情 報 保 護 學 會 誌
第23卷 第3號, 2013. 6

정보보호 국제 표준화 동향 : 보안관리 표준화

오 경 희*, 김 정 덕**

요 약

보안관리 표준화 분야의 국제 표준화를 주도하고 있는 대표적인 표준화 기구로는 ISO와 ITU-T가 있다. 본 논문에서는 먼저 이 두 기구에서 보안관리를 담당하고 있는 부문과 관리하고 있는 표준을 간단히 소개하고, 2013년 4월 진행된 ISO 및 ITU-T 회의에서 논의된 보안관리 분야의 표준화 현황을 설명하고 대응 방안을 논의한다.

Ⅰ. 서 론

정보보호란 정보의 기밀성, 무결성 및 가용성을 보존하는 것으로서 때로 인증, 책임추적성, 부인봉쇄, 신뢰성 등을 포함할 수 있다.[1] 정보보호의 관리(또는 보안관리)는 조직의 정보를 안전하게 관리하기 위한 조직의 노력과 관리적, 기술적, 물리적 대책들을 포함한다.

정보보호는 조직의 거버넌스와 사회적 책임의 기본적인 구성요소의 하나다. 일반적으로 사람들은 조직이 정보보호를 구현하고 관리할 것을 기대하고 때로는 이러한 요구가 법적으로 강제된다.[2]

이러한 조직의 책임을 지원하기 위하여 여러 국제 기구에서 정보보호 관련 표준화를 진행하고 있으나, 관리 분야의 표준은 주로 ISO/IEC JTC 1/SC 27/WG 1과 ITU-T SG 17 Question 3에서 진행하고 있다.

본 논문에서는 이들 두 기구에서 다루고 있는 표준과 2013년 4월 회의에서 논의된 주요 논점을 소개하고, 이러한 표준화 동향에 대한 대응 방안을 논의한다.

Ⅱ. ITU-T 보안관리 표준화 현황

2.1. ITU-T SG17 WP1 Q3

ITU-T에서 보안관리 표준을 담당하고 있는 과제 그룹은 SG17의 WP1에 속한 Question 3이다. 축약하여 Q3/17 또는 Q3로도 불리는 이 그룹은 통신 정보보호 관리(Telecommunication information security management)를 다루고 있다.

통신 조직에 있어 정보와 지원 프로세스, 통신 시성, 네트워크 및 전송 매체는 중요한 업무 자산이다. 정보보호관리는 통신 조직이 이들 업무 자산을 적절하게 관리하고 업무 활동을 정확하게 지속하기 위해 필수적인 사항이다.[3]

이러한 이유로 ITU-T는 통신 조직을 위한 정보보호 관리 지침을 제공하기 위하여 X.1051을 개발하였으며, 이를 기반으로 하여 거버넌스, 관리 프레임워크, 위험, 사고 및 자산의 관리를 위한 상세하고 구체적인 권고들을 개발하고 있다. 또한 클라우드 컴퓨팅, IPv4에서 IPv6로의 전환, 개인식별정보 등의 관리와 같은 새로운 전세계적 대책의 관리에 관련된 사항들 역시 Q3의 연구 범위에 포함하여 고려하고 있다.

Q3는 이 과정에서 ITU-T의 관련 기술 과제 그룹 뿐만 아니라 ISO/IEC JTC1의 여러 부문과 긴밀하게 협력하고 있다.

Q3 : 통신 정보보안 관리는 정보 보안 관리 영역을 책임맡고 있으며, Q3의 라포처(Rapporteur)는 일본의 Miho Naganuma가, 부라포처(Associated rapporteur)는 한국의 오 경희가 맡고 있다.

