특집

정보보호기술 표준화

장청룡(경동대학교)

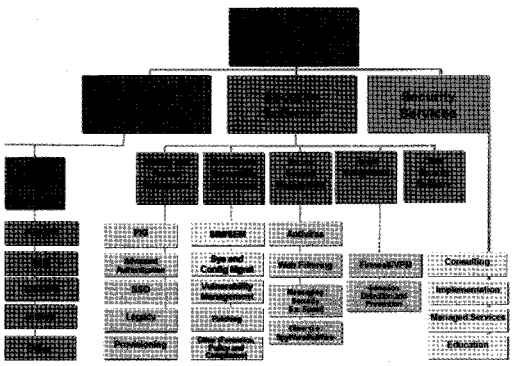
I. 서 론

정보보호 산업은 자국의 기업 정보보호, 지적재산권 보호 그리고 국가 안보를 위해 이미 선진 각국에서 오래전부터 기술 개발 및 표준화 활동을 통하여 시장을 선점해왔다. 특히 이 분야의 거대 사용자인 정부와 정보기관들은 그 내용과 경험을 타 국가에 이전 또는 전수를 기피할 뿐만 아니라 고가의 비용을 지불해야만 확보할 수 있는 기술로 분류되고 있으며 일부 기술은 수출입의 통제도 받고 있는 실정이다.

그러나, 잠재적인 수요와 시장성은 큰 반면 보안이라는 특수성 때문에 시장이 활성화되지 못하고 있기도 하다. 또한 정부의 적극적인 지원이 필요한 국가적으로 매우 중요한 산업분야임에는 틀림이 없다.

더욱이, 정보보호 기술은 지식정보화사회의 인프라를 이루는 컴퓨터와 정보통신을 기반으로 하는 유비쿼터스 컴퓨팅과 통신 환경을 지향함에 있어 서비스의 원활함과 사용자의 프라이버시 보호에 따른 핵심 동력산업으로 선진 각국에서 기술개발 및 표준화경쟁을 통해 시장 선점을 위한 노력을 기울이고 있는 분야로 이에 대한 전략적인 표준화 개발 계획의 수립이 요구되고 있다.

정보보호 분야는 여러 기준에 따라 다양하게 분류되고 있으나 미국의 시장 조사기관인 IDC에 의하면 IT 보안 시장은 <그림 1>과 같이 분류하고 있다. IDC 보고서에 의하면 2006년 세계 보안 시장 규모는 357억 달러를 기록했으며 오는 2011년에는 718억 달러를 넘어설 것으로 전망된다. 또한 2007~2011년 동안 연평균 성장률(CAGR) 15%를 기록하며 보안 시장이 높은 성장세를 보일 것으로 예상되는 가운데, IDC는 보안 시장을 각 부문별로 다음과 같이 전망한다[1,2].



〈그림 1〉 IT 보안 시장의 구조

보안 서비스 시장은 2006년 170억 달러 규모로 2006에서 2011년까지 연평균 17.4% 성장세를 보이며, 2011년 379억 달러 규모가 전망된다. 이 중 매출 가능성이 가장 높은 분야는 구축 서비스 및 관리 서비스 시장인 것으로 보인다.

보안 소프트웨어 시장 중 컨텐츠 보안(SCM: Secure Content Management) 기술은 네트워크 보안의 전 계층에서 위협관리(TM: Threat Management) 기술과 통합되고 있는 SCTM (Secure Content and Threat Management) 시장은 2006년 132억 달러 규모를 형성하고 연평균성장률 11.8%로 성장하여 2011년에는 231억 달러에 달할 것으로 전망된다. 또한, 사용자 인증 및 접근 관리(IAM: Identity and Access Management) 시장은 2006년 30억 달러 규모이며 2011년까지 10.7% 연평균성장률이 예상된다. 그 다음으로는 보안 및 취약점 관리(SVM: Security and Vulnerability Management) 매출액은 2006년 19억 달러로 2005년 16억 달러에 비해 다소 성장했다. 2011년까지 연평균성장률 18.4%를 기록, 44억 달러에 이를 것으로 전망한다.

이와 같은 IT 보안 시장을 형성하는 보안 제품 및 서비스에 사용되거나 포함되는 내용을 기술 및 표준화이라는 관점에서 이를 분류해 보면 크게 기술적인 보안과 관리적인 보안으로 나누어 질 수 있다. 기술적 보안 분야를 좀더 세분화 해 보면 암호 기술, 네트워크보안 기술, 개인정보보호 기술, 사진 또는 동영상의 저작권을 보호하기 위한 멀티미디어 보안 기술, 사이버 범죄 수사에 필요한 디지털 포렌직 기술 등이 있다. 한편 관리적 보안에서는 사람이라는 요소를 보안의 관점에서 다루기 위한 기업의 효과적인 보안 관리를 위한 정보보호 관리체계 및 관련 인증 제도와 보안 제품들의 신뢰를 확보하기 위한 제품 평가 및 인증제도로 분류해 볼 수 있다.

이에 대한 표준화 전문가 그룹으로 국제적인 수준에서는 ISO/IEC JTC1/SC27(IT Security Techniques), ITU-T SG17(Security, languages and telecommunication software), IETF Security Area, IEEE P1363 (Standard Specification for Public-Key Cryptography) 등이 활동하고 있으며 국가적인 수준에서는 한국의 기술표준원, 미국 ANSI, 영국 BSI 등에서 전문가 그룹이 활동하고 있다[3,4,5].

본 고에서는 차세대 암호 기술을 기반으로 하는 암호 기법, 정보보안관리 및 통제/서비스, 시스템 및 제품 평가, ID 관리, 바이오 보안에 관련된 기술에 대하여 국제표준화 활동을 수행하는 ISO/IEC JTC1/SC27을 중심으로 산하의 5개 작업반에서의 표준화 활동 현황과 향후 계획에 대하여 소개한다. 여기에 소개되는 내용은 SC27의 업무 계획과 그 산하의 작업반에서 작성한 작업수행 계획(road map, standing documents)에 기초하여 정리한 것으로 37차 Limassol 회의(2008. 10)의 결과를 기준으로 한다[6~12].

