정보보호 표준 기술 동향 및 로드맵

오흥룡*, 염흥열*

*순천향대학교 정보보호학과

Analysis on Information Security Standardization and Roadmap

Heung-Ryong Oh*, Heung-Youl Youm*

*Department of Information Security SoonChunHyang Univ.

요 약

정보보호 기술 표준화는 인터넷 등의 급속한 발전에 따라 전자상거래 등의 응용 서비스와 새로운 무선 및 이동 인터넷 서비스를 여러 위협요소로부터 보호하는데 목적이 있다. 인터넷을 통해 유통되는 정보나 컴퓨터의 정보 자산을 보호하기 위한 요구사항으로 기밀성 서비스, 무결성 서비스, 인증 서비스, 그리고 액세스 제어 서비스들이 요구되고 있다. 따라서 정보보호 시스템간의 상호 연동성을 가능케 하고, 안전한 지식기반 정보화 사회 구축을 위해서 정보보호 기술 요소들의 표준화 분석은 반드시 필요하다.

I. 서론

정보보호 일반 기술은 인터넷 등의 컴퓨터 통신망을 통하여 전달되는 정보의 위조, 변조, 유출, 무단침입 등을 비롯한 각종 불법 행위로부터 조직 혹은 개인의 컴퓨터와 정보를 안전하게 보호하는 기술을 말하며, 주요 기술 분야는 암호 기술, PKI 기술, 관련 공개키 표준인 PKCS(Public Key Cryptography Standard), 인증서를 저장하는 LDAP(Lightweight Directory Access Protocol) 기술, 네트워크 계층 보안을 위한 IP 계층 보안 및 키 관리 프로토콜(IPsec; IP Security), 전송 계층을 위한 전송 계층 보안(TLS : Transport Layer Security), 전자우편 보안, 어플리케이션 데이터에 적용되는 XML 보안, 통합보안관리시스템(ESM : Enterprise System Management) 기술, 무선 인터넷 보안등으로 구성된다.

최근 정보화의 역작용을 방지하기 위한 정보보호기술의 중요성이 증대됨에 따라 사회 각 분야에서 정보보호에 대한 관심이 매우 고조되고 있다. 특히 지난 1.25 인터넷 대란에서 알 수 있듯이 정보보호 기술이 미흡한 정보통신망은 안정성과 가용성을 보장받을 수 없다는 것을 알 수 있었다.

정보보호 분야의 표준화 활동은 크게 국외 표준화 기구에서 표준화된 국제 표준을 국내 표준화하는 과정, 국내에서 개발된 고유의 기술을 국제 표준화 기구의 국제 표준으로 채택하는 과정, 국내에서 개발된 기술을 국내 표준화 기관에 표준화하는 과정 등으로 구분될 수 있다. 정보보호 분야 표준화도 역시 정보기술 분야의 표준화와 마찬가지로 제품간의 상호 연동성 보장이 매우 중요하다. 이런 표준화 활동을 통해서 제품의 시장 규모를 증가시킬 수 있고, 전용 기술의 채택으로 인한 정보보호 제품의 상품화의 위험을 감소시킬 수 있다. 따라서, 인터넷 정보보호 산업의 육성을 위해서는 정보보호 기술의 표준화 작업이 무엇보다도 시급하다고 할 수 있다[12].

본 논문의 구성은 다음과 같다. 2장에서는 국외 표준화 기술 동향에 대해 분석하고, 3장에서는 국내 표준화 기술 동향에 대해 분석한다. 4장에서는 이 분야의 국내·외 시장현황과 기술개발 현황에 대해서 비교 분석한다. 그리고 5장에서는 이를 바탕으로 표준화 추진전략과 부록에 있는 표준화 3년 로드맵을 예측하고, 6장에서 결론을 맺는다.

II. 국외 표준화 기술 동향

1. PKI

pkix 작업반은 X.509 기반의 PKI 지원을 위한 인터넷 표준 개발을 수행하고 있다. 작업반 문서들은 X.509 v3 인증서와 v2 인증서 폐지 목록에 대한 프로파일, 공개키 인증서의 관리와 요청 및 상태 표시등을 위한 프로토콜, LDAP/FTP/HTTP 등에 의한 PKI 작업, Diffie-Hellman 소유 증명 알고리즘, 적격인증서 프로파일, 데이터 검증/인증 서버 프로토콜, 타임스탬프 프로토콜 등을 규정하고 있다. 현재의 주요 활동은 PKIX 인증서 및 CRL 프로파일 개정작업 (경로 검증, CRL 검증 보완), CRMF, OCSP, CMC 등에 대한 개정 작업, 영구 식별자, 대리 인증서, SCVP, 그룹 이름, LDAPv3, NR, TSA, DPV/DPD, OCSPv2, TSP에 대한 개발 등이다. 표준안은 크게 인증서 관련 표준, 운영 및 인증서 관리 관련 표준, 그리고 응용 프로토콜로 구분될 수 있다. PKI 관련 표준 문서들은 표 1과 같다.

