情 報 保 護 學 會 誌
第 15 卷 第 5 號, 2005. 10

정보보호 표준화 항목 정의 및 로드맵

오 흥 룡*, 오 세 순*, 김 선*, 염 흥 열**

요 약

정보보호기술은 인터넷 등의 컴퓨터 통신망을 통하여 전달되거나 정보시스템에 저장되어 있는 정보에 대한 위조, 변조, 유출, 무단침입 등을 비롯한 각종 불법 행위로부터 조직 혹은 개인의 컴퓨터와 정보를 안전하게 보호하는 기술을 지칭하며, 이들은 무결성, 기밀성, 가용성 서비스를 통하여 실현된다. 본 논문에서는 정보보호 일반 기술중에서 암호 및 인증 기술, 네트워크 보안 기술, 응용 보안 기술, 그리고 평가 및 인증체계 기술 등에 대한 표준화 동향을 파악하고, 이를 근거로 표준화 항목을 정의하고 표준화 추진체계 등을 고찰해 본다.

Ⅰ. 서 론

급속도로 발전하고 있는 초고속 인터넷 사회에서 개인 고유의 프라이버시나 기업 고유의 정보들은 불법적인 공격으로부터 쉽게 노출되고 있다. 따라서 이들 정보를 보호하기 위한 정보보호 기술 개발과 이에 대한 표준화 연구가 필요하다. 정보보호 분야는 BcN 등의 통신망 및 정보시스템에 필수적인 중요 기술로써, 다음과 같은 주요 분야에서 서로 다른 벤더들의 정보보호 제품간에 상호 연동을 가능케 하는 기술이다. 즉, 인터넷 사이버 공간에서 사용자의 신분을 확인하고 전자서명의 유효성을 확인하기 위한 인증 제품들, 망 계층에서 사용자 데이터의 기밀성 기능과 무결성 기능을 제공하기 위한 IP 보안 프로토콜과 키관리 프로토콜(IKE) 등으로 구성되는 인터넷 보안 제품들, 홈네트워크/BcN/USN을 위한 네트워크 보안 제품들, 무선랜 등의 휴대인터넷 보안 제품들, 전자메일과 안전한 전자상거래를 위한 전송계층 보안 제품들과 응용 계층 정보보호 제품들 간에 상호연동성을 보장하는 기술을 말한다. 이러한 정보보호 기술들에 대한 표준화 연구와 작업은 국가의 정책적 지원이 있어야 하며, 국가 및 민간간의 유기적인 협력체제의 구축을 통하여 실현 가능할 것이다. 현재까지의 주요 표준화 활동은 국내 알고리즘의 국내 표준화 작업, 국제 표준을 국내 표준으로 채택하는 작업을 주로 수행해 왔으나, 앞으로는 국내 기술에 대한 국제 표준화 추진이 필요하다. 이를 위해서는 국내 산업체와 국내 연구소의 기술 경쟁력을 향상시키고, 독자적인 정보보호 기술의 개발도 요구되며, 이를 바탕으로 개발된 기술을 국제 표준화하는 방향으로 추진되어야 할 것이다.

본 논문에서는 정보보호 일반 기술들에 대한 표준화 동향을 분석하고, 이를 근거로 표준화 항목을 정의하고 향후 국내 표준화에 필요한 추진체계 및 로드맵을 제시하고자 한다. 주요 내용으로 본론 Ⅱ장에서는 정보보호 일반 기술들에 대한 국내외 표준화 동향을 분석하고, Ⅲ장에서는 이를 근거로 핵심 기술들을 분류하고 정의한다. Ⅳ장에서 국내외 정보보호 기술들에 대한 현황을 비교 분석하고, Ⅴ장에서 국내 정보보호 표준화에 필요한 추진체계와 로드맵을 제시하며, 마지막으로 Ⅵ장에서 결론을 기술한다.

Ⅱ. 본 론

본 장에서는 국외 정보보호 분야의 국제표준화를 추진하고 있는 대표적인 기구들인 IETF, ISO/IEC JTC1/SC27, ITU-T SG17, NIST 등의 동향을 분석하고, 국내 표준화기구 TTA의 현황을 간단히 살펴본다.

본 연구는 정통부 ITRC 지원 사업에 의하여 수행되었음
* 한국정보통신기술협회 표준화본부({hroh, ssoh, skim}@tta.or.kr)
** 순천향대학교 정보보호학과(hyyoum@sch.ac.kr)

2.1 국제 정보보호 표준화 동향

2.1.1 IETF 표준화 동향

IETF에서는 여러 영역(응용, 일반, 인터넷, 운영/관리, 라우팅, 보안, 전송)에서 표준화 작업이 수행되고 있다. 이중 보안 영역은 20개의 작업반으로 세분화되여 표준화 작업이 이루어지고 있으며, 수행되고 있는 연구범위는 표 1과 같다.[8](2005.8.)

(표 1) IETF 보안영역의 작업반

작업반	연구내용	RFC	Draft
btns	Better-Than-Nothing Security	-	1
enroll	Credential and Provisioning	-	-
idwg	Intrusion Detection Exchange Format	1	3
inch	Extended Incident Handling	-	3
isms	Integrated Security Model for SNMP	-	1
kink	Kerberized Internet Negotiation of Keys	1	1
kitten	Kitten (GSS-API Next Generation)	-	12
krb-wg	Kerberos WG	4	5
ltans	Long-Term Archive and Notary Services	-	4
mobike	IKEv2 Mobility and Multihoming	-	2
msec	Multicast Security	5	10
openpgp	An Open Specification for Pretty Good Privacy	2	1
pki4ipsec	Profiling Use of PKI in IPSEC	-	1
pkix	Public-Key Infrastructure (X.509)	29	17
sacred	Securely Available Credentials	3	-
sasl	Simple Authentication and Security Layer	1	5
secsh	Secure Shell	-	16
smime	S/MIME Mail Security	35	4
syslog	Security Issues in Network Event Logging	2	4
tls	Transport Layer Security	7	7

IETF는 실제 구현의 관점에서 표준화를 진행하는 사실표준화 기구로써 enroll, isms, kitten, ltans, pki4ipsec, pkix, sacred, sasl 작업반에서 인증관련 표준화를 진행하고 있다. enroll 작업반은 사용자와 서비스 제공자간에 암호학적인 인증을 제공하기 위한 다양한 방법을 연구하고 있으며, isms 작업반은 SNMPv3를 인증시스템과 접근제어 모델에 적용하기 위한 부분을 연구하고 있다. kitten 작업반은 GSS (Generic Security Services) API 표준의 확장과 구현 부분을 연구하고 있으며, ltans 작업반은 장기간 보관되는 데이터나 공증 서비스 지원을 위한 요구사항, 구조, 프로토콜 등에 대해 연구하고 있다. pki4ipsec 작업반은 IPSec 프로토콜을 PKI 환경(X.509)에 적용하기 위한 부분을 연구하고 있으며, pkix 작업반은 ITU-T PKI 표준들에 대한 프로파일과 X.509 기반의 PKI 지원을 위한 인터넷 표준을 개발하고 있다. sacred 작업반은 신뢰성 확보와 관련된 개인 정보(공개키/개인키 쌍, 인증서, 인증서 체인, 신뢰 기관 정보, 루트인증기관 정보 등)의 안전한 export/import를 위한 메커니즘 부분을 연구하고 있으며, sasl 작업반은 다양한 응용 프로토콜들에게 주요한 보안 서비스를 제공하기 위한 몇 가지 엄선된 SASL 메커니즘을 포함하는 개정된 SASL 기술 명세를 만들기 위하여 연구하고 있다. 시스템 보호와 관련해서는 secsh 작업반에서 원격 로그인, 파일전송, X11 세션, 기타 TCP/IP 세션을 안전하게 지원하기 위한 SSH 프로토콜을 개선하기 위한 작업을 진행하고 있으며, syslog 작업반에서 Syslog 메커니즘에 존재하는 데이터 무결성, 인증성, 기밀성 서비스 등을 개선하고 RFC 문서로 정형화 하려 하고 있다. 네트워크 보호기술(IP, 전송계층, 멀티캐스트)은 btns, kink, krb-wg, mobike, msec, tls에서 작업이 수행되고 있다. btns 작업반은 IPSec의 간략화된 보안 기능 제공을 위한 IPSec, IKE 프로토콜에 대한 확장 및 프로파일 정의를 위해 작업하고 있으며, kink 작업반은 IKE 프로토콜의 대체물로 Kerberos 기반의 중앙 집중형 IPSec 키관리 메커니즘을 정의하고 있다. krb-wg 작업반은 MIT에서 개발된 인증 서비스 Kerberos의 보안성 강화와 구현 시스템의 상호운영성을 작업하고 있으며, mobike 작업반은 IKEv2 프로토콜 확장을 위해 다중 IP 주소나 IP 주소 변환 기술들을 개발하고 있다. msec 작업반은 인터넷에서 다중 사용자를 위한 멀티캐스트 통신 보안을 작업으로 그룹 키관리, 그룹 정책관리, 그룹 키분배 등을 작업하고 있으며,

