 사항들은 최근에 새로운 문제로 부각되고 있는 보안정보객체, 키 관리체계, 보안 관리지침에 대한것들로 아래에 간단하게 현황을 살펴보았다.

1) 보안정보객체(SIO: Security Information Object)

인증정보, 보안 관리정보, 권한 관리정보와 같이 보안 서비스를 제공하는데 사용되는 정보항목을 보안정보객체라 한다. WG1에서는 이 보안정보객체에 대해 일반적으로 사용될 수 있는 명확한 정의를 내리고, 보안정보객체에 대한 명시의 일관성을 촉진하기 위하여 새로운 작업항목으로 채택하여 JTC1/SC21, CCITT/SGVII/Q.19, ECMA/TC32와 협력하에 표준화를 추진하기 시작했다. 현재 보안정보객체의 모델과 명시체계에 대한 작업초안이 작성되어 논의되고 있는 단계이나 극히 초기단계에 불과한 실정이며, 1994년 국제표준으로 완료할 계획으로 작업을 진행하고 있다.

2) 키 관리체계(Key Management Framework)

키 관리체계 표준화는 특정 암호 알고리즘이나 통신 규약에 의존하지 않는 키 관리 절차 및 요소들을 추상적으로 규정하기 위한것으로 암호키 이용자의 등록과 키 생성, 분배, 저장, 및 관리등에 관한 일반적인 체계를 결정한다. WG1에서 작성하는 본 체계에 따라 WG2에서는 키 관리 메카니즘을 검토하고, 다른 ISO 연구그룹에서는 각 통신 응용에 대하여 본 체계를 WG2의 메카니즘에 준거하여 키 관리 방식을 채택하는 형태로 키 관리에 대한 표준화를 추진하고 있다.

현재 키 관리체계 표준화가 새로운 작업항목으로 채택되어 CCITT/SGVII/Q.19와 공동으로 추진되고 있으며, 작업초안이 작성되어 검토되고 있는단계이다.

3) 보안 관리지침(Security Management Guidelines)

정보시스템 사용자들이 보안 요구사항의 결정과 위험분석을 해야하고, 보안 목적에 부합되는 적절한 해결책을 명시하고 선택해야 하는등 보안관리 필요성이 대두됨에 따라, 이를 지원하기 의한 보안 관리지침 문서를 작성하는 새로운 작업항목을 채택하였다. 관리지침서에는 위험관리와 평가, 취약성 식별과 분석, 보안 생명주기(Life Cycle) 관리, 보안 의식관리와 같은 내용들이 포함되며, 현재 활발하게 연구가 진행되고 있다.

관리지침은 세 레벨로 나누어 검토하는중인데, 레벨1은 기본개념과 모델에 대한것으로 보안요구의 해석, 보안대책 분석 및 실시등을 다루고 있고, 레벨2에서는 위험관리, 보호대책 관리, 시스템 개발 관리, 보안감사 관리등의 관리방법을 다루고 있다. 그리고 레벨3에서는 상기

와 같은 관리를 위한 도구, 기술, 메카니즘을 다룬다.

3.2 WG 2 (보안기술과 메카니즘)

WG2는 WG1에서 표준화한 보안 요구사항과 보안 서비스를 실제로 구현하기 위해 필요한 보안기술 및 메카니즘의 표준화를 수행하며 주요 표준화 분야는 다음과 같다.

1) 암호이용 모드

암호이용 모드는 암호알고리즘을 실제로 시스템상에 구현하기 위한 방식을 말하며 WG2에서는 "64비트 블럭암호 알고리즘"과 "n비트 블럭암호 알고리즘"을 이용한 암호이용 모드를 표준화하고 있다.

64비트 블럭암호 알고리즘의 이용 모드는 이미 1987년 8월에 국제표준인 IS 8372("Modes of operation for a 64-bit block cipher algorithm")로 제정되었으며 계속 수정, 보완이 이루어지고 있는 상태이다. IS 8372는 암호알고리즘을 평문의 매 64비트 블럭마다 동일키로서 그대로 적용하는 ECB(Electronic Code Book), 암호문(ciphertext)블럭을 피드백하여 다음 평문블럭과 모듈러 연산을 취한 다음 암호알고리즘을 실행시키는 CBC(Cipher Block Chaining), CBC를 스트림 방식으로 변환한 CFB(Cipher Feedback), OFB(Output Feedback)의 4가지 이용 모드에 대해 명시하고 있다. IS 8372의 내용은 기본적으로 DES(Data Encryption Standard)의 이용 모드와 동일하나 DES 같은 특정 암호알고리즘 뿐만 아니라 ISO에 등록된 모든 암호알고리즘에 적용이 가능하다.

n비트 블럭 암호알고리즘의 이용 모드는 IS 8372의 64비트 블럭방식을 임의의 n비트 방식으로 일반화시킨 것으로 현재 DIS 단계로 표준화가 진행되어 있으며 곧 IS로 제정될 상태에 와있다.