표 1 : PKI 표준 문서

구분	문서번호	제 목	상태	발표월일
인증서	RFC 2459/3280	Internet X.509 Public Key Infrastructure Certificate and CRL Profile	표준	99.1 / 02.4
	RFC 2527	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework	정보	99.3
	RFC 2528	Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	정보	99.3
	RFC 3039	Internet X.509 Public Key Infrastructure Qualified Certificates Profile	표준	01.1
	RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile	표준	02.4
	RFC 3281	An Internet Attribute Certificate Profile for Authorization	표준	02.4
운영/관리	RFC 2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols	표준	99.3
	RFC 2511	Internet X.509 Certificate Request Message Format	표준	99.3
	RFC 2559	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2	표준	99.4
	RFC 2585	Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP	표준	99.5
	RFC 2587	Internet X.509 Public Key Infrastructure LDAPv2 Schema	표준	99.6
	RFC 2875	Diffie-Hellman Proof-of-possession algorithm	표준	00.7
	RFC 2797	Certificate Management Messages over CMP	표준	00.4
응용프로토콜	RFC 2560	Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP	표준	99.6
	RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols	실험	01.2
	RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)	표준	01.8
	RFC 3379	Delegated Path Validation and Delegated Path Discovery Requirements	정보	02.9

2. VPN을 위한 IPsec 기술

ipsec 작업반은 응용 계층과 무관하게 IP 계층에서 암호화와 인증 등의 보안 서비스를 제공하기 위한 프로토콜과 관련 키 관리 프로토콜을 개발하고 있다. ipsec 작업반의 문서들은 IPsec 구조 문

표 2 : IPSec 표준 문서

구분	문서번호	제 목	상태	발표월일
IPsec 구조	RFC 2401	Security Architecture for the Internet Protocol	Proposed Standard	98.11
문서지침서	RFC 2411	IP Security Document Roadmap	Informational	98.11
IPsec 프로토콜	RFC 2402	IP Authentication Header	Proposed Standard	98.11
	RFC 2406	IP Encapsulating Security Payload (ESP)	Proposed Standard	98.11
암호알고리즘	RFC 1829	The ESP DES-CBC Transform	Proposed Standard	95.8
	RFC 2405	The ESP DES-CBC Cipher Algorithm with Explicit IV	Proposed Standard	98.11
	RFC 2410	The NULL Encryption Algorithm and Its Use with Ipsec	Proposed Standard	98.11
	RFC 2451	The ESP CBC-Mode Cipher Algorithms	Proposed Standard	98.11
인증알고리즘	RFC 1828	IP Authentication using Keyed MD5	Proposed Standard	95.8
	RFC 2104	HMAC: Keyed-hashing for Message Authentication	Informational	97.2
	RFC 2085	HMAC-MD5 IP Authentication with Replay Prevention	Proposed Standard	97.2
	RFC 2403	The Use of HMAC-MD5-96 within ESP and AH	Proposed Standard	98.11
	RFC 2404	The Use of HMAC-SHA-1-96 within ESP and AH	Proposed Standard	98.11
	RFC 2857	The Use of HMAC-RIPEND-160-96 within ESP and AH	Proposed Standard	00.6
자동키관리	RFC 2409	The Internet Key Exchange (IKE)	Proposed Standard	98.11
	RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	Proposed Standard	98.11
	RFC 2412	The OAKLEY Key Determination Protocol	Informational	98.11
	RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	Proposed Standard	98.11

서, 인증 메커니즘 문서, 암호화/인증 메커니즘 문서, 키 관리 관련 문서, 인증 알고리즘 문서, 암호화 알고리즘 문서 등으로 분류된다. IPsec은 차세대 IPv6에서는 필수적으로 구현되도록 규정되어 있으나 현재의 IPv4에서는 선택 사항이며, 가상사설망(VPN)의 주요 프로토콜로 사용되고 있다. IPSec 관련 표준 문서는 표 2와 같다.

3. 전송계층 보안

tls 작업반은 트랜스포트 계층 상위에서의 기밀성, 인증, 무결성 구현 방법 제공을 목표로 표준화 작업을 수행하고 있으며, 넷스케이프 SSL을 기초로 하고 있다. 이 작업반은 기존의 TLS 프로토콜을 진화시키며, 다양한 암호 알고리즘이 TLS에 사용되도록 각종 암호 스위트들을 규정하고 있다. 전송계층 보안 표준 문서는 표 3과 같다.