tls 작업반은 전송계층에서의 기밀성, 인증성, 무결성 등을 제공하기 위한 TLS 프로토콜을 개선하기 위한 작업을 하고 있다. 네트워크 보호기술(무선/이동, 통합보안관리, 차세대 네트워크)은 idwg 작업반에서 IDS 구성 요소들, 대응시스템, 관리시스템 사이의 정보 공유를 위한 데이터 포맷이나 교환 절차를 정의하고 있고, inch 작업반에서는 컴퓨터 침해 대응을 위한 침해 대응 조직간에 침해 데이터의 교환과 침해 통계 정보를 원활하게 교환하기 위한 보안 요구사항 및 방법들을 작업하고 있다. 응용서비스 분야는 openpgp 작업반에서 이메일이나 파일저장을 위한 보안으로 MIME 프레임워크, PGP 알고리즘이나 포맷형식 등을 작업하고 있으며, smime 작업반에서는 드래프트 문서로 있는 CMS나 S/MIME 스팩 처리를 위한 상호호환성 테스트 작업을 수행하고 있다.

2.1.2 ISO/IEC JTC1/SC27 표준화 동향

ISO/IEC JTC1/SC27에서는 3개의 워킹그룹(WG)을 구성하여, IT 시스템 보안을 위한 정보보호 원천 기술과 구현 방법들에 대한 표준화가 추진되고 있다. WG1에서는 일반적인 보안요구사항, 정보보호 관리, 보안서비스나 가이드라인 작업을 하고 있으며, WG2에서는 암호 알고리즘 원천기술과 보안서비스 구현을 위한 다양한 보안기술들을 표준화하고 있다. 그리고 WG3에서는 보안 시스템에 대한 평가기준, 평가방법론, 보호프로파일 작성 절차들을 표준화하고 있다. 산하 워킹그룹들의 활동영역은 표 2와 같다.[9]

〔표 2〕 ISO/IEC JTC1/SC27 워킹그룹

WG	연구내용	표준	Draft
WG 1	Requirements, security services and guidelines	7	3
WG 2	Security techniques and mechanisms	46	7
WG 3	Security evaluation criteria	5	14

2.1.3 ITU-T SG17 WP2 표준화 동향

ITU-T에서 SG17은 정보보호 LSG(Lead Study Group)으로 활동하고 있으며, WP2가 정보통신 보안을 위해 7개 연구과제(Question)를 구성하여 표준화 작업을 추진하고 있다. 현재 한국은 보안분야에서 5개의 권고안(생체정보 보안대책 가이드라인, 홈네트워크를 위한 보안기술 프레임워크, 홈네트워크 디바이스 인증 프로파일, 모바일보안/홈네트워크 보안 로드맵, 스팸대응을 위한 기술 프레임워크)의 main-editor로 활동하고 있다. 각 연구과제들의 활동영역은 표 3과 같다.[10]

〔표 3〕 ITU-T SG17 WP2 연구반

연구과제	연구내용	표준	Draft
Q.4	Communication System Security	-	-
Q.5	Security Architecture and Framework	X.800 series, X.805	1
Q.6	Cyber Security	-	-
Q.7	Security Management	X.1051	2
Q.8	Telebiometrics Technology	X.1081	4
Q.9	Secure Communication Services	X.1121, X.1122	5
New Q.17	Countering SPAM	-	3

각 연구과제에서의 주요임무를 살펴보면, Q.4는 보안 전반적인 비전, 로드맵, 요약물 등을 작업하고 있으며, Q.5는 보안구조, 모델, 개념, 프레임워크 등을 작업하고 있다. Q.6은 사이버보안을 위한 취약점 정보에 대한 공유방법, 침해사고 대응방법, 보안솔루션 등을 개발하고 있으며, Q.7은 정보보호 관리 시스템, 침해사고 관리방법, 위협관리 방법론 등을 연구하고 있다. Q.8은 생체인식 멀티모달 모델 프레임워크, 생체정보를 이용한 인증메커니즘, 생체정보 보안대책 가이드라인을 작업하고 있으며, Q.9는 모바일보안, 홈네트워크 보안, 웹서비스 보안을 다루고 있다. 새로운 Q.17은 스팸대응을 위한 프레임워크나 기술들을 위한 가이드라인 등을 개발하고 있다.

2.1.4 NIST 표준화 동향

NIST는 미국 국가 정보 표준화 기구(NISO)에 속한 사무국으로, NISO가 추진하는 정부, 과학, 문헌 그리고 편찬 작업의 표준 개발에 참여하고 있다. NIST의 부설 컴퓨터 시스템 연구소(CSD)는 FIPS 계획을 관리하는 NIST의 주요 기관이며, 발표된 FIPS 표준안은 150개 이상이고, 이중 보안 관련 FIPS 문서는 가이드라인 문서, 패스워드 관련 표준, 인증, 암호학적 모듈, 보안 레이블, 키관리, 암호 분야 등으로 구분된다. CSD 산하 연구그룹들의 활동영역은 표 4

〔표 4〕 NIST CSD 연구반

연구반	연구내용	현재 단계	갯수
WG 1	Cryptographic Standards and Applications	FIPS	15
WG 2	Security Testing	폐지 FIPS	18
WG 3	Security Research / Emerging Technologies	보안 가이드라인	64
WG 4	Security Management and Guidance	Draft 문서	9

와 같다.[11]

WG1에서는 AES, 암호학적 표준 툴킷, 암호 키복구, S/MIME, 개별 식별 검증방법, PKI 분야를, WG2에서는 보안기능 테스트, IT 보안 평가를 위한 공통평가기준, 암호학적 모듈 유효성 프로그램, IP-Sec을 연구하고 있다. WG3에서는 권한부여 관리나 접근제어모델과 같은 RBAC, 모바일 Ad-Hoc 네트워크 보안, 스마트카드, 스팸, 무선보안 등을 연구하고 있으며, WG4에서는 CSD를 관리를 위한 전반적인 정책, 보안관리 가이드라인, 보안교육 등을 연구하고 있다.

2.2 국내 정보보호 표준화 동향

2.2.1 한국정보통신기술협회(TTA) 표준화 동향

TTA는 IT분야의 새로운 표준 발굴, 표준 제정, IT제품의 시험/인증을 One-stop으로 서비스하는 민간자율 표준화 기구로써, 2004.12월을 기준으로 TTA 표준(TTAS)은 총 3,149건이 제정되었다. 이중, 정보보호 관련 표준은 130여건(타 PG에서 제정된 정보보호 관련 표준 포함)이다. TTA 표준화위원회는 2004년에 공통기반기술위원회(TC1) 산하에 3개의 프로젝트그룹(PG)인 정보보호기반(PG101), 인터넷보안(PG102), 생체인식(PG103)을 구성하여 정보보호 표준화를 추진하고 있다. PG101은 "홈네트워크 보안 및 암호알고리즘" 등 총 16건의 표준화 과제에 대해 연구하고 있으며, PG102는 "무선랜보안 및 IPSec" 등 총 13건의 표준화 과제를 연구하고 있고, PG103에서는 "생체정보 보안대책 가이드라인" 등 총 10건의 표준화 과제를 추진하고 있다. 3개의 프로젝트그룹들은 상기 과제들을 대부분 올해나 내년 2006년 12월에 표준제정을 완료하는 것을 목표로 표준화를 진행하고 있다. 다음의 표 5는 정보보호 관련 프로젝트 그룹들의 활동영역이다.[5]

