特輯

개방형통신 안전기술의 국내외 표준화동향

張 靑 龍
韓國通信 硏究開發團

정보통신 안전 서비스의 제공에 따라 사업자 측면에서 관련 장비의 상호운용성 확보, 연구개발 또는 도입제품 평가의 용이성과 제품생산자 측면에서는 생산원가의 저렴화를 위하여 반드시 표준화가 필요하다. 본 논문에서는 안전기술의 표준화 연구를 수행하는 주요 국제기구인 ISO/IEC JTC1 SC21, SC27과 CCITT SG Ⅴ Ⅱ등의 활동과 이에 대응한 국내 표준화 그룹들과 관련 기관들의 활동을 소개하였다. 또한 이러한 국내외 활동과 통신 사업자의 사업여건을 고려하여 통신 사업자가 정보통신 사업에 있어서 소요되는 안전기술 및 이의 표준화 방향을 제시하고자 한다.

Ⅰ. 서 론

정보가 재화로서의 가치를 창출하는 정보화 사회에서 정보통신 시스템들은 더욱 그 역할의 중요성이 증대되고 있다. 이러한 정보통신 시스템의 상호접속성과 상호운용성의 제고를 위하여 국제표준화 기관인 ISO와 CCITT에서는 정보통신 시스템을 계위적으로 조정한 참조 모델을 제시하고 있다. 업체에서는 이를 근거로 저가격 고성능의 다양한 정보자원을 생산하고 있으며, 이의 이용자는 원하는 많은 이기종 정보자원을 망으로 구성하여 사용하게 된다. 더욱이 이러한 자원들로 구성된 개방형 상호접속 통신망 환경을 정보통신의 기반 구조로 하는 정보화 사회에서는 정보의 생산, 전달, 축적 및 폐기의 정보 유통과정에서 정보 자체를 보다 안전하고 신뢰성 있게 처리하여야 할 것이다.

정보통신시스템에 있어 안전에는 재해, 고장 등에 의해 우연히 발생하는 시스템의 이상을 검출, 복구 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.[1] 본 논문에서는 주로 협의의 안전에 대하여 개방형 통신망에 적용가능한 안전기술의 표준화 활동을 소개하고자 한다.

우선, 안전 기술의 표준화 필요성에 대하여 생각해 보기로 한다. 하나의 장치내에 폐쇄된 안전 대책은 각 장치에서 개별적으로 대처가 가능하다. 그러나 예를 들어 회선상의 데이터를 도청이나 변조로부터 보호하려면 회선상의 데이터 암호화 절차를 송신, 수신장치간에 미리 정하여 놓을 필요가 있다.특히 통신망을 개재시켜 불특정 다수의 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 구축 설비 상호간 상호운용성의 확보와 유지 보수의 용이성을 제고할 수가 있다. 또한 표준화의 다른 이점으로 생산업자에게는 양산화에 수반되는 제품 비용의 저렴화를 기대할 수 있다.

본 논문에서는 정보통신을 위한 개방형상호접속시 적용가능한 안전기술 표준화의 대상과 주요 국제표준화 기관들의 표준화 범위를 살펴보고 이의 표준화 활동중 ISO/IEC JTC1 Ⅴ Ⅱ과 CCITT SG 활동을 중심으로한 국제표준화와 이에 대응한 국내의 표준화 활동을 소개한다. 끝으로 국내에서 통신사업자로서 현 사업환경에서 고려할 만한 안전 서비스와 이의 기술표준화 방향을 제시하고자 한다.

Ⅱ. 안전기술의 형태와 분류[2]

1. 기본표준

이 표준에는 지네릭 유저 요구사항을 만족시키기 위한 일반 컴퓨터시스템, 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
- 응용
- 기술 및 메카니즘
- 관리

2. 기능표준 또는 프로파일

이 표준은 조달, 제품검정 및 서비스 공인을 위하여 특히 유용하다. 이것은 근본적으로 비전문가들로 하여금 기본표준의 근본 제정취지 및 목적을 이해할 수 있도록 하는 공통적으로 산업분야에서 취하는 접근 방식이다. 이것은 일반적으로 기능적 적합성을 검증하기 위한 참조 시스템으로서 사용하기 위하여 이 용자, 생산자, 설계자 들을 위하여 기본표준의 선택 사항 중 축소된 세트를 제공한다. 이 분야의 주요 활동기관은 NOIW(NIST OSI implemantor's workshop), EWOS(European workshop for open systems), MAP/TOP(manufacturing automation protocol/technical and office protocol) 및 COS (corporation for open systems)가 있다.

3. 산업표준 및 시행규칙(Codes of Practice)

이러한 형태의 표준은 관련 사업 또는 업무의 성격에 상응하는 특정 이용자 그룹 또는 산업체에 의해 요구되는 기술적 및 절차적 표준이 이에 포함된다.

시행규칙은 이의 이용자 그룹의 멤버쉽을 위한 품질 표준에 대한 이용자 그룹 요구사항의 특별한 경우이다. 이러한 시행규칙은 일반적으로 지엽적인 문제로서 운영되는 반면 적합성 문제는 보통 동등 그룹관리를 통한 자발적인 형태로서 운영된다.

4. 해설문서

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

기본표준, 기능표준, 시행규칙 및 해설문서에 대한 표준의 부분, 특성 및 형태는 표 1과 같다.

표. 1 표준의 분류와 형태

구 분	특성	특성
기본표준	—지네릭 유저 요구사항을 만족위한 · 컴퓨터시스템 · 네트워크 · IT(info. Tech)의 이용과 적용에 필요한 기술적사항	—구조, 프레임워크 및 모델 —서비스 및 프로토콜 —응용 —기술 및 메카니즘 —관리
기능표준 또는 프로파일	—조달제품 검정및 서비스공인에 유용 —기능적 적합성 검증을 위한 참조시스템으로 이용자, 생산자, 설계자들에게 기본표준의 축소된 세트 제공	—Int'l Std. Profile
단체표준및 시행규칙	—특정이용자 그룹 또는 산업에 요구되는 기술적 및 절차적 표준	—Bell Sys. Practice(BSP) —TTA 표준
해설문서	—표준의 사용과 규격화시 이용자, 구매자, 표준개발자를 도와주고 정보제공및 교육용	—지침서 —Glossary —해설자료

Ⅲ. 안전기술 표준화 범위[2][3]

1. 개방형 통신시스템에서의 안전기술 표준화 대상

개방형 통신시스템의 서비스를 이용하는 정보통신 가입자에게 보다 안전하고 신뢰성있게 정보통신 서비스를 제공하기 위하여 요구되는 안전기술의 표준화 대상을

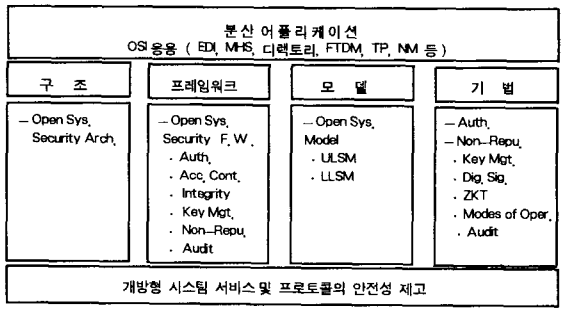


그림 1. 개방형 통신시스템에서의 안전기술 표준화분야

구조, 프레임워크, 모델 및 기법으로 분류할 수 있으며 이들의 세부적 표준화 분야는 각각 그림 1 과 같다.

