情 報 保 護 學 會 誌
第20卷 第6號, 2010. 12

ISO/IEC JTC1 SC27 WG4 침해관리, 운영 및 대응 국제표준화 동향

전 상 훈 *

요 약

ISO/IEC JTC1 SC27는 IT 정보보호에 관한 국제표준 제정 활동을 하는 국제기구로서, 다섯 개의 WG(Working Group)으로 구성되어 있으며, 현재 WG4는 WG1의 정보보호관리체계(ISMS), WG5에서 다루어지고 있는 인증(Authentication), 프라이버시(Privacy) 등과 연계하여, 정보보호 관련 국제표준을 개발 및 제정하고 있다.

본 논문은 2010년 10월 4일부터 8일까지 베를린(Berlin)에서 개최한 회의에서 WG4에서 다루어지고 있는 네트워크 보안 국제표준기술 동향과 표준화에 대한 개요를 소개하고, ISO/IEC JTC1 SC27 WG4 Plenary에서 필자가 제안하여 SP(Study Period) 단계로 승인된 표준안건의 동향과 전망에 대해 소개하고자 한다.

Ⅰ. 서 론

ISO/IEC JTC 1 SC27(IT Security Techniques) 회의가 지난 2010년 10월 4일부터 11일까지 SC27 창립 20주년을 맞이하며 독일 베를린에서 개최되었다[2].

WG4 내에서는 사이버보안(Cyber Security), 네트워크 보안(Network Security), 애플리케이션 보안(Application Security), 침해 관리(Incident Management), 디지털 증거 보존, 확인, 수집을 위한 가이드라인(Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence) 등의 다수의 프로젝트들 표준화가 진행되었다.

본 논문은 WG4 작업반 내에서 진행되었던 표준화 과정인 프로젝트들을 소개하여, 국내의 많은 정보보호 관련 전문가들이 네트워크 보안 관련 기술 표준화 활동에 관심을 가질 수 있도록 하기 위함이다.

그리고 이번 베를린 회의에서 필자가 제안하여 SP(Study Period) 단계로 승인되어 국제표준 기술의 초석을 마련하게 된, "침해관리, 운영 및 대응"에 관한 내용을 소개하고자 한다.

Ⅱ절에서 ISO/IEC JTC1 SC27 위원회와 표준화 절차를 소개하고, Ⅲ절에서는 SC27 WG4에서 다루고 있는 표준화 동향 설명한다. 그리고 Ⅳ절에서 필자가 제안한 침해관리, 운영 및 대응에 관한 안에 관해 간략하게 설명하고, Ⅴ절에서 결론을 정리하겠다.

Ⅱ. 국제표준기구

2.1 ISO/IEC JTC1 SC27

ISO/IEC JTC 1 SC27 IT Security Techniques는 ISO(International Organization for Standardization)와 IEC(International Electrotechnical Commission)가 공동으로 설립한 JTC 1(Joint Technical Committee 1)의 위원회이다[2].

SC(Subcommittee)27은 SC20(Cryptographic Techniques)이 다루고 있던 표준화 범위와 기능이 확대됨에 따라 계승된 위원회로서, 1989년 JTC1이 설립 및 결정되었고, 1990년 스웨덴에서 범위와 조직 등이 갖추어졌으며, 일본 도쿄 회의를 시작으로, 현재까지 매년 2회 회의를 하고, 1회 총회를 개최하고 있다.