〔표 5〕 TTA 정보보호 프로젝트그룹

연구반	활동영역
PG101	- 정보보호 관리 및 사용자 지침 개발 - 정보보호시스템 평가·인증을 위한 관리절차/검증 표준 개발 - 암호알고리즘, 암호키 관리, PKI 등 정보보호 기반기술 표준개발 - Secure OS 표준 개발
PG102	- 전자우편 및 전자상거래 보안기술 표준 개발 - 네트워크 레벨 정보보호 표준 개발 - VPN, IDS 등 네트워크 보안 기술 표준 개발 - 응용 레벨 정보보호 표준 개발
PG103	- 생체인식 관련 표준화 및 기술개발 로드맵 제안 - 동종/이종 생체인식 기법간 호환을 위한 표준화 동향 분석 - BioAPI 적합성 시험규격 등 상호운용 관련 표준화 추진

Ⅲ. 정보보호 표준화 항목 분류 및 정의

정보보호 기술 표준화는 크게 공통기반기술, 시스템 및 네트워크 보호기술, 응용서비스 보호기술, 그리고 정보보호 평가/관리 기술 분야로 나눌 수 있다. 그리고 세부 표준화 항목으로, 공통기반기술 표준화는 암호기술, 키 관리, 전자서명, 인증기술, 생체인식을 포함하며, 시스템 및 네트워크 보호기술 표준화는 정보통신시스템을 구성하는 서버 보호와 인터넷 등의 유·무선 통신시스템 보호를 포함한다. 또한 응용 서비스 보호 기술 표준화는 금융서비스와 전자상거래, 전자지불, 보안전자우편, 전자정부와 같은 응용서비스의 안전신뢰성을 확보하기 위한 기술을 포함하며, 정보보호 평가/관리 표준화는 조직적이고 전사적인 정보보호관리, 보안성 평가기준, 공통평가기준(CC), 표준적합성/상호운용성 시험 인증과 같은 제품의 성능과 신뢰도 향상을 위한 기술로 분류할 수 있다. 정보보호 표준화 항목 분류는 표 6과 같다. 암호기술은 모든 정보보호 기술의 기반이 되는 기술로서 기밀성, 무결성, 메시지 인증, 사용자 인증, 부인방지 등의 서비스를 제공하기 위한 기본 프리미티브이다. 현재 암호 알고리즘은 대칭형 암호 알고리즘, 공개키 암호 알고리즘, 키분배 알고리즘, 해쉬 알고리즘, 전자서명 알고리즘, MAC 알고리즘으로 분류될 수 있다. 암호기술은 암호 알고리즘 자체에 관한 기술과 암호키를 효율적으로 공유하는 기술 및 암호 알고리즘을 효율적으로 구현하는 기술로 다시 구분될 수 있다.

인증기술은 크게 공개키 기반구조(PKI) 기술과 권한관리 기반구조(PMI) 기술, identity 관리, 무선

〔표 6〕 정보보호 표준화 항목 분류 및 정의

대분류	핵심 요소기술	세부 핵심 요소기술	요소 기술 정의
공통기반기술	암호기술	암호 메커니즘	기반 기술로써, 정수론 등의 복잡한 수학 이론에 바탕을 두고 설정된 암호 알고리즘 설계와 해독에 관한 기술
		암호 키관리	키의 생성, 분배, 전달, 인증, 취소, 폐기 등의 키 관리 절차
		암호 구현	암호 알고리즘을 고속 동작으로 실현하기 위한 기술과 암호 알고리즘을 스마트카드 등에 탑재하는 기술
	인증기술	PKI	공개키 인증서의 무결성과 인증성을 제공하기 위한 기술
		PMI(EAM/3A)	권한을 관리하기 위한 프레임워크, 속성 인증서 발행 및 관리, 운영을 위한 기술
		Identity 관리	싱글사이언 기능을 효율적으로 수행하기 위한 ID 연합 기술과 이를 해결하기 위한 공통의 플랫폼 기술
		생체인식	사람의 생체정보(망막, 얼굴, 지문, 정맥 등)를 이용하여 인증하는 기술
시스템 및 네트워크 보호기술	시스템 보호기술	PC 보안	바이러스 백신 툴 관리 지침에 대한 개발 기술과 PC로의 접근 통제를 위한 패스워드 사용에 대한 보호 기술, 전자 증거 수집 정보를 교환하는 방법에 대한 기술
		서버보안	감사추적 자료로 사용되는 로그 형식에 대한 기술과 보안 운영 체제에의 접근 제어 모델을 개발하는 기술
	네트워크 보호기술	침입대응기술	IDS와 IPS 시스템의 문제점으로 제기된 네트워크 기반의 침입탐지 및 DDoS 방지 및 대응기술
		IP 보안	IP 계층에서의 기밀성, 무결성, 인증성 등 보안 서비스를 제공하기 위한 기술
		전송계층	TCP 계층에서의 기밀성, 무결성, 인증 및 점대점 연결 서비스를 제공하기 위한 기술
		멀티캐스트	다중 사용자에게 서비스를 제공하기 위해 그룹 통신에서 필요한 보안 서비스를 제공하기 위한 기술
		통합보안관리	정보보호 장비들을 통합 관리하기 위한 기술
		차세대 네트워크	침해 대응을 위한 라우터 및 스위치에서의 보안 기술과 안전한 네트워크 관리하기 위한 프로토콜 기술
		IT839 네트워크	홈네트워크 보안 기술, 편재형 네트워크, RFID 보안 기술, 단말기 이동성을 위한 휴대인터넷(HPi) 보안 기술 등
응용서비스 보호기술	공공부분 응용서비스 보호	전자정부	전자정부를 구축하여 민원정보를 제공하기 위한 보안기술
		전자투표/공증	전자투표에 대한 시민의 신뢰 및 투표가 강압이나 제3자의 간섭 없이 자유롭고 공정하게 치러지기 위한 비밀 투표 문제와 보안문제를 해결하는 위한 보안 기술
	일반부분 응용서비스 보호	전자우편	전자우편에 기밀성, 메시지 무결성, 송신자 인증 등을 제공하기 위한 기술
		디지털 컨텐츠	디지털 아이템에 대한 저작권 보호 프레임워크, 서비스 및 인증 기법 등을 제공하기 위한 기술
정보보호 평가 및 관리 기술	정보보호 평가	표준적합성시험	정보보호 제품에 대한 표준적합성을 시험하기 위한 기술
		보안성 평가	제품의 보안기능 요구사항 및 보증요구사항에 대한 공통 표준 및 절차에 관한 기술
	정보보호관리 체계	정보보호 정책	정책 수립 및 관리, 조직의 역할 및 책임, 예산편성 방법 및 절차 등에 관한 기술
		위험 분석/관리	위험분석 및 관리를 위한 절차 및 방법에 관한 기술
		정보보호대책 선정 구현 및 교육	정보보호대책 유형 및 위험과의 관계도, 교육 및 훈련 프로그램 수립 절차를 위한 기술
		사후관리	보안감사, 점검, 사고대응, 보안대책 유지보수 등에 관련된 지침에 관한 기술
		관리체계 및 성과측정	관리체계 수립을 위한 계획, 구현, 점검, 개선 등에 관한 기술