II. ISO/IEC JTC 1/SC27의 보안 분야 표준화

ISO/IEC JTC 1/SC27은 정부 기관들뿐만 아니라 많은 사업 영역들의 보안 수요에 부응하는 정보보호 전문식견을 갖고 있는 국제적으로 공인된 단체이다. 이의 활동은 기술 표준은 물론 관리 표준 둘 모두를 관장 한다. SC27이 개발한 표준들은 많은 보안 제품의 설계와 개발에 사용되어 왔다. 이들 제품 중 몇 가지만 열거하자면 암호화

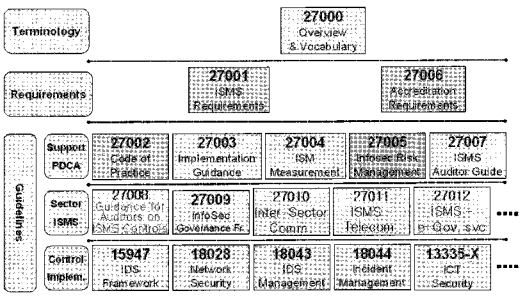
및 디지털 서명 기술, 통신 프로토콜 기술, 스마트카드, 접근제어 장치, 웹 브라우저 기술 등이다. 이 표준들 중 몇몇은 운영체제, 스마트카드, 암호 기술 그리고 접근제어 소프트웨어와 같은 제품들의 보안성을 평가하기 위해 사용되기도 한다.

SC27은 기존의 3개 작업 분야에 Security control/service 그리고 Privacy/Identity/Biometric Security를 보완하여 총 5개 분야로 확대 개편하여 2007년 5월 (19차 SC27 전체회의)부터 추진하고 있다[3,4].

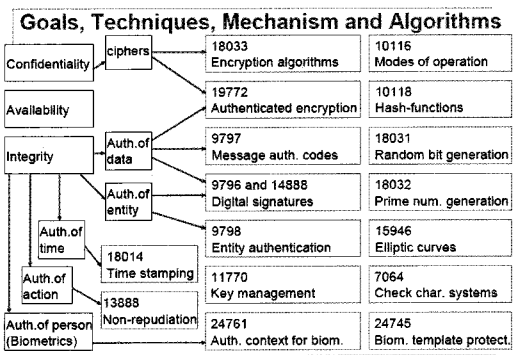
1. ISO/IEC JTC 1/SC27/WG1

WG1은 정보보안관리시스템(ISMS, Information Security Management System)에 관한 표준개발을 목표로 활동 범위는 <그림 2>와 같으며 표준화 과제의 현황과 향후 과제는 <표 1>에 보여 지고 세부 활동은 다음과 같다[7].

- ISMS 표준과 지침 개발.
  - ISO/IEC 27000 ISMS 표준 시리즈의 개발과 유지관리
  - 향후 ISMS 표준과 지침을 위한 요구사항들의 규명
- ISO/IEC 27001에서 정의된 통제와 통제 목표들의 구현을 취급하는 표준에 대하여 SC27 내의 여타 작업반(특히, WG4)들과의 협력.
- ISMS에 대한 산업 분야별 특정 요구사항과 지침을 다루는 외부 전문가 그룹과의 협력.
  - ISO/TC 215 보건
  - ISO/TC 68 은행업무
  - ISO/TC 204 지능형수송시스템
  - ISO/TC 223 민간 방호
  - ISO TMB(Technical Management Board) JTCG(Joint Technical Coordination Group) on Management Systems
  - ITU-T 전기통신
  - ISSEA(International Systems Security Engineering Association)
  - 항공우주
  - 산업 자동화
  - WLA(World Lottery Association)



〈그림 2〉 SC27/WG1 자체 표준 및 관련 표준



〈그림 3〉 SC27/WG2 표준화 체계

〈표 1〉 SC27/WG1 과제 추진현황 및 향후계획

SC27/WG 1 관련 표준명	표준번호	표준화 상태	표준화 일정	적용 단계
WG 1 27000 시리즈 표준				
Information security management system - Overview and vocabulary	27000	FDIS	2009년 완료예정	Planning
Information security management system - Requirements	27001	-	1st ed.(2005), 개정 (27001과 27002의 상호 연계성 유지)	Policy
Code of practice for information security management	27002	-	상동	Implement & Operate
Information security management system implementation guidance	27003	FCD	2009년 완료예정	Implement & Operate
Information security management measurements	27004	2nd FCD	2009년 완료예정	Assessment
Information security risk management	27005	-	1st ed.(2008)	Planning
Requirements for bodies providing audit and certification of information security management systems	27006	-	1st ed.(2007)	all
Guidelines for ISMS auditing	27007	2nd CD	2010년 완료예정	all
MICTS - Part1 - Concepts and models	13335-1	발간	-	Policy
ISM guidelines for e-government services	27012	NP	-	Implement & Operate
Information security management for inter-sector communications	27010	NP	-	Implement & Operate
Guidance for Auditors on ISMS Controls	27008	NP	-	all
Information security governance framework	NP	-	NWI(한국제안)	all
ISMS for Service Sector: Integrated Implementation of ISO 20000-1 and ISO27001	NP	-	NWI(영국제안)	all
ISM guidelines for financial services and insurance industries	NP	-	NWI(미국제안)	all
특정 산업별 ISMS 표준				
Information security management guidelines for telecommunications	27011	-	1st ed.(2008)	Implement & Operate
Sector-Specific ISMS Standards for the World Lottery Association		Study Period 종료	-	Implement & Operate
Information security for Critical Infrastructure - Sector-specific guidance		Study Period 종료	-	Implement & Operate

〈표 1〉의 계속

SC27/WG 1 관련 표준명	표준번호	표준화 상태	표준화 일정	적용 단계
기타 산업별 표준				
Banking and related financial services - Information security guidelines	13569	-	1st ed.(2005), 개정 (TC68/SC2)	Implement & Operate
Health informatics — Security management in health using ISO/IEC 27002	27799	-	1st ed.(2008)	Implement & Operate

2. ISO/IEC JTC 1/SC27/WG2

SC27/WG2는 암호기법 및 보안 메커니즘에 관한 표준개발을 목표로 활동 범위는 <그림 3>과 같으며 개발 표준화 과제의 현황과 향후 과제는 <표 2>에 보여 지고 세부 활동은 다음과 같다[8,11].