2) 개체 인증(Entity Authentication)

개체인증 메카니즘은 컴퓨터 통신망을 통해 상대방의 정체를 확인하는 기법이며 SC27에서는 다음과 같이 3개 부분으로 나누어 표준화를 추진하고 있는데 제1부는 앞에서 설명한바와 같이 WG1에서 담당하고 있으며 제2부, 3부를 WG2가 담당하고 있다.

제1부 : 일반 모델

제2부 : 대칭기술을 사용한 개체인증

제3부 : 공개키 알고리즘을 사용한 개체인증

제2부는 대칭 암호화기술, 즉 비밀키 암호알고리즘을 이용하여 통신시에 통신자 간의 상호인증을 구현하는 프로토콜 및 제3의 통신자인 인증 서버가 통신자를 중계하여 상호인증을 수행하는 개념등을 명시하고 있으며 CD 9798-2로 표준화가 진행되어 있다. 제3부는 공개키 암호알고리즘을 이용하여 통신시에 양 통신자 중 한 통신자의 신원을 증명하는 단일 인증(Single Authentication), 양자 모두를 증명하는 상호인증(Mutual Authentication) 프로토콜등을 명시하고 있으며 CD 9798-3으로 표준화가 진행되어 있다.

3) 키 관리

키관리는 암호시스템에서 암호화/복호화를 위한 키를 생성, 분배, 관리하는 것을 말하며 안전한 키관리는 매우 중요한 문제이다. 따라서 WG2에서는 암호화기술을 이용한 안전한 키관리에 대한 표준화를 다음과 같이 3개 부분으로 나누어 추진하고 있다.

제1부 : 키 관리 개요

제2부 : 비밀키 기술을 사용한 키 관리

제3부 : 공개키 기술을 사용한 키 관리

제1부는 키관리를 위한 체계 및 모델, 제2부는 비밀키 방식을 이용한 키관리, 제3부는 공개키 방식을 이용한 키관리를 다룬다. 키관리의 표준화는 아직 시작 단계로서 모든 부분이 WD 단계에 머물러 있으며 공개키 방식이 비밀키 방식 보다 키관리가 용이한 이유로 인해 제3부가 제2부 보다 표준화 활동이 보다 활발한 상태이다. 또한 그외에도 이번 브뤼셀 회의에서 "공개키 등록을 위한 키 관리"에 대한 표준화를 새로 시작하기로 결정하였다.

4) 데이타 무결성(Data Integrity)

데이타무결성은 저장되거나 통신되는 데이타의 정확성을 유지하는 것, 즉 오류 발생, 고의적인 데이타 변경, 데이타 파괴 등을 방지하는 것을 말한다. WG2에서는 데이타무결성 기법을 "암호화기술을 이용한 방식"과 "영지식 기술(Zero Knowledge Techniques)을 이용한 기법"으로 나누어 표준화하고 있다.

암호화기술을 이용한 방식은 메시지인증 코드(MAC: Message Authentication Code)를 송신 데이타에 삽입시켜 암호화한후 수신시에 복호화시켜 MAC의내용을 검사함으로서 데이타의 무결성을 유지하는 방식으로 IS 9797로 표준화되어 있다. 영지식 기술을 이용한 방식은 암호화기술을 이용하지 않고 후에 설명할 영지식 증명을 이용해서 무결성을 검사하는 방식으로 아직 WD 단계이다.

5) 부인 봉쇄(Non-Repudiation)

통신시에 발생한 내용을 통신자가 부인할수 없도록 하는 것으로 상호거래시에 상대방이 거래사실을 부인하지 못하도록 하는데 사용될 수 있다. WG2에서는 대칭 암호화기술을 이용한 부인봉쇄 기법을 표준화하기로 결정하였으나 아직 시작되지 않고 있으며 비대칭 암호화기술, 즉 공개키 암호알고리즘을 이용한 방식도 새로운 Work Item으로 검토되고 있다.