공개키 기반구조, 생체인식 등으로 분류될 수 있다. PKI 기술은 공개키 인증서를 이용하여 사용자 공개키의 무결성과 인증성을 제공하는 기술이며, 이를 통하여 사용자에게 기밀성, 무결성, 부인방지 등의 정보보호 서비스를 제공하며, PMI 기술은 속성 인증서를 이용하여 사용자에 대한 권한을 관리하기 위한 기술을 의미한다. Identity 관리는 조직과 회사가 연합하여 생성된 표준과 공통의 플랫폼을 이용하여 싱글사이언 기능을 효율적으로 제공하기 위한 기술이다. 무선 공개키 기반구조는 무선망 응용을 위한 공개키 기반구조에 관한 기술이다. 생체인식은 사람의 생체 정보를 이용하여 사용자 인증에 활용하는 기술이다. 시스템과 네트워크 보호 기술은 인터넷 등의 컴퓨터 통신망을 통하여 전달되는 정보의 위조, 변조, 유출, 무단 침입 등을 비롯한 각종 불법 행위로부터 조직 혹은 개인의 컴퓨터와 정보를 안전하게 보호하는 기술이며, 주요 기술 분야는 PC 보안 기술과 서버보안 기술 등으로 구성된다. PC 보안은 바이러스 백신 기술 등을 포함하며, 서버 보안기술은 사용자에 대한 접근 제어 기술 등을 포함한다. 네트워크 보호 기술은 인터넷과 같은 개방형 네트워크 환경에서 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 불법 행위로부터 네트워크를 보호하기 위한 기술을 말한다. 네트워크 보호 기술은 해킹이나 바이러스로부터 네트워크를 보호하기 위한 침입차단 기술과 침입탐지 기술로 구성되는 침해대응기술, VPN 서비스를 제공하기 위한 IP보안 기술(IPSec), 다수의 사용자에게 멀티미디어 정보를 전달하기 위한 멀티캐스트 보안, 종단간 보안 기능을 제공하기 위한 전송계층보안(TLS 보안), 네트워크 보안 장치간의 관리를 자동화 하기 위한 통합보안관리, DDoS 공격 등으로부터 네트워크 요소를 보호하기 위한 라우터 보안과 스위치 보안 기능을 다루는 차세대 네트워크 보안, 그리고 USN, WPAN, 4G 망 등으로 구성되는 IT839 네트워크 기반기술 등으로 구성된다. 행정환경이 종이문서 기반에서 전자문서 기반으로 진화됨에 따라, 주요 행정정보와 다양한 개인정보들이 인터넷을 통해 전달되고 있다. 따라서, 이러한 가상공간에서의 사용자 신원확인과 정보의 안전성, 개인의 프라이버시 보호 등 행정 처리의 신뢰성 확보와 전자문서에 대한 안전성 확보가 필수적으로 연구되고 있다. 공공분야 응용 서비스 보호 기술은 웹 서비스 보안 기술을 포함하는 전자정부 보안기술과 전자투표/공증 기술로 구분된다. 일반부분 응용 서비스 보호 기술은 전자우편 보안, 디지털 지적 재산권을 보호하기 위한 디지털 컨텐츠 보안 등을 포함하고 있다. 정보보호평가 기술은 정보보호시스템의 보안성평가 및 표준적합성 시험을 위한 기준 및 체계를 의미하며 구체적으로는 시험방법론, 세부 보안프로토콜 시험기준 등을 포함한다. 정보보호관리 기술은 조직의 목적 및 전략을 지원하기 위해 정보보호를 조직화/제도화할 필요가 있으며 이를 위한 정보보호 관리체계를 계획, 구현, 운영지원, 감시 및 검토하는 프로세스에 관한 표준, 지침 및 기법 등을 포함한다.[2,3]

Ⅳ. 국내외 정보보호 기술 현황

국내외 정보보호 기술 현황을 핵심 요소별로 살펴보면, 표 7, 8과 같다.[1,2,12]

Ⅴ. 국내 정보보호 표준화 추진체계 및 로드맵

5.1 국내 정보보호 표준화 추진전략

암호기술 분야는 기존의 널리 활용되고 있는 사실 표준상태에 있는 암호 알고리즘에 대해서는 국제표준을 준용하여 국내표준으로 제정하는 것이 바람직하고, 국내 기술이 미흡한 공개키 암호 알고리즘과 새로운 대칭형 암호 알고리즘, 해쉬 알고리즘에 대한 개발을 통하여 자체적인 국내 표준화를 먼저하고, 이를 국제 표준화에 반영하는 전략이 필요하다. 장기적으로는 고비도/고속 암호 알고리즘과 양자 암호 알고리즘을 개발하여 표준화해야 하며, 국가보안연구소에서 개발한 ARIA 암호 알고리즘은 국내 표준화가 필요하다. 인증기술 분야는 IETF에서 표준화 작업을 시작한 분야를 설정하여 국내 기술개발과 표준을 개발하여 독자적인 IPR을 확보하고, 이를 이용하여 국내 표준을 개발 후, 국제 표준화하는 것이 필요하다. 또한, OMA에서 표준화되고 있는 무선 PKI 관련 표준 중 암호 API 관련 표준은 조속히 국내 표준으로 준용하는 것이 필요하다. 현재 IETF에서 새롭게 논의되고 있는 IPsec을 위한 PKI, 안전한 크리덴셜 저장 및 전달 프로토콜, SNMP를 위한 인증 확장, 디지털 엔터테인먼트 컨텐츠를 안전하게 관리하기 위한 프로토콜 등의 분야는 계속적인 연구를 하여 국내외 표준화를 병행하는 것이 필요하다. 단기적으로 표준화가 필요한 기술 항목은 각종 인증서 확장자 표준, 인증서 관리 및 운영 프로토콜, 인증서 정책 프로토콜, 온라인 인증서 상태 검증 프로토콜, 대리 인증서 검증 프로토콜, SIM 표준, 커버로스 관련 프로토콜, 그리고 PKCS 표준 중

〔표 7〕 국내외 정보보호 기술 현황(1)

핵심 요소기술	국내 정보보호 기술	국외 정보보호 기술	기술격차
암호기술	- 대칭키 암호 분야는 민간 표준으로 사용하기 위한 블록 암호 SEED 개발하였고, 2004년 ARIA 알고리즘이 개발되었음 - '05년 SEED RFC 4009, 4010로 채택 - 공개키 암호 연산 고속화 분야에서는 지수승 알고리즘, 유한체 연산 기법, 타원곡선 연산 속도 개선 알고리즘을 발표 - 패스워드 인증 및 키공유, 특수 전자서명 알고리즘 등의 분야, DES 등의 암호해독 분야에서 주목할 만한 연구 실적이 있으나, 공개키 암호 알고리즘 설계 분야는 다소 뒤떨어짐	- 대칭키 암호 알고리즘은 1970년대 중반 미 연방 표준 암호 알고리즘으로 DES가 채택된 이후로 IDEA, MISTY 등을 비롯한 다양한 블록 암호가 개발되었음 - 현재 AES의 실용화를 위한 다양한 안전성 분석, 운영 모드, MAC 등을 비롯한 블록 암호 응용 분야에서 연구가 진행됨 - RSA, ECC, Rabin, ElGamal, XTR, NTRU 등 다양한 공개키 암호가 개발되었으나, 현재는 RSA와 ECC만이 실용적으로 널리 이용되고 있음 - Crypto2004에서 MD5와 SHA1에 대한 암호 해독 가능성을 제시함으로써, 이 분야에 대한 해독과 이를 개선키 위한 새로운 해쉬알고리즘 개발이 수행되고 있음	3-5년
인증기술	- ETRI, 산업체(케이사인, 드림시큐리티, 비시큐어 등)에서 많은 유형의 PKI 제품을 개발하고 있음 - PKI 관련 산업체에서는 IETF PKIX에서 표준화되고 있는 프로토콜을 이용한 제품을 개발하고 있고, 대부분 IETF 표준에 호환성이 있는 제품을 개발하고 있음 - 국내 기술수준은 세계에서도 상당한 수준이라고 평가되고 있으며, 무선 공개키 기반구조 분야의 경우는 세계 선진 수준과 견줄만 하다고 함 - identity 관리 분야의 경우, 선진국도 이제 시작단계에 있으므로, 국내 산업체도 투자와 연구개발을 통하여 선진국 제품에 뒤지지 않은 제품을 상용화하여 함	- IETF의 경우, IPSec을 위한 PKI, 안전한 크리덴셜 저장 및 전달 프로토콜, 초기 등록 등에 관한 표준을 개발하고 있음 - OMA의 경우 무선 인증서 관련 프로파일을 개발하고 있음 - OASIS는 PKI 활성화 방안을 마련하고 전자서명 및 공개키 기반구조 관련 표준을 개발하고 있고, 웹서비스 보안을 위한 SAML, XACML 등의 표준을 개발 중 - 미국의 경우 150개 이상의 조직이 결합한 Liberty alliance 라는 프로젝트를 통하여 연합된 네트워크 구조를 이용한 싱글 사이언에 대한 표준 및 플랫폼을 개발 중 - 대용량 생체 인식 기술과 결합된 공개키 기반구조 제품이 개발되고 있음	1-3년
시스템 보호기술	- 국내 시스템 보안 제품은 바이러스 감지, 개인 파일보호, PC/서버용 방화벽, 서버 접근제어, 서버 로그제어, 암호화 기술, 보안 OS, 취약성 분석도구, 통합 보안 솔루션 제품 등이 있음 - 보안 OS의 경우 일부 산업체가 2004년도에 CC 평가를 대비하고 있고, 고등급 보장을 위한 제품들이 개발되고 있음 - PC 보안 기술은 바이러스 백신 툴 관리 시스템 개발, 전자증거 수집 교환 형식, 접근 통제를 위한 사용자 인증 기술 등이 있음	- 바이러스 백신 툴의 경우, 시그너쳐 관련 기술은 이미 성숙기를 넘어섰고, 알려지지 않은 바이러스를 탐지하기 위한 다양한 기술들이 개발되고 있음 - 서버 보안 기술은 로그 저장 형식과 접근 제어 모델 기술 등을 개발하고 있음	3-6년
공공부분 응용서비스 보호	- 전자정부법과 전자서명법을 제정하였으며 공인인증기관을 통해 발급된 공인인증서를 이용하여 일부 민원발급 업무에 대해서는 실용화하고 있음 - 웹서비스 보안(SAML, XACML)기술이 ETRI와 산업체를 중심으로 개발 중	- 웹 서비스 보안 표준이 OASIS를 중심으로 개발되어 관련 기술이 웹서비스 제품에 포함되고 있음 - 2000년 2월 IOC 총회에서 새 IOC 위원 선출시 전자투표를 활용한바 있음 - 2000년 3월 미국 Arizona 주 민주당 예비선거에서 인터넷 투표로 시행함 - 일본 터치-패널 스크린(touch-panel screen) 방식의 전자투표 도입함 - 2003년 영국 : 18개 지자체, 정부에서의 다양한 전자투표 시행함	2-3년