- IT 시스템과 응용에 보안 기법 및 메커니즘을 적용하기 위한 수요와 요구사항들의 규명
- 보안 서비스에 사용할 보안 기법 및 메커니즘을 위한 용어, 일반 모델 그리고 표준의 개발
- 다음의 기법들을 포함하는 암호 및 비-암호 기법 및 메커니즘의 개발하는 17개의 표준화 과제를 운영하고 있다:
  - 비밀성(confidentiality)
  - 실체 인증(entity authentication)
  - 부인 봉쇄(non-repudiation)
  - 키 관리(key management)
  - 데이터 무결성(data integrity)
    - 메시지 인증(message authentication)
    - 해쉬 함수 (hash-functions)
    - 디지털 서명(digital signatures)

이들 메커니즘들은 일반적으로 대칭 암호, 비대칭 암호 그리고 비-암호 기법들을 포함하여 이용되는 기법들에 대한 선택사항들을 갖고 있다.

〈표 2〉 SC27/WG2 과제 추진현황 및 향후계획

SC27/WG 2 관련 표준명	표준번호	표준화 상태	표준화 일정	비고
암호화(Encryption)				
Encryption algorithms - General	18033-1		[1st ed. (2005)]	Amendment 준비
Encryption algorithms - Asymmetric ciphers	18033-2		[1st ed. (2006)]	
Encryption algorithms - Block ciphers	18033-3	1st WD	[1st ed. (2005), COR1(2006), COR2(2007), COR3(2008)], 한국 SEED 수용	2차 개정에서 한국 HIGHT 수용 준비
Encryption algorithms - Stream ciphers	18033-4	2nd PDAM	[1st ed. (2005), to be amended]	
Modes of operation for an n-bit block cipher algorithm	10116		[3rd ed.(2006), COR1 (2008)]	SC27 N6578

〈표 2〉의 계속

SC27/WG 2 관련 표준명	표준번호	표준화 상태	표준화 일정	비고
Authenticated encryption	19772	FDIS	-	
디지털 서명(Digital signature)				
Digital signature schemes giving message recovery - General	9796-1		[철회]	
Digital signature schemes giving message recovery - Integer factorization based mechanisms	9796-2	study	[개정]	
Digital signature schemes giving message recovery - Discrete logarithm based mechanisms	9796-3		[2nd ed. (2006)] 한국 ECKNR 수용	
Digital signatures with appendix - General	14888-1		[2nd ed. (2008)]	
Digital signatures with appendix - Integer factorization based mechanisms	14888-2		[2nd ed. (2008)]	
Digital signatures with appendix - Discrete logarithm based mechanisms	14888-3	PDAM	[2nd ed. (2006)] 한국 KCDSA, EC-KCDSA, IBS-2 수용	Commonwealth of Independent States(CIS)의 표준인 EC-RDSA(340.10-2004)를 수용하는 Amendment 1을 진행 중임
실체 인증(Entity authentication) 표준			-	
Entity authentication - General model	9798-1	1st CD	[2nd ed. (1997), 개정]	
Entity authentication - Mechanisms using symmetric encipherment algorithms	9798-2	FDIS	[2nd ed. (1999), 개정][COR1(2004)]	parsing ambiguity 공격에 대한 DCOR1 준비
Entity authentication - Mechanisms using digital signature techniques	9798-3	PDAM	[2nd ed. (1998), 개정] amendment: published in 2009	상동
Entity authentication - Mechanisms using a cryptographic check function	9798-4		[1st ed.(1999), Confirmed(2006)]	상동
Entity authentication - Mechanisms using zero knowledge techniques	9798-5	FCD	[2nd ed. (2004), 개정]	
Entity authentication - Mechanisms using manual data transfer	9798-6	1st WD	[1st ed. (2005), 개정]	parsing ambiguity 공격에 대한 DCOR1 준비
메시지인증코드((MACs, Message authentication codes)				
Message authentication codes - Mechanisms using a block cipher	9797-1	FCD	[3rd ed. (1999), 개정]	
Message authentication codes - Mechanisms using a dedicated hash-function	9797-2	FCD	[2nd ed. (2002) 개정]	
Message authentication codes - Mechanisms using a universal hash-function	9797-3	3rd WD		
해쉬함수(Hash-functions)				
Hash-functions - General	10118-1		[2nd ed. (2000)]	
Hash-functions - Hash-functions using an n-bit block cipher algorithm	10118-2	2nd CD	[2nd ed. (2000) 개정]	