- ISO(International organization for standardization)국제표준화기구로 '동등하다'라는 그리스어 'isos'에서 유래되어 ISO로 통일하여 부르고

* 기획재정부 정보화담당관실 재정경제사이버안전센터(randyjeon@mosf.go.kr)

〔표 1〕JTC1 국제표준 개발 절차

단계	표준	개정표준	신속표준작업	기술보고서	국제기능표준	기술오류정정서
0 예비단계						
1 제안단계		NP		NP	NP	
2 준비단계	WD	WD		WD	WD	Defect, Report
3 위원회단계	CD FCD	PDAM FPDAM		PDTR	PDISP FPDISP	DCOR
4 승인단계	FDIS	FDAM	DIS	DTR	FDIS	
5 출판단계	IS	AMD	IS	TR		COR

있는 국제표준화 기구이며, 상품 및 서비스의 국제간 교류를 원활하게 하고 지식, 과학, 기술 및 경제활동 분야의 협력발전을 위한 세계적인 조화 추구하는 국제표준화 기구이다. 157개국이 가입[3].(2008년 12월 기준)

- IEC(International Electrotechnical Commission) 전기·전자분야에서 국제적으로 통용되는 표준 및 적합성 평가기준을 확립하고, 이를 통한 원활한 국제무역 촉진과 시장 효율 극대화를 추구하는 국제표준화 기구이다. 72개국이 가입[3].(2008년 12월 기준)
- JTC1(Joint Technical Committee 1) 정보통신기술 분야의 국제표준화 활동을 위한 ISO와 IEC의 공동 위원회로, ISO와 IEC간 정보기술 분야의 상호 협력적인 국제 표준화를 추진한다.

현재 JTC1은 43개국의 P-member(Participating:정회원국)와 43개국의 O-member(observer:참관회원국) 들이 활동하고 있으며, 국내 전문가들은 1992년부터 P-member로서 SC27-Korea 전문위원회를 통해 활동을 계속해 오고 있다.

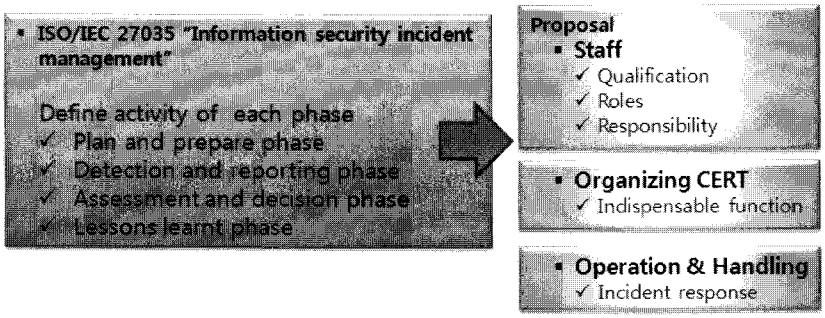
2.2 ISO/IEC JTC1 국제표준화 절차

JTC1의 국제표준 절차는 의무적으로 거치는 예비단계부터 승인, 출판단계로 구분되어 표준개발이 이루어지고 있으며, [표 1]과 같다.

① 예비단계(Preliminary Stage): Study period로서 선택적이나 새로운 작업분야의 NP(New Proposal)를 위해 의무적으로 거쳐야하는 단계이며, 6개월 또는 이상의 기간 동안 조사위원(rapporteur)를 선임하여, 표준개발을 위한 연구 기간을 갖는 단계이다.

② 제안단계(Proposal Stage): 새로운 표준안건을 제안하는 단계로서, 기존 분과위원회나 JTC 1에 NP(New Proposal) 제안이 가능하며, 승인되면, 즉시 분과위원회에 프로젝트가 할당되는 단계이다.

③ 준비단계(Preparatory Stage): 분과위원회 또는 작업반(Working Group)을 통해 추진되며, 분과위원회는 프로젝트 에디터를 선정하고 실제 합의를 통해 WD(Working Draft) 승인 후, CD/FCD로 진행하는 단계이다.



〔그림 1〕 ISO/IEC 27035와 제안 안건의 범위

④ 위원회단계(Committee Stage): 1차 CD(Committee Draft)등록에서 최종 국제표준안 FCD(Final Committee Draft) 등록 승인까지의 단계를 말하며, 투표로 FCD 승인 여부가 결정되면, 승인 단계로 진행된다.

