通信情報保護學會誌
第2卷, 第1號, 1992. 3

정보통신 안전기술의 국제표준화

장청룡* · 원동호**

요 약

정보화사회로의 진행과정에서 공중통신망을 통합 가입자 상호간의 정보유통은 사회경제 활동의 고도화에 따라 더욱 다양하고 다량화될 전망이다. 이들 가입자 상호간에 유통정보를 안전하고 신뢰성있게 전달하기 위하여 안전 서비스 요구는 필연적이 될 것이다.

이러한 안전 서비스의 제공을 위해서 사업자 측면에서는 관련 장비의 상호운용성 확보와 연구개발 또는 도입 제품 평가의 용이성을 위하여 표준화가 요구되며 제품생산자 측면에서는 생산 원가의 저렴화를 위하여 반드시 표준화가 필요하다.

본고에서는 안전 기술의 표준화 연구를 수행하는 주요 국제기구인 ISO/IEC, CCITT 등의 활동 중 특히 ISO/IEC JTC1의 SC 27(정보기술－안전기술)에서의 브뤼셀 회의 결과('91. 10)와 CCITT SG VII(데이터통신)의 4차 회의결과('91. 9)를 중심으로 안전기술 분야의 최근 표준화 활동을 소개함으로써 통신사업자가 정보통신사업에 필요한 안전 기술 및 이의 표준화 방향을 제시하고자 한다.

1. 서 론

정보시스템이 고도 정보화 사회에 있어 주요한 역할을 담당함에 따라 신뢰성 및 안전성이 우수한 시스템을 설계하는 것이 중요하게 된다. 정보시스템의 안전에는 재해, 고장 등에 의해 우연히 발생하는 시스템의 이상을 검출, 회복 또는 회피할 수 있는 신뢰성과 이에 추가하여 시스템에 대한 의도적인 부정공격(예, 데이터의 도청, 변조)을 검출 또는 방지할 수 있는 안전성을 합친 "광의의 정의"와 부정공격에 대한 안전성만을 의미하는 "협의의 정의"가 있다. 본고에서는 주로 협의의 안전에 대하여 개방형 통신시스템에 적용 가능한 안전기술의 국제표준화를 다루도록 한다.

우선, 안전 기술의 표준화 필요성에 대하여 생각해 보기로 한다. 하나의 장치내에 폐쇄된 안전대책은 각 장치에서 개별적으로 대처가 가능하다. 그러나 예를들어 회선상의 데이터를 도청이나 변조로부터 보호하려면 회선상의 데이터 암호화 절

* 한국통신 연구개발단
** 성균관대학교 정보공학과

차를 송신, 수신장치간에 미리 정하여 놓을 필요가 있다. 특히 통신망을 개재시켜 불특정 다수의 암호화 이용자가 자유로이 통신할 수 있게 하려면 통신프로토콜과 동일하게 암호화 절차에 대해서도 암호 알고리즘이나 키 배송절차 등을 표준으로 규정하여 놓을 필요가 있다. 이러한 표준화에 의해 통신사업자는 구축설비 상호간 상호운용성의 확보와 유지 보수의 용이성을 제고할 수가 있다. 또한 표준화의 다른 이점으로 생산업자에게는 양산화에 수반되는 제품 비용의 저렴화를 기대할 수 있다.

본고에서는 정보통신을 위한 개방형 시스템에 적용 가능한 안전기술 표준화 대상과 주요 국제표준화 기관들의 표준화 범위를 살펴보고 정보통신의 안전기술 표준화 활동에 대하여는 이미 많은 자료에 소개된 바 있으나 여기서는 1991년 10월 브뤼셀에서 개최된 ISO/IEC JTC1/SC27회의의 내용과 1991년 9월 제네바에서 개최된 CCITT SG VII 회의 내용을 중심으로 국제표준화의 최근 동향을 소개한다. 끝으로 국내에서의 안전기술 표준화 동향과 통신사업자로서 현 사업환경에서 고려할만한 안전 서비스와 이의 표준화 방향을 제시하고자 한다.

2. 안전 표준의 형태와 분류

가. 기본 표준

이 표준에는 지네릭 유저 요구사항을 만족시키기 위한 일반 컴퓨터 시스템, 네트워크 및 IT(Information Technology)의 이용과 적용에 관한 광범위하고 복잡한 문제들을 적절히 다루기 위하여 필요한 기술적 표준들을 포함한다. 이 분야의 작업은 현재 다음과 같은 내용을 포함한다.

- 구조, 프레임워크 및 모델
- 서비스 및 프로토콜
- 응 용
- 기술 및 메카니즘
- 관 리

나. 기능표준 또는 프로파일

이 표준은 조달, 제품검정 및 서비스공인을 위하여 특히 유용하다. 이것은 근본적으로 비전문가들로 하여금 기본표준이 근본 제정취지 및 목적을 이해할 수 있도록 하는 공통적으로 산업분야에서의 접근 방식이다. 이것은 일반적으로 기능적 적합성을 검증하기 위한 참조시스템으로서 사용하기 위하여 이용자, 생산자, 설계자들에게 기본표준의 선택 사항 중 축소된 세트를 제공한다. 이 분야의 주요 활동기관은 NOIW(NIST OSI Implementors Workshop), EWOS(European Workshop for Open Systems), MAP/TOP(Manufacturing Automation Protocol/Technical and Office Protocol) 및 COS (Corporation for Open Systems)가 있다.

다. 산업표준 및 시행규칙(Codes of Practice)

이러한 형태의 표준은 관련사업 또는 업무의 성격에 상응하는 특정 이용자 그룹 또는 산업에 의해 요구되는 기술적 및 절차적 표준이 이에 포함된다. 시행규칙은 이의 이용자 그룹의 구성원을 위한 품질표준에 대한 이용자 그룹의 요구사항의 특별한 경우이다. 이러한 시행규칙은 일반적으로 지엽적인 문제로서 운영되는 반면 적합성 문제는 보통 동등 그룹관리를 통한 자발적인 형태로서 운영된다.

라. 해설문서

여기에는 안전 요구사항과 관련된 표준의 사용과 규격화시 이용자/구매자/표준개발자들을 도와주고, 정보를 제공하며 또한 교육용으로 필요한 지침서, glossary 및 기타 해설자료가 이에 해당된다.

3. 안전기술 표준화 범위

가. 개방형 통신시스템에서의 안전기술 표준화 대상

개방형 통신시스템의 서비스를 이용하는 정보통신 가입자에게 보다 안전하고 신뢰성있게 정보통신

서비스를 제공하기 위하여 요구되는 안전기술의 표준화 대상을 구조, 프레임워크, 모델 및 기술로 분류할 수 있으며 이들의 세부적 표준화 항목은 (그림 1)과 같다.