〈표 2〉의 계속

SC27/WG 2 관련 표준명	표준번호	표준화 상태	표준화 일정	비고
Hash-functions - Dedicated hash-functions	10118-3		[3rd ed. (2004), AMD1(2006)]	
Hash-functions - Hash-functions using modular arithmetic	10118-4		[1st ed. (1998)]	
Check character systems	7064		[2nd ed. (2003)]	
부인봉쇄(Non-repudiation)				
Non-repudiation - General	13888-1	FDIS	[2nd ed. (2004) 개정]	
Non-repudiation - Mechanisms using symmetric techniques	13888-2	1st CD	[1st ed. (1998), 개정]	
Non-repudiation - Mechanisms using asymmetric techniques	13888-3	FCD	[1st ed. (1998), 개정]	
키관리(Key management)				
Key management - Framework	11770-1	1st CD	[1st ed. (1996, Confirmed(2005), 개정]	
Key management -Mechanisms using symmetric techniques	11770-2		[2nd ed. (2008)]	parsing ambiguity 공격에 대한 DCOR1 준비
Key management - Mechanisms using asymmetric techniques	11770-3		[2nd ed. (2008)]	상동
Key management - Key establishment mechanisms based on weak secrets	11770-4		[1st ed. (2006)] 한국 AMP 수용	상동
시점확인(Time stamping services and protocols)				
Time stamping services - Framework	18014-1		[2nd ed. (2008)]	
Time stamping services - Mechanisms producing independent tokes	18014-2	FCD	[1st ed. (2002), 개정]	
Time stamping services - Mechanisms producing linked tokens	18014-3	FCD	[1st ed. (2004), 개정]	
수리 및 암호 기법(Mathematic and cryptographic techniques)				
Random bit generation	18031	DCOR 1	[1st ed. (2005), 개정]	
Prime number generation	18032		[1st ed. (2005)]	
Cryptographic techniques based on elliptic curves - General	15946-1	DCOR 1	[2nd ed.(2008)]	
Cryptographic techniques based on elliptic curves - Digital signatures	15946-2		[14888-3으로 병합, 철회]	
Cryptographic techniques based on elliptic curves - Key establishment	15946-3		[11770-3으로 병합, 철회]	
Cryptographic techniques based on elliptic curves - Digital signatures with message recovery	15946-4		[9796-3으로 병합, 철회]	
Cryptographic techniques based on elliptic curves - Elliptic curve generation	15946-5	FCD		

〈표 2〉의 계속

SC27/WG 2 관련 표준명	표준번호	표준화 상태	표준화 일정	비고
향후 예상 표준화				
Signcryption	29150	2nd WD		
Key management - Part5: Group key management - Key establishment mechanisms for multiple entities	11770-5	1st WD		
Lightweight cryptography	NP	NWI		
Mechanisms supporting anonymity		Study Period		
Secret sharing mechanisms		Study Period		
Proxy/Delegation			중장기 과제	
Long-term Security with Unconditional Schemes			중장기 과제	

3. ISO/IEC JTC 1/SC27/WG3

WG3은 보안평가기준(Security Evaluation Criteria)에 관한 표준개발을 목표로 활동 범위는 다음과 같다[6,12].

- IT 시스템, 구성장치 그리고 제품의 보안 평가와 인증을 위한 표준 개발을 하고 이를 위해 컴퓨터 네트워크, 분산 시스템 그리고 관련 응용 서비스를 고려한다.
  - 이러한 활동에는 다음의 3가지로 구분한다.
    - 평가 기준
    - 평가 기준의 적용을 위한 방법론
    - 평가, 인증, 인정 기법들에 대한 운영 절차

이러한 활동은 보안 기능성과 보증에 대한 표준에서 나타난 바와 같이 SC27 회원국들과 교섭 전문 기관들을 통해 표명된 것처럼 사회의 관련 산업 분야들의 수요를 반영한다. 이러한 노력이 중복되지 않도록 품질 관리와 시험을 위한 관련 ISO/IEC 표준들이 고려되어야 한다.

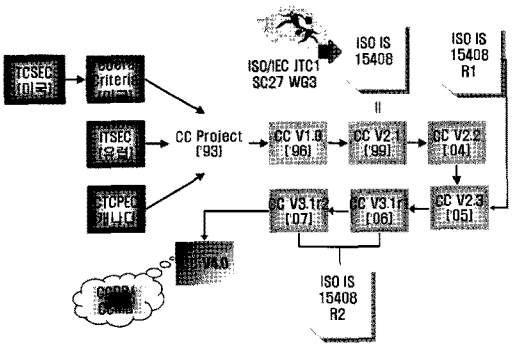
가. SC27/WG3 기존 표준화 과제 현황

1) IT 보안을 위한 평가 기준(ISO/ IEC 15408: 2005(2nd ed.), Evaluation Criteria for IT Security)

CC project의 Common Criteria version 3과 일치시키기 위하여 현재 2005년 발간 표준에 대한 개정 작업 중이며 평가기준 표준화 관련 공통 기준과 표준들의 관계는 <그림 4>에 보여 진다.

2) IT 보안 보증을 위한 프레임워크(ISO/IEC TR 15443, A framework for IT security assurance)

이 기술보고서의 1부와 2부(1st ed. 2005)는



〈그림 4〉 ISO/IEC 15408과 CC 표준화

발간되었으며 3부 - 보증 방법의 분석(Analysis of Assurance Methods) - 도 완료(1st ed. 2007) 하였다.

3) Security Targets and Protection Profiles의 준비를 위한 안내 (ISO/IEC 15446:2004, Guide for the preparation of Security Targets and Protection Profiles)

평가 준비 과정을 위한 훌륭한 지침서로 인정을 받고 있으며 ISO/IEC 15408의 개정으로 ISO/IEC 15446의 개정도 착수되었다. 이의 목적은 ISO/IEC 15408의 차기 버전(CC version 3.x)과 일치시키는 것이며 일부 효력을 잃은 지침들이 삭제될 것이다.

4) IT 보안 평가를 위한 방법론(ISO/IEC 18045 :2005(1st ed.), Methodology for IT Security Evaluation)

ISO/IEC 18045의 발간이후 CCDB에 의해 개발된 CC/CEM version 3과 일치시키기 위한 개정이 진행 중에 있다. 이 과정에서 많은 국가들은 국내 평가와 인증/검증 기법을 준비 중에 있으며 EN45011/ISO Guide 65에 규정된 인증기관에 대한 일반 요구사항 이외에 IT 보안 분야와 관련된 특별한 관심을 유발하는 또 다른 측면들을 고려하고 있다.

