정 보 보 호 학 회 지
제 31 권 제4호, 2021. 8

ISO/IEC 정보보호 통제 국제 표준 개정 현황

오 경 희*, 김 호 진**

요 약

ISO/IEC 27002 정보보호 통제 표준은 ISO/IEC 27001 정보보호관리체계 요구사항과 함께 정보보호관리체계 인증에 필수적인 국제 표준이다. 최근 WG 1에서는 정보보호관리체계 관련 표준들의 다양한 변화가 일어나고 있으며 이들은 ISO/IEC 27002에 기반한 관련 표준들에 연쇄적으로 영향을 미치게 되며 실질적으로 이러한 표준을 사용하는 전세계의 인증 생태계에 영향을 미칠 것으로 예상된다. 본 논문에서는 정보보호관리체계 관련 표준들을 개발 및 유지 관리하고 있는 ISO/IEC JTC 1/SC 27 WG 1의 활동을 소개하고 그 중 가장 중요한 ISO/IEC 27002 정보보호 통제의 개정 현황을 살펴본다. 또한 이에 관련된 전반적인 표준 개정 동향과 이러한 개정이 미치는 영향과 대응 방안에 대하여 논한다.

Ⅰ. 서 론

ISO/IEC JTC 1/SC 27은 정보보호, 사이버보안 및 프라이버시 보호에 관한 표준을 개발하는 특별위원회로서 2020년 설립 30주년을 맞았다. JTC1/SC 27은 매년 가장 많은 국가와 인원이 참석하는 위원회 중 하나이며, JTC 1/SC 27의 대표 표준인 ISO/IEC 27001은 ISO의 대표 표준 중 품질경영시스템 요구사항 표준인 ISO 9001, 환경경영시스템 요구사항 표준인 ISO 14001에 이어 ISO 표준 중에서 3번째로 가장 많이 판매된 표준이다. 즉 ISO./IEC 27001 정보보호관리체계 표준은 그만큼 국제적으로 활용되고 있으며 기업 간의 외주 등 정보 교환 시 상대 조직의 정보보호 수준을 판별하기 위한 기준으로서 실질적인 영향력을 미치고 있다.

JTC1/SC 27은 5개의 작업반으로 구성되어 있으며 이 중 정보보호관리체계에 대한 표준인 ISO/IEC 27000 표준 시리즈들을 개발, 유지 관리하는 것이 WG 1이다. WG 2에서는 암호 및 보안 메커니즘에 대한 표준을 개발하고 있으며, WG 3는 기술적 정보보호 시스템의 보안 평가를 위한 기준과 시험에 관한 표준을 개발하고 있다. WG 4에서는 좀 더 프로세스에 가까운 보안 통제와 서비스에 대한 표준들을 개발하고 있으며, WG 5에서는 신원관리와 프라이버시 기술에 대한 표준을 개발하고 있다.

[그림 1]은 SC 27의 각 작업반에서 다루고 있는 대표적인 표준들을 제품-시스템-프로세스-환경의 가로축과 기술-지침-평가의 세로 축에 따라 배열한 것이다. 이 그림은 국내 SC 27 전문위원회에서 개발한 것으로서 SC 27 내 각 그룹의 활동을 이해하는 데 도움이 될 것이다.

최근 WG 1에서는 정보보호관리체계 관련 표준들의 다양한 변화가 일어나고 있으며 이들은 ISO/IEC 27002에 기반한 관련 표준들에 연쇄적으로 영향을 미치게 되며 실질적으로 이러한 표준을 사용하는 전세계의 인증 생태계에 영향을 미칠 것으로 예상된다.

본 논문의 2장에서는 JTC 1/SC 27 WG 1에서 현재 진행되고 있는 활동을 소개하고 3장에서는 그중 가장 중요한 ISO/IEC 27002 정보보호 통제의 개정 현황을 살펴본다. 4장에서는 이에 관련된 전반적인 표준 개정 동향을 소개하고 결론으로서 이러한 개정이 미치는 사회적 영향과 대응 방안에 대하여 논한다.

