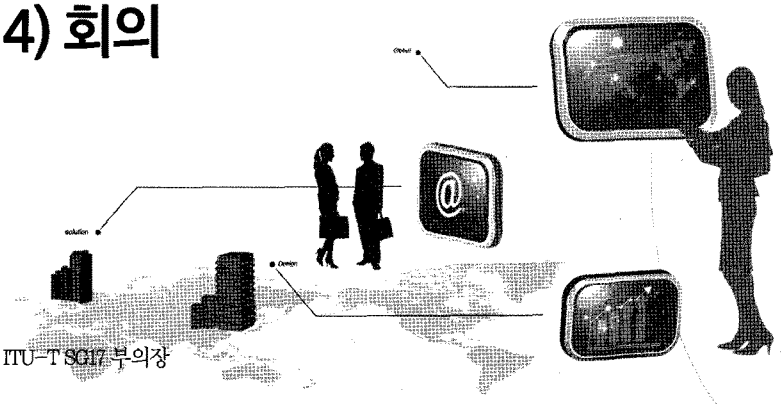
제9회 네트워크 및 응용 보안(SC 27 WG 4) 회의



염흥열 | 순천향대학교 정보보호학과 교수, ITU-T SG17 부의장

1. 머리말

ISO/IEC JTC 1/SC 27 회의가 지난 10월 4일부터 10월 11일까지 독일 베를린에서 열렸다. SC 27은 정보보호 표준화를 담당하고 있으며 올해로 창립된 후 20년이 되었다. 이번 회의는 동서독 통일 20년을 기념해 동서독 분단의 상징이었던 베를린에서 열렸다.

SC 27은 산하에 5개의 작업반(WG: Working Group)으로 구성되어 있으며, 이는 '정보보호관리체계'를 다루는 작업반 1, '암호알고리즘'을 다루는 작업반 2, '공통평가기준'을 다루는 작업반 3, '보안 통제와 서비스'를 다루는 작업반 4, 'ID 관리 및 프라이버시 보호'를 다루는 작업반 5 등이다. 이번 제9회 SC 27 작업반 4 회의에는 미국, 영국, 일본, 한국 등 47명의 보안 표준 전문가가 참석했고 한국에서는 필자를 비롯한 오홍룡 과장(TTA), 전상권 수석(기재부) 등이 참석했다. 본 고에서는 현재 작업반 4에서 추진되고 있는 주요 표준화 현황을 살펴보고, 이번 회의에서 이뤄진 주요 결과를 중심으로 기술한다.

2. 표준화 추진현황

작업반 4에서 추진되고 있는 주요 표준화 분야는 사이버보안, 네트워크보안, 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 같다.

사이버보안에 대한 용어를 정의하고 사이버보안을 위한 참여 주체들의 역할과 대응 방안에 대한 가이드를 개발하기 위한 '사이버보안 가이드라인' 표준(27033-2)은 이번 회의에서 3번째 CD(Committee Draft)로 진입하기로 합의했다.

네트워크보안 표준 분야의 경우, 6개의 파트로 표준이 나눠져서 개발되고 있으며, 네트워크보안 가이드라인에 관한 파트 1(27033-1)과 시나리오에 관한 파트 3(27033-3)은 이미 FDIS(Final Draft International Standard)로 상태로 국제 표준화를 완료했고, 이번 회의에서는 '네트워크보안 설계 및 구현 가이드라인'에 관한 파트 2(27033-2), 필자가 에디터인 '보안 게이트웨이를 이용한 보안 통신'에 관한 파트 4(27033-4), 'VPN(Vitual Privacy Network) 보안을 이용한 보안 통신'에 관한 파트 5(27033-5), '무선보안'에 관한 파

〈표 1〉 주요 표준 목록

표준 번호		표준 제목	표준 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
	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

트 6(27033-5) 등에 대한 표준화 진전이 이뤄졌다. 파트 2의 경우, 작업반 4 프리너리에서는 현재 FCD 상태에 있던 문서를 문서 구조와 내용의 완성도를 제고하기 위해 WD(Working Draft) 상태로 되돌리기로 SG 27 프리너리에 제안했으나 SC 27 프리너리에서는 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 6는 표준 초기상태로 문서 구조와 에디터가 합의되었다.

응용 프로그램 개발 시 필요한 보안 요구사항과 체계를 다루는 응용보안(27034) 표준은 5개의 파트로 구성되어 개발되고 있는데, 이번 회의에서는 '응용보안 개요와 개념'에 관한 파트 1(27034-1)과 응용보안을 위한 '조직 normative 프레임워크'에 관한 파트 2(27034-2) 등이 주로 다뤄졌으며, 파트 1은 FCD(Final

Committee Draft) 상태로, 파트 2는 3번째 WD 상태로 진입하기로 합의했다.

인터넷침해사고대응팀(CSIRT: Computer Security Incident Response Team)을 위해 침해사고를 신속히 검출하고, 적절히 대응하며, 지속적으로 향상하기 위한 구조화된 관리방법을 제시하는 '정보보안 침해사고 관리' 표준(27035)은 FDIS 상태로 진입하기로 합의함으로써 표준화작업을 완료하기로 합의했다.