표 3 : 전송계층 보안 표준 문서

구분	문서번호	제 목	상태	발표월일
프로토콜	RFC 2246	The TLS Protocol Version 1.0	Proposed Standard	1999
	RFC 2817	Upgrading to TLS Within HTTP/1.1	Proposed Standard	2000
	RFC 2818	HTTP Over TLS	Informational	2000
	RFC 3456	Transport Layer Security Extension	Proposed Standard	2003
사이퍼스위트	RFC 2712	Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	Proposed Standard	1999
	RFC 3268	AES Ciphersuites for TLS	Proposed Standard	2002

4. 전자우편 보안

smime 작업반은 RSA 사의 주도로 만들어진 인터넷 전자우편 보안 표준인 S/MIME 버전 2를 수용하여 RFC로 발표하고, 바로 이어 메시지 양식, 처리 절차, 보안성 등을 개선하고 새로운 기능을 추가하기 위한 버전 3 개발 작업에 착수한 이래, S/MIME 메시지 형식과 처리, 인증서 처리, 추가로 도입되는 암호 알고리즘들(IDEA, SKIPJACK, PBE, CAST-128), Diffie-Hellman 알고리즘 관련 사항, 강화된 보안 서비스, 전자서명 정책, 도메인 보안 서비스 등을 규정하고 있다. S/MIME은 안전한 MIME 데이터를 송수신할 수 있는 일관성 있는 방법을 제공하며, S/MIME는 기존의 메일 사용자 에이전트에 의하여 사용되고, 송수신되는 메일에 암호학적 부가 기능을 제공할 수 있다. CMS는 암호학적 메시지 구문으로써, 이 구문은 임의의 메시지 내용을 암호화하고, 인증하

표 4 : S/MIME 표준 문서

구분	문서번호	제 목	발표월일
암호 및 인증 알고리즘	RFC 3565	Use of the Advanced Encryption Standard (AES)Encryption Algorithm in Cryptographic Message Syntax (CMS)	2003.
	RFC 3560	Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)	2003
	RFC 3537	Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) Key or an Advanced Encryption Standard (AES)Key	2003
	RFC 3394	Advanced Encryption Standard (AES) Key Wrap Algorithm	2002
	RFC 3370	Cryptographic Message Syntax (CMS) Algorithms	2002
	RFC 3278	Use of ECC Algorithms in CMS	2002
	RFC 3211	Password-based Encryption for SMS	2001
	RFC 3185	Reuse of CMS Content Encryption Keys	2001
	RFC 3217	Triple-DES and RC2 Key Wrapping	2001
	RFC 2984	Use of the CAST-128 Encryption Algorithm in CMS	2000
	RFC 2631	Diffie-Hellman Key Agreement Method	1999
	RFC 3058	Use of the IDEA Encryption Algorithm in CMS	2001
	RFC 2876	Use of the KEA and SKIPJACK Algorithms in CMS	2000
메시지 타입, 암호학적 구문, 메시지 명세	RFC 3274	Compressed Data Content Type for Cryptographic Message Syntax (CMS)	2002
	RFC 3369	Cryptographic Message Syntax	2002
	RFC 2633	S/MIME Version 3 Message Specification	1999
	RFC 2630	Cryptographic Message Syntax	1999
	RFC 2311	S/MIME Version 2 Message Specification	1998
	RFC 2440	OpenPGP Message Format	1998
	RFC 3126	Electronic Signature Formats for long term electronic signatures	2001
강화된 보안 서비스	RFC 2634	Enhanced Security Services for S/MIME	1999
	RFC 3183	Domain Security Services using S/MIME	2001
	RFC 3156	MIME Security with OpenPGP	2001
인증서 처리	RFC 2632	S/MIME Version 3 Certificate Handling	1999
	RFC 2312	S/MIME Version 2 Certificate Handling	1998
정책	RFC 3114	Implementing Company Classification Policy with the S/MIME Security Label	2002
	RFC 3125	Electronic Signature Policies	2001
공격	RFC 3218	Preventing the Million Message Attack on CMS	2001
	RFC 2785	Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME	2000

고, 서명하고, 메시지 다이제스트 하는데 사용된다. CMS는 데이터를 보호하기 위한 캡슐화 구문을 제공하며, 디지털 서명과 암호를 지원한다. 이 구문은 다중의 캡슐화를 지원하며, 서명 시간과 같은 다양한 속성을 지원한다. 또한 다양한 인증서 기반 키 관리를 위한 구조를 지원한다. 표준 문서는 암호 및 인증 알고리즘, 메시지 타입, 인증서 처리, 보안, 정책, 공격 등으로 구분된다[14]. S/MIME 표준 문서는 표 4와 같다.

5. PKCS

PKCS 표준은 RSA암호 표준, DH(Diffie-Hellman) 키 일치 표준, 패스워드-기반 암호 표준, 확장된 인증서 구문 표준, 암호학적 메시지 구문 표준, 개인키 정보 구문 표준, 선택된 속성 타입, 인증 요구 구문 표준, 암호학적 토큰 인터페이스 표준, 개인 정보 교환 구문 표준, 타원곡선 암호 표준, 암호학적 토큰 정보 포맷 표준 등을 다루고 있다. 이 표준은 PKIX와 관련된 표준과 S/MIME 표준에 영향을 미친 아주 중요한 사실 표준이다. PKCS 표준 문서는 다음의 표 5와 같다.