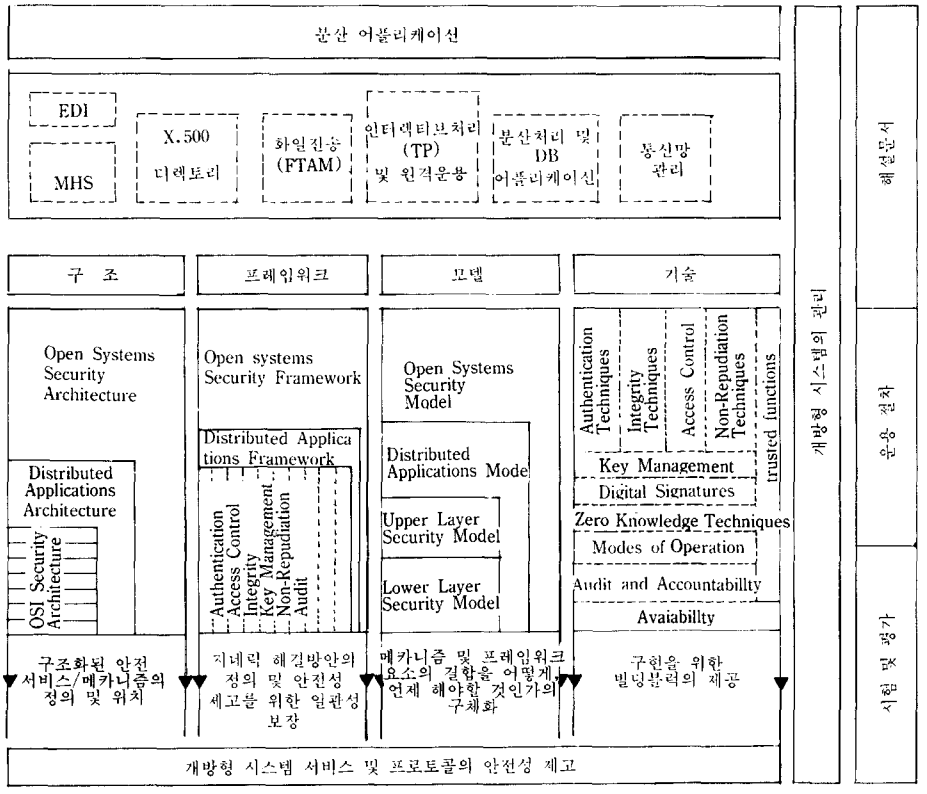

그림 1. 개방형 통신시스템에서의 안전기술 표준화 대상

나. 표준화기관들의 안전기술 표준화 업무 범위

가. 항에서 언급된 많은 안전기술 표준화 대상에 대하여 ISO/IEC의 JTC1, CCITT SG VII 등에서는 서로의 목표분야를 위하여 각자 또는 합동으로 안전기술 표준화 업무를 수행하고 있으며 그들의 표준화 업무범위는 (그림 2)와 같다.

4. 정보통신 안전기술의 국제표준화 활동

안전기술 표준화 분야에서 국제 및 유럽지역의 주요 활동기관으로서는 ISO/IEC, CCITT, ECMA (European Computer Manufacturers Association), EWOS(European Workshop for Open Systems) 및 ETSI(European Telecommunication Standards Institute)가 있다. 이들 기관에서 표준개발을 위해 참여하는 연구그룹중 본절에서는 ISO/IEC JTC 1과 CCITT 활동을 중심으로 소개한다. 또한 이들 국제 표준화기관에 협력하는 국가수준의 연구기관으로는 IEEE, NIST, ANSI, IFIP(International Federation for Information Processing) 등이 있으며 이들도 안전기술에 관한 표준화 활동을 수행하고

있다.

가. ISO/IEC JTC1

ISO에서는 특정 정보통신 응용에 의존하지 않고 정보 안전기술에 관한 연구그룹을 ISO/IEC JTC1 SC27(Security Techniques)로 독립시켜 운영하고 있으며 이는 JTC1의 기존 SC20(Cryptographic Techniques)의 업무를 흡수하여 수행하게 함에 따라 SC20는 그 운영이 중지되었다. 한편 SC27에서 다른 관계 연구 그룹들과 긴밀한 업무교섭을 취하면서 표준화 활동을 하고 있다. ISO/IEC의 JTC1, ISO TC 68등 정보기술 안전에 관한 표준화 현황은 표 1과 같으며 본항에서는 지난 91년 4월 동경 및 91년 10월 브뤼셀에서 개최된 JTC1 SC27 전체 회의의 주요 결정사항을 WG별로 소개하고자 한다.

		사용 범위						응용 서비스									
		OSI/개방형 시스템	텍스트 및 사무용 시스템	무역 시스템	금융 및 유통 시스템	정보 시스템	안전 시스템	메시징	화일 전송	인터랙티브처리	EDI 응용	분산 사무용 서비스	분산처리	DB 응용 서비스	O/S 응용 서비스	통신	관리
ISO/IEC/JTCI	SC 6	M														M	
	SC 14		I	I							I	I					
	SC 17	G	G	G	G	G				G	G	G				G	
	SC 18		M					M	I		I	M	I	I	I	I	
	SC 21	M, F	I, F	I	I	I		I, F	M, F	M, F	I, F	I, F	I, F	M, F	I	M, F	M, F
	SC 22	G	G	G	G	G	G					G	G	G	G		G
	SC 27	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
ISO	TC 46					I								I	I		
	TC 65						I	I	I				I	I	I	I	
	TC 68	I		I	M					I	I					I	
	TC 154	I	I	I						I	I						
	TC 184	I				I		M	M				M			M	
CCITT	SG VII	M, F	M, F	I	I	I		M, F	I, F	M, F	M, F	M, F	M, F	I, F	I	M, F	M, F
ECMA		M, F	M, F	I	I	I		I, F	I, F	I, F	I, F	M, F	M, F	I, F	I	I, F	I, F
ETSI		G	G	G	G	G	G	M								M	
ETSI/EWOS		I	I	I	I	I											

M : 현재의 표준화 주관심분야 G : 일반적인 응용을 할 수 있는 표준의 생산
I : 표준화 관심 분야의 하나 S : 안전 요구사항을 지원하는 지네릭 기술 및 메카니즘의 생산
F : 안전 요구사항을 지원하는 지네릭 구조, 프레임워크 및 모델의 생산

그림 2. 표준화기관들의 안전기술 표준화 업무범위

* 범례 : IS : International Standard
DIS: Draft IS
CD : Committee Draft
WD: Working Draft
NP : New work item Proposal