이 논문은 2020년도 산업통상자원부 및 산업기술평가관리원(KEIT) 연구비 지원에 의한 연구임(20010998)
* 한국정보시스템감사통제협회 (연구책임자, khoh@isaca.or.kr)
** 한국정보시스템감사통제협회 (연구원, hjkim@isaca.or.kr)

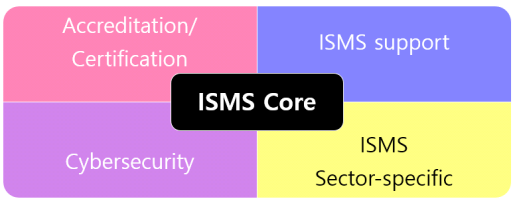
〔그림 1〕 ISO/IEC JTC 1/SC 27 국제 표준 분류 개념도

Ⅱ. JTC 1/SC 27 WG 1 프로젝트 현황

2.1. SC 27 WG 1 표준 카테고리

[그림 1]에서 보듯이 SC 27 WG1은 조직 및 환경의 정보보호를 평가하기 위한 표준들을 개발하고 있다. WG 1의 표준들은 크게 ISMS 코어, 인정 및 인증, ISMS 지원, 분야별 ISMS, 사이버보안의 5개 카테고리로 나누어 볼 수 있다. [그림 2]는 국내 SC 27 전문위원회의 WG 1 전문위원들이 개발한 것으로 이 5개 카테고리를 도식화 한 것이다.

이들은 정보보호관리체계에 대한 핵심 사항을 정의하는 ISMS 코어에서 시작하여 이 기준에 따른 인증을 위한 인정 및 인증 표준, 그리고 정보보호관리체계를 효과적으로 구현하고 관리하기 위한 지원 표준, 정보보호관리체계를 특정 분야에 더 적절하게 적용하기 위한 분야별 ISMS 표준, 그리고 조직의 범위를 넘어서는 사이버보안을 다루기 위한 표준으로 이어진다.



〔그림 2〕 SC 27 WG 1 표준 카테고리 개요

2.2. ISMS 코어

먼저 가장 핵심이 되는 ISMS 코어 카테고리에는 27000 시리즈의 전반적인 개요와 공통 용어를 정의하는 27000, 정보보호관리체계에 대한 요구사항을 정의하는 27001, 그리고 정보보호관리체계 수립 시 고려해야 할 전반적인 정보보호 통제와 그의 구현에 관한 사항을 설명하는 27002로 구성된다.

2.3. 인정 및 인증

인정 및 인증(accreditation/certification) 카테고리는 특정 조직이 구현한 정보보호관리체계가 27001의 요구사항을 만족는지를 심사하고 인증하는 데 필요한 표준들을 포함한다. 이러한 표준으로는 정보보호관리체계 심사 및 인증을 제공하는 인증기관에 대한 요구사항을 정의하는 27006, 정보보호관리체계 심사에 관한 지침인 27007, 그리고 심사 시 각 정보보호 통제를 평가하는 방법에 관한 지침인 TS (technical specification) 27008이 있다.

2.4. ISMS 지원

정보보호관리체계 지원(ISMS support) 카테고리에는 정보보호관리체계 구현을 위한 지침인 27003, 구현된 정보보호관리체계의 모니터링, 성과 측정을 위한

지침은 27004, 정보보호 위험관리를 위한 27005, 정보보호 거버넌스를 설명하는 27014, 정보보호관리체계가 조직에 미치는 경제성을 설명하는 TR (technical report) 27016이 포함된다. 또한 이 카테고리에는 정보보호관리체계를 수립, 운영하는 전문가가 갖추어야 할 능력에 관한 요구사항을 정의하는 27021과 정보보호관리체계 프로세스 지침인 TS 27022, 27001과 27002의 2013년 개정판이 이전 버전인 2005년 판과 어떤 차이가 있는지를 설명한 TR 27023이 포함된다.