2. 표준화기관들의 안전기술 표준화 업무 범위

1 절에서 언급된 다양한 안전기술 표준화 대상에 대하여 ISO/IEC의 JTC1, CCITT SG Ⅶ등에서는 서로의 목표분야에 대하여 각자 또는 합동으로 안전기술 표준화 업무를 수행하고 있으며 그들의 표준화 업무범위는 그림 2와 같다.

Ⅳ. 안전기술 국제 표준화 활동

개방형시스팀을 위한 표준화를 주도하는 ISO와 전기통신 시스팀의 원활한 상호 접속을 위한 표준화를 주도하는 CCITT와 같은 국제 표준화 기구중에서 특히 개방형 통신의 안전기술 표준화 활동은 ISO/IEC JTC1의 SC6(시스팀간의 통신 및 정보 교환),SC21 (개방형시스팀의 상호접속을 위한 정보 검색, 전달

		사용범위						응용서비스									
		OSI/개방형시스템	빌스트웨 사무용 시스템	무역 시스템	금융 및 유통 시스템	정보 시스템	안전 시스템	멀시징	화일 전송	인터랙티브계열	EDI 응용	분산사무용응용서비스	분산처리	DB 응용서비스	O/S 응용서비스	통신	관리
ISO/IEC/JTC1	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																	

M: 현재의 표준화 주 관심분야 G: 일반적인 적용을 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

및 관리), 그리고 SC27(정보기술의 안전 기법)에서 주로 수행하고 있으며 CCITT에서는 SG Ⅶ(데이터 통신)에서 주로 수행하고 있다. 본장에서는 이들의 표준화 수행 범위와 추진 현황을 소개하기로 하며 ISO/IEC JTC1의 안전기술 표준화 현황은 표 2에 요약되어 있다.[4][5][6][7][8]

표 2. ISO/IEC JTC1의 안전기술 표준화현황

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

기관 및 표준화 과제	상 태	관 련 문 서
ISO/IEC		
JTC1(정보기술)		
○ SC6(시스템간의 통신 및 정보교환)		
· 하위계층 안전 지침	WD	SC6N6957
· OSI 하위계층 안전 모델	WD	SC6N5333
· WG3 - 망계층		
- 망계층 안전 프로토콜	CD 11577	SC6N7053
· WG4 - 전달계층		
- 전달계층 안전 프로토콜	DIS 10736	SC6N6779
- 접속 설정 프로토콜	PDAM1	
본 표준화업무는 신설된 SC27에서 계속하기로함		
○ SC20 - 데이터 암호기술		
○ SC21(OSI를 위한 정보검색, 전달 및 관리)		
· WG 1 - OSI 구조		
- SC21의 안전기술 조정	계속	SC21N2540
- Open System 의 안전 개요	WD	SC21N7292
- OSI 안전 구조	IS	ISO 7498-2
- Open System을 위한 안전 프레임 워크		
part 1 : 프레임워크 개요	CD 10181-1	SC21N7083
part 2 : 인증 프레임워크	DIS	DIS 10181-2
part 3 : 접근제어 프레임워크	CD 10181-3	SC21N6947
part 4 : 부인봉쇄 프레임워크	WD	SC21N7082
part 5 : 무결성 프레임워크	WD	SC21N7084
part 6 : 기밀성 프레임워크	WD	SC21N7085
part 7 : 감사추적 프레임워크	CD 10181-7	SC21N7097
part 8 : 키 관리	SC 27 WG1, WG2 참조	
· WG4 - OSI 관리 - part 8 : 안전 감사 추적기능	DIS 10164-8	SC21N7039
- WG4 - OSI 관리 - part 7 : 안전 경보 보고기능	IS	IS 10164-7
- 접근제어를 위한 객체와 어트리뷰트	CD 10164-9	SC21N7227
- 디렉토리 : 인증 프레임워크	IS	ISO 9594-8
- 디렉토리 : 접근제어(5parts)	DAM1 9594 Part1	SC21N6501
	DAM1 9594 Part2	SC21N6502
	DAM1 9594 Part3	SC21N6505
	DAM1 9594 Part4	SC21N6507
	DAM1 9594 Part8	SC21N6512
· WG8 - OSI 상위계층		
- ACSE 인증 서비스와 프로토콜	IS Addendum	ISO 8649
- OSI 상위계층 안전 모델	DIS 10745	SC21N6924
- 안정성 교환 ASE/지네릭 UL 안전		
part 1 : 개요, 모델과 표기	WD	SC21N6992
part 2 : 서비스 요소 서비스 정의	WD	SC21N6993
part 3 : 서비스 요소 프로토콜 정의	WD	SC21N6994
part 4 : 전달 구문 규격		
part 5 : 서비스 요소 PICS 프로포마		
part 6 : 전달 구문 PICS 프로포마	WD	SC21N6995
- 거래처리(TP)안전 모델	WD	SC21WG5N6232
- FTAM 안전	WD	SC21N7160
○ SC27(정보기술의 안전기법)		
· IT - 안전을 위한 지네릭 방법 및 기술 표준화		
· WG1 - 지네릭 안전 요구조건		
- IT 안전성 정의의 Glossary	Standing Document	SC27N437
- 인증 메카니즘 : 일반모델	IS	ISO/IEC 9798-1('91)
- 키관리를 위한 암호 메카니즘	NP	
- 키관리 프레임워크	WD	SC27N602
- 안전성 정보 객체		
part 1 : 방법과 지침	WD	SC27N604
part 2 : 요소와 지네릭 규격	WD	SC27N605
- 정보기술 안전관리를 위한 지침		
part 1 : 개념과 모델	WD	SC27N607