표 5 : PKCS 표준 문서

문서 번호	제 목	개정여부	발표 월일
PKCS #1	RSA Cryptography Standard	버전 2.1	02.6
PKCS #3	Diffie-Hellman Key Agreement Standard	버전 1.4	93.11
PKCS #5	Password-Based Cryptography Standard	버전 2.0	99.3
PKCS #6	Extended-Certificate Syntax Standard	버전 1.5	93.11
PKCS #7	Cryptographic Message Syntax Standard	버전 1.5	93.11
PKCS #8	Private-Key Information Syntax Standard	버전 1.2	93.11
PKCS #9	Selected Attribute Types	버전 2.0	00.2
PKCS #10	Certification Request Syntax Standard	버전 1.7	00.5
PKCS #11	Cryptographic Token Interface Standard	버전 2.2 (검토중)	03.6
PKCS #12	Personal Information Exchange Syntax Standard	버전 1.0	99.6
PKCS #13	Elliptic Curve Cryptography Standard	개발중	-
PKCS #15	Cryptographic Token Information Format Standard	버전 1.1	00.8

6. 커버로스

현재는 활동을 하고 있지 않은 작업반인 aft 작업반은 David Koblas가 개발한 SOCKS 시스템에 기초한 방화벽 통과 인증 구조를 갖는 통과 프로토콜에 대한 작업을 수행한다. cat 작업반은 분산 시스템에서의 인증, 무결성, 기밀성, 권한 부여 등의 보안 서비스 제공을 위한 프로토콜을 개발해 왔으며, 보안 서비스와 하부 보안 메커니즘의 분리를 강조하고 있다. 지원하고 있는 기존 보안 메커니즘으로는 공개키 기반의 DEC 사의 DASS와 공유 비밀키 기반의 MIT의 Kerberos인데, 대부분의 작업은 Kerberos에 치중되어 있다[12, 13].

7. 무선 인터넷 보안

무선 인터넷 보안은 WAP의 후신 조직으로써, OMA에서 표준을 개발하고 있다. 이의 주요 내용은 무선 보안 기반, 무선 보안 프로토콜, 그리고 무선공개키 기반구조 분야로 분류될 수 있다. 무선 보안 기반 분야에서는 암호 API 라이브러리, WIM 에 관한 표준화 작업을 수행하고 있고, 부선 보안 프로토콜 분야에서는 무선 전송계층 프로토콜과 관련 프로파일을 표준화하고 있으면, 무선 공개키 기반구조 분야에서는 무선 공개키 기반구조와 무선 인증서 프로파일에 대한 명세를 표준화하고 있다[3]. 표 6은 OMA 표준 내용이다.

표 6 : OMA 표준

구분	표준화 항목	주요 내용
무선보안 기반	WMLScript 암호 API 라이브러리 명세	WAP 클라이언트에게 암호기능을 제공하기 위한 WML 스크립트를 위한 라이브러리 인터페이스와 WAP 디바이스로부터 서명된 데이터를 전달하기 위하여 사용되는 서명된 내용 포맷에 대한 정의
	WIM(Wireless Identity Module) 명세	응용 보안과 WTLS 보안을 지원하기 위하여 필요한 사용자 신분확인과 인증과 관련되는 개인키를 저장하고 처리하기 위한 스마트카드 등으로 구현되는 토큰 인터페이스를 정의
무선보안 프로토콜	무선 전송계층 보안(WTLS) 명세	무선 전송계층 상위에서 인증, 무결성, 기밀성 서비스를 응용에게 지원하는 프로토콜로, 긴 지연을 갖는 저대역 통신에 적합한 형태로 TLS 프로토콜을 취적화한 프로토콜
	WAP TLS 프로파일 및 터널링 명세	WAP TLS 프로파일을 규정하고, 사이퍼 스위트, 세션등의 TLS 프로파일, 그리고 TLS 터널링 명세를 규정
무선보안 인증	WAP 인증서 프로파일 명세	인증을 위한 사용자 인증서, 디지털 서명을 위한 사용자 인증서, X.509-호환 서버 인증서, 역할 인증서, 그리고 인증기관 인증서 등에 대한 프로파일을 정의
	WAP 공개키 기반구조	서버와 클라이언트 신뢰관계를 가능케 하기 위하여 요구되는 구조와 절차를 정의하고 구체적으로 구현을 위한 WAP PKI 모델을 정의와 루트 CA 키 설치 과정과 클라이언트 등록 과정등의 PKI 동작을 규정

8. 기타 표준 동향

msec 작업반은 2001년도에 구성되어, 인터넷에서의 그룹 통신 보호를 위한 IRTF의 보안 멀티캐스트 RG의 작업에 기반한 프로토콜에 대한 표준화 작업을 수행하고 있다. 프로토콜의 주된 구성요소는 데이터 보호 변환 (당사자 인증과 기밀성),

