情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

ISO/IEC JTC1/SC27 WG4(보안통제 및 서비스) 국제표준화 동향

염 흥 열*

요 약

ISO/IEC JTC 1에서 정보보안 기술에 대한 국제표준화를 추진하고 있는 서브위원회(SC, subcommittee)는 SC 27 서브위원회이다. 이 위원회는 1980년 창립되어 금년으로 21년째 되는 서브위원회로, 정보보호관리체계, 암호 및 보안 메커니즘, 보안성 평가 기준, 보안 통제 및 서비스, 아이덴티티 (identity) 관리 및 프라이버시 기술에 대한 국제표준화를 추진하고 있다. 이중 작업반 4에서는 보안 통제(security control) 및 서비스에 대한 국제표준화를 추진하고 있으며, 2006년에 창립되어 주로 네트워크 보안, 정보보호 침해사고 관리, 사이버 보안, 디지털 증거자료(포렌직), 공급자 체인 보안, 스토리지 보안 등 서비스 및 응용보안에 초점을 맞추어 국제표준화를 추진하고 있다. 본 고에서는 작업반 4에서 최근에 수행되고 있는 주요 국제표준화 내용을 살펴보고 주요 이슈를 제시한다.

Ⅰ. 서 론

ISO/IEC JTC 1 산하 SC27(Sub-Committee)에서는 정보보안기술에 대한 국제표준화가 추진하고 있으며, SC 27 은 산하에 5개의 작업반 (WG, working group)으로 구성되어 있다[1]. 서브위원회 27은 "정보보호관리체계"를 다루는 작업반 1, "암호알고리즘"을 다루는 작업반 2, "공통평가기준"을 다루는 작업반 3, "보안통제와 서비스"를 다루는 작업반 4, "ID 관리 및 프라이버시 보호"를 다루는 작업반 5 등이다[2].

- WG1 (정보보호관리시스템) : 정보보호관리체계(ISMS)에 대한 가이드라인 표준 개발
- WG2 (암호 및 보안 메커니즘) : 보안시스템 및 응용에서 이용되는 암호 및 보안 메카니즘 등의 표준 개발
- WG3 (보안성 평가기준) : IT 시스템 및 제품에 대한 보안성 평가와 인증에 대한 표준 개발 (평가 기준과 평가방법론, 암호모듈검증기준 포함)
- WG4 (보안통제 및 서비스) : 서비스와 응용을 위한 보안 표준을 개발하고 있으며, 네트워크 보안과 사이버보안 등의 응용/서비스 보안 표준 개발
- WG5 (아이덴티티 관리 및 프라이버시 보호 기술) : ID (identity) 관리 기술 및 프라이버스 보호 기술들에 대한 표준들을 개발

ISO/IEC JTC 1/SC 27 회의가 2010년 10월 4일부터 10월 11일까지 독일 베를린에서 열렸다. 지난 10월 SC 27 회의는 20번째 되는 회의였다. 또한, SC 27 산하 작업반 4 회의는 9회째로 미국, 영국, 일본, 한국 등 47명의 보안 표준 전문가가 참석했고 한국에서는 필자를 포함해 양희찬 연구사(기표원) 등이 참석했다[3],[4],[22].

본 고에서는 현재 서브위원회 27의 작업반 4에서 추진되고 있는 주요 표준화 현황을 살펴보고, 지난 10월 회의에서의 주요 이슈 중심으로 기술한다.