⑤ 승인단계(Approval Stage): FCD가 FDIS(Final Draft International Standard)로 등록하고 FDIS 투표 후, 승인까지의 단계로서, 모든 회원국은 FDIS 투표에 대한 의무를 가지며, 문서에 대해 수정할 수 없고 승인 후, 모든 회원국에 승인을 통보 후, 출판 단계로 진행된다.

Ⅲ. SC27 WG4

현재 SC27 WG4에서는 사이버 보안, 네트워크 보안, 애플리케이션 보안, 침해 관리, 디지털 증거 등과 관련된 다양한 프로젝트가 진행 중에 있으며, 각 프로젝트의 진행 경과는 다음과 같다.

3.1. ISO/IEC 27032 GUIDELINES FOR CYBER SECURITY

사이버 보안과 관련한 용어를 정의하고 있으며, 포함하고 있는 각 주체들의 역할과 기능 및 대응 방안의 내용을 포함하고 있으며, 현재 세 번째 CD(3rd CD) 상태로 합의 하였다.

3.2. ISO/IEC 27033 NETWORK SECURITY

네트워크 보안은 6개의 멀티 파트로 나뉘어, 개발되고 있으며, ISO/IEC 27033-1(네트워크 보안 가이드라인), 27033-3(네트워크 보안 시나리오)은 FDIS(Final Draft International Standard)로 이미 표준화를 완료하였다. 27033-2(네트워크 보안 설계 및 구현 가이드라인), 27033-4 (보안게이트웨이를 이용한 보안 통신), 27033-5 (VPN을 이용한 보안 통신), 27033-6(무선 보안) 등의 프로젝트가 다루어 졌다. Part2는 FCD 상태이었지만, 표준 문서의 품질에 대한 지적이 있었다. 그러나 현 상태를 유지하고 표준의 품질을 향상시키는 것으로 합의되었다.

Part4는 문서의 구조를 수정하였으며, 3번째 WD상태로 진입하였고, Part5 Part6는 표준 문서의 구조가 합의된 상태이다.

3.3. ISO/IEC 27034 GUIDELINES FOR APPLICATION SECURITY

애플리케이션 보안을 위한 가이드라인은 Part1은 보안 개요 및 개념을 다루며, Part2 에서는 조직의 규범을 다루는 프레임워크를 다루고 있다. Part1은 FCD(Final Committee Draft)상태로, Part2는 세 번째 WD상태로 합의하였다.

3.4. ISO/IEC 27035 INFORMATION SECURITY INCIDENT MANAGEMENT

정보보호 침해관리는 침해사고 대응을 위한 구조화된 관리 방법을 명시하고 있으며, FDIS 상태로 표준화 작업을 완료하기로 합의 하였다.

Ⅳ. New Strudy Period Proposal

ISO/IEC 27035 정보보호 침해관리 표준만으로는 침해사고를 관리하는데 부족한 점을 보완해야 한다는 필요성을 주장하며, 필자는 2010년 10월 베를린 WG4 총회에서 새로운 안건으로 "Guidelines for Operation and Implementation of Computer Security Incident Response Teams(CSIRT)"을 제안하여, ISO/IEC 27035 정보보호 침해관리 표준의 에디터와 WG4 의장은 제안 안건의 중요성과 필요성을 인지하게 되었으며, WG4 총회에서 의회에서 적극적인 지지를 얻게 되었다.

ISO/IEC 27035는 3.4절에서와 같이 현재 FDIS 단계로 접어들어 수정이 불가능한 상태이기 때문에, 새로운 프로젝트로 개발을 할 것인지 또는 ISO/IEC 27035를 개정하여, 멀티 파트로 나누어 개발할 것인가를 결정하기 위해 6개월 동안 연구기간(Study Period)를 갖기로 승인하였으며, 필자를 조사위원(Rapporteur)으로 선임되어 국제 표준 추진을 위한 발판을 마련하였다.