그룹 키 및 SA 관리, 그룹 정책 관리 등이며, IRTF의 SMRG와 RMRG, IETF의 IPsec, IPSP, Policy, RMT 작업반과 긴밀하게 협조하고 있다.

sacred 작업반은 2000년도에 구성되어 신뢰성 확보와 관련된 개인 정보 (공개키/개인키 쌍, 인증서, 인증서 체인, 신뢰 정보, 루트 인증 기관 정보 등등)의 안전한 export/import를 위한 메커니즘 개발을 목표로 작업을 수행 중이며, 정보의 이동은 credential 서버로부터의 전송 방법과 peer 장비 간의 전송 방법으로 분류된다.

sasl 예비 모임은 SASL(Simple Authentication and Security Layer) 문서인 RFC 2222를 드래프트 표준으로 승격시키기 위한 작업반의 구성을 토의하기 위한 것으로, 이 프로토콜은 인증과 기밀성을 BEEP, IMAP, LDAP, POP, SMTP 등의 상위 어플리케이션 프로토콜에 손쉽게 제공하기 위한 것이다. 작업 방향은 RFC 2222에 대한 개정, SASL 메커니즘 문서들의 개정 등이며, 특히 SASL 메커니즘의 개정은 현재 RFC 2195, 2222, 2831 등에 지정되어 있는 CRAM-MD5, DIGEST-MD5, EXTERNAL 등에 기초하고 있다.

inch 작업반은 컴퓨터 침해 대응에 관한 작업반으로써, 침해 대응 조직 간의 침해 데이터의 교환과 침해 통계 정보를 원활하게 교환하기 위하여 컴퓨터 보안 사고를 다른 조직 간에 교환되어야 할 데이터 형태에 대한 교환 수준의 요구사항, 이 요구사항을 만족하는 데이터 포맷을 기술하는 침해 데이터 언어, 그리고 침해 데이터 언어로 표현된 침해 보고와 연관 표현에 대한 샘플 집합을 규정하는 것을 목표로 하고 있다.

Ⅲ. 국내 표준화 기술 동향

VPN의 경우에는 IETF IPsec 프로토콜을 기준으로 한 VPN 보안 기술 표준안이 인터넷 보안기술 포럼에 의해 작성되어, TTA에 확정되었다. 이 표준은 IP 계층에서의 VPN 터널링 방식인 IPsec 구현 기술과 관련 보안 프로토콜 및 키관리 프로토콜을 정의하고 있는데, IETF RFC 2401, 2402, 2406, 2407, 2408 및 2409를 기반으로 한 기능 규격서 형태의 표준안이다. 이 표준은 키관리 기술들과 보안 연계 및 데이터베이스에 관한 정의, AH와 ESP를 통한 무결성, 인증, 비밀성 기능, 키 보호와 보안 연계를 위한 키관리 메커니즘의 확장성 등의 내용을 담고 있다. 또한 가상사설망 시스템 로그형식 표준(ISTF-019)이 ISTF에서 표준화되고 있다.

국내에서의 전자우편 보안을 위한 표준안 개발 작업은 인터넷 보안 기술 포럼의 네트워크 분과에서 33개 업체 및 기관이 참여하여 IETF S/MIME 버전 3을 기초로 수행되었다. 금년도 내에 추진될 전자메일 관련 국내 표준은 Diffie-Hellman 키동의 방식, CMS에서 CAST-128 암호화 알고리즘의 사용(안), S/MIME V3 인증서 운영 규격, 안전한 전자우편을 위한 보안 서비스 확장, 그리고 암호 메시지 규격 등에 관한 표준이다.

국내 PKI 표준안 개발은 인터넷 보안 기술 포럼의 PKI 분과위원회에서 주로 수행하고 있다. PKI 분과 위원회는 국내 PKI 보안 솔루션 업체,

표 7 : 국내 인터넷 보안 기술 포럼 표준 문서

분야	문서번호	표준 내용	개정현황	발표월일
PKI	ISTF-001	전자서명 인증서 프로파일 표준	초안	2000
	ISTF-002	전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	초안	2000
	ISTF-018	공인인증기관간 상호연동을 위한 PKI 표준	초안	2002
IPSec	ISTF-003	IP 계층에서의 VPN 보안기술 표준	초안	2001
	ISTF-019	가상사설망시스템 로그형식 표준	초안	2003
보안관리	ISTF-004/R	침입차단시스템 로그형식 표준	개정	2003
	ISTF-005/R	침입탐지시스템 로그형식 표준	개정	2003
	ISTF-020	보안시스템의 통합관리를 위한 API 표준	초안	2003
전자메일	ISTF-006	암호 메시지 규격 표준	초안	2002
	ISTF-007	Diffie-Hellman 키합의 방식 표준	초안	2002
	ISTF-008	S/MIME V3 인증서 운영 규격 표준	초안	2002
	ISTF-009	S/MIME 메시지 명세서 표준	초안	2002
	ISTF-010	안전한 전자우편을 위한 보안서비스 확장 표준	초안	2002
	ISTF-011	CMS에서 CAST-128 암호화 알고리즘의 사용 표준	초안	2002
무선인터넷보안	ISTF-012	무선 전자서명 인증서 프로파일 표준	초안	2002
	ISTF-013	무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	초안	2002
	ISTF-014	무선 WTLS 인증서 프로파일 표준	초안	2002
	ISTF-015	무선 전자서명 알고리즘 표준	초안	2002
	ISTF-016	무선 키분배 알고리즘 표준	초안	2002
	ISTF-017/R	무선 인증서 요청형식 프로토콜 표준	개정	2003
	ISTF-021	무선 인증서 관리 프로토콜 표준	초안	2003
	ISTF-022	무선 응용계층 보안 프로토콜 표준	초안	2003

