□ 기술해설 □

국내·외 정보보호관련 표준화 동향

한국정보보호센터 김학범*·이철원·홍기웅**·심주걸

1. 서 론

정보통신은 21세기 고도화정보사회의 기반요소로서 인식되고 있으며 이에 따라 세계 각국은 자국의 생존과 번영을 위하여 정보통신을 통한 국가경쟁력 강화에 총력을 기울이고 있다. 이러한 정보통신의 국가경쟁력을 효율적으로 구현하기 위한 중요한 수단이 바로 정보통신표준화이다. 정보통신 기기 및 시스템간의 원활한 이용을 위해서는 이들 상호간 상호운용성의 확보가 필요하며, 이는 필연적으로 정보통신표준화의 중요성을 증대시키고 있다. 또한 정보통신표준화가 활성화되면 될수록 정보보호에 관한 표준화 역시 중요한 문제로 대두되게 된다.

본 고에서는 정보보호 산업의 육성과 더불어 중요성이 부각되고 있는 정보보호 관련 국 내외 표준화 활동을 조사하였다.

2. 국제표준화 활동

국제표준화의 목적은 국제적으로 통일된 표준 규격을 제정하여 국가간의 통상을 원활히 하며, 과학 및 경제 등 다방면에 걸쳐 국제협력을 추진하는 것이다. 정보보호와 관련한 국제표준화 활동은 ISO/IEC JTC 1, ITU-T를 중심으로 하는 정보처리 및 정보통신 표준화와 인터넷에 관련된 표준을 개발하는 IETF, 초고속정보통신기반과 관련된 표준화 활동, 업체들을 중심으로 활동하는 사실 단체 표준화 활동으로 대별될 수 있다.

2.1 ISO/IEC JTC 1

ISO(International Organization for Standardization)는 지적 과학적 기술적 및 경제적 활동 분야에 있어서의 국제간 협력을 도모하고 국제표준의 제정 심의 및 발행을 촉진하는 비정부간 협의기구로 1947년 스위스 민법 제60조에 의거하여 발족된 사단법인이다.

IEC(International Electrotechnical Commission)는 전기기술 전반에 걸쳐 전기 및 전자, 원자력 분야 등의 표준화에 관한 국제협력을 도모하며 각국의 의사를 집결한 IEC 표준을 발행하는 비정부간 협의기구로 스위스 민법 제60조에 의거하여 1906년 발족된 사단법인이다. IEC도 ISO와 마찬가지로 전문위원회, 분과위원회(SC : SubCommittee), 실무위원회(WG : Working Group)를 구성하여 표준을 작성한다.

정보기술을 담당하는 ISO의 TC97과 IEC의 TC83(정보처리기기)을 통합하여 1987년 11월 설립된 합동기술위원회 JTC 1(Joint Technical Committee 1)은 일반 정보기술표준의 개발을 담당하며 현재 19개의 분과위원회(SC1-용어, SC2-문자세트 코드, SC6-정보통신 및 시스템간 정보교환, SC7-소프트웨어공학, SC11-디지탈데이타 교환용 플렉시블 자기매체, SC14-데이타 요소의 표현, SC17-식별카드 및 관련 장비, SC18-문서처리와 관련 통신, SC21-개방형시스템 상호접속, 데이타 관리 및 개방형 분산 처리, SC22-프로그래밍 언어 및 환경과 시스템 소프트웨어 인터페이스, SC23-정보교환용 광학디스크 카트리지, SC24-컴퓨터 그래

*정 회 원
**종신회원

표 1 ISO/IEC JTC 1 정보보호 관련 표준화 목록

표준번호	제 목	년도	위원회	비 고
ISO/IEC 10736	Information processing-Telecommunications and information exchange between systems-Transport layer security protocol	1995	SC6	KCS-300
ISO/IEC 11577	Information processing-OSI-Network layer security protocol	1995	〃	
ISO 7498-2	Information processing systems-OSI-Basic Reference Model-Part 2 : Security Architecture	1989	SC21	KS C 5869
ISO/IEC 10164-7	Information technology-OSI-System management : Security alarm reporting function	1992	〃	
ISO/IEC 10164-8	Information technology-OSI-System management : Security audit trail function	1993	〃	
ISO/IEC 10181-1	Information technology-OSI-Security frameworks for open systems : Overview	1996	〃	
ISO/IEC 10181-2	Authentication framework	1996	〃	
ISO/IEC 10181-3	Access control framework	1996	〃	
ISO/IEC 10181-6	Integrity framework	1996	〃	
ISO/IEC 10181-7	Security audit and alarm framework	1996	〃	
ISO/IEC 10745	Information technology-OSI-Upper layers security model	1995	〃	
ISO/IEC 11586-1	Information technology-OSI-Generic upper layers security : Overview, models and notation	1996	〃	
ISO/IEC 11586-2	Generic upper layers security : Security Exchange ServElement (SESE) service definitionice	1996	〃	
ISO/IEC 11586-3	Generic upper layers security : Security Exchange Service Element(SESE) protocol specification	1996	〃	
ISO/IEC 11586-4	Generic upper layers security : Protecting transfer syntax specification	1996	〃	
ISO 8372	Information processing-Modes of operation for a 64-bit block cipher algorithm	1987	SC27	KS C 5767
ISO 9160	Information processing-Data encipherment-Physical layer interoperability requirements	1988	〃	KS C 5884
ISO/IEC 9796	Information technology-Security techniques-Digital signature scheme giving message recovery	1991	〃	KS C 5791
ISO/IEC 9797	Information technology-Security techniques-Data integrity mechanism using a cryptographic check function employing a block cipher algorithm	1994	〃	KS C 5792
ISO/IEC 9798-1	Information technology-Security techniques-Entity authentication mechanisms-Part 1 : General model	1991	〃	KS C 5794
ISO/IEC 9798-2	Part 2 : Mechanisms using symmetric encipherment algorithms	1994	〃	
ISO/IEC 9798-3	Part 3 : Entity authentication using a public key algorithm	1993	〃	
ISO/IEC 9798-4	Part 4 : Mechanisms using a cryptographic check function	1995	〃	
ISO/IEC 9979	Data cryptographic techniques-Procedures for the registration of cryptographic algorithms	1991	〃	
ISO/IEC 10116	Information technology-Modes of operation for an n-bit block cipher	1991	〃	
ISO/IEC 10118-1	Information technology-Security techniques-Hash-functions —Part 1 : General algorithm	1994	〃	KS C 5793
ISO/IEC 10118-2	Part 2 : Hash-functions using an n-bit block cipher algorithm	1994	〃	
ISO/IEC 11770-1	Information technology-Security techniques-Key management — Part 1 : Framework	1996	〃	
ISO/IEC 11770-2	Part 2 : Mechanisms using symmetric techniques	1996	〃	