part 2 : 관리와 계획	WD	SC27N608
part 3 : 기법	WD	SC27N609
· WG2 - 안전 기법과 메카니즘		
- 64비트 블럭암호 운용모드	완료	ISO 8372('87)
- n 비트 블럭암호 운용모드	IS	ISO/IEC 10116('91)
- n 비트 알고리즘을 사용하는 암호검사 합 수를 이용한 데이터 무결성 메카니즘	IS	IS 9797
- 인증 메카니즘		
part 2 : 대칭 기법을 이용한 인증	CD	CD 9798-2
part 3 : 공개키 알고리즘을 이용한 인증	DIS	DIS 9798-3
- 영지식증명을 이용한 안전 메카니즘	NP	SC27N319
- 메시지회복형 디지틀 서명	IS	ISO/IEC 9796('91)
- 부가형 디지틀 서명	NP	SC27N135
- 해쉬 함수		
part 1 : 일반모델	CD	CD 10118-1
part 2 : 대칭블럭암호 알고리즘을 이용하는 해쉬 운용	CD	CD 10118-2
part 3 : 모듈로 산술을 이용하는 해쉬	WD	SC27N223
part 4 : 전용 해쉬 함수	WD	SC27N224
- 부인 봉쇄 메카니즘	NP	SC27N209
part 1 : 일반모델	WD	SC27WG2N177
part 2 : 대칭 암호기법을 이용한 부인 봉쇄	WD	SC27WG2N176
part 3 : 비대칭 암호기법을 이용한 부인 봉쇄	WD	SC27WG2N158
- 키 관리		
part 2 : 대칭형 암호기법을 이용한 키관리	WD	SC27WG2N147
part 3 : 비대칭형 암호기법을 이용한 키 관리	WD	SC27WG2N168
WG3 - 안전 평가기준		
- IT 안전성 평가기준		
part 1 : 일반모델	WD	SC27WG3N128
part 2 : IT 시스템의 기능 등급	WD	SC27WG3N129
part 3 : IT 시스템의 보증	WD	SC27WG3N130
- IT 안전성 평가기준을 위한 요구조건의 수집과 분석	WD	SC27N467
- Glossary of terms	WD	SC27WG3N102

1. ISO/IEC JTC1의 표준화 활동

1) ISO/IEC JTC1 SC21

안전기술에 관한 초기의 SC21 활동 범위는 개방형 시스템을 위한 전반적인 분야라기 보다는 OSI에 관한 것이었다. 이의 첫번째 안전기술 표준은 OSI 안전성 구조로서 OSI기본 참조 모델의 제 2부(ISO 7498-2(1989), CCITT X.800(1991))로서 표준화되었다. 그러나 이와같은 구조에 관한 표준은 안전 서비스와 메카니즘을 정의하는 첫단계일 뿐이며 구현을 위한 규격은 되지 못한다. 다음 단계의 표준은 이러한 구조의 개념에 바탕을 두어 만들어진다. 즉, 기존의 OSI 프로토콜 표준에 특정의 정보보호 형태를 규정하는 안전 모델, 안전프레임워크 등이 이에 포함된다. 더욱이 최근에는 전반적인 개방형시스템에 대한 표준화도 SC21의 목표로 고려되고 있다. 그림 3에서는 개방형시스템에서 요구되는 안전기술요소의 상호관계를 보여주고 있다.

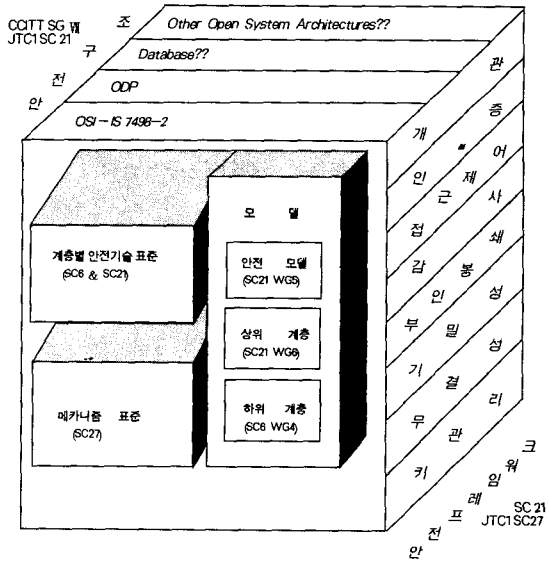


그림 3. 개방형시스템에서의 안전기술 개요

(1) OSI 안전성 구조

ISO7498-2(OSI 안전성구조)는 안전한 통신이 요구되는 환경에 적절히 적용될 수 있는 일반적인 안전성에 관련한 구조적 요소를 정의한다. 특히 이 표준은 OSI기본 참조 모델에서 제공되는 안전서비스와 관련 메카니즘의 일반적 규정과 이러한 모델내의 어디에서 서비스와 메카니즘이 제공될 수 있도록 위치시키냐 하는 것을 정의한다. 또한 여기서는 인증(동등실체 및 데이터발생원), 접근제어, 부인봉쇄(발신, 수신), 무결성(connectionless, selective field

connectionless, connection oriented with/ without recovery, selective field connection oriented) 및 기밀성(통화량 흐름,connectionless, connection oriented, selective field)를 포함하는 많은 통신관련 안전성 서비스를 규정한다.

(2) 안전 프레임워크

이 표준의 목적은 인증과 접근제어와 같은 특정의 기능 분야에 대하여 종합적이며 일관성 있게 규정 하는 것이다. 이들 규정은 특정한 구조와 연계하여 적용함에 있어 이러한 기능 분야의 모든 측면을 포함한다. 또한 암호 기능을 위한 키관리와 같은 공통적 측면도 포함한다.

(가)적용 범위

이 표준은 개방형 시스템(OSI, DB, 분산응용 및 개방형 데이터처리등)에서의 안전서비스 적용에 관하여 규정하고 있다. 이 프레임워크는 시스템 내부적으로 시스템과 객체의 보호수단을 정의하고 시스템간의 상호작용을 규정한다 그러나 시스템이나 메카니즘을 구축하기 위한 방법론은 규정하지 않는다. 또한 특정 안전 서비스를 얻기 위해 사용되는 데이터 요소와 운용절차(프로토콜 요소는 아님)를 규정하며 이러한 안전서비스는 시스템간에 교환되는 데이터는 물론 시스템의 통신 실체에 적용되며 시스템에 의해 관리되는 데이터에도 적용된다.

(나)안전 프레임워크 개관

이 개관 표준은 안전 프레임워크의 제 1부(ISO 10181-1)가 될 것이며 여러 프레임워크(인증, 접근제어, 부인봉쇄, 무결성, 기밀성,감사)를 개략적으로 규정한다. 또한 여타 프레임워크에서 사용되는 안전 도메인, 안전권한 및 안전정책과 같은 공통적 개념을 규정한다.

(다)인증 프레임워크

이 표준은 개방형시스템에 적용하는 인증의 모든 측면, 접근제어와 같은 여타 안전기능과 인증과의 관계 그리고 인증을 위한 관리적 요구조건을 규정한다.

이 인증 프레임워크는 인증 표준의 계위중 그 정상을 차지하고 있으며 개념, 용어 그리고 인증 방법을 위한 분류를 규정한다. 그 바로 아래인 ISO 9798 (실체인증 메카니즘)과 같은 표준은 이들 방법의 특정한 세트를 보다 상세히 규정하며 최종적으로 그 계위의 바닥에 있는 ISO·9594-8(디렉토리 인증 프레임워크 : CCITT X.509)는 특정한 응용과 요구조건에 대하여 이들 개념과 방법을 이용한 것이다.

(라)접근제어 프레임워크

이 표준은 개방형시스템에서의 접근제어의 모든 측면(예, 사용자-프로세스, 사용자-데이터, 프로세스-프로세스, 프로세스-데이터), 인증 및 감사와 같은 여타 안전기능에 대한 관계 및 접근제어를 위한 관리적 요구조건을 규정한다.