5) 암호 모듈(ISO/IEC 19790 and 24759, Cryptographic Modules)

ISO/IEC 15408 규격 언어와 절차들의 광범위한 사용 잠재성에 대한 조사를 통해 ISO/IEC 19790의 발간 이후 이 표준에 대한 조기 검토를 개시하기로 하였다. ISO/IEC 15408과 18045의 검토의 관점에서 ISO/IEC 19790(2006. 1st ed., Security requirements for cryptographic modules)표준의 검토가 약간 지연되었다. ISO/IEC 15408의 개정이 FDIS 수준에 이르자 ISO/IEC 19790을 검토하기로 했다. 현재 WG 3은 또한 방법론의 표준화 과제(ISO/IEC 24759:2008. 1st ed., Test requirements for cryptographic modules)를 개시하였다. 이 작업에서는 ISO/IEC 18045의 적용에 대한 경험은 물론 FIPS 140 검증 분야에 대한 미국/캐나다의 경험을 정리하여 추진할 것이다.

ISO/IEC 19790과 관련 평가 방법론들에 대한 작업 능력으로 보아 암호 모듈의 평가는 ISO/IEC 15408과 18045에 통합될 것이다.

6) 운용 시스템의 보안평가(ISO/IEC 19791: 2006, 1st ed., Security Assessment of Operational Systems)

이 TR은 최근에 발간되었으며 중요하고 복잡한 분야를 다룬다. 이것은 가까운 장래에 target type을 재고할 만큼 성숙단계에 이를 것이다. 따라서 WG 3은 target type을 IS로 변경시킬 것을 고려할 것이다. 관리(ISO/IEC 17799, 24743 등 과제)와 측정 분야(ISO/IEC 24742 과제)를 다루는 WG 1의 작업 결과와 일치시킬 필요가 있으며 또한 진행 중인 ISO/IEC 15408의 개정 결과에 대해 ISO/IEC 19791을 현행화 시킬 필요가 있을 것이다.

7) 생체인식 기술의 보안 평가 및 시험을 위한 프레임워크(ISO/IEC 19792, A Framework for security evaluation and testing of biometric technology)

이 과제는 현재 FCD 상태에 있다. 이 작업은 SC 37과 긴밀한 교섭관계를 맺고 추진하고 있으

며 SC 17, ITU-T SG17과 ISO TC 68과도 어느 정도의 협력하고 있다. 생체인식 평가 방법론(Biometrics Evaluation Methodology)에 대한 이슈는 CCDB내에서 개발될 것이라 시사된다. WG 3은 이 분야에 대한 작업 잠재성을 검토하였으나 어떤 의견도 개진되질 않아 이의 연구 기간을 종료하였다.

8) Systems Security Engineering – Capability Maturity Model (ISO/IEC 21827:2008, 2nd ed.)

이 과제는 ISSEA로부터 제출된 PAS에 기반을 두며 FDIS 단계에 있다.

9) 암호 모듈의 시험 요구사항(Test requirements for cryptographic modules)

이 과제는 FCD 단계에 있다. 이 표준화의 목적은 암호 모듈이 ISO/IEC 19790의 요구사항들에 적합한가를 시험하기 위해 인정된 시험소에 의해 사용될 방법들을 규정하는 것이다.

10) 암호 프로토콜의 검증(ISO/IEC 29128, Verification of cryptographic protocols)

프로토콜 검증 분야는 보안 관점에서 대단히 중요하며 보안에 관한 TMB 자문 보고서(SC 27 N4358)에서 보안 표준의 수요중 한 분야로 규명되었다. 보안상의 실수를 하기가 얼마나 쉬운가의 예들(DES-HMAC에 대한 splicing 공격, Needham-Schroeder 프로토콜 결함 등)이 무수히 많다. 암호 프로토콜에 대한 기본 설계 원칙들(Abadi-Needham과 관련연구 결과)을 먼저 살펴보아야 할 것이다. 안전성 증명에 대한 기법들을 포함하여 검증 방법들이 후속 연구로 포함될 것이다. 이 분야의 연구가 WG2에서 최근에 개시되었으나 이의 업무 추진을 WG3에서 하도록 조정되었다. 또한 SC6과 IETF와의 교섭도 적절할 것이다.

나. SC27/WG3 향후 표준화 분야

1) 평가를 위한 증거 생성에 대한 지침(Guidance on the production of evidence for evaluation)

현재 보안 평가에 관한 대부분의 지침적 자료들은 개발자들보다는 평가 받는 평가자들에 맞추어져 있다. 지네릭한 위협, 정책, 목표, 취약성 등을 규정하는 미리 정의된 패키지뿐만 아니라 증거의 생성을 위한 일반적인 지침에 대한 수요가 있다. 또한 ISO/IEC 15446과 18045의 표준을 보완하는 지침을 개발할 필요가 있다. 이를 위해 WG 3은 이 분야의 활동을 논의하면서 우선 CCDB와 협력관계를 유지하고 어떤 관련 자료가 존재하며 이들이 국제 표준 또는 TR의 개발에 얼마나 기여할 수 있는 가를 조사하고 있다.

2) 적격 인증 기법들에 대한 요구사항들의 조화(Harmonization of requirements for Qualified Certification Schemes)

ISO/IEC 18045에서 언급한 바와 같이 WG 3은 ISO/IEC 15408을 이용한 평가와 인증/검증 기법에 관한 요구사항 분야에 더욱 많이 참여하게 될 것이다. 이것은 ISO/IEC 15408의 적용과 관련하여 사전 평가 활동을 위한 지침과 규칙을 포함할 수 있다.