픽 및 이미지 처리, SC25-정보기기 상호접속, SC26-마이크로프로세서 시스템, SC27-정보보호기술, SC28-사무기기, SC29-오디오, 그림, 멀티미디어 및 하이퍼미디어 정보의 코딩, SC30-개방형 EDI, SC31-Automatic data capture)가 활동 중이며 이중 정보보호 관련 분과위원회로는 SC6, SC21 및 SC27이 있다[1].

SC27의 WG1에서는 특정의 통신 응용에 의존하지 않는 정보보호 기술에 관한 안전성의 요구사항이나 정보보호 서비스를 추출하여 정보기술 분야의 프레임워크를 구축하는 것을 목표로 한다. WG2에서는 WG1에서 규정한 정보보호 서비스에 필요한 안전 기법과 메카니즘의 표준화를 목표로 하며 비암호 방식을 이용한 정보보호 기술에 관한 표준화를 수행한다. WG3에서는 IT 시스템, 부품 및 제품의 안전성 평가와 인증에 관한 표준을 제정하며 평가기준의 개발, 평가기준의 적용방법 개발, 평가와 인증 그리고 보증기법의 관리절차 개발 등의 활동을 한다. 표 1은 ISO/IEC JTC 1의 정보보호 분야의 표준 목록이다.

2.2 ITU-T

ITU-T(International Telecommunication Union-Telecommunication)는 유·무선이 각각 CCITT(International Telegraph and Tel-

표 2 ITU-T의 정보보호 관련 표준 목록

표준번호	제 목	년도	비 고
X.273	Information Technology-OSI-Network Layer Security Protocol	1994	
X.400	Message Handling System and Service Overall	1988	KCS 45
X.402	Message Handling Systems : Overall Architecture	1988	KCS 46
X.411	Message Handling Systems-Message Transfer System : Abstract Service Definition and Procedures	1992	KCS 50
X.419	Message Handling Systems : Protocol Specifications	1988	KCS 52
X.420	Message Handling Systems : Interpersonal Message System	1988	KCS 53
X.435	Message Handling Systems : Electronic Data Exchange Messaging System	1991	KCS 124
X.500	Information Technology-OSI-The Directory : Overview Concepts, Models, and Services	1993	KCS 86
X.509	Information Technology-OSI-The Directory : Authentication Framework	1993	KCS 88
X.519	Information Technology-OSI-The Directory : Protocol Specifications	1993	KCS 91
X.740	Information Technology-OSI-Systems Management : Security Audit Trail Function Technical Corrigendum 1	1995	
X.741	Information Technology-OSI-Systems Management : Objects and Attributes for Access Control	1995	
X.800	Security Architecture for Open Systems Interconnection for CCITT Applications	1991	
X.803	Information Technology-Open Systems Information-Upper Layer Security Model	1994	
X.810	Information Technology-OSI-Security Frameworks for Open Systems : Overview	1995	
X.811	Information Technology-OSI-Security Frameworks for Open Systems : Authentication Framework	1995	
X.812	Information Technology-OSI-Security Frameworks for Open Systems : Access Control Framework	1995	
X.814	Information Technology-OSI-Security Frameworks for Open Systems : Confidentiality Framework	1995	
X.815	Information Technology-OSI-Security Frameworks for Open Systems : INTEMS : Integrity Framework	1995	
X.816	Information Technology-OSI-Security Frameworks for Open Systems : Security Audit and Alarms Framework	1995	
X.830	Information Technology-OSI-Generic Upper Layers Security : Overview, Models and Notation	1995	
X.831	Information Technology-OSI-Generic Upper Layers Security : Security Exchange Service Element(SESE) Service Definition	1995	
X.832	Information Technology-OSI-Generic Upper Layers Security : SESE Protocol Specification	1995	
X.833	Information Technology-OSI-Generic Upper Layers Security : SESE Protecting Transfer Syntax Specification	1995	