(마)부인 봉쇄 프레임워크

이 표준은 ISO 7498-2/CCITT X.800에서 규정된 부인 봉쇄 안전서비스의 개념을 보다 확장시키고 이러한 서비스의 개발과 제공을 위한 프레임워크를 제공한다.

(바)무결성 프레임워크

이 표준(ISO 10181-5)은 정보의 검색, 전달 및 관리상에서의 데이터 무결성을 규정한다. 여기서 규정된 몇몇 절차는 암호화 기법의 적용에 의해 무결성이 이루어진다.

이 프레임워크는 요구된 특성을 나타내는 하나의 특정한 암호기법 또는 여타 알고리즘의 사용에 종속되지 않는다. 실제로 많은 알고리즘이 사용되며 특정한 서비스 제공시는 하나의 알고리즘만이 사용되어야 한다.

(사)기밀성 프레임워크

이 표준(ISO 10181-6)은 정보의 검색, 전달 및 관리상에서의 정보의 기밀성을 규정한다. 기밀성의 목적은 비공인 공개로부터 정보를 보호하는 것이다. 이 프레임워크에서는 정보를 표현하는 데이터의 접근이 가능한 경우와 불가능한 경우 모두를 규정한다. 이에는 또한 통화량 흐름의 기밀성도 규정한다.

(아)안전성 감사 프레임워크

다른 안전서비스와 마찬가지로 안전성 감사(ISO 10181-7)는 정의된 안전성 정책의 범위내에서만 규정될 수 있다. 이 안전성 정책은 안전도메인내에서 안전성 당국에 의해서 정의될 것이다. 이러한 프레임워크에 기초한 메카니즘 을 규정하는 어떤 표준도 다양한 안전성 정책을 지원할 수 있어야 한다.

(자)키관리 프레임워크

JTC1 SC21에서 개발하고 있는 이 프레임워크는 IS 7498-2에서 규정된 안전 서비스에 직접 관련되지 않는 기능에 관한 여타 안전 프레임워크와 특별한 관계를 갖는다.

이들 기능은 암호화가 가능한 어떤 정보기술(IT) 환경에도 적용가능하다. 이 프레임워크는 여러개의 부문(part)로 구성된 표준으로 이루어진다.

제 1부: 키관리 프레임워크
제 2부: 대칭 암호기법을 이용한 키 관리
제 3부: 비대칭 암호기법을 이용한 키 관리

(3)안전 모델

안전 모델의 목적은 안전 프레임워크에서 상세히 규정된 안전성 개념을 개방형 시스템 구조의 특정 분야에 적용하는 것이다. 다만 OSI 기본 참조모델에 관련 한 안전 모델만이 여기에 규정되며 여타(예, ODP, DB)에 대한 모델은 향후 표준화 될 것이다.

(가) OSI 상위계층 안전 모델

이 표준의 목적은 표준개발자에게 OSI의 상위계층에서 안전성을 위하여 응용에 구애받지 않는 서비스와 프로토콜을 개발하기 위한 구조적 모델을 제공하고 다양한 응용에의 안전성 요구조건을 구현하기 위하여 이들 서비스와 프로토콜을 활용하도록 하는 것이다. 그리하여 내부적 안전 서비스를 포함하는 특정 응용을 위한 ASE의 필요성을 최소화한다. 또한 이 표준은 세션, 표현, 및 응용계층에서의 안전 서비스들간의 위치와 관계에 대하여 상세히 규정한다. 응용계층 과 표현계층으로부터의 안전성 변환 함수(예, 암호화) 및 안전성 검사값 함수의 취급도 규정되어 있다. 이러한 기법들은 상위계층에서 제공되는 거의 모든 안전서비스에 사용될 것이다.

(나) OSI 하위계층 안전 지침

이 안전 지침의 개발은 JTC1 SC6의 소관사항이다. 이들 지침의 목적은 표준개발자에게 OSI 기본참조모델의 하위계층에 알맞은 안전 관련 프로토콜과 이 프로토콜 요소의 개발을 위해 필요한 기초를 제공하는 것이다.

(4) OSI 관리의 안전

OSI 관리 표준에서의 안전 관련 사항으로 먼저 OSI 안전 관리 개요는 ISO 10164의 일부로서 안전 관리 기능에 대하여 개요를 수록하고 있으며, 이들이 OSI 기본참조모델 및 감사 프레임워크와 어떤 관계가 있는가를 규정하고 있다.

ISO DIS 10164-5의 경보보고 기능을 이용한 안전 경보 event를 발생시키기 위해 CMIS를 사용하는 응용에 의한 시스템 관리기능을 규정하고 있다. "event forwarding discriminator"의 생성, 삭제 및 수정을 통하여 보안경보 보고에 대한 제어가 가능하다. ISO DIS 10164-8은 audit trail log로 보내지는 event 보고에 관한 시스템 관리 기능을 규정하고 있다. 이는 ISO 10164-5, 6, CMIS등에 기초하고 있다. 또한 접근제어를 위한 객체와 어트리뷰트(ISO CD 10164-9)는 target 단말시스템에서의 관리 객체에 대한 접근제어의 제공을 모델링하고 있 다. 이는 접근제어 서비스를 제공하기 위한 기능을 갖는 관리 객체를 규격화함으로써 가능해진다.

ISO 9595(common management information service 정의)를 수정할 ISO 9595/PDAM 4는 접근제어 파라미터에 대하여 일부 수정하고 있다. 이는 각종 안전에 관련된 파라미터의 목적을 규정할 뿐, 아직 구체적인 특성과 형식이 정해지지 않고 있다. 디렉토리 인증 프레임워크는 certificate라고 하는 데이터 생성원인증 안전서비스와 무결성에 의해 보호되는 안전성 토큰을 규정하고 있다. 이는 공개키 암호시스템의 사용에 보호기능을 제공한다.

디렉토리 접근제어에 관하여서는 ISO 9594-1, 2, 3, 8의 PDAM에 규정되어 있으며 접근제어방식등을 정의하고 있다.

(5) OSI응용 계층의 보안

화일전송(FTAM)은 ISO 8571로 규정되는데 이에 대한 인증과 접근제어를 다루기 위한 새로운 표준화 작업이 시작되었다. 거래 처리(TP)에서의 안전 문제는 인증, 접근제어, 기밀성, 무결성, 부인 봉쇄, 감사, 접근권한 취소 등의 안전 서비스로 매우 광범위하다. ISO CD 10184-1에서 규정하는 단말관리에서의 안전문제는 아직 다루어지지 않고 있다. 그러나 JTM(ISO 8831)은 인증, 접근제어, 계정관리, 감사추적등에 대한 간단한 메카니즘을 제공한다.

현재 검토중인 안전성교환 ASE(application service element) 표준은 OSI 응용 계층에서의 안전 서비스 제공을 지원하는 기본 기능을 정의한다. 선택적 필드 보호의 요구조건 규격을 추상적 구문 형식으로 표현하고 안전성교환 및 변환을 규격화하기 위한 도구를 규정한다. 또한 ASE를 위한 안전 서비스 정의, 프로토콜 규격 및 PICS 프로포마를 규정한다.