2.2 Q3가 관리하는 표준

2013년 현재 이 그룹이 책임지고 있는 권고 및 부록

* TCA 서비스 대표 (khoh@tcaservices.kr)
** 중앙대학교 정보시스템학과 정교수 (jdkimcau@gmail.com)

에는 X.1051, X.1052, X.1054, X.1055, X.1056, X.1057, X.Suppl.13, 및 E.409(SG 2와 공동)가 있으며, 현재 개발 중인 지침에는 X.gpim, X.sgsm, 및 X.sup1056이 있다. 또한 이번 회의에서 X.1051의 개정이 결의되어 차기 회의부터 진행될 예정이다.[3]

2.2.1 Q3의 권고 분석

Q3의 권고(Recommendations)는 다음과 같다.

- X.1051 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- Supplement: User's Guide of X.1051
- X.1052 Information security management framework
- X.1054 Governance of information security
- X.1055 Risk management and risk profile guidelines for telecommunication organizations
- X.1056 Security incident management guidelines for telecommunications organizations
- X.1057 Asset management guidelines in telecommunication organizations

2.2.2 현재 개발 중인 문서

현재 개발되고 있는 문서는 다음과 같다.

- X.sgsm: Security management guidelines for small and medium-sized telecommunication organizations
- X.gpim: Guideline for management of personally identifiable information for telecommunication organizations
- X.1051-rev: Revision work of X.1051
- Supplement of X.1056: Related Recommendations, International Standards and documents for security incident management

2.2.3 ISO/IEC JTC1 SC 27와의 협력

Q3에서 ITU-T에서 ISO/IEC JTC1 SC 27과 긴밀하게 협력하고 있는 사항은 다음과 같다.

- ISO/IEC 27009: The use and application of ISO/IEC 27001 for sector/service-specific Third-Party accredited certifications
- ISO/IEC 19515:Code of practice for protection of personally identifiable information

2.3 4월 회의 논의 사항

2013년 1차 ITU-T SG 17 회의는 스위스 제네바의 ITU-T 본부에서 4월 17일에서 26일까지 진행되었다. 또한 4월 22일 및 23일에는 프랑스 안티폴리스에서 ISO와 합동회의를 진행하였다.

당 회의에서는 15개 기고서 및 35개 임시 문서를 검토하여 다음과 같은 결과를 도출하였다.[4]

2.3.1 X.1051 (ISO/IEC 27011)

X.1051이 참조하고 있는 ISO/IEC 27002이 2013년 말 경 개정될 것이 확실시 됨에 따라, X.1051 및 이에 관련된 X.sgsm의 개정 필요성 및 X.sgsm의 저작권 문제가 논의되었다. Q3는 X.1051이 참조하고 있는 ISO/IEC 27002의 FDIS 버전이 확정된 후 차기 SG17 회의부터 SC27과 협력하여 개정작업을 개시하기로 결의하였다.

또한 한국의 오 경희와 일본의 Wataru Senga를 X.1051의 에디터로 임명하였다.

2.3.2 X.sgsm

X.sgsm에 대한 일본 KDDI 기고를 검토하였으며 현재의 X.sgsm 텍스트를 변경하기로 결정하였다. 그러나 X.sgsm 텍스트는 X.1051 개정안과 일치해야 하므로 상세 사항은 X.1051 개정이 개시되는 다음 SG 17 회의에서 논의하기로 하였다. 일본의 Wataru Senga를 X.sgsm의 에디터로 선임하였다.

2.3.3 ISO/IEC 27009와의 협력 작업

ISO/IEC JTC1 SC27에서 ISO/IEC 27009 (The use and application of ISO/IEC 27001 for sector/service-specific Third-Party accredited certifications)

에 관한 신규 작업을 제안함으로써 이의 논의를 위해 4월 22일 및 23일에 걸쳐 합동 회의를 진행하였다.

이 회의에서는 해당 표준의 개발을 위한 협력 방안을 논의하였고, 인증은 ITU-T의 업무범위가 아니지만 정보보호관리체계 표준과 긴밀한 연관이 있으므로 지속적인 협력 필요성에 합의하고 SC27/WG1의 검토 주기에 따라 이 프로젝트의 개발에 능동적으로 공헌하기로 하였다. SC27/WG1은 이 표준의 개발 회의에 Q3/17 전문가가 참여할 것을 요청하였으며 이에 따라 한국의 염흥렬 교수가 이 역할을 수임하였다.