ephone Consultative Committee)와 CCIR (International Radio Consultative Committee)에서 분리되어 추진되어 오던 것을 데이타 전송과 국제간의 전신전화에 대한 표준화를 담당했던 CCITT가 CCIR의 일부를 통합 조정하여 1993년 세계전기통신표준화회의에서 개칭한 것이다. ITU-T는 ITU의 상설기관으로 전기통신 표준에 대한 연구를 수행한다. 현재 15개의 연구그룹(SG1 : 서비스 정의, SG2 : 통신망 운영, SG3 : 요금 및 계정 원칙, SG4 : 통신망 유지보수, SG5 : 전자기적 방해에서 통신보호, SG6 : 옥외 설비, SG7 : 데이타 통신망과 개발 시스템 통신, SG8 : 텔레마틱 서비스를 위한 단말기, SG9 : TV와 음성 방송, SG10 : 전기통신 응용 언어, SG11 : 교환과 신호방식, SG12 : 통신망과 단말기의 점대점 전송, SG13 : 일반적인 통신망 측면 연구, SG14 : 데이타 전신과 텔레마틱 모뎀과 전송, SG15 : 전송 시스템 장치)이 활동중이며 정보보호에 관한 연구는 미비한 실정이며 SG7 연구그룹에서 활동하고 있다. 표 2는 ITU-T의 정보보호 분야의 표준 목록이다.

2.3 IETF

IETF(Internet Engineering Task Force)는 인터넷에 대한 프로토콜 공학과 개발 수단을 제공한다. IETF는 인터넷 구조와 운용에 관련된 망 설계자, 운영자, 벤더 및 연구자들로 구성된 국제적인 집단이다.

IETF의 실제 기술적인 작업은 주제별로 나누어진 작업반에서 이루어진다. 회의는 1년에 3번씩 개최되며 수시로 메일을 통해 작업이 된다. IETF에서는 9개 분야(응용, 일반, 인터넷, 망관리, 운용 요구사항, 라우팅, 정보보호, 트랜스포트, 사용자 서비스)로 나뉘어져 활동을 하고 있으며, 정보보호 분야는 9개 분야(인증된 Firewall 트래버설, 공통 인증 기술, 도메인 명 시스템 보안, IP 보안 프로토콜, 일회용 패스워드 인증, 공개키 구조, 단순 공개키 구조, 수송층 보안, 웹 트랜잭션 보안)로 세분화되어 작업이 진행중이다[2].

표 3은 IETF의 정보보호 분야의 표준 목록이다.

2.4 DAVIC

DAVIC(Digital Audio-Visual Council)은 디지탈 방송 등을 포함하는 멀티미디어 정보서비스의 세계통일규격 책정을 목표로 광대역 디지탈 음성 및 화상서비스에 대한 국제표준을 제정하는 국제 비영리 순수 표준화기구로 연 4회 북미, 유럽, 아시아지역을 순회하면서 회의를 개최한다. DAVIC의 목적은 초고속 통신망 또는 디지탈 위성방송 등 다양한 통신매체를 이용하여 전세계 멀티미디어 서비스의 상호운용성을 보장하기 위한 광대역 디지탈 서비스의 국제 표준안 제정이다. 그리고 광대역 대화형 음성 및 영상 서비스의 호환성 및 상호 운용성을 보장하는 기술규격을 작성하며, 잠정 표준 규격 확인을 위한 상호 운용성 시험을 실시한다.

스위스에 본부를 두고 있는 DAVIC은 1994년 8월에 출범하였으며 현재 25개국 이상의 200개 회사가 넘는 오디오-영상 사업의 모든 분야를 대표하는 정부기관 및 연구기관 뿐만 아니라 기업체(컴퓨터, 전송장비) 및 서비스(방송, 통신, CATV) 관련 분야를 포함하는 회원을 확보하고 있다[3].

DAVIC의 명세서는 버전 DAVIC 1.0, DAVIC 1.1, DAVIC 1.2, DAVIC 1.3 등으로 발행되었으며 DAVIC 1.0은 TV 배포, VOD(Video On Demand), 텔레쇼핑의 몇가지 기본적인 형태와 같은 초기 응용을 지원하는 시스템의 배치를 허용하는 명세서이다. DAVIC 명세서에서는 DAVIC 시스템에서 요구되는 기능들의 규정을 그 기능을 사용하는 응용들의 사용을 허용하는 기술적인 "도구"를 정의한다. 각각의 버전에는 각 분야별로 이들 도구들을 정의하고 있는데 정보보호에 관련된 부분이 part 10에 정의되어 있으며 현재의 버전은 DAVIC 1.2 Specification Part 10(Basic Security Tools for DAVIC 1.0)이다[4].

이 명세서의 내용에는 스크램블링 알고리즘, 키관리, 인증, 정보보호 장치 및 안전한 금융 트랜잭션을 가능하게 하는 기술 등을 포함한다. 표 4는 DAVIC 1.2 명세서의 분야별 제목이다.