ACSE(association control service element)의 인증 서비스는 ISO 8649/AMI에서 정의한다. 이는 A-associate request/confirmation에서 인증 정보를 전달할 필드를 제공하고 있다.

표현 계층에서의 기밀성 및 무결성은 connection oriented 표현계층 서비스 및 프로토콜 표준인 ISO 8822와 ISO 8823은 현재 개정 작업이 진행중이다.

표현계층의 암호기법은 connection-oriented 안전 서비스를 제공하며, 동등실체, 접속기밀성, 선택필드

기밀성, 접속무결성, 선택필드 접속 무결성등과 이를 표현계층에 수용하기 위한 표현계층 프로토콜도 규정하고 있다.

(6) 개방형 분산처리에서의 안전

이의 안전에 관한 표준은 개방형 분산처리 참조모델의 제 2부에 규정된 분산시스템의 6가지 측면중 하나이다. 이러한 안전성의 활용과 조직에 관한 학습자료가 본 참조모델의 1부에 수록되어 있다. 또한 이를 지원하는 특정 기능에 대한 요구조건은 3부에 규정되어 있다.

2) ISO/IEC JTC1 SC27

특정 정보통신 응용에 의존하지 않으면서 정보의 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, SC27에서는 다른 관련 연구그룹인 SC6와 SC21들과 긴밀한 업무교섭을 취하면서 표준화 활동을 하고 있다.

본절에서는 최근 SC27 제 4차 전체회의('92.10. 가이더스버그)에서 이루어진 표준화 과제에 대한 주요 결정사항을 실무작업반별로 소개하기로 한다.

(1) SC27/WG1(안전 요구조건, 안전 서비스 및 가이드라인)

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

또한 WG1에서 설정한 안전 서비스에 준거하여 WG2에서는 암호화 기법등을 이용한 안전 메카니즘을 연구한다.

(가)안전성 정보 객체

금융 업무와 사무자동화 시스템에서 안전성을 확보하기위하여 안전 서비스를 제공할 필요성이 여러가지 측면에서 논의되고 있다. 그러나 정보를 상대 시스템에 전송하는 기본적인 통신 형태에 있어 대단히 중요한 것 중의 하나로 안전성을 확보해야 하는 정보객체가 있다. 구체적으로 인증정보, 안전관리정보, 특권관리정보등에서 안전성을 주관하기 위하여 중심이 되는 객체를 가리킨다. WG1에서는 이러한 객체를 "안전성 정보 객체"(SIO: security information object)로 규정하고 있으며 관련 연구그룹과 함께 이를 명확히 표준화 시키고 있다. 이 SIO에는 안전성 레이블도 포함되어 있다.

현재 3차 작업 초안이 작성되어 각 회원기관에서 검토되고 있으며 '93.3까지 CD를 목표로 하고 있으며 관련 문서는 다음과 같다.

-SIO 제 1부: 방법과 지침(SC27 N604)

-SIO 제 2부: 요소 및 지네릭 규격(SC27 N605)

-SIO 제 3부: (SC27 N611)

(나)정보기술(IT) 안전관리 지침(GMITS)

이용자가 어떻게 안전성을 생각하고 관리하면 좋을 것인가의 지침을 작성하는 것을 목적으로 한다. 구체적으로는 다음의 3가지 부분으로 나누어 '93.3까지 CD를 목표로 표준화를 추진하고 있다.

- GMITS 제 1부(개념과 모델): 안전성 요구조건(리스크 리스트), 안전성 대책분석, 시행등을 규정(SC27 N607)
- GMITS 제 2부(관리 방법): 리스크, 보호대책, 시스템구성, 개발, 감사등의 관리 방법을 규정(SC27 N608)
- GMITS 제 3부(관리기법 및 메카니즘): 각 부분별 관리 방법, 기법 및 메카니즘을 규정(SC27 N609)

(다)키관리

SC27에서는 일반적인 암호키 관리 방식의 국제 표준화를 추진함을 목적으로 하지만 본 WG1에서는 키관리를 위한 프레임워크를 규정한다. 이 프레임워크는 특정 암호 알고리즘과 해쉬 함수, 특히 특정 통신 프로토콜에 의존하지 않는 키 관리를 위한 절차요소를 추상적으로 규정한다. 즉 암호키의 이용자 등록, 생성, 분배, 저장 및 관리에 관한 프레임워크를 결정한다.

이를 근거로 WG2에서는 이 프레임워크에 부합되는 키관리 메카니즘(비밀키 방식, 공개키 방식)을 검토하며 여타 ISO 연구그룹에서는 각 통신 응용에 알맞게 이 프레임워크와 WG2의 메카니즘에 준거한 키관리를 채택하여 표준화하고 있다.

현재 3차 작업 초안(SC27 N602: 키관리 제1부, 프레임워크)이 진행중에 있으며 '93년 CD로 추진할 예정이다.

(라)인증

통신시 상대 시스팀 또는 상대 이용자를 식별하고 검증하는 인증의 중요성이 인식되고 있다. WG1에서는 인증을 위한 일반 모델(IS 9798-1)을 표준화 시키기 위하여 SC21에서 표준화된 인증 프레임워크(CD 10118-2)에 준거하여 WG2가 검토하고 있는 비밀키 및 공개키를 이용한 인증 메카니즘을 위한 기본 모델을 규정한다.

이용자의 인증이라고 하는 관점에서 CCITT SG VⅡ이 다루는 디렉토리 서비스에서도 디렉토리 이용자의 인증을 표준화하고 있어 이들간에 호환성을 유지하고 있다.

(2) SC27/WG2(안전 기법과 메카니즘)

본 그룹은 SC27/WG1에서 규정한 안전 서비스에 필요로 하게 되는 안전기법과 메카니즘의 표준화를 주목표로 하며 비암호 방식을 이용한 안전기술에 대하여도 표준화함을 목표로 한다.

(가) 64비트 블럭 암호운용모드

암호운용모드는 암호알고리즘의 운용방법이다. ISO 8372(1987)로 표준화된 이 운용모드에서는 64비트 블럭암호에 대하여 암호 알고리즘을 그대로 이용하는 ECB(electronic codebook)모드, 암호출력 데이터에 다시 암호화와 XOR등의 연산을 하는 CBC (cipher block chaining)모드, CFB(cipher feedback)모드, 및 OFB(output feedback)모드를 규정하고 있다. 이들 암호 운용모드를 이용하면 암호강도를 강화시킬 수 있으며 암호화 단위를 1비트, 8비트, 64비트등으로 변경시킬 수 있다.

한편, 이번 가이더스버그 회의에서는 ISO/IEC 10116(n 비트암호운용모드,1991)과의 검토를 통하여 ISO/IEC 10116에서 n=64일 때의 적합성은 IS 8372와 적합함을 의미하는 것으로 검토되어 폐지하려 하였으나 64비트의 운용특성을 감안하여 그대로 두기로 결의하였다.