표 1. ISO/IEC의 안전기술 표준화 현황

기관 및 표준화 과제	상 태	관련 문서
ISO/IEC		
JTC1(정보기술)		
◦ SC6(시스템간의 통신 및 정보교환)		
· WG3－망계층	NP	SC6N274
－망계층 안전		
· WG4－전달계층		
－OSI 하위계층 안전 모델	Early WD	SC6N5333
－전달계층 안전 모델	NP	SC6N529
◦ SC14(EDI 안전)		
◦ SC17(IC 안전)		
· WG4－IC 카드		
· ID 카드 : 접점이 있는 IC 카드		
－part 1 : 물리적 특성	IS	IS 7816－1
－part 2 : 접점의 번호와 위치	IS	IS 7816－2
－part 3 : 전자 신호 및 교환 프로토콜	IS	IS 7816－3
－part 4 : 정보교환용 부호	DIS	DIS 7816－4
• SC18(Text 및 Office System)		
· WG1－사용자 요구조건 및 관리 지원		
－안전에 과한 사용자 요구조건	WD	SC18WG1N497
－ISO 8613에의 부록안의 제안 (안전에 관한 Office Document Architecture(ODA) 및 상호교환포맷)	부록안의 제안	SC18N2003
• SC20(데이터 암호기술)	본 표준화 업무는 신설된 SC 27에서 계속하기로 함	

기관 및 표준화 과제	상 태	관련 문서
• SC21(OSI를 위한 정보검색, 전달 및 관리)		
· WG1－OSI 구조		
－SC21의 안전 조정	계 속	SC21N2540
－Open System의 안전 개요(Roadmap)	WD	SC21N42
－OSI 안전 구조	IS	IS 7498－2
－Open System을 위한 안전 프레임워크：		
－part 1：프레임워크 개요	Early WD	SC21N4210
－part 2：인증 프레임워크	DP	SC21N4207
－part 3：접근제어 프레임워크	Mature WD	SC21N4206
－part 4：부인봉쇄 프레임워크	Early WD	SC21N4209
－part 5：무결성 프레임워크	Outline WD	SC21N4208
－part 6：비밀 프레임워크	Outline WD	SC21N3618
－part 7：감사추적 프레임워크	Early WD	SC21N3775
－part 8：키 관리		
· WG4－OSI 관리		
－OSI 안전관리－7차 초안	Mature WD	SC21N4091
－OSI 시스템관리－part x：안전 감사추적기능	WD	SC21N4092
－OSI 시스템관리－part 7：안전 정보보고기능	DP	SC21N4064
－OSI 적용을 위한 접근제어	WD	SC21N4094
－안전 감사추적을 위한 프레임워크	Mature WD	SC21N4093
－디렉토리 인증	IS	9594－8
－디렉토리 접근제어(3 parts)	DP	SC21N4041～3
· WG5－특정 응용서비스		
－거래처리 안전 요구조건	WD	SC21N3379
· WG6－OSI 세션, 프리젠테이션 및 공통 응용서비스		
－ACSE 인증：Addendum 1：Association설정 동안 등등 엔터티 인증	IS addendum	IS8649
－OSI 상위계층 안전 모델	Early WD	SC21N4109
· WG7－개방형분산처리(ODP)		
－ODP에 대한 안전 개념	WD	SC21N066
◦ SC22(운영체제 안전)		
◦ SC27(정보기술－안전기술)	세부 표준화 활동 결과는 4절 가. 항 1) (ISO/IEC JTC1 SC27의 안전기술 표준화 활동)참조	
－IT－안전을 위한 지네릭 방법 및 기술의 표준화		
· WG1－안전 요구조건, 안전 서비스 및 가이드라인		
· WG2－안전 기술과 메카니즘		
· WG3－안전 평가기준		

기관 및 표준화 과제	상 태	관련 문서
TC46 : 정보시스템 안전 TC65 : Safety Critical Security TC68 : 은행 및 관련 금융서비스 ◦ SC2－운용 및 절차 · WG2－메세지 인증(Wholesale Banking을 위한 안전) • SC6－금융거래카드, 관련 미디어 및 운용 · WG6－Retail Banking에서의 안전 · WG7－IC 카드를 사용한 Banking System의 안전 구조 TC154 : EDI 안전		

1) ISO/IEC JTC1 SC27의 안전기술 표준화 활동

가) SC27/WG1(안전 요구조건, 안전 서비스 및 가이드라인)의 활동목표 및 추진결과

WG1에서는 특정의 통신 어플리케이션에 의존하지 않는 정보안전기술에 관한 안전성의 요구조건이나 필요로 하게 되는 안전서비스를 추출하여 IT(정보기술) 분야에 있어서의 안전기술 프레임워크를 구축하는 것을 목적으로 한다. 구체적으로는 '부인봉쇄서비스'를 연구하는 경우 그 서비스에 필요한 요구조건과 이용방법(가이던스)를 여러가지 측면에서 검토하여 ISO의 여타 연구그룹에서 이용 및 활용할 수 있도록 환경을 구축하는 것을 목표로 한다. 이를 위하여 계도적 해설서를 작성하기도 한다.

또한 WG1에서 구축한 안전 서비스에 준거하여 WG2에서는 암호화 기술 등을 이용한 안전 메카니즘을 연구한다. WG1에서의 표준화 추진결과는 표 2와 같다.

표 2. JTC1 SC27 WG1의 표준화 추진결과

과 제 명	내 용	동경회의 주요 결정사항	브뤼셀회의 주요결정사항
안전정보 오브젝트 (JTC1. 27. 13)	· 정보를 상대 시스템으로 전송하는 기본적 통신형태에 있어 가장 중요한 것 중 하나는 안전을 확보해야 할 "정보 오브젝트"임 · 인증정보, 안전관리정보, 특허관리정보 등으로 안전을 취급하기 위해 중심이 되는 오브젝트	이상적인 작업초안의 완성단계 (WG1/N110)	· NP : 신규과제로 승인하여 JTC1에 제출 (SC 27 N327, WG 1/168) · WG 1/N169를 WD로 하여 각국에 기고요청