표 3 IETE의 정보보호 관련 표준 목록

표준번호	제 목	년도
RFC 1244	Site Security Handbook	1991
RFC 1281	Guidelines for the Secure Operation of the Internet	1991
RFC 1319	The MD2 Message-Digest Algorithm	1992
RFC 1320	The MD4 Message-Digest Algorithm	1992
RFC 1321	The MD5 Message-Digest Algorithm	1992
RFC 1352	SNMP Security Protocols	1992
RFC 1411	Telnet Authentication . Kerberos Version 4	1993
RFC 1412	Telnet Authentication ' SPX	1993
RFC 1421	Privacy Enhancement for Internet Electronic Mail : Part I : Message Encryption and Authentication Procedures	1993
RFC 1422	Privacy Enhancement for Internet Electronic Mail : Part II : Certificate-Based Key Management	1993
RFC 1423	Privacy Enhancement for Internet Electronic Mail : Part III : Algorithms, Modes, and Identifiers	1993
RFC 1424	Privacy Enhancement for Internet Electronic Mail : Part IV : Key Certification and Related Services	1993
RFC 1455	Physical Link Security Type of Service	1993
RFC 1457	Security Label Framework for the Internet	1993
RFC 1472	The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol	1993
RFC 1507	DASS-Distributed Authentication Security Service	1993
RFC 1509	Generic Security Service API : C-bindings	1993
RFC 1510	The Kerberos Network Authentication Service (V5)	1993
RFC 1535	A Security Problem and Proposed Correction With Widely Deployed DNS Software	1993
RFC 1675	Security Concerns for IPng	1994
RFC 1704	On Internet Authentication	1994
RFC 1750	Randomness Recommendations for Security	1994
RFC 1760	The S/KEY One-Time Password System	1994
RFC 1810	Report on MD5 Performance	1995
RFC 1824	The Exponential Security System TESS : An Identity-Based Cryptographic Protocol for Authenticated Key-Exchange (E.I.S S.-Report 1995/4)	1995
RFC 1825	Security Architecture for the Internet Protocol	1995
RFC 1826	IP Authentication Header	1995
RFC 1827	IP Encapsulating Security Payload (ESP)	1995
RFC 1828	IP Authentication using Keyed MD5	1995
RFC 1829	The ESP DES-CBC Transform	1995
RFC 1847	Security Multiparts for MIME : Multipart/Signed and Multipart/Encrypted	1995
RFC 1848	MIME Object Security Services	1995
RFC 1851	The ESP Triple DES-CBC Transform	1995
RFC 1852	IP Authentication using Keyed SHA	1995
RFC 1858	Security Considerations for IP Fragment Filtering	1995
RFC 1864	The Content-MD5 Header Field	1995
RFC 1910	User-based Security Model for SNMPv2	1996
RFC 1915	Variance for The PPP Connection Control Protocol and The PPP Encryption Control Protocol	1996
RFC 1938	A One-Time Password System	1996
RFC 1948	Defending Against Sequence Number Attacks	1996
RFC 1949	Scalable Multicast Key Distribution	1996
RFC 1961	GSS-API Authentication Method for SOCKS Version 5	1996
RFC 1964	The Kerberos Version 5 GSS-API Mechanism	1996
RFC 1969	The PPP Encryption Control Protocol (ECP)	1996
RFC 1984	IAB and IESG Statement on Cryptographic Technology and the Internet	1996
RFC 1991	PGP Message Exchange Formats	1996
RFC 1994	PPP Challenge Handshake Authentication Protocol (CHAP)	1996
RFC 2003	IP Encapsulation within IP	1996
RFC 2065	Domain Name System Security Extensions	1996
RFC 2078	Generic Security Service Application Program Interface, Version 2	1997
RFC 2082	RIP-2 MD5 Authentication	1997
RFC 2104	HMAC : Keyed-Hashing for Message Authentication	1997

표 4 DAVIC 1.2 명세서의 분야별 제목

Part	제 목
Part 1	Description of DAVIC Functionalities(Technical Report)
Part 2	System Reference Models and Scenarios(Technical Report)
Part 3	Service Provide (Technical Report)
Part 4	Delivery System Architecture And Interfaces
Part 5	Service Consumer System Architecture and High Level API(Technical Specification)
Part 6	Reserved
Part 7	High and Mid-Layer Protocol(Technical Specification)
Part 8	Lower-Layer Protocols and Physical Interfaces (Technical Specification)
Part 9	Information Representation(Technical Specification)
Part 10	Basic Security for DAVIC
Part 11	Usage Information(Technical Specification)
Part 12	Reference Points, Interfaces and Dynamics(Technical Specification)
Part 13	Conformance and Interoperability

2.5 IISP

IISP(Information Infrastructure Standards Panel)는 ANSI가 후원하며, GII(Global Information Infrastructure)에 중요한 표준 개발을 용이하게 하기 위하여 국가적인 자발적 표준 시스템 내에 설립되었다. 실제 표준화 작업은 IISP 회원들이 포함된 전 산업적인 표준 개발 조직에 의해 수행되어진다. IISP는 필요한 표준을 개발하기 위한 개념, 운영방법 및 작업계획 등의 동의를 얻음으로서 정보 인프라의 개발을 쉽게 한다. IISP 작업그룹은 7개(WG1-공통적인 개념, WG2-표준 프레임워크 관리, WG3-표준 개발 및 트래킹 시스템 WG4-User/Content Provider 표준 요구사항(정보보호 포함), WG5-NII/GII의 국제적인 양상, WG6-범 산업적인 이해와 협동, WG7-정부의 역할)로 나뉘어져 활동하고 있다[5].