2.3.4 X.cc-control (ISO/IEC 27017)

이 표준은 Q8을 지원하기 위한 것이므로 이에 관한 사항은 클라우드 표준화 현황에서 논한다.

2.3.5 X.gpim (ISO/IEC 29151)

이 표준은 Q10와 함께 진행하고 있으므로 이에 관한 사항은 개인정보보호 표준화 현황에서 논한다.

2.3.6 신규 권고 초안

러시아 연방에서는 “Extended level of information security of network operators”를 신규 표준화 항목으로 제안하였다. 이 제안을 검토하고 범위를 논의한 결과, 일부 용어의 모호함이 있으나 1차 초안을 수취한 후 이를 논의하기로 하고 신규 작업 항목으로 채택하였다.

부탄에서는 SG17에 “Implementing Information Management and Security Policy RGoB”를 신규 표준화 항목으로 제안하였다. Q3는 이 제안이 포함하는 활동이 Q3 업무 범위에 포함된다고 판단하고 차기 회의에서 논의할 수 있도록 부탄에 추가적인 기고를 요청하였다.

이란에서는 신규 표준화 항목으로서 “Telecommunication information security management” 및 “Security aspects of information assets in telecommunication systems”의 2개 항목을 제안하였고, Q3는 이러한 내용은 이미 X.1055 및 X.1057에서 다루고 있다고 판단하였다. 그러나 제안자가 회의에 참가하지 않아 이에 대한 논의는 차기 회의로 미루어졌다.

2.3.7 향후 계획

이번 연구 기간에는 신규 표준인 X.sgsm의 최종안을 개발하고 승인할 예정이다. 또한 X.gpim 최종안은 2015년, Supplement of X.1056은 2014년 까지 개발할 예정이다. Supplement of X.1056은 개발도상국을 위해 X.1056 보안사고 관리 지침과 관련 국제 표준, 권고 및 기타 문서와의 사상(mapping)을 제공하기 위한 것이다.

또한 WTSA-08 Resolution 15에 대한 지원 활동으로서 Q4 및 Q22/ITU-D와의 협력을 지속하고, CIRT 수립을 위한 적절한 현안 연구 및 X.1056 (Security incident management for telecommunication organizations)에 따른 핸드북을 제공할 것이다.

또한 PII 관리와 그 관리에 대한 신뢰를 제공하기 위한 공통 기반을 제공하기 위하여 Guideline for management of personally identifiable information을 개발할 것이다. 단 여기에는 PII의 보호를 위한 관리체계를 포함하지 않는다.

차기 회의는 8월 26일에서 9월 4일까지 스위스 제네바에서 개최될 예정이다.

Ⅲ. ISO 보안관리 표준화 현황

3.1 ISO/IEC JTC1 SC27 WG1

ISO에서 보안 및 프라이버시 표준을 다루는 특별위원회(Special Committee)는 IEC와 함께 수립한 공동기술위원회 1(Joint Technical Committee 1) 산하의 SC 27이다. 보안관리 표준은 SC 27 산하의 작업반 1(Working Group 1)이며 WG1의 의장은 영국의 Edward Humphreys가 맡고 있다. SC 27의 주제 영역과 담당 작업반을 도시한 [그림 1][1]에서 보듯[5] WG1에서는 일차적으로 정보보호 관리체계(ISMS) 관련 요구사항, 방법, 절차를 다루며, 이러한 관리체계에서 사용하는 보안 통제, 실무규약, 프레임워크에 관한 표준을 다룬다. 또한 관리체계를 위한 승인, 증명, 감사 요구사

1) ⓒ copyright ISO/IEC JTC 1/SC 27, 2012. 이 그림은 SC27의 공식 문서로서 오직 SC 27 표준의 인식제고 및 촉진을 목적으로 배포하는 것임. 따라서 상업적 목적이나 이익을 위해 사용할 수 없음. 이 그림을 변경하거나 다른 문서/자료에 포함시키고자 하는 경우 ISO/IEC JTC 1/SC27 Secretariat (krystyna. passia@din.de)의 사전 허가를 요함.