과 제 명	내 용	동경회의 주요 결정사항	브뤼셀회의 주요결정사항
IT안전을 위한 관리 가이드라인 (JTC1. 27. 14)	· 이용자가 어떻게 안전성을 생각하고 관리하면 좋을 것인가의 작성을 목적으로 함.	-제 1 레벨 : 기본방침과 모델 · 안전요구의 해석(리스크분석), 안전 대책분석, 실시 등을 연구 -제 2 레벨 : 관리방법, 리스크보호대책, 시스템구성, 개발, 감사 등의 관리방법 연구 · 상기레벨에 있어서 관리를 위한 방식, 기술 및 메카니즘 연구	· 본 과제의 주제명을 "Guidelines for the Management of IT Security"로 확정하고 JTC 1에 필요한 조치 요청 · WG 1/N174를 본 표준화의 초기 초안으로 하여 이에 대한 각국의 기고 요청
키 관리 (JTC1. 27. 18)	-일반적인 암호키 관리방식의 국제표준 규정 -키 관리를 위한 프레임워크의 검토 · 특정 암호알고리즘, 해쉬함수 또는 특정 통신프로토콜에 의존하지 않는 키 관리를 위한 절차요소를 추상적으로 규정 · 암호키의 이용자 등록, 생성, 배포, 실장 및 관리 *WG2에서는 키 관리 메카니즘(비밀키 암호, 공개키 암호)을 검토	-이상적인 작업초안의 완성단계 (WG1/ 1063)	-NP 신규과제로 승인하여 JTC1에 제출 · Part 1 : 프레임워크 (SC27N329, WG1/N175) · WG1/N177을 WD로 하여 이의 기고 요청 -키관리의 NP가 승인되어 기존에 WG1과 WG2가 공동으로 수행하던 "Cryptographic Mechanisms for Key Management"(JTC1. 27. 11)을 "Key Management Framework"(JTC1. 27. 18)으로 변경
인 증 (JTC1. 27. 03. 1)	-인증을 위한 일반 모델(IS 9798-1)의 구축을 진행 -본 모델은 SC21에서 개발된 인증 프레임워크에 준거하여 인증 메카니즘을 위한 기본 모델 -CCITT SG VII에서의 디렉토리 이용자 인증과 긴밀한 협력관계 유지	-국제표준 IS 9798-1으로 결정(SC27 N230)	

나) SC27/WG2(안전기술과 메카니즘)의 활동목표 및 추진결과

본 그룹은 SC27/WG1에서 추출된 안전 서비스에 필요로 하게 되는 안전기술과 메카니즘을 표준화함을 주목표로 하며 비 암호방식을 이용한 안전기술에 대하여도 표준화함을 목표로 한다. WG2에서의 표준화 추진결과는 표 3과 같다.

표 3. JTC1 SC27 WG2의 표준화 추진결과

과 제 명	내 용	동경회의 주요 결정사항	브뤼셀회의 주요결정사항
64비트 블럭암호 이용모드 (JTC1. 27. 01)	-64비트 블럭암호 이용모드(IS8372) · ECB(Electronic Code Book) 모드 : 64비트 블럭암호 알고리즘을 그대로 이용 · CBC(Cipher Block Chaining) 모드 : 암호출력 데이터에 다시 암호화와 Exclusive OR의 조작 · CFB(Cipher Feedback) 모드 · OFB(Output Feedback) 모드	1987년 8월에 IS8372로 표준화됨	IS 8372(1987)의 검토를 차기 SC27 전체회의에서 하도록 준비
n 비트 블럭 암호이용모드 (JTC1. 27. 02)	-DIS 10116에서는 64비트 블럭암호를 n비트 블럭암호로 일반화한 암호이용모드를 검토	국제표준 IS 10116으로 표준화할 것을 결정(SC27 N222)	-DIS 10116의 처리 (Model of operatioon of n-bit block cipher algoritm)
상대방 인증 (JTC1. 27. 03)	-통신상대가 정당한 상대인가를 인증하기 위한 메카니즘 · part1 : General model +프레임워크, 여타 part에서 공통으로 사용되는 기술을 규정 · part2 : Entity authentication using symmetric algorithms +비밀키암호의 이용 +메카니즘 : ┌ 2개의 Entity만의 경우, └ 제3의 통신자인 인증 서버를 개재시킨 경우 · part3 : Entity authentication using public key techniques +공개키 암호의 이용	· 국제표준 9787-1로 표준화할 것을 결정(SC27 N230) · 당초 RSA 알고리즘을 이용하는 것으로 하여서술 되었으나 RSA 알	-국제표준 9798의 처리 · part1의 최종판(ISO/IEC 9798-1)의 발간 -CD 9798-2 초안을 재작성하여 차기 WG회의에서 3차 CD 투표위한 준비

과 제 명	내 용	동경회의 주요 결정사항	브뤼셀회의 주요결정사항
	1)Single Authentication : 통신하고 있는 양자중에서 한쪽측만이 신원을 증명할 수 있음 2)Mutual Authentication : 통신하고 있는 양측 모두가 신원을 증명할 수 있음	고리즘이 암호 알고리즘으로 간주되어 이에 관한 서술이 삭제되었으며 RSA 알고리즘의 복호화에 의해 실현할 수 있는 '서명'이나 RSA 알고리즘의 암호화로 실현할 수 있는 '서명검증'을 추상화한 기술에 의하여 서술하기로 함	· CD 9798-3 초안의 기술적 내용변경으로 재작성하여 차기 WG 회의에서 CD 투표를 위한 준비
데이터 무결성 (JTC1. 27. 05)	-통신데이터의 변조유무를 검출하기 위하여 변조검출에 사용되는 메세지 인증자(MAC : Message Authentication Code)를 생성하여 검증하는 메카니즘 -ISO/IEC 9797에서는 송신자와 수신자에서의 MAC 생성법으로서 n비트 블럭암호화와 2개의 비밀키를 사용하는 것을 규정하였음	1988. 6에 ISO/IEC 9797로 표준화 되었음	ISO/IEC 9797(JTC1. 27. 04)의 결함이 제시되어(WG2/N87) 이를 인정하여 개정안 작성 준비
비밀키암호를 이용한 부인 봉쇄 (JTC1. 27. 06)	-서명자가 서명한 사실을 차후에 부인하는 경우 사실관계의 판정 -신뢰할 수 있는 센터가 양자간의 거래 데이터로그를 축적하는 방식과 하지 않는 방식으로 분류		· ad hoc 그룹의 권고를 기초한 새로운 초안작성을 '91말까지 완료
영지식증명을 이용한 안전 기술(ZKT : JTC1. 27. 17)	-증명자가 어떠한 기밀정보를 알고 있다는 것이 검사식을 만족시키는 것 이외의 여하한 정보도 누설하지 않고 검사자에게만 증명시키는 개념	· 표준화 문서를 2개 part로 나누어 작성	· ZKT의 정의 권고 : (SC 27 N325) "ZKT는 정보의 소유를 검사자나 제3자든지 누구에게도 그 정보의 일부도 누설하지 않고 증명시키는 수단" 이 기술은 다음과 같은 분야에 적용 가능 : -실체 인증 -디지틀 서명