6) 디지탈 서명(Digital Signature)

통신망을 통하여 메시지를 전송할때, 메시지내에 인가된 비밀키로만 생성해낼수 있는 서명을 첨가시킴으로서 메시지의 정당성을 확인하는 기법이다. WG2는 디지탈서명 기법을 복구형("Digital signature scheme giving message recovery)과 부가형("Digital signature scheme with appendix")으로 분류하여 표준화를 추진하고 있다.

복구형은 디지탈서명이 첨부된 메시지가 수신되었을때 디지탈서명이 정당하다고 검증된후에만 메시지가 복구되어 읽혀지는 방식으로 비밀키 암호방식이나 공개키 암호방식을 모두 이용할수 있으며, 부가형은 디지탈서명과 메시지가 동시에 읽혀진후 디지탈서명이 검증되는 방식이다.

현재 복구형만이 표준화가 진행되어 WD 단계에 와있으며 부가형은 아직 표준화가 시작되지 않았으나 이번 브뤼셀 회의에서 표준화를 시작하는 것이 결정되었다.

7) 해쉬 함수(Hash Function)

해쉬함수는 주로 디지털서명시 메시지를 압축함으로서 디지털서명을 보다 효율적으로 수행하기 위해 사용되는 함수로서 다음과 같이 4개 분야로 구분되어 표준화가 수행되고 있다.

제1부 : 일반 모델

제2부 : 대칭 블럭암호 알고리즘을 사용한 해쉬동작

제3부 : Modular Arithmetic을 사용하는 해쉬함수

제4부 : 전용 해쉬함수

제1부는해쉬함수의 요구조건 및 제2, 3, 4부에서 공통으로 사용되는 기법, 제2부는 비밀키 암호방식을 이용한 해쉬함수에 대한 기술, 제3부는 2승합동식을 이용한 해쉬함수등을 다루며 제4부는 일본에서 제안한 N-해쉬 방식과 미국 RSA사에서 제안한 MD4 방식이 표준후보로 상정되어 있다. 제1부와 제2부는 현재 WD 단계로 표준화가 진행되고 있으며 제3부와 제4부는 새 작업항목으로 JTC1에 상정되어 있다.

8) 영지식 증명(ZKIF : Zero Knowledge Interactive Protocol)

영지식증명은 어떤 정보를 알고 있으면서 그내용을 상대방에게 공개하지 않고 상대방에게 자신을 증명시키는 기법으로서 패스워드 방식에 의한 인증방식의 문제점, 즉 패스워드의 노출을 해결할수 있는 기법이다. WG2는 제2차 동경회의에서 영지식 기술에 대한 표준화문서의 구성부분을 다음과 같이 결정하였다.

제1부 : 일반 모델

제2부 : Identity와 Factorization에 근거한 메카니즘

제1부는 영지식증명 기술이 필요한 이유, 전문가이외의 일반인에게 영지식증명을 이해시키기 위한 목적 및 기본 개념을 설명하며 제2부는 영지식기술을 이용한 상호인증 방법에 대해 명시한다. 현재 표준화는 WD 단계이며 이번 브뤼셀 회의에서 그동안 논란이 많았던 영지식기술에 대한 정의를 확정함으로서 중요한 표준 문제가 해결되었다.

3.3 WG 3 (보안 평가)

WG3는 1990년에 설립되어 보안평가의 표준화를 주로 수행하고 있으며 활동기간이 짧은 이유로 인해 WG1과 WG2에 비해 표준화 활동이 활발하지는 못하나 다음과 같은 표준화 과제를 수행하고 있다.

1) 보안 평가기준(Security Evaluation Criteria)

보안평가기준이란 보안제품의 등급을 정하고 각 등급별 제품이 가져야할 보안기능을 정의한 지침을 말하며 보안제품을 명확하게 평가하는데 이용될수 있으므로 매우 중요하다. WG3는 다음과 같은 부분으로 나누어 표준화를 수행하고 있다.

제1부 : 개요 및 모델

제2부 : 정보시스템의 Functionality

제3부 : 정보시스템의 Assurance

제1부는 평가 모델, 평가과정의 흐름도, 평가 항목 등을 명시하며, 제2부와 제3부는 아직 뚜렷한 제안이 없는 상태이다. WG3는 이러한 작업을 미국의 보안 평가지침서인 TCSEC(Trusted Computer Security Evaluation Criteria)에 대항해서 유럽이 최근 개발한 ITSEC(Information Technology Security Evaluation Criteria)에 기초해서 추진하려 노력하고 있으며 현재 표준화는 WD 단계에 와있다. WG3는 '92년 CD, '93년 DIS, '94년 IS를 목표로 표준화를 추진할 계획에 있다.