2.5. 분야별 ISMS

ISMS 27002는 모든 조직에서 활용할 수 있는 포괄적이고 전반적인 정보보호 통제를 제공하는 것을 목적으로 개발되었으나, 실제 적용과 인증 경험이 쌓이고 새로운 IT 기술 분야들이 나타나면서, 특정 분야에는 추가적인 통제가 필요하며, 기존 통제들 역시 해당 분야 특유의 구현 지침이 필요하다는 각성에서 시작되었다. 처음에는 통신회사, 클라우드 서비스 등에서의 필요성이 인지되어 관련 표준들이 별도로 개발되었고, 결국에는 새롭게 나타나는 다양한 분야의 정보보호 요구사항을 고려하기 위하여 27001을 특정 산업 분야에 적용하기 위해서는 어떻게 표준을 개발해야 하는지를 설명하는 메타 표준인 27009가 개발되었다.

분야별 ISMS (ISMS sector-specific) 카테고리에는 기 언급한 메타 표준인 27009로 시작하여, 27002에 기초하여 통신 분야에 추가적으로 필요한 정보보호 통제와 구현 방법을 설명한 27011, 클라우드 서비스에 필요한 정보보호 통제를 설명하는 27017, 개인정보를 처리하는 공용 클라우드에서의 개인식별정보의 보호를 위한 추가 통제를 제공하는 27018, 에너지 유틸리티 산업분야에 필요한 정보보호 통제를 제공하는 27019가 포함된다. 이들은 모두 27002의 통제를 기반으로 하여 각 산업 분야별 추가적인 통제와 구현 지침을 제공한다. 내용적으로는 개인정보보호 관리체계를 다루는 27701 역시 이 카테고리에 속하지만 이 표준은 WG 1과 WG 5가 공동으로 개발한 것으로서 프라이버시 표준을 개발하는 WG 5에 속한 것으로 간주하고 있어 이 분류에는 포함시키지 않는다.

또한 서로 다른 분야 및 조직 간의 정보 교환에 필요한 정보보호 관리 요소를 설명하는 27010, 정보보호 관리체계 요구사항과 IT 서비스 관리체계 요구사항인 20000-1을 통합 구현하기 위한 지침인 27013 역시 이 카테고리에 속한다.

2.6. 사이버 보안

마지막으로 상대적으로 최근에 개발이 개시된 사이버보안 카테고리가 있다. 조직의 범위는 물론 국경을 넘어 발생하는 사이버 침해사고에 대응하기 위한 체계적인 표준이 필요하다는 요구에 따라 사이버보안의 개요와 개념을 설명하는 TS 27100, 사이버보안 사고에 대응하기 위한 사이버 보험의 제공사와 가입 시에 필요한 사항을 설명하는 27102, 사이버보안에서 참조할 수 있는 ISO와 IEC에서 개발된 기존 표준들을 소개하는 TR 27103, 사이버보안 프레임워크를 개발하기 위한 지침인 TS 27110이 여기 속한다.

Ⅲ. ISO/IEC 27002 정보보호 통제 개정 현황

3.1. ISO/IEC 27002 개정의 진행

3절에서는 현재 DIS (dreaft international standard) 단계에 와 있는 정보보호관리체계의 핵심 표준인 ISO/IEC 27002 표준의 개정 현황을 소개한다.

현재 사용되고 있는 27002는 27001과 마찬가지로 2013년 개정된 버전이다. SC 27 WG 1은 클라우드 등 IT 신기술의 등장과 진화하는 보안 위협 및 이에 대응하기 위한 보안 관제 등 기술적 변화를 반영하기 위하여 2018년 3월 27002의 개정을 개시하기로 결정하였다. 영국의 Sabrina Feng, 프랑스의 Fourat Alia, 아르젠티나의 Veronica Marinelli 3명의 여성 에디터가 임명되어 작업을 진행하고 있다.