과 제 명	내 용	동경회의 주요 결정사항	브뤼셀회의 주요결정사항
	· part1 : General Model +영지식증명 기술이 필요한 이유 · part2 : Mechanism Based upon Identity and Factorization	· WD 수준 (SC27 N78)	· part 1의 검토 +ZKT를 이용한 안전 메카니즘을 위하여 다음 사항을 포함 : -context 모델 -메세지 교환 모델 -수학적 모델 +context 모델의 표준초안 개발시작
메세지회복형 디지틀 서명 (JTC1. 27. 07) (JTC1. 27. 08)	-데이터와 그 작성자의 정당성을 인증하는 메카니즘 +메세지회복형 : 서명검증한 후에 메세지가 읽혀지는 방식 +임프린트형 : 메세지와 서명을 열거한 것으로 메세지는 즉시 읽혀지는 방식 (브뤼셀회의에서 부가형으로 명칭 변경)	· 메세지회복형이 먼저 검토되었으며 임프린트형은 차후 검토예정 (SC27 N236)	-ISO/IEC 9796의 처리 · 임프린트형은 ISO/IEC 9796에서 사용된 용어와 호환성이 없어 부가형(Digital signature with appendix)로 변경
해쉬 함수 (JTC1. 27. 09)	-디지틀서명의 효율화를 위하여 사용되는 데이터 압축기능 · part1 : General Model +함수의 요구조건, 여타 part에서 공통으로 사용되는 기술이 규정 · part2 : Hashing Operation Using a Symmetric Block Cipher Algorithm +n 비트암호를 이용한 작성방법 · part3 : Modular Arithmetic +자승합동식을 이용한 작성방법 · part4 : Dedicated Hash Function 일본제안의 N-Hash와 RSA사(미국)의 MD4를 표준안 후보로 고려	DIS 수준 (SC27 N109)	· 임의 길이의 서명 메세지에 대하여 기고 요청 · 해쉬함수의 등록에 대하여 각회원국의 견해와 이에 대한 기고를 요청 -CD 10118-1(Part1) -CD 10118-2(Part 2)의 본문을 수정한 표준안을 차기 CD 투표처리를 위하여 준비 · Part 3 및 4에 대하여 1992년 차기 SC27 전체회의에 NP로 제출할 수 있도록 각국의 기고 요청

과 제 명	내 용	동경회의 주요 결정사항	브뤼셀회의 주요결정사항
키관리 (JTC1. 27. 18)	-WG2에서는 다음 중 part 2와 3만을 검토 · part1 : Framework · part2 : Mechanism Using Symmetic Techniques · part3 : Mechanism Using Asymmetric Techniques *TC 68/SC2에서의 키 관리와 밀접한 관계가 있음		· 당분간 certificate을 주요 주제로 다루기로 함. · SC21에서 "인증 디렉토리의 확장"에 대한 NP의 제안이 JTC1에서 승인되면 본 과제에 대하여 공동으로 표준화 수행 · "Key Management for Public Key Register"를 위한 과제를 SC27에 요구하였으나 새로 승인된 키관리 과제(Key Management Framework : JTC1. 27. 18) 또는 이의 Part3 Annex (JTC1 27. 18. 3)의 일부로 수행하는 것으로 하여 그 요구를 받아들이지 않음 · 과제 개편(JTC1 27. 11, JTC1. 27. 18) 내용은 WG1의 키관리 과제 참조

다) SC27/WG3(안전 평가기준)의 활동목표 및 추진결과

(1) WG3의 활동목표

WG3에서는 IT시스템/제품/시스템 구성요소의 안전평가와 인증에 관한 표준을 만드는 것을 목표로 한다. 이 표준화 대상에는 단일 시스템 뿐만 아니라 분산 시스템, 컴퓨터 네트워크, 관련 어플리케이션 서비스까지도 포함하고 있다. 여기서는 이들에 대한 다음 사항을 표준화하고 있으며, 그 중 평가기준이 그 핵을 이루고 있다.

◦ 평가기준
◦ 평가기준 적용방법
◦ 평가, 인증, 검정에 관한 관리절차

(2) 평가기준에 대한 국제적 활동 및 JTC1/SC27의 입장

안전에 관한 평가기준에 대하여는 선진기술국을 중심으로 국가기밀을 취급하는 시스템에의 적용을 중심으로 80년대 후반부터 그 기준을 적용, 시험하고 있으며 그 세부내용은 다음과 같다.

- 1985 미국 DoD Trusted Computer System Evaluation Criteria(*) (통칭 Orange Bock)
- 1989 영국 CESG CESG Memorandum Number 3 (Red Book)(*)
  DTI Green Book Series
  독일 ZSI IT-Security Criteria (Blue & White Book)
  불란서 SCSSI Blue-White-Red Book
- 1990 영·불·독·화란 Information Technology Security Evaluation Criteria (ITSEC)
- 1991 캐나다 CSSC Canadian Trusted Computer Product Evaluation Criteria

(*) 국가기밀을 취급하는 시스템용(국가안전보장, 국방, 외교용)

더욱이 미국에서는 국립컴퓨터보안센터(NCSC)에서 시험 및 인증을 하도록 하는 체제가 되어 있으며 1991년 부터는 classified data system의 정부조달에 대하여는 이 인증을 반드시 받도록 규정되어 있다. 1990년 영·불·독·화란 4개국에 의한 ITSEC는 영·불·독의 개별적 활동에 대하여 EC권역 시장통합등의 사정을 고려하여 유럽공업회연합(EUROBIT)및 EC 위원회가 제시한 현안 문제이며 이들의 상호조화 작업의 후원은 EC 위원회의 DG(Directorate General)이다. EC로서는 공통적인 평가기준이 마련되면 EC 표준(EN : European Norm)으로 만들 예정이다. 또한, 캐나다에서는 이와같은 국가기준을 만들기로 계획하여 그 구체적 작업을 진행하고 있다.

이와같은 각국의 개별적 기준제정은 이의 제품화를 하는 제작회사 측면에서 상당한 문제점이며 또한 국제적인 상호인증의 관점에서도 그 해결이 곤란하다. 이를 범세계적 차원에서 해결하기 위하여 JTC1 SC27에서 평가기준의 표준화를 과제화한 것이다.

(3) WG3의 표준화 추진결과

WG3은 1990년에 발족하여 동경 회의 이전에는 뮌헨 회의가 개최되었다.

(가) 뮌헨 회의의 주요 결정사항(90년 가을)

이 회의에서는 WG3의 작업수행방법에 대한 논의가 이루어져 다음의 4개 업무분야가 확정되었다.