Ⅱ. 주요 표준화 현황

작업반 4에서 추진되고 있는 주요 표준화 분야는 사이버보안, 네트워크 보안, 응용보안, ICT 공급체인 보안, 디지털 증거자료 수집, 디지털 리덱션 (redaction), 그리고 침입차단/탐지시스템 (intrusion detection/protection system) 등으로 구분될 수 있다. 현재 SC 27 WG 4에서 추진되고 있는 주요 표준 목록은 [표 1]과

본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2011-C1090-1131-0005)
* 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

〔표 1〕 현재 개발중인 주요 국제 표준 목록

표준 번호		표준 제목	표준화 진행 상태
ISO/IEC 27032		Guidelines for Cybersecurity	3rd CD
ISO/IEC 27033	Part 1	Network security – Part 1: Part 1: Guidelines for network security	FDIS
	Part 2	Network security – Part 2: Guidelines for the design and implementation of network security	FCD
	Part 3	Network security – Part 3: Part 3: Reference networking scenarios - Threats, design, technologies and control issues	FDIS
	Part 4	Network security - Part 4: Securing Communications between networks using security gateways	3rd WD
	Part 5	Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	WD
	Part 6	Network security - Part 6: Securing IP Network Access using Wireless	WD
ISO/IEC 27034	Part 1	Application security – Part 1: Overview and concepts	2nd FCD
	Part 2	Application security - Part 2: Organization Normative Framework	3rd WD
	Part 3	Application security – Part 3: Application Security Management	-
	Part 4	Application security – Part 4: Application Security Validation	-
	Part 5	Application security – Part 5: Protocols and Controls Data Structure	-
ISO/IEC 27035		Information Security Incident Management	FDIS
ISO/IEC 27036	Part 1	Information security for supplier relationships - Part 1: Overview and Concepts	PD (preliminary draft)
	Part 2	Information security for supplier relationships – Part 2: Common Requirements	PD
	Part 3	Information security for supplier relationships - Part 3: Guidelines for ICT Supply Chain	PD
	Part 4	Information technology – Security techniques - Part 4: Guidelines for security for outsourcing	4th WD
ISO/IEC 27037		Guidelines for Identification, Collection and/or Acquisition and Preservation of Digital Evidence	CD
ISO/IEC 27038		Specifications for Digital Redaction	2nd WD
ISO/IEC 27039		Selection, deployment, and operation of intrusion detection and prevention systems (IDPS)	WD
ISO/IEC 29149		Best practices for time stamping services	3rd PDCR
-		Storage security	NWIP

같다[4],[5].

ISO/IEC 27032 : “사이버보안 가이드라인” 표준(27032)은 인터넷상에서 사이버보안 수준을 향상하기 위한 가이드라인을 제공한다[6]. 여기서는 사이버보안에 대한 정의 및 개요, 사이버보안 주요 주체의 정의 및 역할 확인, 사이버보안 문제를 해결하기 위한 가이드라인, 그리고 각 주체간의 협력을 가능케 하는 프레임워크를 제공하고 있다. “사이버보안 가이드라인” 표준(27032)은 지난 10월 회의에서 3번째 CD (committee draft)로 진입하기로 합의했다.

ISO/IEC 27033 : 네트워크 보안 표준 분야의 경우, 6개의 파트로 표준이 나눠져서 개발되고 있다[4]. ISO/IEC 27033-1 [7] 은 네트워크 보안 개요와 개념에 대한 표준으로, 네트워크 보안에 대한 용어와 개념과 네트워크보안 관리 가이드라인을 제공한다. 다시 말해, 네트워크 보안 위협과 위험(risk)을 분석하고 확인하기 위한 방법 가이던스, 네트워크 보안 구조와 기술 세부 보안통제를 제공하며, 최적의 네트워크 보안 구조 등을 제시한다. ISO/IEC 27033-2 [8] 은 종단간 네트워크 보안을 위한 네트워크 보안 구조를 정의하고 있다. ISO/IEC 27033-3 [9] 네트워크 시나리오에 따른 리스크, 설계기법, 보안 통제를 정의하고 있다. ISO/IEC 27033-4 [9]