그러나 신규 통제 제안에 따른 통제 전반의 재분류 등 전반적인 구조 변경이 이루어지면서 매번 수천개의 코멘트가 기고되어 회의 기간 내에 코멘트를 다 처리할 수 없는 상황이 지속되었다. 3인의 에디터들은 수천개의 코멘트를 분석하여 전반적인 영향을 미칠 수 있는 중요한 이슈들을 선정하여 우선적으로 논의하고, 그 다음 신규 통제 또는 통제의 분할 합병 등 중요 코멘트를 다루고, 논란 없이 채택될 수 있는 단순 코멘트들은 별도의 이견이 제시되지 않는 한 검토하지 않고 넘어갈 수 있도록 준비하여 체계적으로 대응하였으나, 하나의 결정이 전반적인 구조 또는 다른 통제에

대한 영향을 미치게 되는 경우 회의 기간 중 그 영향을 다 처리하고 검토할 수 없었다. 이에 따라 회의에서는 가능한 만큼의 중요 이슈들을 검토하여 결의하고, 결의에 따른 변경 결과는 검토하지 못한 채 에디터들에게 전권을 위임하여 변경을 수행하게끔 하는 방식으로 진행되었다.

특히 DIS 진행을 위한 지난 4월 회의는 20개 국가가 총 1310개에 달하는 코멘트를 제출하였으며, 회의가 온라인으로 진행됨에 따라 더욱 검토 시간이 부족하여 6월에 2일간의 추가 회의를 가짐으로써 검토를 마무리했지만 의사결정에 따른 반영은 다시 에디터들에게 위임되었다.

이러한 상황에 따라 2021년 1월 DIS 투표가 시작되었으나 한국을 포함, 전반적인 텍스트의 완성도를 중요시 하는 소수의 국가들은 DIS 단계 진행에 반대하고, 미국 등 적극적으로 의견을 개진하는 국가 중에서도 에디터들의 노고를 이해하는 차원에서 기권 투표를 하였지만 실질적으로는 회의에 참석하지 않는 국가들이 많은 찬성표를 던짐으로서 4월 DIS 승인이 이루어졌다.

현재는 정리된 DIS 버전이 회람되기를 기다리는 상태로, FDIS 투표는 2021년 하반기에 진행될 예정이다. 초기 출판 목표일은 2021년 11월 말이었으나 현재의 진도상으로는 불가능하다. 프로젝트 일정 상 최종 출판 기한은 2022년 3월 말이며, 이 기한을 넘길 경우 프로젝트 진행에 문제가 생기므로 내년 초에는 출판될 것으로 예상된다.

3.2. ISO/IEC 27002 구조 변화

현 DIS 버전은 2013년 버전과는 구조가 크게 달라졌다. 2013년 버전에서는 5절에서부터 18절까지 14개의 보안 통제 절로 구성되었으며 각 절은 하위 범주로 나누어져 35개의 보안 범주가 있었고, 최종 보안 통제는 하위 범주 아래 구성되어 총 114개의 통제가 포함되었다.

반면 현재의 27002 DIS 버전에서는 통제 절을 크게 조직적 통제, 인적 통제, 물리적 통제, 기술적 통제 4개의 절로 구분하였다. 또한 중간 단계의 보안 범주가 사라졌다. 조직적 통제 절은 37개의 보안 통제를, 인적 통제 절은 8개, 물리적 통제 절은 14개, 기술적 통제 절은 34개의 보안 통제를 포함하여 4개 분야 93개 통제 항목으로 구성되었다.

3.3. 통제의 속성 분류 표

또 하나의 큰 변화는 각 통제에 대하여 통제의 속성을 5가지 측면에서 분류한 표를 추가한 것이다. [표 1]은 이 5개의 속성과 각 속성이 가질 수 있는 값을 보여주고 있다. 5개의 속성은 통제 유형, 정보보호 특성, 사이버보안 개념, 운영 능력, 보안 도메인으로 나누어진다.