3) 안전한 시스템 설계(Secure System Design)

WG3 제품들을 이용한다는 것은 안전성 설계와 같은 안전성 엔지니어링 결과물들을 이용한다는 것이다. 이는 ISO/IEC 15408의 2부를 포함할 것 같으며 또한 ISO/IEC 19790, 19791,

19792, 21827의 관련 분야를 포함할 것이다. 이는 TR 형태의 작업 결과물을 도출할 것이다. 최근 Limassol 회의(2008. 10)에서 "Secure System Design"의 Study Period 의 종료 후 과제명을 "Secure System Engineering Principles and Techniques"변경하고 신규과제로 추진을 준비 중이다.

4) Tamper protection requirements and evaluation

보호의 anti-tampering 측면에 대한 분야로서 SC 27에서 이전부터 논의되어 왔다. 이의 논의 시점에서 WG 2의 표준화 분장의 이슈가 WG 2는 암호학적 및 비-암호학적 보안 메커니즘 둘 모두에 책임을 진다는 사실의 관점에서 논의되었다. 그러나 WG 2는 비-암호학적 보호 메커니즘들에 대한 분야의 충분한 전문식견이 부족함을 주목하였다. 한편, TC 68은 이 분야의 표준으로 IS 13491을 발간하였다.

SC 27의 차원에서, anti-tampering 이슈들은 ISO/IEC 19790 과제와 관련이 있다. 그럼에도 불구하고, anti-tampering 수단은 또한 IT 보안 영역(하드웨어 자원의 보호, 패스워드와 암호학적 키를 위한 전달 장치, 생체인식 센서 장치 등)의 관련 분야에 적용이 가능하다.

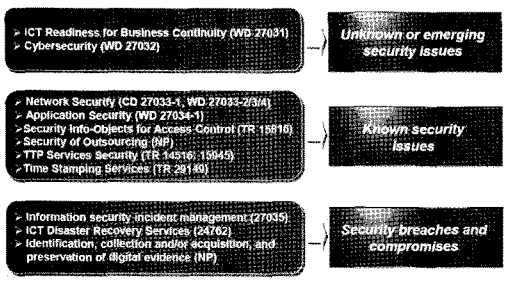
4. ISO/IEC JTC 1/SC27/WG4

WG4는 보안통제 및 서비스(Security Controls and Services)에 관한 표준개발을 목표로 표준화 추진 현황 및 향후 추진 과제들은 <표 3>에 보여지며 활동 범위는 다음과 같다[9,12].

- ISO/IEC 27001에서 정의된 통제와 통제 목표들의 구현을 취급하는 표준과 지침들의 개발과 유지관리 활동을 하며 이를 위해 다음 분야들을 포함한다:
  - IT 네트워크 보안(ISO/IEC 18028)
  - 정보보안 침해사고 관리(ISO/IEC TR 18044)
  - ICT 재난복구 서비스를 위한 지침(ISO/IEC 24762)
  - 침입탐지시스템(IDS, Intrusion Detection System)의 선택, 설치 및 운영 (ISO/IEC 18043)
  - 신뢰적 제 3자 서비스(TTP)의 사용 및 관리 지침(ITU-T X.842 | ISO/IEC TR 14516)
  - 디지털 서명의 응용을 지원하는 TTP 서비스의 규격(ITU-T X.843 | ISO/IEC TR 15945)
  - 접근제어를 위한 SIO(Security Information Objective)(ITU-T X.841 | ISO/IEC TR 15816)
- 향후 요구될 다음과 같은 분야의 서비스와 응용을 위한 표준과 지침에 대한 요구사항 규명과 개발:
  - 업무 연속성
  - 사이버 보안(Cyber Security)
  - 아웃소싱(Outsourcing)
- ISMS 표준과 지침에 대하여 SC27내의 여타 작업반(특히, WG1)들과의 협력.
- 서비스와 응용별 특정 요구사항과 지침을 다루는 외부 전문가 그룹과의 협력:
  - ITU-T 전기통신
  - ISO/TC 215 보건
  - ISO/TC 68 은행업무
  - ISSEA(International Systems Security Engineering Association)
  - 항공우주
  - 산업 자동화

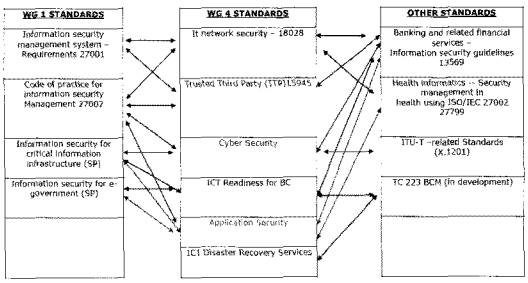
- WLA(World Lottery Association)

WG4에서 수행하고 있는 표준화 과제들은 WG1에서 기존(2006년 9월 이전)에 수행하던 일부 과제들과 심층 방어(defence-in-depth) 프레임워크에 기반을 두어 새로이 설계하고 구조화된 과제들로 구성되며 이는 <그림 5>에 보여 진다. 이 프레임워크는 요구사항들을 3개 분야로 구분하며 이는 (1)미지의 그리고 신생 보안 이슈들을 준비하여 대응하는 수요, (2)기지의 보안 이슈들의 발생을 관리하고 예방하는 수요, 그리고 (3)정보보호시스템의 고장 혹은 자연 재해로 인하여 발생한 정보보안 이슈들 혹은 사고를 조사하는 것을 포함한 관리적 수요로 구성된다. WG4의 개발 표준들은 WG1에서 개발된 ISO/IEC 2700x 계열 표준의 구현을 지원하지만 이의 작업 범위는 반드시 ISO/IEC 2700x 계열 표준의 범위내로 제한되지는 않는다. 예를 들면 Cybersecurity 이슈들은 조직에서 기존의 ISMS보다 더 많은 것을 참여시키며 이는 또한 Internet/ Cyberspace 관련 응용과 서비스의 안전한 프로비저닝 그리고 사이버공간에서의 개인적인 안전한 사용(WD ISO/IEC 27032 참조)과 관련된다.