보안 게이트웨이를 이용한 네트워크간의 안전한 통신을 위한 표준으로, 네트워크 보안 게이트웨이 구성 방법 및 선택 기준을 제시하고 있다. 네트워크 보안 개요와 개념인 파트 1 (27033-1)과 네트워크 보안 시나리오에 관한 파트 3 (27033-3)은 이미 FDIS (final draft international standard) 상태로 국제표준화를 완료되어 있다[9]. 지난 10월 회의에서는 "네트워크 보안 설계 및 구현 가이드라인"에 관한 파트 2 (27033-2)[8], 필자가 에디터인 "보안 게이트웨이를 이용한 보안 통신"에 관한 파트 4(27033-4)[10], "VPN (virtual privacy network) 보안을 이용한 보안 통신"에 관한 파트 5 (27033-5) [11], "무선 보안"에 관한 파트 6(27033-5) [12] 등에 대한 표준화 진전이 이뤄졌다. 파트 2의 경우, 작업반 4 프레너리(Plenary)에서는 현재 FCD(final committee draft) 상태에 있던 문서를 표준 구조와 완성도의 문제가 제기되어 WD (working draft) 상태로 되돌리기로 SC 27 프레너리에 제안했으나 SC 27 프레너리에서는 이런 작업 규정이 없다는 이유로 현재 문서 상태를 유지하기로 합의하고, 향후 문서의 품질을 계속 향상하기로 NB (national body) 에게 추가 기고서 제출을 요구했다. 파트 4는 미국, 일본, 영국 등에서 온 의견을 수렴했고, 문서의 상태를 3번째 WD 상태로 진행하기로 합의했다. 파트 5와 파트 6은 표준 초기상태로 문서 구조와 에디터가 합의되었다.

ISO/IEC 27034: 응용 프로그램 개발 시 필요한 보안 요구사항과 체계를 다루는 응용 보안 (27034) 표준은 5개의 파트로 구성되어 개발되고 있다. 파트 1은 응용 보안 개요와 개념에 대한 것으로, 응용의 전주기동안 보안의 무결성을 확보하기 위한 개념, 원칙, 프레임워크, 과정 등을 개발하고, 응용을 외주 개발하기 위해 개발자를 선택하기 위한 기준을 만들기 위한 가이드라인 등을 제공한다[13]. 지난 10월 회의에서는 "응용보안 개요와 개념"에 관한 파트 1 (27034-1)과 응용보안을 위한 "조직 normative 프레임워크"에 관한 파트 2 (27034-2) [14] 등이 주로 다뤄졌으며, 파트 1은 FCD (final committee draft) 상태로, 파트 2는 3번째 WD 상태로 진입하기로 합의했다.

ISO/IEC 27035: 이 표준은 보안 관리자, 정보시스템/서비스/네트워크 관리자를 위한 침해사고 관리를 위한 가이드라인을 제공한다[15]. 인터넷침해사고대응팀(CSIRT, computer security incident response team)을 위하여 침해사고를 신속히 검출하고, 적절히 대응하며, 지속적으로 향상하기 위한 구조화된 관리방법을 제시하는 "정보보안 침해사고 관리"표준 (27035)은 FDIS 상태로 진입하기로 합의함으로서 표준화작업을 완료하기로 합의했다.

ISO/IEC 27036: 2010년 4월 말레이시아 말라카 SC27 회의에서 설립되었던 ICT 공급자보안에 관한 연구회기(SP, study period) 보고서 검토 결과, 27036 표준을 전체 4개 파트로 구성키로 합의했다[3]. 파트 1은 "ICT 공급자 체인 보안의 개요 및 개념"[16], 파트 2는 "공통 요구사항"[17], 파트 3은 "ICT 공급자 체인 가이드라인"[18], 파트 4는 "아웃소싱 보안"을 다루기로 했다[4]. 파트 1,2,3은 예비 문서를 준비하기로 합의했다. 아웃소싱 보안을 다루던 표준 (27036)의 경우, 새로 "공급자 관계를 위한 정보보안"을 만들기로 했다. 현재 개발중인 "아웃소싱 보안" 표준은 "공급자 관계를 위한 정보보안" 표준 (27036)의 파트 4로 하여 개발하기로 했다. 파트 1은 공급자 체인의 개요와 개념에 대한 표준으로, 공급자 관계에서 정보보안에 대한 가이드라인을 제공한다. 파트 2는 공통 요구사항에 대한 것으로, 획득 과정에서 공급자 관계를 설정하고, 구현하며, 운영하고, 모니터링하며, 관리하고 향상하기 위한 공통의 요구사항을 정의하고 있다.

