情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

정보보호관리 국제표준화 동향

김 정 덕*

요 약

정보보호관리 표준은 ISO/IEC JTC1/SC27 WG1에서 주도적으로 진행하고 있으며, ITU-T SG17 Q.3에서는 SC27과의 긴밀한 협력 관계를 유지하면서 정보통신조직에 특화된 정보보호관리 표준에 치중하고 있다. 현재 제정된 정보보호관리 국제표준으로는 정보보호관리체계에 관한 요구사항 (27001) 및 통제표준 (27002)과 이와 관련된 지침 성격 표준들이 상당 부분 국제표준으로 발표되었다. 최근에는 기 발표된 국제표준에 대한 개정 작업과 정보통신조직, 금융조직 등 특정 산업이나 정보보호 거버넌스 등 특정 이슈에 해당되는 정보보호관리 표준 제정 작업이 한창 진행 중에 있다. 인터넷의 확산과 정보화의 역기능 증가에 따라 능동적인 정보보호관리체계의 수립을 위하여, 국내에서도 정보보호관리 표준의 제정 과정에 적극적으로 참여할 뿐 아니라 국내 많은 조직에서 정보보호관리 표준이 적용되어 전반적인 정보보호관리 수준이 향상될 수 있도록 할 필요가 있다.

Ⅰ. 서 론

최근 전 세계적으로 스마트, 모바일, 클라우드 등 새로운 형태의 컴퓨팅 환경이 등장함에 따라 역기능 또한 증가하고 있어 사회 각 분야에서 정보보호에 대한 관심이 고조되고 있다. 이러한 역기능에 의한 피해는 작게는 개인 및 조직에 대한 부정적 영향뿐만 아니라 심각한 국가, 사회문제로까지 확대되고 있다. 이러한 새로운 보안 위협의 증가에 따라 개별적이고 기술 중심의 단편적인 정보보호관리로는 한계가 있으며, 지속적이며 통합적 접근방법으로 보안이슈를 다루고자 하는 정보보호관리체계가 요구되고 있다. 이를 위한 정보보호관리체계의 표준화 또한 국내외적으로 활발히 진행되고 있다. 본 논문에서는 ISO/IEC와 ITU-T 등 국제 표준화 기구의 정보보호관리 표준을 살펴봄으로써 정보보호관리 국제표준의 현황과 전망을 파악해보고자 한다.

Ⅱ. JTC1 SC27 정보보호관리 표준화

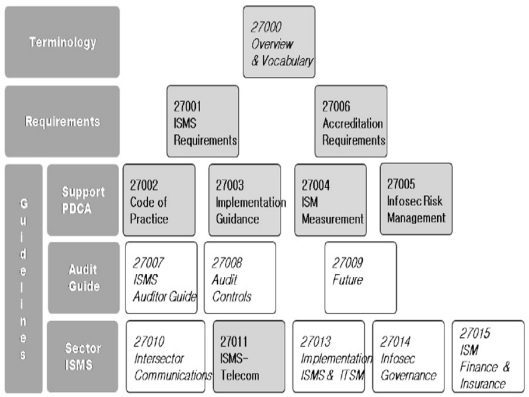
2.1. SC27 정보보호관리 국제표준화 구조

국제적인 정보보호 관련 표준화 기구 중 가장 대표적인 그룹이 ISO/IEC JTC1 SC27이다. SC27은 관련 기술이 복잡해지고, 범위가 넓어지면서 ISO와 IEC의 표준화 활동이 중복되는 경향이 생기게 되어 중복 투자를 줄이고 보다 나은 결과를 도출하기 위해 연합으로 조직된 JTC1에서 안전성 평가 및 감사 기술 분야를 포함하여 정보보호 기술 전반에 대한 표준화를 수행하기 위해 1989년 6월 JTC1 총회에서 새롭게 구성되었다.

현재 JTC1 SC27 (Information Technology, Security Techniques)은 5개 작업그룹(WG; Working Group)으로 구성되어 각각 정보보호 관리 및 기술 표준화를 담당하고 있으며, 정보보호관리 표준화는 WG1에서 진행 중이다.