① Glossary of Terms Related to the Evaluation, Certification and Accreditation of IT Security
② Functionality Classes
③ Assurance Aspects of Security Evlauation Criteria
④ Collection and Analysis of Requirements for Security Evaluation Criteria

(나) 동경 회의의 주요 결정사항('91, 4)

뮌헨회의 결과를 JTC1에 신규 연구과제(NP)로 제안하기 위한 논의가 이루어졌으며 다음 2개의 NP 제안을 JTC1으로 상정하기로 결정하였다.

◦ Collection and Analysis of Requirements for IT Security Evaluation Criteria(뮌헨 회의의 4번째 항)

- 각국의 대응 표준화 기관을 통하여 이용자 제조업체 등 관련 단체에 질의서를 송부하여 평가기준에 대한 요구조건을 수렴하기로 하였다.

◦ Evaluation Criteria for IT Security

뮌헨 회의의 결과 중 2항과 3항을 통합하여 3개 part로 표준화하기로 하였다.

- Part I : Introduction and Model
- Part II : Functionality of IT System etc.*
- Part III : Assurance of IT System etc.*

(주*) 상기의 IT System etc.는 IT Systems, Components and Products, Computer Networks Distributed System, Associated Application Services etc.를 생략한 것이다.

(다) 브뤼셀 회의 주요 결정사항('91. 10)

WG3에서 상정한 "IT 안전을 위한 평가기준" (Evaluation Criteria for IT Security : JTC1. 27. 16)으로 연구 과제명을 정정하고 SC27 사무국에서

이에 필요한 조치를 취하도록 하였다.

◦ Collection and Analysis of Requirements for IT Security Evaluation(JTC1. 27. 16)

– SC27의 "안전성 평가 질의서"(N 237)의 기고문에 대하여 다음과 같은 논평을 함

+ WG3/N45(목적의 명확화 요구) : 이는 목적을 수정한 WG3/N60로 해결

+ WG3/N45(위협문제) : 요구조건 생성과정에 대한 필수 입력으로서 위협 형태만을 고려토록 함.

+ WG3/N60(질의서에 대한 2차 초안) : 질의서에서 사용된 필수 용어의 간단한 Glossary를 포함시켜 본 질의서를 수정하여 92년 WG 회의에서 3차 초안을 최종 질의서의 기초로 발전시킴

◦ Evaluation Criteria for IT Security(JTC1. 27. 16)

– Part I : Introduction and Model

• Part 1의 입력문서로서 다음 기고를 접수함

+ WG3/N48 : 평가 절차 흐름도

+ WG3/N57 : 통합될 headlines

본 과제는 초기단계로서 당초 표준화 일정계획보다 6개월 지연되어 이를 다음의 일정으로 조정 : WD '92. 3 : CD '93. 4 : DIS '94. 4 : IS '95. 4

– Part II : Functionality of IT System etc.

본 과제도 초기단계로서 Part I 과 같은 일정으로 지연조정하였으며 WG3/N58을 WD로 인정함

– Part III : Assurance of IT System etc.

◦ WG3/N44를 WD로 하고 이의 근거를 WG3/N43으로 함

나. CCITT

CCITT에서는 '85~'88 연구회기에서 통신망 구조 및 프로토콜에서 상대의 확인을 위하여 요구되는 안전기술 중 인증에 대하여 디렉토리 시스템에 적용할 인증 프레임워크를 ISO/IEC JTC1/SC21과 협력하여 X.509로 권고 하였다. 또한 '89~'92 연구회기에는 SG VII에서 메세지처리 시스템(Q.18/VII), 분산응용의 지원 위한 프레임워크(Q.19/VII) 및 디렉토리 시스템(Q.20/VII)의 3개 연구과제에 대한 안전기술 표준화를 수행하고 있으며 SG VIII에서는 텔레마틱 서비스에서의 안전(Q.28/VII)에 대한 표준화 연구를 수행하고 있으며 이들의 표준화 활동현황은 표 4와 같다.

표 4. CCITT의 안전기술 표준화 현황

표준화 기관 및 과제	상 태	관련 문서
◦ SG VII Q.18(MHS)		
–메세지처리 시스템의 프레임워크	완 료	X.400 계열
–X.400을 통한 EDI 안전	완 료	X.435
–인터렉티브 EDI를 위한 안전	완 료	F.435
◦ SG VII Q.19(분산응용 시스템의 지원 위한 프레임워크)		
–OSI 안전 구조	완 료	X.800
–OSI 안전 프레임워크	연 구 중	
–상위계층 안전 모델	연 구 중	
–분산응용을 위한 안전 모델	연 구 중	JTC1N544
◦ SG VII Q.20(디렉토리 시스템)		
–인증 프레임워크	완 료	X.509
–접근제어	연 구 중	X.509의 개정 (COM VII-147)
◦ SG VIII Q.28(텔레마틱 서비스에서의 안전)		
–텔레마틱 서비스를 위한 안전 프레임워크의 제안	연 구 중	JTC1 SC18 참조

본 항에서는 CCITT '89~'92 연구회기 중 정보통신 분야의 안전기술 표준화의 중심을 담당하는 SG VII의 활동을 소개하기로 한다.

1) CCITT SG VII의 안전기술 표준화 활동

CCITT '88~'92 연구회기 중 SG VII WP4에 부여된 안전기술에 관한 과제는 Q.18(메시지 처리 시스템), Q.19(분산 응용시스템의 지원 위한 프레임워크) 및 Q.20(디렉토리 시스템) 중 그들 과제의 소과제에 포함시켜 ISO/IEC JTC1과 협력하여 표준화 작업을 수행하고 있다. 본 절에서는 WP VII/4에서 이번 연구 회기에 표준화 연구결과로 권고화가 가능한 Q.19 및 Q.20의 안전기술에 대한 활동목표와 87년 7월부터 91년 9월까지 4차에 걸친 회의결과를 토대로 안전기술 표준화 현황을 소개한다.

가) Q.19/VII의 활동목표 및 표준화 활동

본 과제의 전문가 그룹은 MHS와 디렉토리 시스템의 표준화 과정에서 일반 유틸리티가 될 것으로 예상되는 안전에 대한 메카니즘과 기술개발 필요성을 인식하고 ISO/IEC JTC1에서 안전기술에 대한 표준화 활동을 고려하여 분산 응용 시스템 및 데이터통신에 일반적으로 정의되어 사용할 수 있는 관련 안전 프레임워크 및 안전 모델의 표준화 연구를 수행한다. 또한 이러한 프레임워크를 정의하고 지원하기 위하여 사용할 수 있는 안전 메카니즘(예, 접근 제어, 인증, 공증, 디지틀 서명등)과 안전관리 원칙 및 기술의 표준화 연구를 수행한다. 본 과제의 표준화 추진결과는 표 5와 같다.