통제 유형은 보안사고 발생 결과로 나타나는 위험에 통제가 영향을 미치는 시점 및 방식을 나타내며 #예방, #검출, #교정의 값을 가진다. 정보보호 특성은 통제가 보존하고자 하는 정보의 속성을 나타내며, #기밀성, #무결성, #가용성의 값을 가진다. 세 번째 속성인 사이버보안 개념은 TS 27110 사이버보안 프레임워

〔표 1〕 통제의 속성 및 속성 값

Attributes	Attribute values
Control types	#Preventive, #Detective, #Corrective
Information security properties	#Confidentiality, #Integrity, #Availability
Cybersecurity concepts	#Identify, #Protect, #Detect, #Respond, #Recover
Operational capabilities	#Governance, #Asset_management, #Information_protection, #Human_resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance.
Security domains	#Governance_and_Ecosystem, #Protection, #Defence, #Resilience

〔표 2〕 정보보호 정책 통제의 속성 표

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

크에서 정의된 개념 분류를 따르며 #식별, #보호, #검출, #대응, #복구의 값을 가진다. 네 번째 속성은 운영 능력은 정보보호 능력을 관리하는 실무자 관점에서 본 통제 속성을 말한다. 이 속성은 매우 많은 값을 가질 수 있다. #거버넌스, #자산관리, #정보_보호, #인적자원관리, #물리보안, #시스템_및_네트워크_보안, #응용보안, #신원_및_접근 관리, #위협_ 및_취약성_관리, #연속성, #공급자_관계_보안, #법_ 및_준거성, #정보보호_사건_관리, #정보보안_보증이 포함된다. 마지막 5번째 보안 도메인은 정보보안 분야, 전문성, 서비스 및 제품의 측면에서 본 통제 속성이라고 설명되며, #거버넌스 및 생태계, #보호, #방어, #회복력의 값을 가질 수 있다.

이 속성들과 그 값의 적정성은 계속해서 토론의 대상이 되었는데 특히 운영 능력과 보안 도메인이 적정한 분류인가에 대해서는 많은 이견이 있었으나 제안국의 강력한 의지와 회의 시간의 한계로 인해 유지되게 되었다.

3.4. 통제의 구성

각 통제는 통제 명 바로 다음에 5개의 속성과 해당 통제에 관련된 속성 값을 표시한 표가 제시된다. 그 다음 통제에 대한 설명, 목적이 제시되며, 지침이 설명되고 필요한 경우 기타 정보가 추가된다. 속성 표를 제외하면 중간 카테고리에 있던 목적이 각 통제로 내려갔다는 것 외에는 큰 변경은 없다.

예를 들어 5.1 정보보호 정책은 [표 2]와 같은 통제 속성 표를 갖는다. 또한 부록 A에서는 모든 통제에 대한 통제 속성 표를 모아서 보여주며, 이러한 속성 표를 위험 처리 계획에 활용하는 방법을 설명하고 있다.

3.5. 통제의 재구성 및 신규 통제

27002 DIS 버전은 많은 내용을 추가, 삭제, 수정하였으나, 통제 항목 별로 보면 기존의 통제 개념을 그대로 가져간 것도 있고, 서로 다른 통제를 융합하여 하나의 통제로 합친 것도 있고, 하나의 통제를 두 개의 통제로 나눈 것도 있다. 또한 삭제한 통제와 새롭게 추가한 통제도 있다.

전반적으로는 관련 통제를 묶어 하나의 통제로 만든 경우가 많다. 예를 들어 5.1 정보보호 정책은 기존의 5.1.1 정보보호 정책과 5.1.2 정보보호 정책 검토를 통합하여 하나의 통제로 만들었다. 이러한 변경을 쉽게 확인할 수 있도록 부록 B에서 신규 버전 대비 2013년 버전의 통제와 2013년 버전 대비 신규 버전의 통제를 보여주는 2개의 표를 제공하였다.

또한, DIS 버전에서는 보안 기술의 변화를 반영하기 위한 11개의 새로운 신규 통제가 추가되었다. 이 신규 통제들을 [표 3]에 보였다.

이러한 신규 통제의 일부는 기존 버전에서도 기본적인 개념들을 포함하고 있었지만 별도의 통제로 만들어지면서 많은 내용이 추가되어서 신규 통제로 분류되었다. 한편 2013년 버전의 11.2.5 Removal of assets는 삭제된 것으로 분류되었으나 해당 통제의 내용은 7.10 Storage media와 8.10 Information deletion에 포함되었다.