WG1 (Requirements, security services and guidelines)에서는 정보보호관리체계(ISMS: information security management system) 관련 표준화를 ISO/IEC 27000 시리즈로 명명하여 작업 중에 있다. 현재 개발되었거나 개발 중인 27000 패밀리 국제표준화 프로젝트는 다음과 같이 구분할 수 있다([그림 1] 참조). 전체 27000 패밀리 표준의 개관 및 주요 용어를 정의하고 있는 27000, 2) ISMS 구현과 ISMS 인증기관에 대한 요구사항을 명시한 27001과 27006, 3) 27001에서 규정하고 있는 정보보호관리과정을 실현시키기 위해 필요한

* 중앙대학교 정보시스템학과 교수 (jdkimsac@cau.ac.kr)



〔그림 1〕 ISO/IEC 27001 국제표준 패밀리 구조

통제사항 및 관련 지침을 포함하는 27002, 27003, 27004, 27005, 4) ISMS 감리를 위한 27007, 27008, 5) 섹터별 정보보호관리 이슈에 대한 표준으로 27010, 27011, 27013, 27014, 27015 등이 개발 중에 있으며 클라우드 컴퓨팅 보안관리 등 새로운 이슈에 대응하는 신규 표준들이 지속적으로 개발될 예정이다.

2.2. SC27 WG1 정보보호관리 표준화 동향

2010년 10월에 개최된 41차 SC27 WG1 베를린 회의의 결과를 요약하면 다음과 같다.

(1) ISO/IEC 27000: 27000 패밀리 표준을 위한 주요 63개 용어 정의 및 전체 구조를 보여주는 문서로 2009년에 국제표준으로 발표되었다. 현재는 WG4의 작업내용을 포함하고 새롭게 개정된 ISO Guide 73 등 새로운 용어 정의의 필요성이 있어 개정 작업 중에 있다. WG4 표준화 프로젝트와의 일관성을 유지하기 위해 WG4에서 Study Period를 가지기로 하였다. 폴란드의 Elzbieta와 스웨덴의 Anders가 editors로 활동하고 있다.

(2) ISO/IEC 27001: ISMS의 요구사항을 포함하는 가장 중요한 문서로서 2005년도에 국제표준으로 발표되었지만, 현재는 새로운 요구사항을 반영하기 위해 개정작업 중에 있다. 2011년 3월 현재 4th WD 문서 상태이다. 회의에서는 정보보호 통제를 수록한 부록(Normative Annex)을 유지할 지 아니면 폐지할 지에 대해 논란이 있었으며, 최종 결론은 부록을 유지하기로 결정하였다. 또한 ISO/TMB JTCG 작업반(TF 1: 구조, TF3: 용어정의)의 중간결과물인 공통경영시스템표준(Common Management System Standard: CMSS)문서의 공통적인 main/sub-clause 제목 (1. Context of Organization, 2. Leadership 3. Planning, 4. Support, 5. Operations, 6. Performance Evaluation, 7. Improvement)에 따라 27001 수정 작업을 진행하기로 최종 결정하였다. 4th WD는 새로운 구조로 재 작업된 문서이다.

(3) ISO/IEC 27002: 정보보호 통제/실무규정을 포함하는 문서로서 역시 2005년도에 국제표준으로 발표되었지만, 현재는 개정작업 중에 있다. 2011년 3월 현재, 3rd WD 문서로 앞으로도 참가국의 가장 높은 관심과 가장 많은 기고문이 예상된다. 지난 회의에서도 약 800여개의 코멘트를 회의기간 중 처리하지 못하여 회의 종료 후 전자회의 등을 통해 처리할 정도이다. 문서 제목도 과거의 정보보호관리 (Management)실무규약(Code of Practice)에서 정보보호통제 (Control) 실무규약으로 변경하였다.

(4) ISO/IEC 27005: 정보보호 위험관리에 대한 과정을 전반적인 위험관리 과정에 기초하되 정보보호의 특성을 고려하여 작성된 문서로서 2008년도에 국제표준으로 발표되었지만, 현재는 ISO 31000, Guide 73이 개정됨에 따라 27005의 개정작업 중에 있으며 Fast track으로 작업을 진행하기로 결정되었다. 따라서 현재 FCD 문서인 27005를 Final DIS/DTR 투표를 위해 회람 중에 있다.

(5) ISO/IEC 27007: ISMS 심사시 사용할 수 있는 지침 성격의 문서로 ISO 19011과 17021-1의 내용을 ISMS 환경에 적합하도록 수정한 3rd CD 문서이다. 매우 안정된 상태이며 따라서 final CD로 등록하고 투표에 회부 중에 있다. 2012년에는 국제표준으로 발표될 예정이다.

(6) ISO/IEC 27008: ISMS 통제 구현 여부에 대한 기술적 평가를 위한 Technical Report로서 ISMS 심사인이 사용할 수 있는 지침이다. Anders Carlstedt (스웨덴)이 편집인으로 현재 PDTR 상태이며 Final DIS/DTR 투표를 위해 회람 중에 있다. 문서 제목을 Guidelines for auditors on information security controls 로 수정하였다.