〈그림 5〉 보안 통제와 서비스에 대한 3개 분야의 수요와 기존 및 신규 표준화과제들 간의 관계

또한 <그림 6>에서는 SC27/WG4의 표준들과 WG1의 표준들 그리고 여타 표준화 전문가 그룹에서 개발된 표준들 간의 관계를 보여 주고 있다.



〈그림 6〉 SC27/WG4와 여타 표준화 전문가 그룹들에서 개발한 표준들의 관계

5. ISO/IEC JTC 1/SC27/WG5

WG5는 ID 관리와 프라이버시 보호 기술에 관한 표준개발을 목표로 활동 범위는 다음과 같다[10].

- ID 관리, 생체인식 그리고 개인 데이터의 보호의 보안 측면을 다루는 표준과 지침들의 개발과 유지관리 활동을 하며 다음 분야에 관한 과제를 수행한다;
  - ID 관리를 위한 프레임워크(ISO/IEC 24760)
  - 생체인식 템플릿 보호(ISO/IEC 24745)
  - 생체인식을 위한 인증 콘텍스트(ISO/IEC 24761)
- 이들 분야의 향후 도래할 표준과 지침들에 대한 요구사항 규명과 개발. ID 관리 분야에 대한 예로는 다음과 같은 주제가 있을 수 있다.
  - 역할기반 접근제어
  - 프로비저닝
  - 식별자

〈표 3〉 SC27/WG4 과제 추진현황 및 향후계획

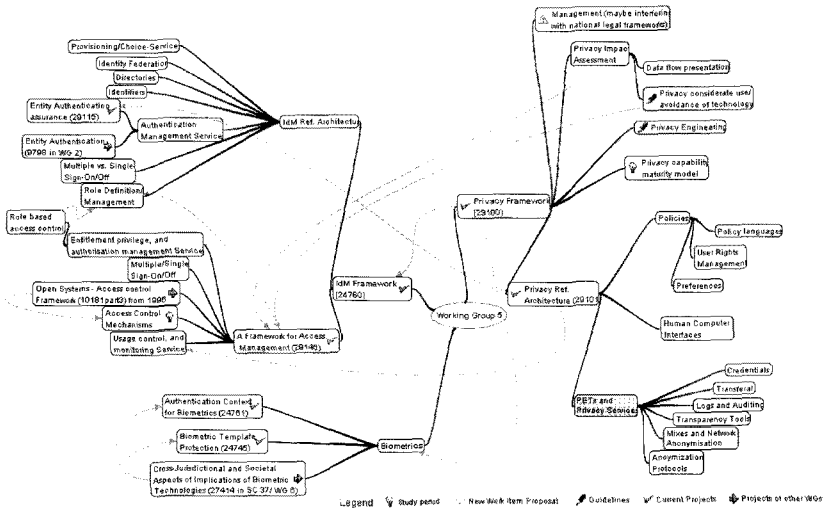
SC27/WG 4 관련 표준명	표준번호	표준화 상태	표준화 일정	적용 단계
WG 4 보안 통제 및 서비스 표준				
Guidelines on the use and management of Trusted Third Party services	14516		1st ed.(2002)	Implement & Operate
Security information objects for access control	15816		1st ed.(2002)	Implement & Operate
Specification of TTP services to support application of digital signatures	15945		1st ed.(2002)	Implement & Operate
Information security incident management	18044		1st ed.(2004), 개정	Implement & Operate
Guidelines for information and communications technology disaster recovery services	24762		1st ed.(2008)	Implement & Operate
Specification for ICT Readiness for Business Continuity	27031	2nd WD		Implement & Operate
Guidelines for Cybersecurity	27032	1st WD		Implement & Operate
Network security — Part 1 — Guidelines for Network Security	27033-1	FCD	18028(2005/2006)의 개정	Implement & Operate
Network security — Part 2 — Guidelines for Secure Design and Implementation of Network Security	27033-2	CD	상동	Implement & Operate
Network security — Part 3 – Reference Networking Scenarios	27033-3	WD	상동	Implement & Operate
통신망 보안 시나리오 – 위험, 설계, 기법 및 통제 이슈				
Network security – Part 4 – Security communications between networks.using security gateways	27033-4	WD	상동	Implement & Operate
Network security – Part 5 – Security communications between networks using Virtual private network	27033-5		상동	Implement & Operate
Network security – Part 6 – IP Convergence	27033-6		상동	Implement & Operate
Network security – Part 7 – Wireless	27033-7		상동	Implement & Operate
Guidelines for Application Security – Part 1 – Overview and Concepts	27034-1	2nd WD		Implement & Operate

- SSO(Single Sign-On)

• 프라이버시 분야에 대한 예로는 다음과 같은 주제가 있을 수 있다:

- 프라이버시 프레임워크
- 프라이버시 참조 구조
- 프라이버시 인프라스트럭쳐
- 익명성 및 크리덴셜
- 특정 프라이버시 고도화 기술(PET, Privacy Enhancing Technologies)
- 프라이버시 엔지니어링

• 생체인식에 대한 예로는 다음과 같은 주제가 있을 수 있다:



〈그림 7〉 SC27/WG5 표준화 작업 현황

- 생체인식 데이터의 보호
- 인증 기법

• SC27내의 여타 작업반들과의 협력으로 WG1과는 관리 측면, WG2와는 특정 암호기법에 대하여 그리고 WG3과는 평가 측면에서 상호 협력한다.