나) Q.20/VII의 활동목표

본 과제의 전문가 그룹에서는 인증을 위하여 디렉토리를 활용하는 응용 시스템의 요구조건을 만족시키기 위하여 88년에 권고 X.509로 표준화한 디렉토리 인증 프레임워크에서 기본적 접근 제어 기술을 지원하기 위하여 본 권고를 개정하였다. 본 과제의 표준화 추진결과는 표 5와 같다.

표 5. CCITT SG VII의 안전기술 표준화 추진결과

과 제 / 회 의	-Q.19/VII 분야 : 분산응용 시스템의 지원 위한 프레임워크	-Q.20/VII 분야 : 디렉토리 시스템
제 1 차 회의 ('89. 7)	◦ 신규 권고초안인 OSI 안전구조(X.800)의 작성 및 1990년 말까지 신속 권고화 처리 절차 준비	◦ 디렉토리 시스템을 위한 접근 제어 모델링 작업을 안정화하여 1990. 6까지 합의를 이루려고 노력함 ◦ 그러나 본 작업은 접근 제어의 한측면만이 고려되어 접근 제어관리와 같은 여타 측면도 고려되어야 함에 합의
제 2 차 회의 ('90. 2)	◦ 신규 권고안인 OSI 안전구조(X.800)의 작성이 '90말 차기 회의까지 신속 권고화 처리절차를 밟기 위한 준비 완료	◦ 기본적 접근 제어 모델링 개발은 제한적인 기술적 작업만이 남겨진채 대부분 정리되었으며 나머지 작업을 다음의 다섯주제로 분류함 : +복제와 지식 +확장 정보 모델 +스키마 +고도 탐색 +분산 엔트리

과 제 / 회 의	-Q.19/VII 분야 : 분산응용 시스템의 지원 위한 프레임워크	-Q.20/VII 분야 : 디렉토리 시스템
제 3 차 회의 ('90. 11)	◦ 신규 권고안인 OSI 안전구조(X.800)을 신속 권고화 처리절차를 밟도록 승인 ◦ 인증 프레임워크(X.9xx)의 신속 권고화 처리 위한 초안 작성준비 ◦ 개방형 시스템 및 분산응용 시스템을 위한 안전기술 표준의 권고화 작업을 차기연구회기('93~'96)에 계속 수행	◦ 접근 제어 모델링 작업이 거의 기술적으로 안정화 됨 -이는 X.500('88) 권고의 개정을 수반함 -나머지 작업을 4개의 주제로 분류함 : +복제 +스키마 +고도 탐색 +분산 엔트리
제 4 차 회의 ('91. 9)	◦ 인증 프레임워크는 SC21에서 DIS 10181-2로 표결에 붙여짐 +1992년중 CCITT에서 승인을 얻도록 제출될 것임 ◦ 상위계층 안전모델은 JTC1 SC21에서 6095로 CD 표결에 붙여짐 +1992년중 CCITT에서 승인을 얻도록 제출될 것임 ◦ 접근 제어 및 감사 프레임워크는 CD 상태임 ◦ 안전성 교환 ASE(Application Service Element)는 작업초안으로서 승인되었으며 차기회의에서 CD로 발전될 것임 ◦ 현재 검토 가능한 안전관련 권고초안 -안전 프레임워크 일반 TD 4191 -안전 감사 프레임워크 일반 TD 4190 -부인봉쇄 프레임워크 일반 TD 4192 -신뢰성 프레임워크 일반 TD 4193 -무결성 프레임워크 일반 TD 4194	◦ OSI 관리 및 안전 분야에 대한 업무연락 문서의 송신(TD 0094, TD 4183)을 차기 기술회의에서 검토키로 지연시킴 ◦ X.500 계열권고중 '88년도판의 내용 보완 및 오류수정이 COM VII 135부터 147까지에서 규명됨 -X.509(디렉토리 인증 프레임워크)에 대한 것은 COM VII-147에 규명됨

2) '89~'92 연구회기 중 SG VII에서의 안전기술 권고(안) 처리 및 향후 권고화 계획

'89~'92 연구회기 중 SG VII에서는 Q.19/VII과 관련하여 X.800를 제정하여 1991. 3 신속 권고 처리절차에 의거 권고로 확정하였으며 Q.20/VII과 관련하여서는 X.509에 기본적 접근 제어 기술을 지원하기 위한 사항을 보완하여 1992년 중 권고로 확정할 예정이다. 더욱이 개방형 안전시스템 및 분산응용 시스템의 지원위한 프레임워크에 대한 안전기술 표준안을 '93~'96 연구회기에 X.9xx 계열로 표준화할 계획을 가지고 있으며 그 내용은 표 6과 같다.

표 6. CCITT SG VII 안전기술 표준화 추진계획

분 야	권고(안) 번 호	재. 개정	제 목	권고 승인 년도			최근 관련 문 서
				신 속 처 리	X 차 총 회	차기연 구회기	
Q.19/VII	X.800	제 정	OSI 안전구조	0 (1991)			X.800
	X.9xx	제 정	개방형시스템 안전 프레임워크 : 인증 프레임워크	0 (1992)			
	X.9xx	제 정	분산응용 시스템의 지원 위한 프레임워크 : 상위계층 안전 모델		0 (1993)		
	X.9xx	제 정	분산응용 시스템의 지원 위한 프레임워크 : 안전개요		0 (1993)		
	X.9xx	제 정	분산응용 시스템의 지원 위한 프레임워크 : 인증 서버			0 (1993)	
	X.9xx	제 정	개방형 시스템 안전 프레임워크 : 안전 프레임워크 개요			0 (1993)	TD 4191 ('91. 9)
	X.9xx	제 정	분산응용 시스템의 지원 위한 프레임워크 : 분산응용 시스템의 안전모델			0 (1994)	
	X.9xx	제 정	분산응용 시스템의 지원 위한 프레임워크 : 안전 응용지침			0 (1994)	
	X.9xx	제 정	개방형 시스템 안전 프레임워크 : 접근제어 프레임워크			0 (1994)	
	X.9xx	제 정	개방형 시스템 안전 프레임워크 : 부인봉쇄 프레임워크			0 (1995)	TD 4192 ('91. 9)
	X.9xx	제 정	개방형 시스템 안전 프레임워크 : 무결성 프레임워크			0 (1995)	TD 4194 ('91. 9)
	X.9xx	제 정	개방형 시스템 안전 프레임워크 : 신뢰성 프레임워크			0 (1995)	TD 4193 ('91. 9)
	X.9xx	제 정	개방형 시스템 안전 프레임워크 : 안전감사 프레임워크			0 (1996)	TD 4190 ('91. 9)
Q.20/VII	X.509	개 정	디렉토리-인증 프레임워크	0 (1992)			COM VII -147