(7) ISO/IEC 27010: 주요 정보통신시설을 운영하는 산업간 그리고 조직간 침해사고 정보 등 민감한 정보(Sensitive Information)를 공유할 수 있는 신뢰 구조

(TICE: Trusted Information Communication Entity)의 구축 등을 주요 내용을 다루고 있다. 섹터간의 보안정보(위험지식, 배포 및 유통, 모니터링 등)를 교환, 공유할 경우 적용될 요구사항과 통제를 포함하고 있다. 27001에서의 요구사항 외에 추가적인 요구사항을 규정하고 있으며 27002에서의 보안통제외에 추가적인 통제를 규정하고 있다. 현재 1st CD 상태이다.

(8) ISO/IEC 27013: ITSM과 ISMS을 통합해서 개발할 경우에 적용되는 문서로 영국 BSI에서 "ISMS for Service Sector: Integrated Implementation of ISO 20000-1 and ISO27001"을 제안하여 지난 레드몬드 회의에서 새로운 프로젝트로 결정되었고 현재 2nd WD 상태이다. 주요 내용은 상호 관련이 있는 두 개의 경영시스템을 통합해서 구현할 경우의 이로운 점, 계획 수립, 기타 충고사항 등을 포함하고 있다. editor로 영국의 Bridget Kenyon이 활동 중에 있다.

(9) ISO/IEC 27014: 정보보호의 효과적인 구현을 위해 최고경영층의 정보보호에 대한 전략과 통제체계를 규정하고 있는 정보보호 거버넌스에 관한 표준으로서 현재 1st CD 상태인 문서이다. ISMS는는 주로 정보보호를 실행하는 측면에서 계획, 구현, 평가 등 정보보호 담당자 또는 정보보호 관리자가 참조할 수 있는 프로세스를 제시하고 있는 반면, 27014는 비즈니스와 정보보호와의 연계성 및 가치 전달을 위해 ISMS를 적절히 지휘 및 통제할 수 있는 원칙, 과정, 활동 등을 포함하고 있다. Editor로 김정덕 (한국, 중앙대), Kei Harade (일본, IPA)가 활동하고 있다. 이 표준은 SC27과 ITU-T SG17에서 공동으로 진행하고 있다.

(10) ISO/IEC 27015: 미국 ANSI에서 제안하였고 주도하고 있는 금융서비스 조직의 정보보호관리에 관한 문서로 법적인 측면, 추가적인 구현 지침, 추가적 통제항목 등을 포함하고 있는 문서이다. 현재 2nd WD이며 27001과 27002 외에 추가적인 요구사항과 통제를 포함할 예정이다. 룩셈부르크의 Benoit Poletti와 David Prendergast가 편집인으로 결정되었고 editor와 NB로부터 적극적인 기고문 작성이 필요하다.

(11) ISO/IEC 27016: 경제학적 관점에서 정보보호관리 제반 이슈 (ISM-Organizational Economics)에 관한 지침으로서 지난 베를린 회의에서 신규 프로젝트로 결정되었다. 현재 1st WD 문서로 보안통제평가, 위험평가, 보안측정 등에서의 경제학적 의미와 접근방법을 보여주고 있으며, ROI 등 정보보호 경제모델을 제시하고 있다.

(12) 예상 신 프로젝트 - 클라우드 보안 및 프라이버시: 베를린 회의에서 일본의 주도로 관련 국제표준 동향 등 발표가 있었고 최종적으로 WG 1, 4, 5와 공동으로 국제표준화를 위한 Study Period를 통해 새로운 프로젝트로 상정될 가능성이 높다.

III. ITU-T SG17의 정보보호관리 표준화

3.1. ITU-T SG17 Q.3 정보보호관리 표준화 구조

정보통신 정보보호 국제표준을 처리하는 SG17의 Q. 3에서는 정보통신조직을 위한 정보보호관리 관련 표준을 개발하고 있다. 2011년 3월 현재 다음과 같은 3개의 국제표준이 발표되었다: 1) X.1051 (information security management guideline for telecommunication organizations, editor: Koji Nakao, 일본), 2) X.1055 (information security risk management and profile for telecommunication organizations, editor: Ted Humphrey, 영국), 3) X.1056 (information security incident management for telecommunication organizations, editor: 김정덕, 한국).

현재 주요 참가국은 일본, 한국, 중국, 러시아, 벨기에, 프랑스 등 약 7 ~ 8 개 국가에서 10명 내외의 전문가가 참여하고 있다.