항 및 방법에 관한 표준을 포함한다.

WG1은 또한 정보보호의 거버넌스 측면 및 경제적 측면을 다룬다. 프라이버시에 관한 거버넌스 및 경제적 측면은 WG5에서 다룬다.

3.2 WG1 관리 표준

WG1이 다루는 표준은 다양한 형태로 존재하는 정보의 보안에 관한 것이다. 이러한 정보에는 종이로 출력, 기록되거나, 전자적으로 저장되거나, 우편 또는 전자적 수단으로 운송되거나, 필름으로 보여지는 정보 및 대화 중의 정보를 포함한다. 또한 보안의 실패로 인해 발생하는 피해를 제한하기 위한 메커니즘 역시 대상이 된다.[2]

WG1의 표준은 크게 ISMS 관련 표준인 유형 A와 분야별 표준인 유형 B의 2가지 유형으로 분류할 수 있다. ISMS 관련 표준인 유형 A에는 용어표준인 27000, 요구사항 표준인 27001, 27006, 27009가 포함되며 ISMS 관련 지침인 27002, 27003, 27004, 27005, 27007, 27008이 포함된다. 분야별 표준인 유형 B에는 27010, 27011(X.1051), 27013, 27014, 27015, 27016, 27017이 포함된다.[6]

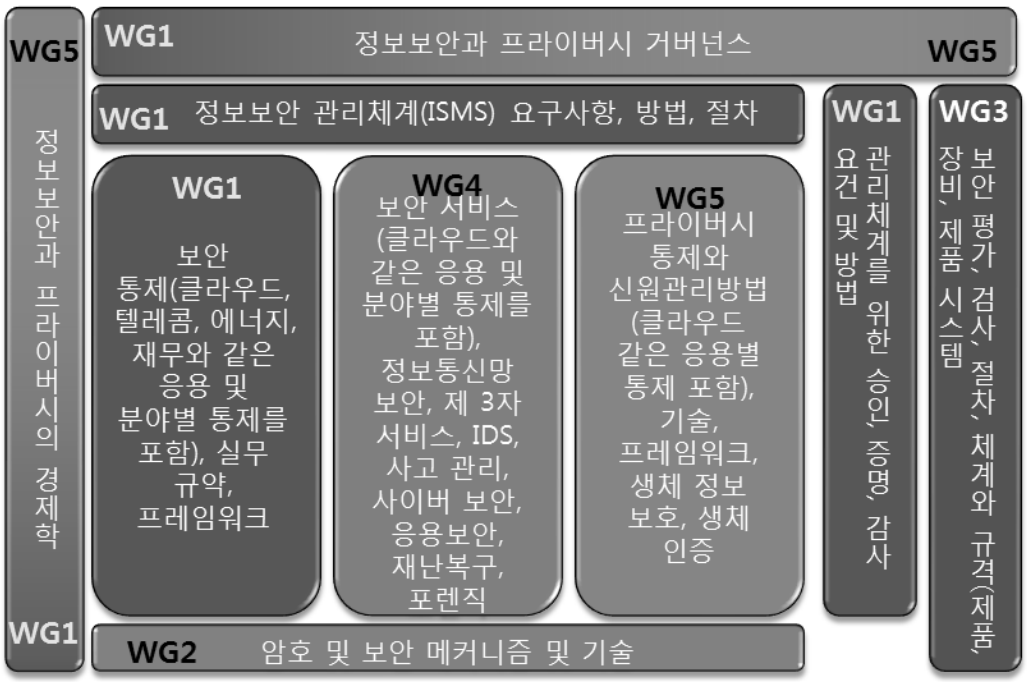
3.3 4월 회의 논의 사항

2013년 1차 ISO/IEC JTC 1/SC 27/WG 1회의는 프랑스 안티폴리스의 ETSI에서 4월 22일에서 26일까지 진행되었다. 이 회의의 결과는 다음과 같다.[7]