(나)실체인증

통신실체가 정당한 실체인가를 인증하기 위한 메카니즘으로서 기존의 3개의 부문에서 이번 가이더스버그 회의 결과 비가역 인증 메카니즘을 추가하여 표준화를 추진하고 있다.

- 실체인증 메카니즘 제 1부(일반모델): 실체인증의 프레임워크이며 다른 부문에서 공통적으로 사용하는 기법을 규정하고 있으며 ISO/IEC 9798-1 (1991)로 표준화되었음.
- 실체인증 메카니즘 제 2부(대칭기법 이용): 비밀키를 이용하는 경우를 규정하고 있다. 메카니즘으로서 2개의 실체뿐인 경우와 제 3자인 인증 서버를 개재시킨 경우로 표준화를 검토하고 있다. 현재 CD로서 우편투표를 진행중에 있으며 '93.3이후 DIS수준으로 발전시킬 예정임.
- 실체인증 메카니즘 제 3부(공개키기법 이용): 공개키 암호를 이용하여 통신실체를 인증하는 메카니즘을 표준화시키고 있다. 이 표준에서는 통신하고 있는 양측 중 한쪽만이 신분을 증명할 수 있는 single authentication과 양측 모두가 신분을 증명할 수 있는 mutual authentication으로 나누어 규정하고 있다.

  현재 DIS 9798-3의 우편투표를 진행중에 있으며 가이더스버그 회의 결과의 수정된 부분이 수록된 SC27 N573을 참고하여 투표하도록 권고함.
- 실체인증 메카니즘 제 4부(비가역함수 이용):가이더스버그 회의에서 신규과제(WG2 N183)로 채택되었음.

(다)데이터 무결성

통신데이터의 변조유무를 검출하기 위하여 사용되는 메시지 인증자(MAC: message authentication code)를 생성하고 검증하는 메카니즘이다. ISO/IEC 9797(1989)으로 표준화되었으며 송신자와 수신자의 MAC 생성법으로서 n비트 블럭암호와 2개의 비밀키를 이용한 방법 등을 규정하고있다. 이번 가이더스버그회의 결과, 제 4절의 "padding and blocking"의 note를 다음과 같이 교체토록 하고 이를 DIS 투표로 추진할 것을 결의하였다.

+note:검증자가 데이터의 크기를 모르면 padding mothod 2가 사용되어야 하며 그 이유는 이에 의해 검증자가 trailing '0' 비트의 추가 또는 삭제를 보호받도록 허용하기 위함임.

(라)부인봉쇄

서명자가 서명한 사실을 차후에 부인하는 경우 사실 관계를 판정하기 위하여 부인봉쇄 기술 표준화를 추진하고 있다. 신뢰할 수 있는 센터가 통신하는 양자 간의 데이터로그를 축적하는 방식과 축적하지 않는 방식으로 분류할 수 있다. 이는 3개의 부문으로 표준화 시키고 있다.

- 부인봉쇄 제 1부(대칭 암호 알고리즘을 이용한 일반 모델: WG2 N177)
- 부인봉쇄 제 2부(대칭 암호기법을 이용한 부인봉

쇄: WG2 N176)

- 부인봉쇄 제 3부(비대칭 암호기법을 이용한 부인봉쇄: WG2 N158)

현재 작업문서 형태로 표준화의 초기 상태이다.

(마)영지식 증명을 이용한 안전기법

영지식 증명이란 정보의 소유자를 검사자나 제 3자든지 누구에게나 그 정보의 일부도 누설시키지 않고 증명하는 수단으로서 실체인증, 데이터 인증, 디지틀 서명등에 적용되는 기술이다. 이 표준은 2개의 부문으로 표준화를 추진하고 있으며 이에는 context모델, 메시지 교환 모델 및 수학적 모델이 규정될 것이다.

-제 1부: 일반 모델

-제 2부: 식별 및 인수분해에 기초한 메카니즘

현재 표준화는 초보적 작업문서 수준에 불과하다.

(바)디지틀 서명

데이터와 그 작성자의 정당성을 인증하는 메카니즘으로서 2개의 연구과제로 표준화를 추진하여 메시지 복원형은 ISO/IEC 9796(1991)으로 표준화가 완료되었으며 부가형은 부뤼셀 회의(1991.10)에서 임프린트형을 ISO/IEC 9796과의 용어 호환성 유지를 위해 표준명을 부가형으로 변경시켜 Ad hoc 회의('92. 7.) 결과를 반영하여 작업문서를 보완시킬 예정이다.

- 메시지 회복형: 서명검증후에 메시지가 읽혀지는 방식
- 부가형: 메시지에 서명을 덧붙혀 메시지가 즉시 읽혀지는 방식으로 서명 부분의 길이는 메시지 길이에 무관하게 처리함.

(사) 해쉬함수

디지틀 서명의 효율화를 위하여 사용된 데이터 압축기능으로서 4개의 부문으로 표준화를 추진하고 있다.

-제 1부(일반 모델): 해쉬함수의 요구조건, 여타 부문에서 공통적으로 사용되는 기법을 규정함.

-제 2부(대칭 블럭암호 알고리즘을 이용한 해쉬): n비트 암호를 이용하여 해쉬함수를 만드는 방법을 규정함.

-제 3부(전용 해쉬 함수): 미국 RSA사의 MD5와 일본의 N-Hash등의 제안을 검토하고 있다.

-제 4부(모듈로 산술): 자승 합동식을 이용하여 해쉬함수 작성법을 검토하고 있다.

이번 가이더스버그 회의 결과, 제 1부와 제 2부는 각각 WG2 N177과 WG2 N181을 참고로 CD 10118-1과 CD 10118-2를 보완하여 DIS 투표를 진행중에 있다. 한편 제 3부와 제 4부는 계속 연구과제로 검토하기로 하였다.

(아)키관리 메카니즘

WG2에서는 키관리의 표준화중 프레임워크를 제외한 메카니즘을 2개의 부문으로 나누어 표준화를 추진하고 있음.

-제 2부: 대칭형 암호기법을 이용한 키관리

-제 3부: 비 대칭형 암호기법을 이용한 키관리

이번 가이더스버그 회의 결과 제 2부와 제 3부에 대하여 각각 WG2 N147과 WG2 N168을 수정보완하여 CD 투표를 준비중에 있다.

(3) SC27 WG3(안전 평가 기준)

(가)WG3 의 활동목표

WG3 에서는 IT 시스템/ 부품/ 제품의 안전성 평가와 인증에 관한 표준을 제정함을 목표로 한다. 이 표준화 대상에는 단일 시스템 뿐만아니라 분산 시스템, 컴퓨터망, 관련 응용 서비스까지도 포함하고 있다. 여기서는 이들에 대한 다음 사항을 표준화하고 있으며 그 중 평가기준을 중점 추진하고 있다 :

o 평가기준

o 평가기준 적용방법

o 평가, 인증, 검정에 관한 관리 절차

(나)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 Book)
- 1989 영국 CESG CESG Memorandum Number 3 (Red Book) (*)
  DTI Green Book Series
  독일 ZSI IT-Security Criteria
  (Blue & White Book)
  프랑스 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

주:(*)국가기밀을 취급하는 시스템용 (국가안전보장, 국방, 외교용)

더욱이 미국에서는 국립컴퓨터보안센터(NCSC)에서 시험 및 인증을 하도록 하는 체제가 되어 있으며 1991년부터는 기밀 데이터시스템의 정부조달에 대하여는 이인증을 반드시 받도록 규정되어 있다.