한국정보보호진흥원, 한국전자통신연구원, 공인인증기관 등으로 구성된 민간을 중심으로 하는 표준화 기구로서 국내 PKI 관련 기술의 표준화 작업을 주도하고 있다. PKI 분과위원회의 주요 역할은 PKI 관련 국제 선진 기술 및 표준화 기술 동향 파악과 함께 국내 환경에 적합한 PKI 관련 보안 기술을 표준화 추진함으로 국내 PKI 관련 기술의 상호 연동성 확보 및 점차 국내 표준화 기술을 국제적인 표준화 기구에 적극적인 기고를 통한 국제 표준화 유도를 주요 목적으로 하고 있다. 2000년 8월 2개의 표준(안)을 TTA에 상정하여 국내 단체 표준 2건이 제정되었다.

현재 무선인터넷 보안과 관련하여 6개의 국내 표준이 개발되어 있으며, 이들은 무선 전자서명 인증서 프로파일 표준, 무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준, 무선 인증서 요청 형식, 무선 WTLS 인증서 프로파일, 무선 키 분배 알고리즘 표준, 무선 전자서명 알고리즘 표준이다. 또한 현재 진행 중인 표준은 ISTF에서 표준안이 마련된 무선 인증서 관리 프로토콜 표준(ISTF-021), 무선 응용계층 보안 프로토콜 표준표준(ISTF-022) 등이다.

국내 커버로스, LDAP 관련 표준안은 현재 없는 상태이다. 또한 PKCS 표준도 국내 표준안이 거의 없지만, IETF 정보 RFC를 참조로 하여 개발된 무선 인증서 요청 형식에 대한 표준화가 현재 진행 중인 암호학적 메시지 구문 등의 표준에 간접적으로 반영되고 있다. 표 7은 국내 인터넷 보안 기술 포럼 표준 문서이다[1, 7].

Ⅳ. 국내·외 비교 분석

1. 국내·외 정보보호 시장

국내 정보보호시장은 2003년 현재 5,700억원 규모에 이른 것으로 파악되며, 2007년에는 1조 1천억원 규모에 이를 것으로 전망되며, 안티바이러스, 침입차단시스템 등 기본적 정보보호 솔루션에서 침입예방시스템(IPS), 침입탐지/차단 및 앤티바이러스/폭주트래픽검출 등의 통합형 네트워크 보안제품, PKI, 전자거래 보호솔루션 등으로 시장이 형성되고 있다.

국외 정보보호 시장은 2002년 200억 달러를 넘어선 것으로 파악되며, 연평균증가율 20.8%로 계속 증가될 것으로 전망되며, 고성능, 통합형 제품인 하드웨어 부문이 각광 받을 것으로 전망되어지고, 소프트웨어 부문에서는 바이러스 백신이 기본적 정보보호 솔루션으로서 안정적 성장을 지속할 전망이며 IDS와 content-filtering 소프트웨어의 이용이 확대될 전망이다.

2. 국내·외 기술개발 현황

국내 기술개발은 ETRI(한국전자통신연구원)와 KISA(한국정보보호진흥원)등에서 암호 및 PKI 핵심기술이 개발되고 있으며, 보안업체를 중심으로 침입차단시스템, 침입탐지시스템, 바이러스 백신, 전자우편 보안, 인증서 발행을 비롯한 PKI 서비스, VPN등이 개발 및 상용화되고 있다.

국외 기술개발은 미국과 유럽을 중심으로 침입차단시스템, 침입탐지시스템, 바이러스 백신, 전자우편 보안, 인증서를 기반으로 하는 PKI 제품 및 PKI 서비스, VPN, 암호 라이브러리 등이 개발 및 상용화되고 있고, 암호 알고리즘은 주로 표준인 RSA가 많이 사용되고 있으며, 현재 AES가 각종 표준 프로토콜에 적용되고 있다[9, 10].

Ⅴ. 표준화 추진전략

암호기술은 유럽 NISSIE, 일본 CRYPTOREC 표준 동향을 주시하고 이를 활용하여 중·장기적인 암호 알고리즘 개발이 필요하며, KIISC를 중심으로 개발을 하고 KISA가 이를 관리하는 체계가 좋을 것으로 생각된다.