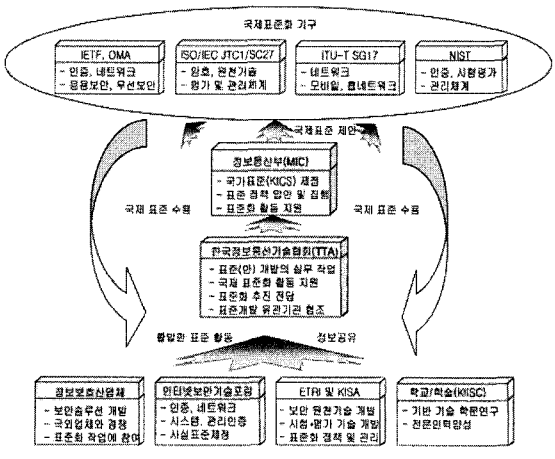
〔표 8〕 국내외 정보보호 기술 현황(2)

핵심 요소기술	국내 정보보호 기술	국외 정보보호 기술	기술격차
네트워크 보호기술	- 방화벽, VPN, 고속 네트워크 보안 장치 등에 대한 기술 개발과, 새로운 네트워크에 대한 보안 기술들이 개발되고 있음 - HTTP에서의 SSL 기반 프로토콜에 대한 제품화와 무선 환경에서의 TLS 기능을 제공하는 방식에 대해 상용화가 진행 중 - ETRI를 중심으로 40Gbps 급의 차세대 네트워크 보안 장치를 개발하고 있음 - IT839 추진과 더불어, 홈네트워크, 이동통신망, 무선 통신망, BcN, 그리고 편재형 네트워크에서 소요되는 보안 기술들이 정의 되고 있으며, 이에 대한 보안 기술들이 개발되고 있음 - BcN의 경우, ITU-T와 ETSI에서 NGN이라는 이름으로 표준화가 수행되고 있으며, 국내에서는 이들의 동향을 근거로 관련 제품과 서비스를 개발하려 함 - 홈네트워크 보안 제품은 인터넷 정보가전용 미들웨어 개발이 초기 단계이므로 이를 위한 기술개발과 표준 연구가 필요함	- 인터넷 침입대응기술은 IETF idwg, inch에서 IDS 요소 시스템간에 데이터 형식과 교환 절차를 위한 프로토콜을 개발과 데이터 언어, 침해 보고와 관련된 샘플 집합을 정의하고 있음 - IETF syslog에서는 네트워크 이벤트와 네트워크 로깅을 위한 사실상의 표준인 BSD 시스로그를 표준화하고 있음 - 멀티캐스트 보안은 시장형성 초기단계이며, 상용화/제품화가 초기 단계임 - 홈네트워크와 무선 근거리통신망(IEEE 802.11i)에 대한 보안 제품이 일부 상용화되고 있음 - BcN 보안 제품은 BcN 프레임워크에 대한 표준화가 완료된 시점에서 개발될 예정임 - 홈네트워크 보안 기술은 UPnP 표준화 기구를 통한 다양한 보안 프레임워크와 인증 및 인가 기술들이 개발되고 있음	3-5년
일반부분 응용서비스 보호	- ETRI와 KISA 등에서 암호 및 PKI 기술을 주도하고 있으며, 이를 기초로 하는 전자우편 보안이 상용화되고 있음 - 국내 전자우편 시장의 경우, 독립적인 전자우편 클라이언트 프로그램에서 MIME을 지원할 경우 다양한 MIME 처리 객체를 구현해야 하므로, 많은 노력이 요구됨 - S/MIME 버전 2나 PGP를 이용한 웹 메일 솔루션이 개발되고 있으며, ETRI와 KISA는 SMIME 버전 2에 기반을 둔 웹 메일 제품에 대한 상호 운용성 시험기술을 개발하고 있음 - 디지털 컨텐츠 보안의 경우, 저작권 보호 시스템과 서비스 분야에 많은 경험과 기술을 축적하고 있으며, 여러 DRM 전문 업체가 독자적인 기술을 개발하거나 외국 전문 기술을 도입하여 국내 시장을 개척하고 있음	- 미국과 유럽을 중심으로 전자우편 보안기술이 개발되어 상용화되고 있음 - 디지털 컨텐츠 보호 기술은 Intertrust, ContentGuard 등의 선도 기술을 보유한 DRM 전문업체가 기술개발을 주도적으로 수행했으나, 최근에는 MS, Adobe 등의 업체들이 기존의 제품에 DRM 기능을 부여함으로써, DRM 시장을 장악하고 있음	2-3년
정보보호 평가 및 관리 체계	- 기존의 위험분석 표준을 새로운 환경에 적합하도록 개정 작업이 필요하며 정보보호 아키텍처, 성과측정 등 새로운 지침 및 표준개발이 요구됨 - 평가 도구 개발 분야는 아직 초기 단계를 벗어나지 못하고 있는 실정임 - 정보보호 제품 평가의 경우, 지금까지는 K 시리즈 기준과 CC가 공동 기준으로 평가되어 왔으나, 최근 정보보호 제품 평가를 방화벽, IDS, VPN에서 지문, 보안 OS, 스마트카드 분야까지 확대하였고, 점차적으로 확대할 추세임 - 상호인정협정 가입을 공식적으로 추진하고 있고, 평가 제품이 다양화되면 민간 평가기관의 도입도 검토될 전망임	- 정보보호 관리기술은 정보보호 관련 전문 공공기관 및 민간기업에서 여러 지침 및 기준 등을 개발하고 있으며, 특히 정보보호컨설팅 업체를 중심으로 위험분석 도구가 개발되고 있음 - 정보보호 평가의 경우 미국은 1983년도부터 TCSEC 기반의 평가를 실시하였고, 1998년 상호인정협정 가입후, CC기반으로 정보보호 제품을 평가하고 있으며, 관련 인증기관으로는 NIST와 NSA가 공동으로 운영하는 NIAP가 있으며, 6개의 민간 분야 평가기관도 지정되어 운영되고 있음. 지금까지는 TCSEC와 CC를 동시에 인정하였으나, 최근 CC만을 공식 평가기준으로 인정하고 있음	2-3년