1990년 영, 불, 독, 화란 4개국에 의한 ITSEC는 영, 불, 독의 개별적 활동에 대하여 EC권역 시장통합등의 사정을 고려하여 유럽공업연합회(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 이와 같은 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 이 평가기준의 표준화를 과제화한 것이다.

(다)WG3의 표준화 활동

WG3에서는 3개의 표준화 과제를 추진하고 있으며 가이더스버그 회의 결과까지의 표준화 활동은 다음과 같다 :

○ Glossary of terms

SC27과 그 산하의 WG의 표준화 활동을 원활히 추진하기 위한 용어 및 정의의 기본 근거를 제공하기 위하여 SC27의 활동과 관련된 신뢰할만한 자료에 근거한 안전에 관한 용어집으로 WG3 N102를 선택, 결정하였다.

○ IT 안전성 평가 기준

3개의 부문으로 나누어 표준화를 추진하고 있으나 초보적인 작업문서 수준이다.

제 1부(일반 모델): WG3 N128에 따라 현행화 시키기로 함.

제 2부(IT 시스템의 기능 등급): WG3 N129에 따라 현행화 시키기로 함.

제 3부(IT시스템의 보증): WG3 N130에 따라 현행화 시키기로 함.

○ IT안전성 평가 기준을 위한 요구조건의 수집과 분석

국제적인 안전기술연구기관과의 공동보조를 취하기 위하여 WG3에서는 이 연구과제를 하위 우선순위를 부여하기로 하였다.

2. CCITT SG VⅡ의 표준화 활동

CCITT '89-'92 연구회기중 SG VⅡ WP4에 부여된 안전기술에 관한 과제는 Q.18(메시지처리시스팀), Q.19(분산 응용시스팀의 지원위한 프레임워크) 및 Q.20(디렉토리 시스팀)중 그들 과제의 소과제에 포함시켜 ISO/IEC JTC1과 협력하여 표준화 작업을 수행하고 있다. 본절에서 WP /4에서의 이번 연구회기에 표준화 연구결과의 권고화가 가능한 Q.19 및 Q.20 본과제의 안전기술에 대한 활동목표와 87년 7월부터 92년 10월까지 5차에 걸친 회의 결과를 토대로 안전 기술 표준화 현황을 소개한다.

1) Q.19/VⅡ

본과제의 전문가 그룹은 MHS와 디렉토리 시스팀의 표준화 과정에서 일반 유틸리티가 될 것으로 예상되는 안전에 대한 메카니즘과 기술개발 필요성의 인식과 ISO/IEC JTC1에서 안전기술에 대한 표준을 정의함을 인식하여 분산응용 시스팀 및 데이터통신에 일반적으로 정의되어 사용할 수 있는 관련 안전 프레임워크 및 안전모델의 표준화 연구를 수행한다. 또한 이러한 프레임워크를 정의하고 지원하기 위하여 개발하고 사용할 수 있는 안전 메카니즘(예, 액세스 제어, 인증, 공증, 디지틀서명 등)과 안전관리 원칙 및 기술의 표준화 연구를 수행한다.

2) Q.20/VⅡ

본과제의 전문가 그룹에서는 인증을 위하여 디렉토리를 활용하는 응용시스팀의 요구조건을 만족시키기 위하여 88년에 권고 X.509로 표준화한 디렉토리 인증 프레임워크에서 기본적 엑세스 제어 기술을 지원하기 위하여 본 권고를 개정하였다.

3) '89-'92 연구회기중 SG VⅡ에서의 안전기술 권고(안) 처리 및 향후 계획

'89-'92 연구회기중 SG VⅡ에서는 Q.19/VⅡ과 관련하여 X.800를 제정하여 1991. 3 신속권고 처리절차에 의거 권고로 확정하였으며 Q.20/VⅡ과 관련하여서는 X.509에 대하여 사용자 공개키 획득에 관한 ASN.1 표기의 명확화 등에 대한 일부사항 개정을 제 10차 총회(세계 전기통신 표준화회의)에서 권고로 확정할 예정이였다.

더욱이 개방형 안전시스팀 및 분산응용 시스팀의 지원을 위한 프레임워크에 대한 안전기술 표준안을 '93-'94 연구회기에 X.9xx 계열로 표준화할 계획을 가지고 있으며 그 내용은 표 3과 같다.

표 3. CCITT SG Ⅶ의 표준화활동 현황 및 계획

분 야	권고(안) 번 호	제.개정	제 목	권 고 승 인 년 도			최근 관련 문서
				신속처리	제 1 차 WTSC (X차총회)	차기 연구 회기	
Q.19/Ⅶ	X.800	제정	OSI 안전구조	○ (1991)			X.800
	X.9xx (X.authfw)	제정	개방형시스템 안전프레임워크 : 인증 프레임워크		○ ('93.6)		
	X.9xx (X.ulsm)	제정	분산응용시스템의 지원위한 프레임워크 : 상위계층 안전모델		○ ('93.6)		
	X.9xx	제정	분산응용시스템의 지원위한 프레임워크 : 안전개요			○ (1994)	
	X.9xx	제정	분산응용시스템의 지원위한 프레임워크 : 인증서버			○ (1994)	
	X.9xx	제정	개방형시스템 안전프레임워크 : 안전 프레임워크 개요			○ (1994)	TD 5380 ('92.10)
	X.9xx	제정	분산응용시스템의 지원위한 프레임워크 : 분산응용시스템의 안전모델			○ (1994)	
	X.9xx	제정	분산응용시스템의 지원위한 프레임워크 : 안전 응용지침			○ (1994)	
	X.9xx	제정	개방형시스템 안전프레임워크 : 접근제어 프레임워크			○ (1994)	
	X.9xx	제정	개방형시스템 안전프레임워크 : 부인봉쇄 프레임워크			○ (1995)	TD 5379 ('92.10)
	X.9xx	제정	개방형시스템 안전프레임워크 : 무결성 프레임워크			○ (1995)	TD 5376 ('92.10)
	X.9xx	제정	개방형시스템 안전프레임워크 : 기밀성 프레임워크			○ (1995)	TD 5375 ('92.10)
	X.9xx	제정	개방형시스템 안전프레임워크 : 안전감사 프레임워크			○ (1996)	TD 4190 ('91.11)
Q.20/Ⅶ	X.509	개정	디렉토리-인증 프레임워크		○ ('93.3)		COM Ⅶ-R50
Q.21/Ⅶ	X.NLSP	제정	OSI 상위계층 안전 프로토콜		○ ('93.6)		
	X.TLPS	제정	OSI 상위계층 안전 프로토콜		○ ('93.6)		