2.6 기타

●암호 알고리즘 표준화

암호알고리즘 DES(Data Encryption Standard)는 1972년 미국의 NBS(National Bureau of Standards, 현재는 NIST(National Instsitute of Standards and Technology))에서 공모하여 IBM이 개발한 암호알고리즘으로 1977년 미연방 표준으로 공표되었다. 이외에 구소련의 GOST(GOvernment STandard of the U.S.S.R), 스위스에서 개발하여 유럽표준이 된 IDEA(International Data Encryption Algorithm) 등이 있다. 또한 디지탈서명과 관련된 알고리즘으로는 미국은 NIST가 제안한 DSS(Digital Signature Standard)를 연방표준으로 제정하였으며, SHA(Secure Hash Algorithm)도 1993년 미연방표준인 FIPS 180으로 제정하였다. 현재 미국에서는 NIST를 중심으로 AES(Advanced Encryption Standard) 작업을 추진 중에 있다[6].

●Secure Web

OSF(Open Software Foundation) DCE (Distributed Computing Environment)는 분산 컴퓨팅 환경에 대한 산업표준으로 보안서비스를 제공하며 거의 대부분의 컴퓨팅 플랫폼에서 동작하며 이기종의 하드웨어 및 소프트웨어 환경에서 분산 응용을 제공하기 위하여 설계된 것이다. DCE Secure Web에서는 서버 및 클라이언트에서 인증 서비스가 제공되며, 접근통제, 프라이버시, 데이타 무결성, 감사 서비스가 제공된다[7].

●LAN 정보보호

IEEE(Institute of Electrical and Electronics Engineers)에서는 802.10(Local Area Network Security Working Group)을 구성하여 근거리 통신망의 정보보호를 위한 표준화 작업을 수행하고 있다. 표준안으로는 SILS(Standard for Interoperable Local area network Security)를 제안하고 있다. SILS 표준안은 SILS 모델, 안전한 데이타 교환, 키관리 프로토콜, 시스템 보안 및 관리 프로토콜의 4분야로 구성되며 데이타 발신처 인증, 비밀보장, 비접속 무결성과 접근통제 서비스를 제공한다[8].

●SDNS

SDNS(Secure Data Network System)는 미 국가안보국(NSA:National Security Agency), 국방부(DoD), NIST 등이 시작한 프로젝트로 중요한 정보를 다루는 DoD 및 관련 사용자들의 안전한 통신을 할 수 있도록 키관리[9], 시스템 보안 관리, 암호화, 신분확인, 접근통제[10] 등의 보안 서비스를 제공한다. SDNS

표 5 응용에 적합한 CAPI

Application	Recommended CAPI
Word Processor	GSS-API
Mail Application	IDUP-GSS-API
SMTP; X.400	GSS-API
Directory Service, X.500	GSS-API
SNMP; SNMPv2	GSS-API
IPSP; NLSP; TLSP; GULS; MSP	GSS-API
HTTP	GSS-API
Key Management Application	GCS-API
Key Management Protocol	GCS-API
Authentication Application	GCS-API
Security Association Protocol	GCS-API
Certification Manager	GCS-API or Cryptoki
Certificate Manager	Cryptoki
Cryptographic Token Application	Cryptoki

의 보안 구조는 데이타 링크 계층, 네트워크 계층(SP3)[11], 트랜스포트 계층(SP4)[12] 및 응용 계층을 위한 보안 구조를 개발하였다.

● Security API

상용 암호 제품을 위한 모듈성과 유지보수성을 제공하고자 보다 융통성 있는 강력한 대안으로서 표준화된 CAPI(Cryptographic Application Program Interface)를 사용하는 것이다.

대표적인 것으로 GSS-API(Generic Security Service-Application Program Interface), GCS-API(Generic Cryprographic Service-Application Program Interface), Cryptoki, IDUP-GSS-API(Independent Data Unit Protection-GSS-API) 등이 있다. 표 5에 응용에 적합한 CAPI를 나타내었다[13].

3. 국내 표준화 동향

국내의 정보보호 기술에 대한 연구는 일부 관련 기관에 의해 제한적으로 수행되어 선진국에 비해 상당히 저조한 실정이나, 80년대부터 통신망의 안전 문제에 대해 관심을 갖고 암호화 알고리즘 및 이의 실용화 기술개발 연구가 ETRI 등에 의해 수행되어 왔다. 1990년대 말에는 산, 학, 연의 정보보호 및 암호화 기술에 대한 정보 교류와 연구의 활성화를 위해 한국통신정보보호학회가 설립되어 국내 정보보호 기술 발전에 기여하고 있다.

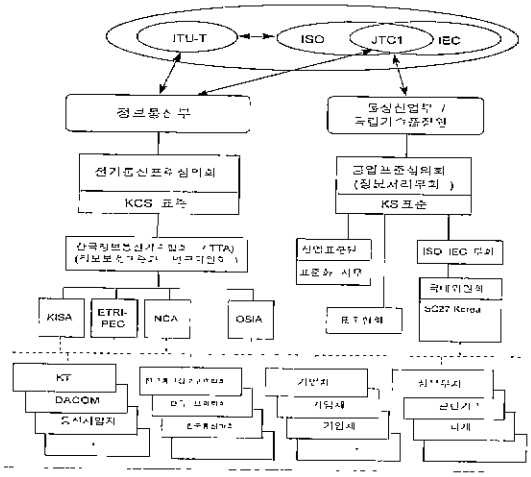


그림 1 정보보호 관련 표준화 체계

국내의 정보보호 기술 표준화 활동은 이제 시작 단계로써 아직 활성화되어 있지는 못하지만, 국가기간전산망 사업 등의 국책사업을 통해 정보통신 설비 및 전산망의 보급이 급속히 확대되면서 정보보호기술의 적용 필요성이 증대되어 정보통신부에서는 "정보통신 설비에 관한 안전 신뢰성 기준"과 "전산망 안전 신뢰성 기준"을 고시하였다. 정보통신부에서 고시한 안전 신뢰성 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[14].