PKI 관련 표준안은 전자서명 인증서 프로파일, 인증서 효력 정지 및 폐지목록 프로파일, 그리고 공인 인증기관간의 상호 연동 규격 등의 세 가지이다. 단기적인 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(Subscriber Identification Method) 표준, 커버로스 관련 프로토콜, 그리고 PKCS 표준 중 일부 프로토콜에 대하여 표준화가 필요하다. PKCS는 ITEF의 표준안을 활용하여 일부 프로토콜을 표준화하고, 커버로스는 국내 시장이 형성되지 않은면 굳이 표준화가 필요 없으므로 국내 시장 동향을 주시해야 한다. LDAP은 IETF PKIX 작업반의 표준안을 활용하고 국내 시장의 규모에 주목해야하며, SIM에 대한 표준은 현재 KISA에서 PKIX 작업반의 표준화 항목으로 채택되어 있다. 이 분야는 ISTF 공개키 기반구조 분과를 중심으로 초안을 작성하고 TTA의 TC10 표준 작업반을 통하여 이를 검토해야 한다.

전송계층은 국제 표준을 적극적인 수용을 통한 국내 표준을 제정하고 국내 시장의 요구를 반영하여 표준화 범위와 시기를 조정하고 ISTF 네트워

크 분과를 중심으로 초안을 작성하고 TTA의 TC10 표준 작업반을 통하여 검토해야 한다.

IPSec/VPN은 IETF IPSEC WG의 국제 표준을 활용하여 ISTF 네트워크 분과를 중심으로 초안을 작성하고 TTA의 TC10 표준 작업반이 이를 검토해야 한다.

전자우편은 공개키 기반구조와 상호운용을 보장하는 표준을 마련하고 IETF의 S/MIME v3을 국내 표준에 반영하여 TSTF 네트워크 분과를 중심으로 초안 작성과 TTA의 TC10 표준 작업반이 이를 검토해야 한다.

침입탐지 및 예방시스템은 국외 표준화 동향을 주시하여 이를 수용하고 Draft 문서를 근거로 우리만의 독자적인 표준마련이 필요하다. 이를 TSTF 네트워크 분과를 중심으로 초안을 작성하고 TTA의 TC10 표준 작업반이 이를 검토해야 한다.

무선 인터넷 보안은 국제 표준화 단체인 IETF TLS 작업반과 OMA 표준을 참조하여 무선 전송계층 프로토콜, 무선 공개키 기반구조, 무선 WIM, 무선 API, 응용 서비스를 위한 표준, WIM 토큰 관련 인터페이스 표준과 WIM 토큰 내의 정보 구문에 대한 표준이 필요하다. 이를 TSFT 무선 분과를 중심으로 초안을 작성하고 TTA의 TC10 표준 작업반이 이를 검토해야 한다.

그림 1과 부록 표 8은 국·내외 표준화 기술 동향과 정보보호 시장, 기술개발 현황 분석 결과를 바탕으로 국내 정보보호 표준화 추진 체계와 향후 정보보호 분야의 표준화 3개년 로드맵의 제안이다.

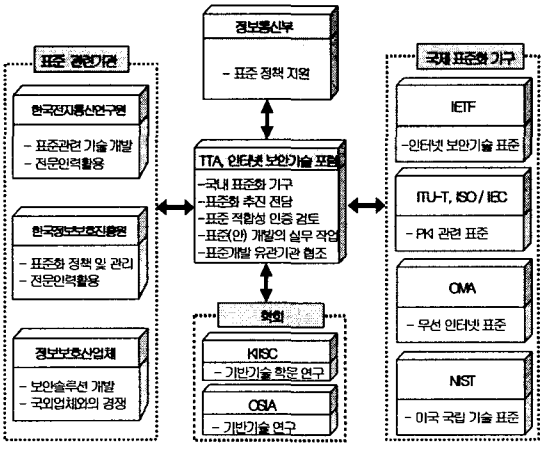

그림 1 : 표준화 추진체계

Ⅵ. 결론

본 논문에서 급속도로 발전하는 정보보호 분야에 있어서 핵심 표준화대상이 되는 제품에 대한 국내·외 시장현황, 기술현황, 표준화현황에 대해 비교 분석하였으며 이를 토대로 국내 정보보호 표준화 체계와 향후 3년간에 표준화 로드맵을 제안하였다. 이런 분석은 각 제품의 특징들을 쉽게 파악 할 수 있고 각 분야에 필요한 표준화를 알아보는데 활용 가능할 것이다.

우리도 국제 표준화 단체들의 표준들을 많이 활용하여서 국내 정보보호 시장에 적합한 표준을 만들고 이를 바탕으로 안전한 정보화 사회 인프라를 구축해야겠다.

참고문헌

[1] KISA, http://www.kisa.or.kr/, 정보보호 표준화 목록, 2003.