2) 보안평가기준 요구사항의 수집 및 분석

WG3는 정보기술 보안평가기준에 대한 요구사항의 수집 및 분석 과제에 대하여 각국 표준기구(한국은 공진청) 및 협력기구에게 보안요구사항을 제안하도록 요청하였으며 이를 취합하여 WD로 발표하였다.

그외에도 보안평가기준에 관련된 용어의 표준화를 WG1과 협조하여 수행하고 있다.

3.4 주요 작업항목별 표준화 현황

SC27이 추진하고 있는 보안 표준화작업의 주요 작업항목과 각 항목의 표준화 현황을 요약하면 <표.2>와 같다.

4. 향후전망

SC27은 기존의 SC20에서 수행하던 데이타 암호화 관련 표준화 작업들을 넘겨받고, 개방 시스템 환경에서 적용될 다양한 정보 보안기술 표준화를 추진하기 위한 새로운 작업항목들을 추가하여 점차 표준화의 범위를 넓혀가고 있다. 현재 검토되고 있는 새 작업항목으로는 Modular Arithmetic을 사용한 해쉬함수와 전용 해쉬함수에 대한 표준화를 계획하고 있으며 현재 JTC1의 승인을 요청해놓고 있는 단계이다. 또한 1990년 4월에 작업항목으로 채택하였으나 작업이 저조했던 부인봉쇄 메카니즘의 경우 이를 일반모델, 대칭 암호화기술을 사용한 부인봉쇄, 비대칭 암호화기술을 사용한 부인봉쇄로 세분하여 표준화를 추진하기로 결정하고 JTC1의 승인을 기다리고 있다.

이밖에 보안과 관련되는 용어의 표준화와 각종 보안 서비스 및 메카니즘의 확대 개발을 추진중에 있으며, 특히 보안정보객체, 보안지침, 보안평가기준등의 항목은 최근에 대두된 이슈들로 표준화의 초기 단계이고, 그 개념이 확실하게 정립되지 않은 분야들로 각국의 전문가가 많은 관심을 가지고 표준화를 추진하고 있다.

번호	제 목	현황 (문서번호)	담당
JTC1.27.01	Modes of operation for a 64-bit block cipher algorithm	ISO 8372	SC27
JTC1.27.02	Modes of operation for n-bit block cipher algorithm	DIS 10116	WG2
JTC1.27.03.1	Entity authentication mechanisms, part 1 : General Model	DIS 9798-1	WG1
JTC1.27.03.2	Entity authentication mechanisms, part 2 : Entity authentication using symmetric techniques	DIS 9798-2	WG2
JTC1.27.03.3	Entity authentication mechanisms, part 3 : Entity authentication using a public key algorithm	CD 9798-3	WG2
JTC1.27.04	Data cryptographic techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm	ISO 9797	SC27
JTC1.27.05	Integrity mechanism using zero knowledge techniques	WD (N78)	WG2
JTC1.27.06	Non repudiation techniques using symmetric encipherment algorithms	WD (N209)	WG2
JTC1.27.07	Digital signature scheme giving message recovery	WD (N236)	WG2
JTC1.27.08	Digital signature with appendix	없음	WG2
JTC1.27.09.1	Hash functions for digital signatures and authentication mechanisms, part 1 : General Model	WD (N109)	WG2
JTC1.27.09.2	Hash functions for digital signatures and authentication mechanisms, part 2 : Hashing operation using a symmetric block cipher algorithm	WD (N110)	WG2
JTC1.27.10	Register of encipherment algorithms	DIS 9979	WG1
JTC1.27.11.1	Cryptographic mechanisms for key management, part 1 : Key Management overview	WD	WG1
JTC1.27.11.2	Cryptographic mechanisms for key management, part 2 : Key Management using secret key techniques	WD (N15)	WG2
JTC1.27.11.3	Cryptographic mechanisms for key management, part 3 : Key Management using public key techniques	WD (N82)	WG2
JTC1.27.12	Key management for public key register	없음	WG2
JTC1.27.13	Security Information objects	WD (N226)	WG1
JTC1.27.14	Guidelines for the management of IT security	WD (N227등)	WG1
JTC1.27.15	Collection and analysis of requirements for security evaluations and criteria	WD (N234등)	WG3
JTC1.27.16	Evaluation criteria for IT security	WD (N235)	WG3
JTC1.27.17	Zero knowledge techniques	WD (N221등)	WG2
JTC1.27.18	Key management	WD (N229등)	WG1, WG2