타원곡선 알고리즘과 토큰 인터페이스 기술, 토큰내의 정보 교환 기술 등은 국내표준화가 필요하다. 또한, 권한 관리 기반구조 분야와 글로벌 차원의 상호 연동 모델의 개발 및 관련 표준을 개발하여 글로벌 경제 시대에 대비하여야 하고, 인증서를 보관하는 LDAP 관련 표준들은 현재 IETF pkix 작업반에서 표준안이 거의 완료된 상태이므로, 이를 국내 환경에 맞게 수용하여야 한다. 시스템 보안기술은 국외 표준을 국내 환경에 맞게 일부 수용하거나 국내 독자적인 표준 개발이 가능한 분야이고, 바이러스 관련 정보교환을 위한 표준을 IETF 표준을 근거로 국내 독자 표준의 개발이 가능하다. 그리고 바이러스 이름 명명 및 호스트 기반 IDS의 데이터 교환 형태 및 API를 표준화해야 한다. 네트워크 보안 기술은 침입대응기술, IP 계층 보안기술, 전송계층보안 기술, 멀티캐스트 보안기술, 이동 IP 보안 기술, 통합 보안 관리 분야는 IETF 표준들을 준용하는 것이 가능한 분야이고, 선도기술개발과제를 통한 국내 표준개발이 가능한 홈네트워크 보안, 편재형 네트워크 보안, 센서네트워크 보안 프로토콜, 휴대 인터넷 보안기술, BcN 보안 분야들은 국내 표준을 개발하고 이를 국제표준을 추진하는 것이 가능할 것으로 사료된다. ETRI 선도 기술개발을 통한 휴대 인터넷과 공중망 무선랜의 안전한 상호 연동 표준화는 국제 표준이 가능한 분야이고, 무선 인터넷을 위한 보안 기술은 무선 근거리통신망 보안 기술의 경우 IEEE 802 표준안을 준용하고, 이중 패스워드 기반 인증 및 키교환 프로토콜은 독자적인 개발을 통한 국내 표준 개발이 가능한 분야이다. BcN 보안 기술의 경우, ITU-T NGN 표준화 동향과 국내 BcN 기술 개발을 참고하여 국내 독자 보안 표준을 개발하여 국제표준으로 추진하여야 하며, IETF의 IPSec 관련 표준중 IKEv2 프로토콜은 조속한 국내 표준이 필요하다. 무선인터넷 보안 분야의 경우는 무선 전송계층 프로토콜, 무선 WIM, 무선 API, 그리고 각종 응용서비스의 추가를 위한 표준화 작업이 추진되어야 한다. 공공부분 응용서비스 보호기술은 전자투표 분야의 기술개발을 통한 IPR 확보가 가능하며, 이를 통한 국제 표준화 추진이 요구된다. 또한 웹서비스 보안의 경우 전자정부에 활용하기 위하여 기존 OASIS 표준을 조속히 수용하는 것이 필요하다. 일반분야 응용서비스 보호 분야인 전자우편 보안 기술은 IETF에서 표준화된 전자우편 보안 관련 표준인 OpenPGP, S/MIME v2, S/MIMEv3, 그리고 S/MIMEv3에 대한 강화 및 개정 작업이 진행 중이므로, 이에 대한 국내 표준 보완이 요구된다. 평가 및 관리체계 인증 분야는 완성도가 높은 ISO/IEC 표준을 준용하여 국내 표준을 제정하여야 하며, 특정 분야에 대한 표준을 우리의 평가 및 관리체계 인증과정에서 얻은 경험을 기반으로 개발하여 이를 국제 표준으로 반영해야 한다. 정보보호 평가를 수행하고 있는 평가기관과 평가를 받을 피평가 기관에서 활용되고 있는 일부 표준들은 국내 환경에 적합하지 않을 수 있으므로, ISO/IEC, ITU-T에서 개발된 표준들을 일부 국내 실정에 적합하게 변형하는 작업이 필요하다. 정보보호 평가·관리 분야의 경우 표준적합성과 관련된 시험 방법론, S/MIME 및 IPSec 표준 적합성 시험 기준 등의 기술 검증이 국내 표준으로 필요하고, 보안성 평가 부분은 ISO/IEC SC37 및 NIST, 국제 공통평가기준 등의 표준화 동향을 적극 반영하여 국내 표준화 작업을 추진하여야 한다.

5.2 국내 정보보호 표준화 추진체계

국내 정보보호 표준화 추진체계는 그림 1과 같이 도식화 할 수 있다. KISA, ETRI를 중심으로 암호기술, 보안 원천기술, 시험·평가기술, 표준화 정책 및 관리체계에 대한 표준들을 개발하여야 하며, 정보보호 산업체에서는 보안솔루션 개발과 국외업체와 경쟁할 수 있는 기술개발, 이런 기술에 대한 표준화 작업이 필요하다. 또한, ISTF는 국내 업체들에서 실제적으로 활용되고 있는 인증기술, 네트워크보안 기술, 시스템 보안 기술, 정보보호 제품 관리 기술 등에 대한 사실 표준들을 제정하고, 학교 및 학술단체에서는 전문인력 양성과 기반기술을 바탕으로 하는 학문연구에 힘써야 된다. 이렇게 개발된 표준안은 상호협력하여 TTA를



〔그림 1〕 국내 정보보호 표준화 추진체계

통하여 국내 단체표준으로 제정하여야 하고, 필요시 IETF, ISO/IEC, ITU-T 등의 국제 표준화기구에 제안하여 국내 기술을 국제표준에 반영하여 지적재산권(IPR)을 확보하여야 한다. 또한, 일부 기술들에 대해 국제표준으로 입증된 기술들은 그대로 준용하거나 국내 환경에 맞게 변경하여 국내표준으로 개발하는 것이 필요하다.

5.3 국내 정보보호 표준화 로드맵('05-'07)

선도기반 표준 과제의 선정은 선도기술의 상호운용성 여부, 국제표준, 시급성, IPR 존재 여부, 미래지향기술 등의 평가항목으로 선정하였고, 산업체 기술인 경우 상호운용성, 시장성, 시급성 등의 평가항목을 근거로 선정하였으며, 일부 항목은 정보보호 산업체 요구에 의한 표준화 항목이다.

다음의 표 9, 10은 공통기반기술에 대한 3개년 로드맵이고, 표 11, 12, 13은 시스템 및 네트워크 보호기술에 대한 3개년 로드맵이다. 또한 표 14는 응용레벨 보안기술에 대한 3개년 로드맵이고, 표 15는 정보보호 평가 및 관리체계에 대한 3개년 로드맵이다.[2,3]

Ⅵ. 결 론

본 논문에서는 국내 정보보호 표준화를 효율적으로 추진하기 위하여 국제 표준화기구인 IETF, ISO/IEC JTC1/SC27, ITU-T SG17, NIST의 정보보호 동향을 분석하였고, 이를 근거로 정보보호 분야를 크게 공통기반기술, 시스템 및 네트워크 보호기술, 응용레벨 보안기술, 정보보호 평가 및 관리체계로 분류한 후, 이를 좀더 세부적인 표준화 항목으로 분류하였다. 그리고 분류된 항목에 대한 국내외 기술을 비교분석하였으며, 이들을 근거로 국내 정보보호 표준화 추진 시 활용할 수 있는 표준화 추진전략과 추진체계, 그리고 향후 3년간의 표준화 로드맵을 제안하였다.

〔표 9〕 국내 정보보호 표준화 로드맵 - 공통기반기술(1)

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진선도 표준화 과제	국제 표준 완료 시기	기술개발 완료시기	
		'05	'06	'07	이후			국내	국외
암호기술	- 암호메카니즘 · 중비도/중속(2048비트 수준,Gbps) 공개키 암호 알고리즘			▶		선정	'06	'08 이후	'08 이후
	· 중비도/중속(AES 수준,Gbps) 블록 암호 알고리즘		▶						
	· 하드웨어 전용 스트림 암호 알고리즘		▶						
	· 가변길이 해쉬 알고리즘		▶			선정			
	· 특수 전자서명 알고리즘		▶			선정			
	· 대칭키 암호 운영 모드		▶						
	· 의사 난수 발생기		▶						
	· 경량 암호 알고리즘			▶		선정			
	· 고비도/고속 암호 메카니즘(4096비트, Tbps)				▶				
	- 암호 키관리 · 암호 키 복구 기술		▶			선정	'07	'08	'07
	· 암호 키 관리 시스템 지침	▶							
	· KMI 기술		▶			선정			
	· 패스워드 기반 인증 및 암호 키 분배 기술		▶						
	· 멀티캐스트 키 관리 기술			▶		선정			
	· 그룹키 관리 기술			▶		선정			
	- 암호구현 · Side Channel Attack 방지 암호 구현 기술	▶					'08 이후	'09	'08
	· 암호 서비스 API 구현 지침		▶						
	· RSA 암호 고속화 기술		▶			선정			
	· 타원곡선 암호 고속 구현 기술		▶			선정			
	· 암호 컴포넌트 인터페이스 지침	▶							
	· 암호 분석 S/W 기술	▶							
	· 암호 모듈 구현 취약성 검증 기술	▶							
	· H/W 암호 모듈 구현 기술	▶							
	· 범 아시아 호환 교통카드 규격 표준화 연구			▶		선정			