3.3.1 ISO/IEC 27000

지난 회의에서는 용어표준인 ISO/IEC 27000 : ISMS-Overview and vocabulary에 곧 개정될 27001 및 27002에서 사용될 용어를 포함하기 위하여 ISO/IEC 27000의 신속 개정을 위한 신규 작업 제안을 투표에 붙이기로 결의하였다. 이에 따라 2013년 4월 국가 투표가 이루어 졌고 그 결과 개정이 결의되어 이번 회의에서는 1차 CD 문서 초안에 대한 의견을 검토하였다. 또한 27000 표준을 27001/2와 연계하기 위한 수정방안에 대한 연구가 이루어졌으며, 관련 작업으로서 Vocabulary Editing Document 역시 6월 7일까지 개정하기로 하였다.

회의 결과 5월 10일까지 개정본을 작성하고 DIS 투표에 회부하기로 결의하였다.



〔그림 1〕 ISO/IEC JTC 1/SC 27 보안 및 프라이버시 주제 영역

3.3.2 ISO/IEC 27001

ISO/IEC 27001 : ISMS - Requirement은 지난 회의에서 만들어진 DIS 문서로서 4월 투표 결과 22개국 찬성, 6개국 반대로 DIS로 승인되었다. 본 회의에서는 반대 6개국의 코멘트에 대한 해결방안을 중점적으로 논의하였다. 대부분의 코멘트는 해결되었으나 Statement of Applicability에 대해서는 에디터가 안을 마련하기로 하였다.

이 결과를 기초로 5월 20일까지 개정본을 작성하고 FDIS 투표에 회부하기로 의결하였다.

3.3.3 ISO/IEC 27002

ISO/IEC 27002: Code of practice for information security controls 역시 지난 회의에서 만들어진 DIS 문서로서 투표 결과 DIS로 승인되었으나 다수의 코멘트가 제시되어 이번 회의에서 변경된 사항이 많아 전체적인 문서가 안정되지 못한 상황이다.

이번 회의 결과를 기초로 5월 20일까지 개정본을 작성하고 FDIS 투표에 회부하기로 결의하였다.

3.3.4 ISO/IEC 27003

ISO/IEC 27003 - ISMS Implementation Guidance는 지난 회의에서 early revision 신규 작업 제안에 대한 투표가 결의되었으며 투표 결과 개정 작업이 개시되었다.

이번 회의에서는 개발방안이 주로 논의되어 5월 31일까지 WD를 개발, 각국의 코멘트를 받기로 하였다.

3.3.5 ISO/IEC 27004

ISO/IEC 27004 : ISM- Measurements는 지난 회의에서 결의된 바 대로 개정작업의 방향, 범위, 포맷 등에 대한 16개의 질문을 각 국에 배포하였고 이번 회의에서는 그 회신 결과를 바탕으로 작성한 WD를 검토하였다.

측정 모델로서는 ISO/IEC 15939: 2007을 따르기로 하고 영국에서 제안한 tool-box 접근 방법에 따라 27001 프로세스의 효과성과 정보보호 프로그램의 효과성을 함께 측정하기로 하였다.

이 회의 결과를 기초로 5월 31일까지 1st WD를 작성하고 각국의 코멘트를 받기로 하였다.

3.3.6 ISO/IEC 27006

ISO/IEC DIS 27006 : Requirements for bodies providing audit and certification of ISMS는 이번 회의에서 2차 WD에 대한 코멘트를 검토하였다. 이 결과에 따라 5월 20일까지 3차 WD를 개발하고 각국의 코멘트를 받기로 하였다.