아웃소싱 보안을 다루던 표준(27036)의 경우, 새로 '공급자 관계를 위한 정보보안'을 만들기로 했다. 현재 개발 중인 '아웃소싱 보안' 표준은 '공급자 관계를 위한 정보보안' 표준(27036)의 파트 4로 하여 개발하기로 했다. 또한, 지난 4월 말레이시아 말라카 SC27 회의에서 설립되었던 ICT 공급자보안에 관한 연구회기(SP: Study Period) 보고서 검토 결과, 27036 표준을 전체 4개 파트로 구성키로 했으며 파트 1은 'ICT 공급자 체인 보안의 개요 및 개념', 파트 2는 '공통 요구사항', 파트 3은 'ICT 공급자 체인 가이드라인', 파트 4는 '아웃소싱 보안'을 다루기로 했다. 파트 1, 2, 3은 예비 문서를 준비하기로 합의했다.

'디지털 증거자료의 확인, 수집, 보존을 위한 가이드라인' (27037)은 CD(Committee Draft) 상태로 진입하기로 합의했다. 조직이나 국가 기관에서 공개되는 디지털 문서에서 민감한 개인정보를 효과적으로 제거하는 방법을 표준화하는 '디지털 리덕션' 표준(27038)은 두 번째 WD로 진입하기로 합의했다.

디지털 침입탐지시스템 분야의 경우, 'IDS(Intrusion Detection System)의 설치, 운영' 등에 대한 표준(27039)는 이전 표준 번호가 18043이었으나, 표준 번호를 27039로 변경하기로 했다. 제목을 '침입 탐지 및 방지 시스템의 선택, 설치, 운영'으로 결정했으며, 영국 등으로부터 에디터진을 보강하기로 합의했다.

또한 신규 표준화 아이템 추진 타당성을 검토하기 위해 5개의 연구회기를 시작하기로 합의했으며, 이는 '디지털 증거자료 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 신규표준아이템 제안(NWIP: New Work Item Proposal)으로 추진키로 합의했다.

3. 주요 이슈 및 논쟁사항

이번 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.

일본은 클라우드 컴퓨팅 보안을 위한 정보보호관리체계(ISMS)를 표준화하기 위한 신규표준아이템 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 2011년 4월 싱가포르 회의에서 발표하기로 했으며, 표준 개발 시 SC 38, ITU-T SG17과 협력하기로 했다. 다만, 토론기간 동안 미국 대표가 기존의 8개 이상의 표준화 기구에서 클라우드 컴퓨팅 국제 표준화가 추진되고 있는데, SC 27이 표준화 작업을 추진해서 얻을 수 있는 이점이 무엇인지와 기존 표준문서를 어떤 방법으로 SC 27 표준화로 연결하는 지에 대한 질문이 있었으며, 대체로 각 표준화 조직마다 고유의 특성이 있어서 표준화가 추진되어야 하며, 이번 클라우드 보안을 위한 SP를 통해 그 해답을 얻어야 한다는 것에 합의가 이뤄졌다.

사이버보안 표준 관련 이슈는 역시 사이버보안에 대

한 정의와 범위였다. 영국 대표는 '사이버보안'과 기존 '인터넷보안'과의 차별을 확인해야 하고 사이버보안의 범위에 사이버안전도 넣어 확대해야 한다고 주장했다. 이러한 제안은 일본, 싱가포르, 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 프리너리에서 규제와 연관되므로 연구회기 추진을 반대했으나, SC 27 프리너리에서 별다른 이의 없이 연구회기를 시작하기로 결의했고, 기존 디지털 포렌직 표준(27037)과는 별도의 표준으로 개발하며 신규 표준워크아이템을 위한 6개월간의 연구회기를 추진을 합의했다.

한국(기재부 전상훈)은 기존 27035 표준이 미비한 침해사고 대응조직 신설 절차와 조직 구성원이 가져야 할 요건 등의 내용을 위한 'CSIRT를 위한 운영 및 구현'에 관한 신규 표준워크아이템을 위한 SP를 필자와 더불어 제안했다. 이 제안은 WG4 프리너리에서 싱가포르 등의 적극적인 지원에 힘입어 미국과 영국 등의 일부 우려의 목소리를 잠재우고 채택되었다. 토론기간 동안 27035의 미흡한 부분이 확인되었고, 표준 추진방법으로 기존에 27035의 개정 추진, 멀티파트 표준, 또는 별도 추진 등의 안이 제시되었고 SP 동안 이에 대한 해답을 찾기로 확인하기로 했다. 또한 한국(전상훈), 일본(코지 나카오), 영국 전문가 등이 연구회기의 라포처로 선임되어 국제 표준 추진을 위한 발판을 마련했다.

4. 맺음말

이번 독일 베를린 SC 27 WG4 회의에서는 디지털 증거자료 수집, 침해사고 대응조직을 위한 운영 및 구현, 그리고 클라우드 컴퓨팅 보안 표준을 위한 연구회기를 시작하기로 하고, 많은 기존 개발 중인 표준에 진전을 이뤘다. 따라서 이들 신규 추진이 예상되는 표준들은 파급효과가 클 것으로 예측되어 국내 보안 산업과 서비스에 영향을 줄 수 있을 것으로 판단된다. 따라서 2011년 4월 싱가포르 SC 27 회의에 대비해 국내 차원의 에디터 추천 및 국내 실정이 반영된 표준 추진 방법 등의 전략적 대응이 요구된다. TTA