또한 '95년 7월에는 "정보화촉진기본법"이 제정되었으며 민간부분의 정보보호 관련 제반 활동을 담당할 한국정보보호센터가 '96년 4월에 설립되어 활동하고 있다.

정보보호와 관련하여 국내에서 추진중인 표준화 현황은 표 6과 같다.

3.1 한국정보통신기술협회(TTA)

한국정보통신기술협회(TTA : Telecommunications Technology Association)는 전기통신관련 사업의 민영화, 개방화 추세에 따라 '전기통신 설비의 기술기준에 관한 규칙' 제8조에 규정하고 있는 전기통신 관련 표준화 활동을 민간 주도로 전환하여 모든 이해 당사자간의

표 6 국내 정보보호 관련 표준화 목록

표준번호	제 목	년도	구 분
KS C 5766	64비트 블록 부호 알고리즘의 연산 모드	1986	한국공업규격
KS C 5767	데이터 부호 알고리즘(DEA) 1 명세	1986	〃
KS C 5823	정보처리 용어 (신뢰도, 유지보수 및 이용도)	1988	〃
KS C 5817	정보처리 용어 (규제, 완전성 및 안전보호)	1990	〃
KS C 5869	개방형 시스템간 상호접속의 기본 참조 모델-보안구조	1993	〃
KS C 5884	물리층에서의 데이터 암호화	1993	〃
KS C 5791	메시지 복원형 디지털 서명 방식	1994	〃
KS C 5792	블록 암호 알고리즘을 사용한 데이터 무결성 기법	1994	〃
KS C 5793	정보보안의 n비트 블록암호 알고리즘의 운영모드	1994	〃
KS C 5794	보안기술의 실체인증 기법-제1부 일반모델	1994	〃
KS C 5946	금융업의 개인 식별번호관리와 보안-제1부 : PIN 보호원칙과 기법	1995	〃
KS C 5947	금융업의 개인 식별번호관리와 보안-제2부 : PIN 암호화를 위한 승인 알고리즘	1995	〃
KS C 5954	금융업의 메시지 인증을 위한 요건(도매금융)	1995	〃
KS C 5955	금융업의 메시지 인증을 위한 승인된 알고리즘(도매금융) -제1부 : 데이터 암호화 알고리즘(DEA)	1995	〃
KS C 5958	금융업의 메시지 암호화 절차(도매금융)-제2부 : DEA 알고리즘	1995	〃
KS C 5963	금융업의 키관리(소매금융)-제1부 : 키관리 개요	1995	〃
KS C 5964	금융업의 키관리(소매금융)-제2부 : 대칭암호화 방식을 위한 키관리 기법	1995	〃
KS C 5965	금융업의 키관리(소매금융)-제3부 : 대칭암호화 방식을 위한 키의 생명주기	1995	〃
KCS 45	MHS 기본표준 : 메시지 처리 시스템 및 서비스 개관	1992	전기통신표준
KCS 46	MHS 기본표준 : 전체구조	1992	〃
KCS 50	MHS 기본표준 : 메시지 전송시스템 : 추상서비스 정의 및 절차	1992	〃
KCS 52	MHS 기본 표준 : 규약 사항	1992	〃
KCS 53	MHS 기본 표준 : 개인간 메시지통신 시스템	1992	〃
KCS 86	디렉토리 기본표준 : 개념, 모형 및 서비스 개관	1994	〃
KCS 88	개방시스템 상호접속-등록부 표준 : 인증골격	1996	〃
KCS 91	디렉토리 기본표준 : 규약사항	1994	〃
KCS 124	MHS/EDI 메시지 통신시스템 기본 표준	1994	〃
KCS 221	부가형 디지털 서명방식 표준	1996	〃
KCS 299	800MHz 대역 이동전화 인증 알고리즘 정합 표준	1997	〃
KCS 300	개방시스템 상호접속-수송계층 보안 규약 표준	1997	〃

의견을 수렴한 표준화 활동을 장려하기 위하여 국내통신 산업계의 발의에 의하여 1988년 12월에 설립, 1989년 2월부터 한국통신기술협회로 업무를 개시하였으며, 1997년 1월부로 한국정보통신기술협회로 명칭 변경하였다[15]. 최근 조직 개편을 통해 ITU 표준화 활동뿐만 아니라 전기통신과 밀접하게 관련이 있는 JTC 1 표준화 활동에 적극 대응하기 위하여 협회 내에 정보보호 기술과 관련이 있는 JTC 1/SC6, SC21, SC27에 대응되는 국내위원회가 조직되었으나 아직은 시작단계이다. 일반보안기술 실무작업반이 통신정보기술 연구위원회(SC 7) 산하에 조직되어 활동하였으나 정보보호 분야의 표준화 활동을 활성화 하고자 '97년 초에 정보보호 기술관련 연구위원회를 신설하여 한국정보보호센터를 중심으로 활동을 시작하였다.