〔표 10〕 국내 정보보호 표준화 로드맵 - 공통기반기술(2)

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진도 표준화과제	국제 표준 완료시기	기술개발 완료시기	
		'05	'06	'07	이후			국내	국외
인증기술	- PKI 기술					선정	'06	'08 이후	'08 이후
	· 유무선 인증서 요구 메시지 형태	▶							
	· 개인키 소유증명		▶						
	· 인증기관 인증서 정책 및 인증업무준칙	▶							
	· 타임스탬프 인증서 정책 및 업무준칙	▶							
	· SIM 인증서 확장자 · 무선 LAN 확장자		▶						
	· 보증 확장자 · 로고타입 확장자		▶						
	· 항구적인 식별자 · 암호 알고리즘 확인자		▶						
	· 해쉬 알고리즘			▶					
	· ECC 알고리즘 표준		▶						
	· 경로 생성 표준		▶						
	· 인증 경로 검증 표준			▶					
	· 위임 인증서 프로파일		▶						
	· 적격 인증서 프로파일		▶						
	· PKCS 표준	▶							
	· 유무선 인증서 관리		▶						
	· 인증서 운영		▶						
	· X.509 PKI를 위한 LDAP 스키마		▶						
	· 시점확인 서비스		▶						
	· 온라인 인증서 검증	▶							
	· 대리 인증 경로 발견 및 검증 요구사항		▶						
	· SCVP		▶						
	· 데이터 인증 및 검증 서비스		▶						
	· 신뢰된 아카이브 프로토콜			▶					
	· 레포지터리 위치 확인 서비스		▶						
	· 글로벌 상호 연동 프레임워크			▶					
	· 장기간 아카이브 서비스			▶					
	· IPSec을 위한 PKI			▶					
	· 크리덴셜 정보 전달 프로토콜			▶					
	· 초기 등록 모델			▶					
	· SNMP를 위한 인증 확장				▶				
	· 보호된 엔터테인먼트 관리를 위한 보안 프로토콜				▶				
	· 오프라인 전자서명 표준		▶						
	· 대리서명 방식 및 프로토콜		▶						
	· 서명 관리를 위한 로그 형식		▶						
	· XML 서명 방식	▶							
	· XML 암호 방식	▶							
	· XML 키관리 방식	▶							
	- PMI 기술						'07	'08	'07
	· 속성/인가 인증서 프로파일		▶						
	· 속성 인증서 정책 및 CPS		▶						
	· 속성 인증서 관리 표준		▶						
	· 속성 인증서 요청 메시지 형태			▶					
	· 속성 인증서 운영 프로토콜			▶					
	· 권한관리구조			▶					
	- Identity 관리						'07	'09	'08
	· ID 호스팅			▶					
	· ID federation			▶					
	· e-프라이버시 보호			▶					
	- 무선 공개키기반구조						-	'09	'08
	· 무선 인증서 규격 보완	▶							
	· 무선 PKI를 위한 보안 API	▶							

〔표 11〕 국내 정보보호 표준화 로드맵 - 시스템 및 네트워크 보호기술(1)

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진선도 표준화 과제	국제 표준 완료 시기	기술개발 완료시기	
		'05	'06	'07	이후			국내	국외
시스템 보안기술	- PC 보안 기술								
	· 바이러스 백신 툴 관리 지침	▶							
	· 패스워드 표준	▶							
	· 전자증거 수집 교환		▶			선정	'07	'07	'06
	· 통합 프레임워크		▶						
	· 통합 API		▶						
	· 바이러스 명명법	▶							
	- 서버 보안 기술								
	· 로그형식		▶						
	· 접근제어 모델(RBAC)		▶			선정			
	· 보안 DBMS	▶							
	· 감사추적		▶						
	· 전자증거 수집 교환			▶					
	· SSH		▶						
	· 포렌직 기술			▶			'06	'09	'08
	· 신뢰경로 암호화			▶					
	· ACL 형식	▶							
	· AC 방식	▶							
	· CL 방식	▶							
	· IFC(Information flow control)		▶						
	· 인증 프레임워크	▶							
네트워크 보안기술	- 침입대응기술								
	· 침입차단시스템 통과를 위한 인증 방식	▶							
	· 침입탐지/차단 로그 형식		▶			선정			
	· 침입탐지/경고 메시지 교환형식		▶						
	· 침입탐지 메시지 포맷 구현언어		▶						
	· 침입차단 통신 프로토콜	▶							
	· 침입자 역추적 프로토콜/메시지		▶			선정			
	· 라우팅 프로토콜 보안		▶						
	· 라우터 기반 DDoS 필터링 형식	▶					'08	'08	'07
	· 보안 DNS 구조		▶						
	· 개인 방화벽 시스템 모델		▶			선정			
	· 침해사고 정보교환형식(IODEF)			▶					
	· 침입 패턴	▶				선정			
	· 침입 패턴 교환	▶							
	· 침입 패턴 공유		▶			선정			
	· 침입차단시스템 로그 형식 및 통계		▶			선정			
	· 침입 탐지 로그 형식		▶						
	- IP 계층 보안기술								
	· IP 보안 프로토콜(AH, ESP, IKE)	▶							
	· IPSec에서의 IKE 암호 알고리즘		▶						
	· IP 보안정책		▶						
	· IPSec MIB		▶						
	· NAT 경유 프로토콜		▶						
	· DNS에서의 IPSec 키저장방식		▶						
	· IPSec 기반 접근제어		▶				'06	'10	'09
	· IPSec 기반 원격 사용자 인증		▶						
	· 4G망에서의 IP 보안 기술			▶					
	· IKE를 위한 국내 암호 알고리즘 (SEED, HAS, KCDSA) 변환 ID	▶				선정			
	· 로그 형식	▶				선정			
	· UDP 캡슐화 · 리키(IPSec, IKE)	▶							
	· NAT-T 검출	▶							

〔표 12〕 국내 정보보호 표준화 로드맵 - 시스템 및 네트워크 보호기술(2)

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진선도표준화과제	국제표준완료시기	기술개발완료시기	
		'05	'06	'07	이후			국내	국외
네트워크 보안기술	- 전송계층 보안기술								
	· HTTP 프로토콜을 위한 TLS	▶							
	· AES Ciphersuite 기반 TLS		▶						
	· ECC Ciphersuite 기반 TLS			▶			'06	'08	'07
	· 국내 암호기반 TSL Ciphersuite	▶							
	· TLS 인증(Kerberos SRP)			▶					
	· TLS 압축 방식 · TLS 기능 확장 방식			▶					
	- 멀티캐스트 보안								
	· 암호 메시지 교환 방식	▶							
	· 멀티캐스트 그룹키분배 프로토콜	▶							
	· 멀티캐스트 보안 구조	▶					'09	'08	'07
	· 멀티캐스트 인증 구조 및 보안 정책		▶						
	· IPsec을 이용한 멀티캐스트 보안 프로토콜	▶				선정			
	- IT839 네트워크 기반 보호								
	① 홈네트워크 보안 기술			▶		선정			
	· 홈네트워크 보안 프레임워크	▶							
	· 홈게이트웨이 보안 서버		▶						
	· 홈네트워크 미들웨어 보안 기술		▶						
	· 홈네트워크 인증 및 접근제어		▶						
	· 보안 프로토콜			▶					
	② 편재형 네트워크 보안 기술				▶	선정			
	· 보안 프레임워크 개발			▶					
	· RFID/USN 노드 및 미들웨어 정보보호			▶					
	· 경량화된 보안 프로토콜 개발			▶					
	· 보안 디바이스 기술 개발			▶					
	③ 센서네트워크 보안 프로토콜 기술				▶	선정			
	④ 휴대인터넷(HPi) 보안기술		▶			선정			
	· 보안 프레임워크		▶						
	· 링크레벨 보안		▶						
	· AAA 보안 프로토콜 및 보안 구조		▶						
	· 휴대인터넷과 공중망 무선랜의 안전한 상호연동 표준화		▶			선정			
	· 응용 보안 프로토콜			▶			'07	'12	'10
	⑤ BcN 보안				▶	선정			
	· BcN 보안 프레임워크			▶					
	· BcN서의 AAA 구조 및 보안 프로토콜			▶					
	· BcN 모바일 IP 기술			▶					
	· BcN 링크레벨 보안			▶					
	· 유 무선 연동 기술			▶					
	⑥ 무선 근거리통신망		▶			선정			
	· IEEE 802.1x 인증기술	▶							
	· IEEE802.11i 기술		▶						
	· EAP-TLS 기술	▶							
	· TTLS 기술	▶							
	· PAK 기반 보안 프로토콜		▶			선정			
	⑦ 4G 이동통신망(W-CDMA)보안			▶					
	· 이동 IP 보안 기술			▶					
	· AAA 보안 구조 및 보안 프로토콜.기술			▶					
	· 유무선망간 보안 연동 기술			▶					
	⑧ WPAN 보안								
	· 보안 프레임워크 · 인증 기술								
	· 보안 프로토콜								