ISO/IEC 27037: ISO/IEC 27037 [19] 은 국경을 초월한 디지털 범죄의 증거를 수집하고 보호하기 위한 세부적인 가이던스를 표준화하고 있다. "디지털 증거자료의 확인, 수집, 보존을 위한 가이드라인"(27037)은 CD (committee draft) 상태로 진입하기로 합의했다[19].

ISO/IEC 27038: 조직이나 국가 또는 기관에서 공개되는 디지털 문서에서 민감한 개인정보를 효과적으로 제거하는 방법을 표준화하는 "디지털 리덕션" 표준(27038)은 두 번째 WD로 진입하기로 합의했다[20].

ISO/IEC 27039: 디지털 침입탐지시스템 분야의 경우, "IDS (intrusion detection system)의 설치, 운영" 등에 대한 표준(27039)은 이전 표준 번호가 18043이었으나, 표준 번호를 27039로 변경하기로 했고[21], 또한 제목을 "침입 탐지 및 방지 시스템의 선택, 설치, 운영"으로 결정했으며, 영국 등으로부터 에디터 진을 보강하기로 합의했다.

그 외 표준 추진 동향: 신규 표준화 아이템 추진 타당성을 검토하기 위해 5개의 연구회기를 시작하기로 합의했으며, 이는 "디지털증거자료 준비 및 분석", "디지털

증거자료 검증 및 타당성", "WG4 용어 정의", "클라우드 보안", "침해사고 관리/운영/대응" 등이다. 스토리지 보안(storage security)은 연구회기를 마치고 신규 표준화 아이템 제안(NWIP, new work item proposal)으로 추진키로 합의했다.

III. 2010년 10월 작업반 4 회의 주요 표준화 이슈

지난 10월 베를린 회의에서의 주요 이슈는 일본이 제안한 클라우드 컴퓨팅 보안을 위한 정보보호관리체계(ISMS, information security management system) 신규 SP 제안, 사이버보안 표준 관련 이슈, 그리고 한국 제안 침해사고대응조직을 위한 SP 제안 등을 들 수 있다[3],[4].

일본은 클라우드 컴퓨팅 보안을 위한 정보보호관리체계 (ISMS)를 표준화하기 위한 신규 표준화 아이템 설정을 위한 SP를 제안했다. 이 제안은 광범위한 토론 후 ISMS, 클라우드 서비스, 그리고 프라이버시 보호와 연관되므로 WG1/WG4/WG5 조인트 작업반의 연구회기를 시작하는 것으로 합의했고, 현재 일본어로 된 ISMS 기준을 영어로 번역해 내년 4월 싱가폴 회의에서 발표하기로 했으며, 표준 개발시 SC 38, ITU-T SG17과 협력하기로 했다. 다만, 토론하는 동안 미국 대표가 기존의 8개 이상의 표준화 기구에서 클라우드 컴퓨팅 국제표준화가 추진되고 있는데, SC27에서 표준화 작업을 추진해서 얻을 수 있는 이점이 무엇인지와, 기존 표준 문서를 어떤 방법으로 SC27 표준화로 연결하는 지에 대한 질문이 있었으며, 대체로 각 표준화 조직마다 고유의 특성이 있어서 표준화가 추진되어야 하며, 클라우드 보안을 위한 SP를 통해 그 해답을 얻어야 한다는 데 합의가 이뤄졌다.