3.2 한국정보보호센터(KISA)

1995년 5월 13일 입법 예고하여 8월 4일 제정 공포된 정보화촉진기본법[16] 제14조에서 정부는 건전한 정보통신 질서의 확립과 정보의 안전한 소통을 위하여 필요한 정보보호 시책을 효율적으로 추진하기 위한 정보보호센터를 설립 운영할 수 있도록 하였으며, 제15조에서는 정보통신부 장관이 정보보호시스템의 성능과 신뢰도에 관한 기준을 고시하고 정보보호시스템의 제조 또는 수입에 대한 기준 및 보완을 권고할 수 있도록 규정하고 있다[17]. 또한 1995년 10월 9일 입법 예고하여 1995년 12월 29일 제정 공포된 정보화촉진기본법 시행령은

정보화촉진기본법에서 위임된 사항과 그 시행에 필요한 사항을 규정하기 위하여 제정된 것으로 센터의 명칭을 한국정보보호센터(KISA : Korea Information Security Agency)라 하고 이 센터의 설립, 센터의 운영, 센터의 업무, 시험평가 등에 관한 사항을 규정하고 있다[18].

정보화촉진기본법 시행령 제15조 제1항 5호(정보보호시스템의 성능과 신뢰도에 관한 기준 제정 및 표준화 지원)에 의해 정보보호 분야 표준화 활동의 중추적인 역할을 하고자 한국정보통신기술협회에 정보보호 연구위원회(SC10)를 신설하여 보안관리, 암호 및 디지탈 서명, 키관리 기술, 정보보호 응용서비스, 인터넷 보안, 정보보호시스템 평가기술 등의 분야를 중심으로 표준화 활동을 추진하고 있다.

3.3 국립기술품질원

1996년 2월 12일 공업진흥청이 중소기업청으로 확대 개편되면서 국립공업기술원이 국립기술품질원으로 확대되어 기존의 업무 외에 기술분야별 시험, 검사 및 기술지도 기능과 공업진흥청이 담당하던 표준, 계량 및 품질안전에 관한 기능을 담당하게 되었다.

ISO 및 ISO/IEC JTC 1 조직에 대응한 국내 전문위원회가 중소기업청 국립기술품질원 산하에 조직되어 있고, 한국산업표준원이 간사기관 역할을 하고 있다. 즉, JTC 1/SC6, SC21, SC17, SC18, SC27 등 정보보호 기술과 관련있는 국제 표준화 조직에 대응되는 국내 표준화 전문위원회가 조직되어 국가의 산업진흥에 관련한 다양한 표준들을 다루고 있다. 또한 정보처리 분야의 국가권고 표준과 관련하여 ISO/IEC JTC 1의 국가대표기관(national body)으로서 산하의 SC(sub-committee)들을 중심으로 활동하고 있다.

3.4 개방형컴퓨터통신연구회(OSIA)

1987년에 4월에 설립된 개방형컴퓨터통신연구회(OSIA : Open Systems Interconnection Association)는 OSI 참조모델에 근거한 개방시스템 관련 연구 활동을 수행하는 조직으로, 응용서비스의 형태 및 표준화 기술별로 기술위원회를 조직하여 산, 학, 연의 전문가가 참여하는 가운데 표준화연구 및 기술교류 활동을 수행하고 있으며, 활동영역 다변화를 위한 연구범위 확대의 일환으로 최근 많은 사람이 관심을 가지고 있는 인터넷에 대한 연구 목적으로 OSIA SG-Internet이라는 특별 그룹을 조직하였다.

OSIA 산하에 조직되어 있는 보안기술위원회(TG-SEC)에서는 컴퓨터 시스템 및 정보통신망 환경에서 요구되는 정보보호 표준의 연구와 국내 관련 전문가간의 정보교류 및 국내 표준(안) 개발 작업을 추진한다.

3.5 한국통신정보보호학회(KIISC)

정보통신망 보호를 위한 학술 및 기술의 진흥과 관련분야의 발전에 공헌하기 위해 1990년 12월에 설립된 한국통신정보보호학회(KIISC : Korea Institute of Information Security & Cryptology)는 국내 정보보호 기술에 대한 연구의 활성화 방안으로 산하에 7개의 연구분과위원회를 구성하여 활발한 학술활동을 진행하고 있으며 앞으로 더욱 이 분야의 연구가 체계적으로 수행될 수 있을 것으로 기대된다. 현재 학회 내에 구성중인 연구분과위원회는 정보보호 표준 연구회, 통신망 보호기술 연구회, 암호이론 연구회, 컴퓨터시스템 보호연구회, 컴퓨터 바이러스 및 해커 대책위원회, 통신정보보호 정책 연구회, 전산감사 연구회 등이 있다. 연구활동을 살펴보면 통신망 보호기술 연구회를 중심으로 전자공학회, 통신학회 등 유관학회와 공동으로 매년 JCCI(Joint Conference on Communications & Informations) 학술대회를 개최하고 있으며 최근에는 정보보호 응용 연구회를 중심으로 스마트카드 관련 알고리즘 및 프로토콜을 연구하고 있다.