〔표 3〕 신규 추가된 통제

5.7	Threat intelligence
5.23	Information security for use of cloud services
5.30	ICT readiness for business continuity
7.4	Physical security monitoring
8.9	Configuration management
8.10	Information deletion
8.11	Data masking
8.12	Data leakage prevention
8.16	Monitoring activities
8.22	Web filtering
8.28	Secure coding

Ⅳ. 정보보호관리체계 표준 개정 동향

4.1. 27002 개정이 미치는 영향의 평가

ISO/IEC 27002의 개정은 WG 1 뿐만 아니라 WG 4, WG 5에서 진행되는 다른 여러 표준에 영향을 미친다. 27002 3차 개정판이 출판되면 2015년 버전은 철회되며, 이 경우 더 이상 존재하지 않는 27002:2015 버전을 참조하는 모든 표준 문서는 유효할 수 없기 때문이다.

SC 27 WG 1은 WG 1 프로젝트에 대해 27002 개정이 미치는 영향을 평가하였다. WG 1에 많은 전문가들이 참여하기는 하지만, 표준 문서를 개정하기 위해서는 사무국의 관리도 필요하고 경험있는 에디터 선정 뿐만 아니라 전문가들의 적극적 검토와 참여가 필수적인데 WG 1의 자원을 고려할 때 그 많은 관련 프로젝트들을 동시에 개정하는 것은 불가능하기 때문이다. 따라서 가장 큰 영향을 미치는 중요한 프로젝트부터 단계적으로 개정을 진행하고자 관련 프로젝트의 식별과 영향 평가를 시행하였다.

27002에 관련된 프로젝트 중 가장 큰 영향을 받는 것은 ISO/IEC 27001이다. 27001은 필수 부속서인 부속서 A에 27002에 포함된 정보보호 통제 목적과 통제를 나열하고 있으며, 본문의 6.1.3 정보보호 위험처리에서는 위험처리 방안의 구현에 필요한 통제를 결정한 후 이를 부속서 A의 통제와 비교하여 필요한 통제 중 누락된 것이 없는지를 검증하도록 요구하고 있다. 27002:2015가 철회되면 이를 따르는 부속서 A는 무효가 되고 이에 기반한 27001 인증도 문제가 되기 때문이다.

또한 분야별 인증 표준의 기반이 되는 메타 표준인 27009 역시 27002의 구조를 따른 내용을 설명하고 있기 때문에 그 중요도 만큼이나 큰 영향을 받게 된다. 클라우드 인증에 실제로 많이 사용되고 있는 27017 역시 영향이 높은 것으로 평가되었으며 ITU-T와의 공통 표준인 27011도 상대적으로 영향이 큰 것으로 평가되었다.

이 외에도 27008, 27010, 27019, 27003, 27004 등이 중간 정도의 영향도를 갖는 것으로 평가되었다. 이러한 평가 결과에 따라 우선 순위가 높은 표준부터 개정 계획을 논의하였다.

4.2. ISO/IEC 27001 개정 방안

4.1에서 설명하였듯이 ISO/IEC 27001은 27002 기반 필수 부속서 A를 포함하고 이를 ISMS 인증 과정에서 필수적으로 활용하도록 요구하고 있다. 따라서 27001 표준이 무효화되지 않고 개정된 27002가 실제 인증에 활용되기 위해서는 그 내용을 부속서 A에 포함하고 있는 27001의 개정이 필수적이다.

지난 4월 SC 27 WG 1 총회에서는 이 개정을 어떻게 처리해야 할 지에 대한 논의가 진행되었다. 27001 전체를 개정하는 방법과 부속서 A 만을 수정본(Amendment)으로 출판하는 방안이 비교되었다. 27001의 전반적인 개정 필요성도 제시 되었으나 전반적 개정은 최소한 2년 이상의 시간이 걸리므로 그동안 27001 인증에 혼란이 발생할 것이 우려되었다. 이에 따라 27002의 출판과 동시에 27001의 부속서 A를 수정본으로 출판함으로써 기존의 27001 표준 문서 + Amd1에 따라 신규 27002를 기반으로 하는 27001 인증을 제공할 수 있게끔 하는 방안이 채택되었다.