사이버보안 표준 관련 이슈는 역시 사이버보안에 대한 정의와 범위였다. 영국 대표는 "사이버보안"과 기존 "인터넷보안" 과의 차별이 확인해야 하고 사이버보안의 범위에 사이버안전도 넣어 확대해야 한다고 주장했다. 이러한 제안은 일본, 싱가폴, 남아공 등의 에디터그룹에 의해 거부되었고, 에디터그룹은 개발 일정을 고려하고 표준의 성숙도를 고려해 다음 문서 상태를 FCD (final committee draft) 로 진입할 것을 주장했으나, 영국, 미국, 말레이시아, 캐나다, 한국 등은 사이버 안전 등의 범위 포함 여부 등 여러 논쟁거리가 남아 있으므로 3번째 CD (committee draft) 로 추진할 것을 주장해 3번째 CD로 추진할 것으로 합의했다.

영국 주도로 "디지털 증거 준비와 분석", "디지털 증거의 검증" 등에 대한 두 개의 새로운 워크아이템을 추진을 위한 SP를 제안했고, 미국 대표는 WG4 프레너리에서 규제와 연관되므로 연구회기 추진을 반대했으나, SC 27 프레너리에서 별다른 이의 없이 연구회기를 시작하기로 결의했고, 기존 디지털 포렌직 표준(27037)과는 별도의 표준으로 개발하며 신규 표준화 워크아이템을 위한 6개월간의 연구회기를 추진하기로 합의했다.

한국은 기존 ISO/IEC 27035 표준이 침해사고대응조직 신설 절차와 조직 구성원이 가져야 할 요건 등의 측면에서 부족한 부분이 있다고 주장하고, "CSTRT를 위한 운영 및 구현" 에 관한 신규 표준화 워크아이템을 위한 SP를 제안했다. 이 제안은 WG4 프레너리에서 싱가폴 등의 적극적인 지원에 힘입어 채택되었다. 토론하는 동안 ISO/IEC 27035의 미흡한 부분이 확인되었고, 표준 추진방법으로 기존에 ISO/IEC 27035의 개정 추진, 멀티파트 표준, 또는 별도 추진 등의 안이 제시되었고, SP 동안 이에 대한 해답을 찾기로 확인하기로 했다. 또한, 한국, 일본, 영국 전문가 등이 연구회기의 공동 라포처(Rapporteur)로 임명되어 한국 주도의 국제 표준 추진을 위한 발판을 마련했다.

Ⅵ. 결 론

본 고에서는 2010년 10월 독일 베를린에서 열린 SC 27 WG 4에서 다뤄지고 있는 주요 국제표준화 현황을 살펴보고, 지난 10월 베를린 회의의 주요 이슈를 다뤘다. 본 고는 [22]에 기반해 국제표준화의 세부내용을 구체화하고 주요 내용을 현행화 하였다. 현재 WG4에서는 클라우드 컴퓨팅 보안 기술에 대한 국제표준화를 준비하고 있고, 디지털 증거자료 수집을 위한 포렌직 기술, 네트워크 보안, 사이버 보안, 공급자 체인 보안, 응용 보안 등의 파급효과가 예상되는 국제표준을 개발하고 있다. 특히, 지난 10월 회의에서 디지털 증거자료 수집, 침해사고대응조직을 위한 운영 및 구현, 그리고 클라우드 컴퓨팅 보안 표준을 위한 연구회기를 시작하기로 하고, 많은 기존 개발 중인 표준에 진전을 이뤘다. 따라서 이들 클라우드 컴퓨팅 보안과 공급자체인보안, 스토리지 보안 등의 신규 추진이 예상되는 표준들은 파급효과가 클 것으로 예측되어 국내 보안 산업과 서비스에 영향을 줄 수 있을 것으로 판단된다. 따라서, 국내

실정과 요구가 반영된 국제표준화 추진 방법 등의 전략적 대응이 요구되고 있다.

참고문헌

[1] ISO/IEC JTC 1 홈페이지, http://www.iso.org/iso/jtc1_home.html

[2] ISO/IEC JTC 1 SC 27 홈페이지, http://www.iso.org/iso/iso_technical_committee?commid=45306

[3] ISO/IEC JTC 1 SC27 N9084, Resolutions of the 9th SC 27 WG 4 Plenary Meeting held in Berlin, Germany from 4 – 8 Oct. 2010.