5. 안전기술의 국내 표준화 활동 및 방향

국내에서는 80년대 부터 통신분야의 안전문제에 관하여 특정연구소를 중심으로 암호화 알고리즘 및 실용화 기술개발 연구를 수행하여 왔으나 90년 말에 한국통신정보보호학회가 발족하여 산·학·연의 정보보호, 암호학 및 표준화에 관한 연구의 활성화를 유도하고 있다. 또한 91년말에는 정보 산업분야에서의 국내 및 국제표준화 활동의 활성화와 이의 표준화 작업효율성 극대화를 목표로 정보산업표준원이 설립되어 산하위원회를 조직 운영하고 있다. 최근 국내 JTC1 SC27에 대응한 연구활동 활성화를 위한 회의를 개최하여 향후 안전기술의 표준화 추진방향 및 국제활동에 대한 협의를 하였다.

한편 국내표준화 결과로서는 정보통신 설비에 관한 안전 신뢰성 기준이 체신부 고시로 제정(제 103호, 90. 10) 되었으며, 이의 이행을 위하여 세부 운영관리기준을 기간통신사업자와 정보통신 역무 제공업자가 제정, 시행하고 있다. 또한 최근 전산망 안전 신뢰성 기준(안)에 대한 사업자 의견을 수렴한 바 있으며 곧 체신부 고시로 제정될 전망이다.

더욱이 이러한 기술기준에 대하여 기술기준의 적합의무를 전기통신 기본법(제 25 조)에서 명시함에 따라 통신사업자들은 이를 준수하기 위한 표준평가 및 적합성시험 연구활동을 보다 강화해가야 할 것이다.

또한 현 통신제도 환경에서는 통신채널을 통한 전송정보의 암호화 서비스를 제외한 전송정보의 무결성 서비스, 통신상대의 인증 서비스, 송수신 정보의 부인 봉쇄 서비스 등이 가입자에 제공 가능한 안전 서비스로 고려될 수 있으므로 이를 MHS, EDI, 디렉토리 등 각종 정보통신 텔레마틱 서비스에 적용하여 상용화할 수 있을 것으로 생각된다. 따라서 각 통신사업자간의 안전서비스 상호연동을 위하여 3절에서 제시한 안전서비스의 요소기술을 사업자, 제조업자, 사용자간 상호조화를 이루어 단계적이며 점진적인 표준화활동을 추진해 가야 할 것이다.

6. 결 론

정보화 사회에서는 정보가치가 재화 또는 상품으로 평가되며 또한 개인정보에 대하여 프라이버시가 보장되어야 할 것이다. 이에 따라 대부분의 정보를 전달하게 될 공중통신망에는 전송정보를 보호하고 이를 적절히 구현하기 위한 표준화가 요구된다.

본고에서는 정보통신 안전기술 중 개방형 정보통신 시스템에서 표준화해야 할 범위에 대하여 특정 통신 어플리케이션에 의존하지 않는 정보안전기술에 관한 ISO/IEC JTC1 SC27 표준화 연구활동과 전기통신분야에서 분산응용과 디렉토리 시스템에 대한 CCITT SG VII의 최근 국제표준화 연구활동을 중심으로 소개하였으며 또한 국내에서의 안전 기술 표준화 활동을 파악함으로써 통신사업자가 정보통신 사업에서 소요되는 안전 기술 및 이의 표준화 방향을 제시하였다.

또한 국내 통신사업자 및 기업체에서도 독자적으로 자체고유의 안전 체제에 의한 정보통신설비 구축 및 운용이 예상되고 있으며 모든 기업에서 이러한 형태로 해결할 경우 국가전체의 투자비 증가 및 상호운용성에 문제가 야기될 수 있으므로 통신망사업자들은 이를 해결하기 위하여 신기술의 개발을 선도하고 표준화를 위한 상호 조화를 해가야 할 것이다.

참 고 문 헌

1. CEN/CENELEC Ad Hoc Security Group, "Towards a Taxonomy for Standardisation of Security," ISO/IEC/JTC1/SC27/WG20.1 N 248, 1990. 4.

2. C. Siuda, "Security Standards for Open Systems" Proceedings of Symposium IFIP WG6.5 MHS System and Application Layer Communica-

tion Protocols, B4-1~B4-20, Oct 3-5, 1990.

3. CCITT SG VII, "Report of Working Party VII/4" COM VII-R21, Geneva, Dec. 1990.

4. CCITT SG VII, "Report of Working Part VII/4" COM VII-R31, Geneva, Oct. 1991.

5. CCITT SG VII, "Proposed Revision to Recommendation X.509 for Access Control" COM VII-147, June 1991.

6. ISO/IEC JTC1/SC27 N327, "Resolution taken at the plenary meeting of ISO/IEC/JTC1/SC 27," Brussels, 1991. 10.

7. ISO/IEC JTC1 N1509, "Report of JTC1 SC27 to the october 1991 JTC1 plenary meeting in Madrid", 1991. 8.

8. 中尾康二 外 1人 "OSI における セキコリティア-キテクチャの 檢討," 信學技報, IN 86-4, pp. 19-23, 1986.

9. 中尾康二, 太田和夫, "ISO/IEC JTC1/SC27 (情報 セキコリティ) の 國際標準化動向," ISEC 91-4 pp. 17-22, 1991.

10. 太田和夫, "情報 セキコリティの 標準化の動向に ついて," 電子情報通信學會誌, Vol. 72, No. 3 pp. 297-304, 1989. 3.

11. 日本 ITU協會, "CCITT 加速權告承認 一覽" ITU ジャ-ナル Vol. 21, No. 7, pp. 32-37, April 1991.

12. 장청룡 외 2인, "정보통신망의 시큐리티 국제표준화," 전기통신연구, 제 5 권 제 4 호, pp. 48-57, 1991. 12.

13. 이용준 외 3인, "JTC1/SC27의 정보통신 보호기술 표준화 현황," 통신정보보호학술발표 논문, Vol. 1. No. 1, pp. 165-175, 1991. 11.

□ 著者紹介

元 東 豪(正會員)

本 學會誌 第 1 卷 第 2 號 參照

張 青 龍(正會員)

1980년 成均館大學校 電子工學科 卒業(學士)
1986年 延世大學校 大學院 電子工學科 卒業(碩士)
1979年~1983年 韓國電子通信研究所 研究員
1984年~現在 : 韓國通信 研究開發團 先任研究員
關心分野 : 暗號理論, 情報安全技術