현재 제안 안은 침해관리 운영 및 대응(Incident Management Operation and Response)이라 임시 명명되어 ISO/IEC 27035과 중복성, 그리고 타 표준들 간의 연계성 등을 연구 조사 중에 있으며, 새로운 프로젝트로 개발할 것인가 또는 멀티 파트로 개발할 것인가에 대한 타당성을 조사하고 있는 상태이다.

ISO/IEC 27035[1]는 3.4절과 같이, 침해에 대한 대

응을 구조적인 체계를 다루고 있는 반면, 제안 안건은 CSIRT(Computer Security Incident Response Teams)라는 침해 대응을 위한 구현 방법 및 운영 기법이라는 점이, 확연한 차이점을 두고 있다.

[그림 1]의 좌측은 ISO/IEC 27035에서 정의하고 있는 내용을 나타내고 있으며, 우측은 제안 사항의 일부로서, 침해 대응팀원의 자격, 역할, 책임, 침해 대응팀을 구성하는데 필요한 요소, 운영 및 대응방법, 프로세스 등을 정의하며, 아래와 같은 침해사고에 대한 대응 방법을 정의하고 있다.

- Denial of Service Incidents
- Unauthorized Access Incidents
- Malicious code Incidents
- Inappropriate Usage Incidents
- Social engineering Incidents

이 외에 SP단계로 승인된 안건은 다음과 같다.

- DIGITAL EVIDENCE READINESS AND ANALYSIS
- DIGITAL EVIDENCE VERIFICATION AND VALIDATION
- WG 4 VOCABULARY AND TERMINOLOGY STANDARD
- JOINT STUDY PERIOD WITH WG1, WG 3 AND 5 ON CLOUD COMPUTING SECURITY AND PRIVACY

V. 결 론

지난 2010년 10월 4일부터 11일까지 ISO/IEC JTC 1 SC27-IT Security Techniques- WG4 회의에서 진행되었던 프로젝트들과 필자가 제안한 안건에 대한 동향과 전망을 간략하게 살펴보았다.

ISO/IEC 27035의 부족한 부분을 보완하는 제안을 위한 자료수집 및 동향 파악의 목적에서 더 나아가 각국의 전문가 대표와 함께 1차, 2차 토론을 거쳐, 의회의 적극적인 지지를 이끌어낸 이번 제안은 국익에 부합되는 국제표준 기술을 선점하기 위한 초석을 마련했다는 점은 큰 성과라 볼 수 있다.

싱가폴, 일본, 중국, 남아프리카, 말레이시아, 네덜란드, 미국 등의 각국 대표들의 적극적인 지지를 얻어 냈지만, 향후 입장을 언제든지 변경할 수 있기 때문에 지속적인 관리가 요구되며, NWIP(New Work Item Proposal)를 제안에 앞서, 단계별 전략적 대응 계획을 준비해야 할 것으로 사료된다.

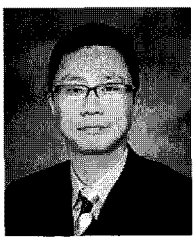
참고문헌

[1] ISO/IEC FCD 27035, "Information technology - Security techniques-Information Security Incident Management,"ISO/IEC JTC1, 2010.

[2] ISO/IEC JTC1 SC27 Standardization Activities, http://www.iso.org

[3] "국제표준화 업무 매뉴얼", 한국표준협회, 2009

〈著者紹介〉



전 상 훈 (Sang-Hoon, Jeon)
정회원

2009년 8월 : 숭실대학교 대학원 컴퓨터학과 박사 졸업
2009년 11월~7월: 전자부품연구원 통신네트워크센터 연구원
2010년 1월 현재: ISO/IEC JTC1 SC27 전문위원
2010년 8월~현재: 기획재정부 정보화담당관실 재정경제사이버안전센터 수석연구원
<관심분야> 정보보호, 침해대응, 정보보호표준화, 인증, IC카드