3.3.7 ISO/IEC 27009

ISO/IEC 27009 : Use of ISO/IEC 27001 for Sector-Service Specific Third Party Accredited Certifications은 지난 NWIP 투표를 통과하여 신규 표준으로 개발이 개시되었다. 한국의 박 태완 대표를 비롯하여 Eisaku Takeda, Angelika Plate가 에디터로 임명되었다.

본 회의에서는 표준 제목 변경, 문서 구조 등을 논의하였으나 이견이 많아 합의가 이루어지지 않았으며 최종 WG1 Plenary에서 프로젝트 제목의 변경을 결정하고자 하였으나 회원국의 동의가 부족하여 의결 자체가 취소되었다. 5월 20일까지 WD를 개발하고 9월 13일까지 코멘트를 받기로 결정하였다.

3.3.8 ISO/IEC 27011

ISO/IEC 27011 : ISM guidelines for telecommunications organizations based on ISO/IEC 27002는 ITU-T와 공동 개발하는 문서로서 이번 회의에서 개정이 결의되었으며, Brian O''Toole, 오 경희, Wataru Senga가 에디터로 임명되었다.

3.3.9 ISO/IEC 27014

한국의 김 정덕 교수와 Kei Harada가 에디터를 맡은 ISO/IEC 27014 : Information Security Governance가 5월 1일 국제표준으로 발간되었으며 ITU-T에서도 X.1054로 동시에 출간하게 되었다.

3.3.10 ISO/IEC 27016

ISO/IEC 27016 : Information Security Management-Organizational Economics은 PDTR 문서에 대한 코멘트를 검토하고 이 결과를 기초로 5월 20일까지 개정본을 작성하고 DTR 투표에 회부하기로 의결하였다.

3.3.11 ISO/IEC 27017

ISO/IEC 27017 : ISM- Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002는 클라우드 표준화 현황에서 논한다.

3.3.12 신규 표준 제안 투표

2012년부터 1년간 진행된 International Certification of Information Security Management Specialists에 관한 study period가 종료되고 본 회의의 결과로 신규 표준 제안을 위한 국가 투표를 진행하기로 하였다. 현장 투표 결과를 보면 최종 통과 가능성이 높아 잠정적으로 27021 표준번호가 논의되고 있다. 또한 에디터로는 오경희, Yonosuke Harada, Andreas Fuchsberger가 임명되었다.

기타 ISO/IEC 27005 : Information security risk management에 대한 2차 개정 및 ISO/IEC 27013 : Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1에 대한 1차 개정안을 투표에 회부하기로 하였다.

3.4 향후 일정

ISO/IEC JTC 1/SC 27 차기 회의는 10월 21일에서 25일까지 인천 송도에서 개최될 예정이다. 또한 25일 오후에는 “Applying SC 27 Standards to Cyber World”라는 제목으로 SC 27 Business Workshop을 개최하기로 결정되었다.

Ⅳ. 결론: 정보보호관리 국제 표준화 대응 방안

지금까지 살펴본 바와 같이 다양한 보안관리 표준이 존재하며 보안관리 분야에서 한국의 에디터 참여 등 참여자의 개인적 기여도는 매우 높은 편이지만 이러한 표준들의 국내 기관 또는 산업과의 연계나 활용도는 충분하지 못하다.

이러한 연계 부족은 여러 측면에서의 위험 또는 기회 상실로 나타날 수 있다. 개정이 머지않은 ISO/ IEC 27001의 경우 선진적 관리 개념을 도입하고 있지만 표준 문안에 대한 해석이 각 국의 상황에 따라 다양해 질 수 있다는 우려가 나타나고 있다. 그러나 국내에서는 ISMS에 대해 직접적 이해관계나 실행력을 가진 기관의 참여가 저조한 형편이어서 이러한 국제 동향과는 차이나 오해가 발생할 수 있다.

필자가 에디터로 참여하고 있는 ISO 정보보호 전문가 인증 기준의 경우 기존 국내 정보보호 전문자격은 국제 표준의 요구수준을 만족하지 못하는 것으로 판단된다. 표준 개발에 2~3년이 걸리므로 이 기간 동안 국내 제도의 변경 또는 개발을 통해 국내 자격의 국제 표준 인증을 준비하는 것이 바람직할 것이다. 이런 측면에서 실행력 있는 기관의 참여가 필요하다.