[4] ISO/IEC JTC 1/SC 27 N9085, ISO/IEC JTC 1/SC 27/WG 4 Meeting No. 9 Berlin, Germany October 4-8, 2010 Meeting Report

[5] Walter Fumy, "ISO/IEC JTC1/SC27-IT Security Technique", ITU-T Workshop, Geneva Swiss, 6-7 Dec. 2010.

[6] ISO/IEC 2nd CD 27032 – Information technology – Security techniques – Guidelines for Cybersecurity (N7917), Dec. 2010.

[7] ISO/IEC 27033-1 - Information technology – Security techniques -- Network security – Part 1: Part 1: Guidelines for network security

[8] ISO/IEC FCD 27033-2 - Information technology – Security techniques -- Network security – Part 2: Guidelines for the design and implementation of network security (N8626), Dec. 2010

[9] ISO/IEC 27033-3 - Information technology – Security techniques --Network security – Part 3: Part 3: Reference networking scenarios - Threats, design, technologies and control issues

[10] ISO/IEC 2nd WD 27033-4 - Information technology - Security techniques -- Network security -- Part 4: Securing Communications between networks using security gateways (N8634), Dec. 2010

[11] ISO/IEC WD 27033-5 - Information technology - Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs) (N8647), Dec. 2010.

[12] ISO/IEC WD 27033-6 - Information technology - Security techniques - Network security – Part 6: Securing IP Network Access using Wireless (N8647), Dec. 2010

[13] ISO/IEC FCD 27034-1 - Information technology – Security techniques -- Application security - Part 1: Overview and concepts, Dec. 2010

[14] ISO/IEC 2nd WD 27034-2 - Information technology – Security techniques - Application security - Part 2: Organisation Normative Framework, Dec. 2010

[15] ISO/IEC FCD 27035 – Information technology – Security techniques - Information Security Incident Management, Dec. 2010

[16] ISO/IEC WD 27036-1 – Information technology – Security techniques – Information security for supplier relationships - Part 1: Overview and Concepts, Dec. 2010

[17] ISO/IEC WD 27036-2 – Information technology – Security techniques – Information security for supplier relationships – Part 2: Common Requirements, Dec. 2010

[18] ISO/IEC 27036-3 – Information technology – Security techniques – Information security for supplier relationships - Part 3: Guidelines for ICT Supply Chain, Dec. 2010.

[19] ISO/IEC 3rd WD 27037 – Information technology – Security techniques – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, Dec. 2010.

[20] ISO/IEC WD 27038 – Information technology – Security techniques – Specifications for Digital Redaction, Dec. 2010

[21] SO/IEC WD 27039 (18043) – Information technology – Security techniques - Selection, deployment, and operation of intrusion detection and prevention systems (IDPS), Dec. 2010

[22] 염흥열, "제9회 네트워크 및 응용보안(SC 27 WG 4) 회의," TTA 저널, No.132, TTA, 2010. 11월

〈著者紹介〉

염흥열 (Heung-Youl YOUM)
종신회원

1981년 2월: 한양대학교 전자공학과 졸업
1983년 2월: 한양대학교 전자공학과 석사
1990년 2월: 한양대학교 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월: 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재:한국정보보호학회 총무이사, 학술이사, 교육이사, 상임부회장, 수석부회장(2010), (현) 회장
2004년 1월~현재 : 한국인터넷정보학회 이사, (현)논문지 편집위원
2003년 9월~2004년 3월 : ITU-T SG17/Q10 Associate Rapporteur
2004년 3월~현재 : ITU-T SG17/Q9 Rapporteur
2008.10 ~현재: ITU-T SG17 부의장
2009.2 ~현재: ITU-T SG17 WP2 의장
2006년 11월~2008년 2월 : 정보통신부 정책자문단 정보보호 PM
2006년 11월 ~2009년 2월 : 한국정보통신연구진흥원 정보보호전문위원
<관심분야> 네트워크 보안, 전자상거래 보안, 공개키 기반 구조, 부호이론, 이동통신보안