[2] IETF, http://www.ietf.org/, IETF, PKIX, IPSec, S/MIME, MSEC 등의 작업반 홈페이지, 2003.

[3] OMA, http://www.wapforum.org/, OMA 홈페이지, 2003.

[4] ITU, http://www.itu.int/home/index.html, ITU 홈페이지, 2003.

[5] NIST, http://www.nist.gov/, NIST 홈페이지, 2003.

[6] ISO/IEC JTC1, http://www.jtc1.org/, ISO 홈페이지, 2003.

[7] TTA, http://www.tta.or.kr, TTA홈페이지, 2003.

[8] MIC, http://www.mic.go.kr/index.jsp, MIC 홈페이지, 2003.

[9] MIC, 정통부 정보보호 중장기 기술개발계획서, 초안, 2003.

[10] MIC, 정통부 정보보호 중장기 기술개발계획서, 2002.

[11] 이계상, 류재철, 이광수, 이재광, 염홍열, 정수환, 채기준, IETF 정보보호 표준화 동향 분석에 관한 연구, 한국정보보호진흥원, 2002.12.

[12] 염홍열, "정보보호 기술 표준화", 한국정보통신기술협회, 중점 기술표준화 로드맵 검토워크숍, 2003.9.

[13] 이광수, "정보보호일반 기술표준기획보고서", 한국정보통신기술협회, 2002.

[14] 이광수, "인터넷 전자우편 보안 기술의 표준화", TTA 간행물 IT Standard Weekly, 2003-44호.

<부 록>

표 8 : 표준화 3개년 로드맵

표준화대상 기술분야		선도 수용	중요 표준화 대상 항목	국내 표준 개발 시기				국제 표준 성숙 시기 예측	상용화 시기 (기술 개발 완료)	관련표준기구	
기술 분야	세부 기술 항목			04	05	06	기술 격차			국외	국내
정보 보호 일반	암호 기술	수용/ 선도	- 대칭형 암호 알고리즘(중비도) 공개키 암호 알고리즘(중비도) 해쉬 알고리즘(중비도) 서명 알고리즘(중비도) 난수 생성기 타원곡선 암호 알고리즘			▶ ▷ ▶ ▷ ▶ ▶	3년	10	10년 이후	NISTE TSI,Cry ptoRec,I ETF	ISTF, TTA
	PKI, PKCS, LDAP, 커버로스 보안	수용/ 선도	- 인증서 확장자 표준 속성/인가/자격 인증서 표준 권한관리구조 표준 개인키 소유증명 인증서 관리, 운영 프로토콜 - 시점 확인 프로토콜, 데이터인증 및 검증 프로토콜 온라인 인증서 상태 프로토콜 대리 인증 경로 발견/검증 글로벌 상호연동 프레임워크 인증서 정책/인증업무준칙 SIM 표준 LDAP 인증서 속성 표준 PKCS 표준중 토큰 인터페이스 등 커버로스 표준: 국내 산업고려	▶ ▶	▶ ▶ ▶ ▶ ▶ ▶ ▶ ▶	▶ ▷ ▶ ▶ ▶ ▶ ▶	2-3 년	05	06	IETF	ISTF, TTA
	IPsec /VPN	수용	- AH, ESP, IKE 인증/암호 알고리즘 후속 IKE IKE를 위한 암호 알고리즘 NAT 경유 프로토콜 원격 사용자 인증 IPSEC 정책 IPSec MIB	▶ ▶	▶	▶ ▶ ▶ ▶ ▶	2년	05	06	IETF	ISTF, TTA
	전송 계층 보안	수용/ 선도	- TLS 프로토콜 수용 및 개정 TLS 인증(커버로스, SRP) HTTP를 위한 TLS ECC 사이퍼스위트 TLS 압축 국내 암호 알고리즘 TLS 스위트		▶ ▶ ▶	▶ ▶ ▶	2년	03	04	IETF	ISTF, TTA
	전자 우편 보안	수용/ 선도	- 암호 메시지 구문 인증서 처리 S/MIME 메시지 명세 패스워드 기반 암호 - 암호알고리즘(CAST, AES, IDEA) ECC 암호 기법 사용 CMS 대칭키 관리 및 분배 SEED 암호화 알고리즘 채택	▶ ▶	▶	▶ ▶ ▶ ▶ ▶	2년	04	05	IETF	ISTF, TTA
	침입 탐지 및 예방 시스템	수용	- 메시지 교환 요구사항 데이터 모델 및 데이터 포맷 구현 언어 통신 프로토콜		▶ ▶ ▶		2년	05	06	IETF	ISTF, TTA
	무선 인터넷 보안	선도/ 수용	- 무선 공개키기반구조 무선 전송 보안 프로토콜 무선 WIM 보안 API 무선 응용 프로토콜 무선 PKI 상호 연동	▶ ▶	▶ ▶	▶ ▶	2년	06	07	IETF, OMA	ISTF, TTA