• 이 분야에서의 서비스와 응용별 특정 요구사항과 지침을 다루는 외부 전문가 그룹과의 협력
  - ISO/IEC SC37 생체인식
  - ECRYPT
  - ISO/TC 68/SC2 금융서비스 보안
  - ISO/TC 68/SC6/WG10 금융서비스-소매 금융서비스-프라이버시
  - ITU-T SG17 보안, 언어 및 전기통신 소프트웨어
  - 정보 사회에서의 신분에 대한 미래(FIDS, Future of Identity in the Information Society)
  - 데이터 보호 및 프라이버시 행정관 국제회의(The International Conference of Data Protection and Privacy Commissioners)
  - The Open Group(IdM Forum and Jericho Forum)

<그림 7>은 WG5에서의 기존에 수행하고 있는 표준화 과제와 작업 항목 등의 활동 현황은 물론 논의되고 있는 향후 작업 분야에 대해서도 보여준다. 더욱이, 이 그림에서의 연결선들은 각 항목들의 상호종속성과 상호연결성을 제한적으로 명확히 하기 위한 것이다. 트리 구조는 각 항목들의 계위적 관계를 보여주며 이들의 상호종속성을 그림에서는 서로 이어 표현되어 있다.

표준화 활동을 "전략적", "전술적" 그리고 "시행적" 항목의 3개의 줄기로 초기 모델화 했으며 이는 "무엇을 할 것인가"(관리적 관점)와 "어떻게 할 것인가"(엔지니어링 관점)의 두 줄기로 진화한다. 그림에서 기본 줄기로 향한 관계들은 그림의 중심으로부터의 거리만큼으로 개략적으로 결정될 수 있다. 즉, "무엇을 할 것인가"라는 항목들은 중심 근처에 있으며 반면, "어떻게 할 것인가"라는 항목들은 가장자리에 위치한다.

Ⅲ. 결 론

신생 및 향후의 위험들에 대한 분석을 통해 정보와 ICT에 대한 보호와 정부기관과는 물론 다양한 민간 산업 분야들 간의 안전한 상호연동과 통신 환경을 제공할 필요성이 있다. 특히, 이와 같은 보호는 위기와 재난 시에 주요 인프라를 정상화시키기 위해서 뿐만 아니라 자국의 경제 성장과 존속성을 위해 산업계의 내부와 그들 상호간의 사업 환경 내에서 안전하고 지속적인 운용 환경들을 유지하기 위해 필요하다.

본 고에서는 이들에 대한 국제표준화를 위한 전문가 그룹인 ISO/IEC JTC1/SC27을 중심으로 기존의 3개영역(정보보안관리, 암호 기법, 보안성 보증/평가)에서 2개영역(통제/서비스, ID 관리/바이오 보안)을 확장하여 활동하고 있는 각 작업반에 대하여 기존 표준화 과제의 추진 현황과 향후 과제에 대한 활동계획들을 SC27의 업무계획, 각 작업반의 작업추진계획 그리고 37차 Limassol 회의 결과를 기초로 정리하였다.

이 그룹 내에서 한국의 활동은 보안 선진국에 비하여 미진하지만 최근 6건(SEED, KCDSA, EC-KCDSA, EC-KNR, IBS-2, AMP)의 국내 개발 알고리즘을 표준화하고 4개 과제(18033-3, 27101, 24745 등)에서 에디터 활동을 하고 있다.

이 분야는 신성장동력 산업으로 부가가치가 높고 건전한 지식정보사회의 구현을 위한 전략적 가치가 높아 산업계의 관심과 국가적인 지원이 수반되어 할 것이다. 그러나 보안 기술력의 확보와 이의 관리를 소홀히 할 경우 업무의 연속성이 훼손되어 국가 경영은 물론 산업계의 큰 혼란을 야기 시킬 수 있는 부정적인 측면도 있다.

참고문헌

[1] 박예리, "세계 보안 시장 동향", 2008-05-26, http://www.idckorea.com/product/Getdoc.asp?idx=387&field=Analyst View

[2] "전세계 보안시장 크게 증가", 연평균 15% 성장, 2008-04-15, http://www.idckorea.com/product/Getdoc.asp ?idx=216&field=Newsletters

[3] W. Fummy, "SC27 Business Plan Oct. 2008-Sep. 2009", ISO/IEC JTC1/SC27 N7311, 2008. 10. 9

[4] E. Humphreys, "Information and ICT Security Standards-An innovative to the past, present and future work of SC27, ISO/IEC JTC1/SC27 SD 11 v. 2.0, 2008. 9

[5] H.Bertine, "Telecommunication Security", GSC-12, 2007, http://www.itu.int/ITU-T/special-projects/security/presentations/Telecommunication_Security.ppt#3

[6] ISO/IEC JTC 1/SC 27 N5690, Draft Revised WG3 Road Map, 2007-04-22

[7] ISO/IEC JTC 1/SC 27 N6618, WG1 SD1 Road Map, 2007-07-03

[8] ISO/IEC JTC 1/SC 27 N6716, Rapporteur's report on WG 2 road map held during the April 2008 WG 2 meeting in Kyoto , 2008-04-17

[9] ISO/IEC JTC 1/SC 27 N6751, WG4 SD1 Road Map, 2008-07-14

[10] ISO/IEC JTC 1/SC 27 N6754, WG5 SD1 Road Map, 2008-04-17

[11] ISO/IEC JTC 1/SC 27 N7304, Report of the 37th meeting of SC 27/WG 2, 2008-10-18

[12] 기술표준원, 보안기술 표준화(JTC 1/SC 27) 작업동향, pp. 41~76, SWIST-2008, 제14회 정보보안기술 표준화 워크샵 자료집, 2008.11.21.

저자소개

장 청 룡

1980년 2월 성균관대학교 학사
1986년 8월 연세대학교대학원 석사
1995년 2월 성균관대학교대학원 박사
1979년 12월 ~ 1983년 12월 한국전자통신연구원
1984년 1월 ~ 1997년 1월 한국통신 연구개발본부
1997년 3월 ~ 현재 경동대학교 컴퓨터미디어공학부

주관심분야 : 통신망보안, 암호/인증기법, 보안기술 표준화