〔표 13〕 국내 정보보호 표준화 로드맵 - 시스템 및 네트워크 보호기술(3)

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진선도표준화과제	국제표준완료시기	기술개발완료시기	
		'05	'06	'07	이후			국내	국외
네트워크 보안기술	- 차세대 네트워크 보안기술 · 시큐어 보안 라우터 · 시큐어 보안 스위칭 허브 · 망 보안 구조 · 네트워크 관리를 위한 안전한 네트워크 보안 프로토콜 · 능동 인터넷 기반의 차세대 네트워크 인프라 및 서비스		▶ ▶ ▶ ▶	▶ ▶		선정	'06	'09	'08
	- 이동 IP 보안 · 모바일 IPv4 보안 · 모바일 IPv6 보안 · 다이아메터 기반 보안 구조 및 보안 프로토콜		▶ ▶	▶			-	'08	'07
	- 통합보안관리 · ESM 보안관리 구조 및 정보전달 프로토콜 · 로그 형식 · 보안 정책 · 취약성 표준화 · 취약성 DB 표준화 · 연계 분석 · 대응 · 타시스템 연동 · 수사 증거자료 · 보안 사고 처리 · 보안사고 평가 정량화	▶				선정	'05	'07	'06

〔표 14〕 국내 정보보호 표준화 로드맵 - 응용레벨 보안기술

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진선도표준화과제	국제표준완료시기	기술개발완료시기	
		'05	'06	'07	이후			국내	국외
공공부분 응용서비스 보호	- 전자정부 관련 보안기술 · 웹 서비스 보안(SAML, XACML) · 민원 발급 보안 · 전자지불 보안 · 보안 정책 및 기술 적용 지침	▶	▶ ▶ ▶			선정	'07	'07	'06
	- 전자투표/공증 · 전자투표 방식 · 전자투표 프로토콜 · 전자투표 보안 문서 · 전자공증 방식 · 전자공증 프로토콜 · 전자공증 보안 문서			▶ ▶ ▶ ▶ ▶ ▶			'05	'10	'09
일반부분 응용서비스 보호	- 전자메일 보안 · 암호 메시지 구문 · S/MIME 메시지 명세 · 패스워드 기반 암호 · ECC 암호 기법 사용 · CMS 대칭키 관리 및 분배 · SEED 암호화 알고리즘 국제 표준 채택 · 차세대 전자우편보안 프로토콜	▶	▶ ▶ ▶ ▶ ▶	▶			'06	'06	'05
	- 디지털 컨텐트 보안 · E-Book 저작권 보호 · 멀티미디어 저작권보호		▶	▶			-	'07	'06

〔표 15〕 국내 정보보호 표준화 로드맵 - 정보보호 평가 및 관리체계

핵심 요소기술	세부 핵심 요소기술	국내 표준화 완료시기				우선추진선도 표준화 과제	국제 표준 완료 시기	기술개발 완료시기	
		'05	'06	'07	이후			국내	국외
정보보호 평가	- 표준적합성 시험 기술 · 표준적합성 시험 방법론 · S/MIME 시험기술 · IPSec 시험기술	▶ ▶ ▶					'05	-	-
	- 보안성 평가 기술 · 국제공통표준 · 보호프로파일 및 보안목표명세서	▶ ▶					'05	'07	'06
관리체계	- 정보보호 정책/조직 · 정보보호 정책 수립 절차 · 정보보호 예산편성 절차 및 기법 · 정보보호 조직의 역할 및 책임 · 서비스 계약 · 침해사고 대응 절차 · 관리체계 표준	▶ ▶ ▶	▶ ▶	 ▶			-	'06	'06
	- 위험 분석/관리 · 위험관리 절차 및 위험분석 기법		▶				'05	-	-
	- 대책 구현 및 교육 훈련 · 정보보호 대책 목록 및 선정지침 · 정보보호 아키텍처 · 정보보호 교육훈련 프로그램 수립 · 정보시스템 보안성 평가 및 승인	▶ ▶	 ▶ ▶				'06	'06	'05
	- 사후 관리 · 보안 감사 · 보안사고관리 · 업무지속성관리 · 보안 로그 및 감시	 ▶	▶ ▶ ▶				'06	'07	'07
	- 관리체계 및 성과측정 · 정보보호 관리체계 · 정보보호성과측정 척도개발		▶	▶			-	'08	'07

정보보호 분야의 표준화는 BcN, U-센서 네트워크 등의 통신망과 모든 IT 정보시스템을 안전하게 사용하기 위하여 필수적인 기술이며, 특히 BcN, 홈네트워크 분야의 정보보호는 국외에서 이제 막 논의가 시작되고 있으므로, 국내에서도 적극적으로 대응하여 국내 기술을 국제표준에 반영하고 IPR 확보에 힘써야 한다. 그리고 국제 표준화가 성숙도에 있는 기술들에 대해서는 빠르게 검토를 하여 국내 환경에 맞게 준용하여야 하며, 국내 연구기관 및 정보보호 산업체에서는 국내 고유표준 개발에 힘써야 될 것으로 사료된다.

참 고 문 헌

〔1〕 염흥열, "정보보호일반 표준화 로드맵(v2004)", TTA, 2003.12.

〔2〕 염흥열, "정보보호일반 표준화 로드맵(v2005)", TTA, 2004.12.

〔3〕 "정보보호 표준화 로드맵", KISA, 2004.7.

〔4〕 MIC Homepage, http://www.mic.go.kr

〔5〕 TTA Homepage, http://www.tta.or.kr

〔6〕 KISA Homepage, http://www.kisa.or.kr

〔7〕 ETRI Homepage, http://www.etri.re.kr

〔8〕 IETF Homepage, http://www.ietf.org

〔9〕 ISO/IEC JTC1 SC27 Homepage, http://www.iso.org

〔10〕 ITU-T Homepage, http://www.itu.int

〔11〕 NIST Homepage, http://www.nist.gov

〔12〕 "2003년 정보통신 기술·산업전망(2003년 ~ 2007년)", ETRI, 2003.4.

〈著 者 紹 介〉

오 흥 룡 (Heung-Ryong Oh)
정회원

2002년 2월 : 순천향대학교 전자공학과 졸업
2004년 2월 : 순천향대학교 정보보호학과 석사
2004년 2월~현재 : 한국정보통신기술협회(TTA)
〈관심분야〉 보안 프로토콜, 정보보호표준

오 세 순 (Se-Soon Oh)

1996년 2월 : 충남대학교 컴퓨터과학과 졸업
1996년 1월~1998년 2월 : 금호텔레콤 멀티미디어팀
2000년 8월~2004년 3월 : 한국표준협회(KSA) 표준연구개발팀
2004년 4월~현재 : 한국정보통신기술협회(TTA)
〈관심분야〉 생체인식, 인터넷보안

김 선 (Sun Kim)

1992년 2월 : 항공대학교 전자공학과 졸업
1991년 9월~현재 : 한국정보통신기술협회(TTA)
〈관심분야〉 BcN, 정보보호, IPv6, 홈네트워크

염 흥 열 (Heung-Youl Youm)
정회원

1981년 2월 : 한양대학교 전자공학과 졸업
1983년 2월 : 한양대학교 전자통신공학과 석사
1990년 2월 : 한양대학교 전자통신공과 박사
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보기술공학부 교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~현재 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국통신정보보호학회 총무이사, 학술이사, 교육이사
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associative Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Associative Rapporteur
〈관심분야〉 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안