<표.2> SC27의 보안 표준화 현황 ('91.10 현재)

5. 결 론

SC27의 표준화 활동은 SC27이 아직 설립된지 얼마되지 않아 현재까지는 활발하게 진행되지 못하였으나 그동안 3차에 걸친 회의를 통해 보안기술 표준화를 위한 준비가 어느정도 마무리됨에 따라 앞으로 활발한 표준화 활동이 시작되리라고 예상된다. 특히 이번 제3차 브뤼셀 회의에서 대부분의 표준화 작업항목을 1993년까지 IS 단계로 진행시키는 것을 목표로 하고 이를 위해 다른 표준화기구와의 협력을 강화하기로 결정함에 따라 보안기술의 표준화가

앞으로 더욱 신속하게 진행되리라고 생각된다.

SC27은 아직 초창기인 SC이고 참여인원이 비교적 적은 소규모 SC이나 보안기술의 중요도로 볼때 발전 가능성이 크며, 보안기술의 연구, 개발이 군이나 정부기관을 중심으로 이루어져 일반인에게 기술공개가 통제되어 온데 반해 SC27에서는 표준화기구의 성격상 모든것이 외부에 공개되어 있으므로, SC27회의에는 군이나 정부기관 이외에도 일반 기업체나 학계에서 많은 인원이 참여하고 있다. 또한 일본에서도 SC27에 많은 관심을 갖고 2차 SC27회의를 동경에서 개최한 바 있으며 다수의 기고문을 제출하는등 활발한 참여를 하고있다.

우리나라의 경우 선진 각국에 비해 정보기술 분야가 상대적으로 뒤져 있으므로 SC27과 같은 표준화 기구의 설립 초창기부터 적극적인 참여 및 활동이 요구된다. 현재 주요 JTC1의 국내위원회가 조직되어 활동하고 있는것과 같이, SC27 국내위원회를 조직하여 보안기술에 관심을 갖고있는 국내 각계 전문가들이 JTC1/SC27의 활동에 적극적으로 참여할 수 있도록 추진하는 방안 및 SC27에의 정식 회원국으로 가입하는 문제들이 앞으로 신중하게 고려되어야 할 것으로 생각된다.

참고문헌

1. 이용준, 진병문, 김영회, 강신각, "정보통신 보안기술의 연구 및 표준화 동향", 전자통신연구소 표준연구2실 Technical Memo, 1991.10.

2. ISO/IEC JTC1/SC27 N190, ISO/IEC JTC1/SC27 Secretariat's Report to SC27 2nd Plenary Meeting, 1991.4.

3. ISO/IEC JTC1/SC27 N217, Resolution of 2nd meeting of JTC1/SC27/WG1, 1991.4.

4. ISO/IEC JTC1/SC27 N218, Recommendation taken at 2nd SC27/WG2 meeting, 1991.4.

5. ISO/IEC JTC1/SC27 N219, Convenor's Report of JTC1/SC27/WG2, 1991.4.

6. ISO/IEC JTC1/SC27 N232, Convenor's Report to SC27 Plenary (JTC1/SC27/WG1), 1991.4.

7. ISO/IEC JTC1/SC27 N233, Resolution taken at 2nd meeting of SC27/WG3, 1991.4.

8. ISO/IEC JTC1/SC27 N290, ISO/IEC JTC1/SC27 Secretariat's Report No.3 for presentation to 3rd JTC1/SC27 Plenary, Brussels, Belgium, 1991-10-17/18.

9. ISO/IEC JTC1/SC27 N324, Resolution taken at the Brussels Meeting of JTC1/SC27/WG1, 1991.10.14.

10. ISO/IEC JTC1/SC27 N325, Resolution taken at the Brussels Meeting of JTC1/SC27/WG2, 1991.10.14.

11. ISO/IEC JTC1/SC27 N326, Resolution taken at the Brussels Meeting of WG3, 1991.10.14.

12. ISO/IEC JTC1/SC27 N327, Resolution taken at the Plenary meeting of ISO/IEC JTC1/SC27, Brussels, 1991-10-17.

13. Kouji NAKAO, "Standardisation Activity on Security", 일본전자정보통신학회지, ISEC 90-7, 1990.

14. Kouji NAKAO, Kazuo OHTA, Tomoyuki SUGA, "Trends on International Standardisation of ISO/IEC JTC1/SC27", 일본전자정보통신학회지, ISEC 91-4, 1991.