4. 결 론

본 고에서는 ISO/IEC JTC 1, ITU-T, IETF 등의 국제 표준화 활동과 DAVIC, IISP 등의 표준화 활동 및 기타 표준화 동향으로 암호 알고리즘 표준화, Secure Web, LAN 정보보호, Security API 및 SDNS 등의 정보보호 관련 표준화 동향에 관하여 기술하였다. 또한 국내

의 표준화 활동에 대하여 한국정보통신기술협회, 한국정보보호센터, 한국품질기술원, 개방형 컴퓨터통신연구회 및 한국정보보호학회 등의 현황을 소개하였다.

이상으로 살펴본 바와 같이 최근의 국내외 초고속정보통신망 확충 등 정보화 진전속도를 고려해 볼 때 국내에서도 다가올 미래의 정보화 시대 발전상을 예측하여 정보화를 효율적으로 촉진시키고 국내 정보보호 산업 육성을 위한 정보보호 관련 표준 개발에 대한 지속적인 노력을 기울여야 할 것으로 사료된다. 이를 위하여 한국정보보호센터를 중심으로 관련기관, 단체, 산업체, 학계 등과의 체계적인 표준화를 추진하여 실용적인 정보보호 관련 표준을 개발해야 할 것으로 사료된다.

참고문헌

[1] http : //www.iso.ch/list2, 1997.

[2] http : / / www.cis.ohio-state.edu / rfc 1825, 1997.

[3] http : //www.davic.org/, 1997.

[4] DAVIC 1.2 Specification Part 10-Basic Security Tools for DAVIC 1.0, 1997.

[5] http : //www.ansi.org/iisp, 1997.

[6] NIST, "Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard", http://csrc.ncsl.nist.gov/encryption/newcrypt.txt, 1997. 1.

[7] 홍기융, "인터넷의 발전과 보안", '96 정보보호 심포지움, pp. 121-166, 1996, 7.

[8] IEEE, Standard for Interoperable Local Area Network Security(SILS), IEEE 802.10/D6. Sep. 1989.

[9] SDNS Secure Data Network System, Overview, Document SDN.201, Revision 1.5, 1989. 5.

[10] SDNS Secure Data Network System, Access Control Concept, Document SDN 801, Revision 1989. 5.

[11] SDNS Secure Data Network System, Security Protocol 3, SP 3. Document SDN 301, Revision 1989. 5.

[12] SDNS Secure Data Network System, Security Protocol 4, SP 4, Document SDN 401, Revision 1989. 5.

[13] 이철원, 홍기융, 김학범 외, "국내외 정보보호관련 연구 동향", 정보과학회지, 제15권, 제4호, pp. 6-13, 1997. 4.1.

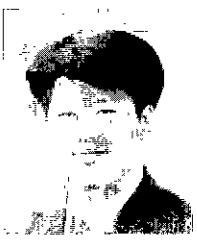
[14] 일반보안기술 표준화 활동 조사 분석, 한국통신기술협회, 1995. 12.

[15] 신용섭, "정보통신 표준화정책 방향", TTA 저널, 제49호, pp. 12-18, 1997. 2.

[16] 법률 제4969호, "정보화촉진기본법," 관보 제13080호, '95. 8. 4.

[17] 대통령령 제14847호, "정보화촉진기본법 시행령," 관보 제13201호, 1995. 12. 29.

[18] 홍기융, "국내외 정보보호 정책 및 기술 동향", 한국전산원, 1996. 3.



김 학 범

1988 경기대학교 전자계산학과 (학사)
1990 중앙대학교 대학원 전자계산학과(석사)
1991～1996 한국전산원 주임연구원
1996～현재 아주대학교 컴퓨터공학과 박사과정 재학중, 한국정보보호센터 주임연구원
관심분야 : 컴퓨터 네트워크 정보보호, 정보보호시스템 기준 평가, 정보보호기술 표준화

이 철 원

1987 충남대학교 수학과(학사)
1989 중앙대학교 대학원 전자계산학과(석사)
1989～1996 한국전자통신연구소 선임연구원
1996～현재 한국정보보호센터 선임연구원
관심분야 : 컴퓨터 네트워크 정보보호, 정보보호시스템 기준 평가, 정보보호기술 표준화

홍 기 웅

1982 진남대학교 전자계산학과(학사)
1985~1995 한국전자통신연구소 선임연구원
1990 중앙대학교 대학원 전자계산학과(석사)
1992~1993 이태리, Alenia Spazio사 Senior Researcher
1994 정보처리기술사
1995~1996 한국전산원 선임연구원
1996 아주대학교 컴퓨터공학과(박사)
1996~현재 한국정보보호센터 책임연구원, 응용연구팀장, 기준개발팀장
관심분야 : 컴퓨터 네트워크 정보보호, 정보보호시스템 기준평가, 정보보호기술 표준화

심 주 걸

1979 중앙대학교 전자공학과(학사)
1991 건국대학교 대학원 전자공학과(석사)
1997~현재 성균관대학교 정보공학과 박사과정 재학중, 한국정보보호센터 기준평가부장
관심분야 : 정보보호시스템 기준평가, 암호체계, 정보보호기술 표준화

● '97 전산교육 워크샵 ●

- 일 자 : 1997년 6월 27일
- 장 소 : 전주대학교
- 주 최 : 전산교육연구회
- 문 의 처 : 전주대학교 전자계산학과 심동희 교수
  T. 0652-220-2523