에디터는 중립적 입장에서 각국의 의견을 종합하여 표준을 개발해야 하며 그 방향이나 의사결정은 실제 회의에 참가한 국가 대표의 의견 개진과 투표를 통해 이루어지므로 국내 상황을 반영하기 위해서는 에디터 외에 의견개진을 위한 인력 참여가 필수적이다. 실제 일본의 경우 중요 표준에 대해서는 다수의 인력이 참여하여 상호 지원함으로써 언어적 문제를 극복하고 국가 이익을 관철하기 위해 노력하고 있다.

ISO에서는 그 전 회의에서 논의된 사항을 재론할 경우 더 충실한 근거를 요구하고, ITU-T에서는 기고를 하더라도 불참하는 경우 그 기고에 대한 논의를 연기하므로 제안을 관철시키기 위해서는 직접적이고 지속적인 참여가 필요하다. 특히 과제 제안이 채택된 후 참여가 저조한 경우 국가 이미지에 영향을 미칠 수 있으므로 유의할 필요가 있다.

한편 본문에 소개하지는 않았지만 이번 ISO 회의에서는 미국의 주도로 SC27의 모든 작업반 뿐만 아니라 SC2, SC 6, 그리고 ITU-T, ETSI, ISACA, VISA/ MASTERCARD가 참여하는 “PKI Policy/ Practices/ Audit”에 관한 Study preiod를 개시하기로 하였고 이를 수행하기 위한 연구 그룹이 수립되었다.[8] 국내에서도 PKI가 여러 가지로 현안이 되고 있지만 ISO나 ITU-T

의 PKI 분야에 대한 담당 기관의 참가가 미흡하여 적절한 대응이 우려된다.

이러한 현안의 해결을 위해서는 담당기관의 직접 참여가 필수적이며, 국내의 직간접적 이해당사자들의 의견을 수렴할 수 있는 저변 확대 및 활성화가 필요하다.

특히 차기 ISO SC27 회의는 국내에서 개최되므로 개최국의 의견이 쉽게 반영될 수 있다. 이러한 기회를 활용하기 위해서 많은 보안관리 전문가의 적극적 참여가 필요할 것이다.

참고문헌

[1] N11903, Information technology - Security techniques - Information security management systems - Overview and vocabulary, 2nd edition, ISO, Dec. 2012.

[2] N11102_WG1_SD1_WG1_Roadmap, ISO, June 2012.

[3] http://www.itu.int/en/ITU-T/studygroup s/2013-2016/17/Pages/q3.aspx

[4] TD 0036 Rev.3 Q3/17 Meeting report, ITU-T, 26 April 2013

[5] Corporate presentation of ISO/IEC JTC 1/SC 27, Feb. 2013

[6] Session 3-1 ISO WG1 ISMS Starndards, E. Humphreys, *ETSI - ISO/IEC JTC 1/SC 27 SECURITY WORKSHOP*, 26, April 2013.

[7] N12440 Resolutions of the 46th SC 27 WG 1 Plenary Meeting held in Sophia Antipolis, France, ISO, 26, April, 2013.

[8] N122333, Joint SC27 WG Study Period Meeting on PKI Policy/Practices/Audit, ISO, 23, April 2013.

〈著者紹介〉

오 경 희 (Kyeong Hee Oh)
1988년 8월 : 서강대학교 전산과 학사
1992년 2월 : KAIST 전산과 석사
현재 : TCA 서비스 대표
<관심분야> 정보보호관리, 감사, PKI

김 정 덕 (Jungduk Kim)
1986년 2월 : South Carolina niv. MBA
1990년 2월 : Texas A&M Univ 박사
현재 : 중앙대학교 정보시스템학과 정교수
<관심분야> 정보보호관리, 거버넌스, 평가