Ⅴ. 안전 기술의 국내 표준화 활동 및 방향

국내에서는 80년대부터 통신분야의 안전문제에 관하여 일부 연구기관에서 암호화 알고리즘 및 실용화 기술개발 연구를 수행하여 왔으며 90년 말에 한국통신 정보보호학회가 발족하여 산.학.연의 정보보호, 암호학 및 표준화에 관한 연구의 활성화를 유도하고 있다. 또한 91년말에는 정보 산업분야 국내 및 국제표준화 활동의 활성화와 이의 표준화 작업의 효율성 극대화를 목표로 정보산업 표준원이 설립되어 산하위원회를 조직 운영하고 있다. 최근 JTC1 SC27에 대응한 연구활동 활성화를 위한 국내 위원회를 설립하여 정보 안전기술의 표준화 연구를 수행하고 있으며 제4차 SC27 전체회의('92. 10, 가이더스버그)에 'O' 회원으로 참여하여 국제 표준화에도 기여하고 있다.

그러나 'O' 회원에 대한 표준화 활동의 한계로 인하여 '92년말에 'P' 회원으로 정식 가입함에 따라 국내 및 국제 표준화 활동시 한국의 입장을 반영키기 위한 많은 노력이 요구되고 있다. 한편 CCITT SG Ⅴ Ⅱ에 대응하여서는 한국통신 기술협회에 ITU 국내연구단 SG ⅤⅡ이 운영되고 있으나 안전기술관련 표준화 연구는 미진한 상태이다.

그러나 국내표준화 활동 결과로서는 정보통신 설비에 관한 안전 신뢰성 기준이 체신부 고시로 제정(제103 호.90.10)되었으며 이의 이행을 위하여 세부 운영관리기준을 기간통신 사업자와 정보통신 역무제공업자가 제정 시행하고 있다. 또한 최근 전산망 안전신뢰성 기준(안)에 대한 사업자 의견을 수렴한 바 있으며 곧 체신부 고시로 제정될 전망이다.

더욱이 이러한 기술기준에 대하여 기술기준의 적합의무를 기본법(제25 조)으로 명시함에 따라 통신사업자들은 이를 준수하기 위한 표준평가 및 적합성 시험 연구, 안전 요소기술 표준화 활동을 보다 강화해 가야 할 것이다.

또한 현 통신제도 환경에서는 공중통신 채널을 통한 전송정보의 암호화와 같은 기밀성 서비스를 제외한 전송정보의 무결성 서비스, 통신 상대의 인증서비스 등이 가입자에 제공가능한 안전 서비스로서 고려될 수 있으므로 이를 MHS, EDI, 디렉토리 등 각종 정보통신 서비스에 적용하여 상용화할 수 있을 것으로 생각된다. 따라서 각 통신 사업자간의 안전서비스 상호연동을 위하여 Ⅳ장 에서 제시된 안전서비스의 요소기술을 통신사업자, 제조업자, 사용자간 상호조 화를 이루어 단계적이며 점진적인 표준화 활동을 추진해 가야할 것이다.

Ⅵ. 결 론

정보화사회로의 진행과정에서 개방형 통신망을 통한 가입자 상호간의 정보유통은 사회 경제 활동의 고도화에 따라 더욱 다양하고 다량화될 전망이다. 이들 가입자에게 유통정보를 안전하고 신뢰성 있게 전달하기 위하여 안전 서비스 요구는 필연적이 될 것이다.

이러한 안전 서비스의 제공에 따라 사업자 측면에서는 관련 장비의 상호운용성 확보와 연구개발 또는 도입제품 평가의 용이성을 위하여 표준화가 필요하며 제품생산자 측면에서는 생산 원가의 저렴화를 위하여 반드시 표준화가 필요하다.

본 논문에서는 개방형시스팀 안전기술중 개방형 정보통신에서 표준화해야 할 범위에 대하여 OSI기본참조모델에 기초한 안전기술의 구조, 프레임워크 등의 표준화와 특정 통신 어플리케이션에 의존하지 않는 안전 기술의 표준화에 대하여 ISO/IEC JTC1의 SC21과 SC27 및 CCITT SG ⅤⅡ의 국제표준화 연구 활동을 중심으로 소개하였다. 또한 국내에서의 안전 기술 표준화 현황을 파악함으로써 통신사업자가 정보통신 사업에서 소요되는 안전 기술 및 이의 표준화 방향을 살펴보았다.

한편 국내 통신망사업자 및 기업체에서도 정보통신 안전서비스를 위하여 독자적으로 자체고유의 안전 체제에 의한 망구축 및 운용이 예상되어 국가전체적인 측면에서 투자비 증가 및 상호운용성의 문제가 야기될 수 있다. 이에 대하여 본 논문에서 소개한 다양한 안전성 알고리즘과 기법을 체계적이고 적절히 표준화시켜 적용함으로써 이를 해결할 수 있겠으며 특히 통신 사업자들은 이를 위하여 안전기술을 적용할 서비스와 설비에 대하여 관련표준화 기관과의 상호조화에 의한 선행기술 표준화를 통한 신기술의 개발을 선도해가야 할 것이다.

參 考 文 獻

[1] 太田和夫, "情報 セキュリテイの 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

[2] CEN/CENELEC AD Hoc Security Group, "Towards a Taxonomy for Standardisation of Security", ISO/IEC JTC1/SC27/WG20.1 N248, 1990. 4

[3] C.Siuda, "Security Standards for Open Systems", Proceedings of Symposium IFIP WG6.5 MHS System and Application Layer Communication Protocols, B4 -1~B4-20, Oct 3-5. 1990.

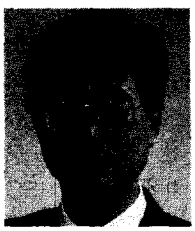
[4] ISO/IEC JTC1/SC21, "Revised Guide for Open Systems Security", ISO/IEC JTC1/ SC27 N519, 1992.5

[5] 장청룡외 1인, "ISO/IEC JTC1 SC27 제4차 전체회의 및 WG 회의 참석", 공무국외 여행 귀국보고서, 1992. 11

[6] CCITT SG VⅡ, "Status Report on CCITT SG Activities", Geneva, June 1992.

[7] ISO/IEC JTC1/SC27, "Report of JTC1 SC27 to the October 1991 JTC1 Plenary Meeting in Madrid 25", ISO/IEC JTC1/SC27 N1940, 1991.8

筆 者 紹 介



張 靑 龍

1957年 5月 27日生

1980年 3月 성균관대학교 전자공학과 졸업

1986年 8月 연세대학교 대학원 전자공학과 졸업

1979年 12月 ~ 1983年 12月 한국전기통신연구소 연구원

1984年 1月 ~ 현재 한국통신 연구개발단 선임연구원

주관심분야 : 암호 이론, 정보보호기술