3.2. SG17 Q.3 정보보호관리 표준화 동향

현재 진행 중인 표준화 프로젝트는 X.isgf (information security governance framework, editor: 김정덕, 한국), X.ismf (information security management framework, editor: Chen, 중국), X. amg (Asset management guidelines in telecommunication organizations, editor: 이진태, 정태인, 한국), X.sgsm (Information security management guidelines for small and medium-sized telecommunication organizations, Wataru Senga, 장항배, 정정윤) 등 4개 프로젝트가 진행 중이며 신규 프로젝트로서 1) 클라우드 보안관리, 2) IPv6에서의 보안관리, 3) X.1051 사용자 지침, 4) 개도국 CIRT 보안 핸드북 등 4개 항목이 지난 일본에서 개최된 Q.3

임시회의에서 승인되어 진행될 예정이다.

특히 X.isgf 와 클라우드 보안관리는 JTC1 SC27과 공동작업으로 진행되고 있다는 점을 주목할 필요가 있다.

X.amg와 X.ismf는 2011.4월에 국가별 의견수렴(Consent)으로 승인될 예정이며, X.sgsm은 2011.8월에 Consent를 추진 예정으로 작업 중에 있다. X.isgf는 2012년에 국제표준으로 최종 결정(determination)될 예정이다.

IV. 결 론

본 논문에서는 JTC1 SC27과 ITU-T SG17 에서의 정보보호관리 표준화 현황 및 전망을 간략히 살펴보았다. ISO의 정보보호관리 표준은 ISMS 관련 표준개발이 안정화 단계에 진입했다고 요약할 수 있다. 즉 ISMS 관련 주요 표준은 이미 국제표준으로 개발되었거나 개정 중이며, 신규 이슈를 반영하기 위한 섹터별 표준이 지속적으로 개발 중에 있다. ITU-T에서의 보안관리 표준화 활동은 SC27과 비교할 때 상대적으로 활발하게 진행되고 있다고 볼 수 없으나, 정보통신조직에 필요한 이슈들이 최근 많이 반영되어 개발 중에 있다.

정보보호관리는 증가하는 보안사고정보보호 역기능에 능동적으로 대처하고, 기업간 거래의 신뢰성을 확보하기 위한 기반으로 그 중요성이 날로 증가하고 있음에도 불구하고, 한국의 국제표준화 회의에서의 공헌은 만족할 만한 수준이라고 말할 수 없다. 국내 관련 전문가들의 적극적 참여와 더불어 관련 부처에서의 지원이 필요하다. 또한 국제표준화 노력이 활성화되기 위해서는 국내 표준화 활동이 뒷받침되어야 할 것이다.

참고문헌

[1] ISO/IEC 27000 - Information security management systems - Overview and vocabulary, 2nd WD

[2] ISO/IEC 27001 - Information security management systems - Requirements, 4th WD

[3] ISO/IEC 27002 - Code of practice for information security controls, 3rd WD

[4] ISO/IEC 27005 - Information security risk management, FDIS

[5] ISO/IEC 27007 - Guidelines for ISMS auditing, FCD

[6] ISO/IEC 27008 - Guidelines for auditors on information security controls, DTR

[7] ISO/IEC 27010 – Information security management for inter-sector and inter-organisational communications

[8] ISO/IEC 27013 - Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001, 3rd WD

[9] ISO/IEC 27015 - Information security management for financial services, 2nd WD

[10] ISO/IEC 27016 - Information security management – organizational economics, 1st WD

[11] ITU-T X.1051 - Information security management for telecommunication organizations, 2008

[12] ITU-T X.1056 - Information security incident management for telecommunication organizations, 2009

[13] ITU-T X.amg - Asset management guideline for telecommunication organizations, 4th WD

[14] ITU-T X,ismf - Information security management framework in telecommunication organizations, 4th WD

[15] ITU-T X,smsg - Information security management guidelines for small and medium-sized telecommunication organizations, 3rd WD

〈著者紹介〉

김 정 덕 (Jungduk Kim)

종신회원

1979 연세대학교 정치외교학과, 학사
1981 연세대학교 경제학과대학원, 석사
1986 Univ. of S. Carolina, MBA
1990 Texas A&M University, Ph. D. in MIS
1991 ~ 1993 한국전산원, 선임연구원
1995 ~ 현재 중앙대학교, 교수
관심분야 : 정보보호관리 및 거버넌스, 시스템감사, 정보시스템의 전략적 응용