한편 ISO 규정은 하나의 표준에 대해서 2개의 수정본만을 인정한다. 즉, 3번째의 수정본이 만들어지면 자동으로 이들 수정본들을 포함하는 원본 문서의 개정 작업이 개시되게 된다. 그런데 ISO/IEC 27001에 대해서는 지금까지 2014년, 2015년에 2번의 오류정정(Corrigendum)이 이루어졌다. 따라서 부속서 A에 대한 수정본(Amd1)이 출판되게 되면, 규정에 따라 지금까지 출판된 Cor1, Cor2, 및 신규 Amd1이 포함되는 27001 전체 문서에 대한 개정 작업이 즉시 개시되어야 한다.

즉, 27002가 출판되면 27001 부속서 A의 수정본이 함께 출판되어 27001 인증은 개정된 27002에 따라 이루어질 수 있게 하고, 동시에 27001 문서의 개정이 개시되도록 하는 것이 지난 회의의 결론이다.

현재는 지난 회의 결의에 따라 부속서 A의 변경만을 내용으로 하는 27001 AMD 1이 CD 단계로 등록된 상황이다. 27002의 FDIS 투표 결과에 따라 이 27001의 AMD 1의 출판에 대한 투표도 진행될 것이며, 향후의 일정이 확정될 것이다. 이 일련의 과정이 계획대로 진행된다면 2022년 이후의 ISMS 국제 표준 인증은 개정된 27002에 기초하여 이루어질 수 있게 된다.

4.3. 27002에 기초한 타 표준의 개정

2.5절에서 설명한 분야별 ISMS 카테고리에 속하는 27009, 27011, 27017, 27019 표준은 ISO/IEC 27002를 기반으로 하고 있다. 즉 ISO/IEC 27002의 구조를 따라서 일반 통제에 대한 각 분야별 통제 구현 지침을 설명하고 있으며, 부록에서 분야별 통제를 제시하고 있다. 이것은 WG 5와 함께 개발한 27701도 마찬가지이다. 또한 JTC 1/SC 27이 아닌 ISO TC 215 의료정보 위원회에서 개발한, ISO/IEC 27002에 기초한 의료정보보호관리 표준인 ISO 27799도 존재한다. 따라서 27002의 개정은 이 모든 관련 표준들의 현행화를 위한 개정을 요구하게 된다.

또한 ISMS 지원 카테고리에 포함되는 표준들도 27002의 내용을 참조하고 있는 것들이 있기 때문에 WG 1은 4.1절에서 설명한 표준들의 영향 평가 결과에 따라 이들을 개정하기 위한 계획을 마련하였다.

먼저 가장 중요한 표준인 27001에 대한 개정 계획은 4.2절에서 설명하였다. 다음으로 중요한 표준은 27009, 27017, 27011인데 27011은 지난 2020년 정기검토 기간에 이러한 개정 현황을 파악하고 27002 개정을 반영하기 위한 개정을 이미 개시하였다. 따라서 이번 회의에서는 개정 1단계로 27009와 27017의 개정을 위한 PWI 수립 결의를 진행하였으며, 2022년 초 완료를 목표로 설계 명세 단계와 개정 일정을 논의하고 에디터를 모집, 선정하였다. 한국에서도 27011, 27009, 27017에 코에디터로 참여하고 있다.

2단계 개정은 27008, 27010, 27019를 대상으로 2021년 말에서 2024년 초까지 진행할 예정이며, 3단계 개정은 27003, 27004 등 기타 표준을 대상으로 2023년 4월부터 진행할 예정이다.

4.4. 분야별 인증제도 수립을 위한 관련 표준 개정

27002 뿐만 아니라 이미 진행되고 있는 다른 표준의 개정도 있는데 이중 중요한 사항으로 인정 및 인증 카테고리에 속하는 ISO/IEC 27006 ISMS 인증기관 요구사항에 대한 개정은 언급해 둘 필요가 있다.

ISO/IEC 27006은 본래 정보보호관리체계의 심사 및 인증을 제공하는 기관에 대한 요구사항이다. 이의 개정은 지속적으로 논의되고 있었다. 1차적인 이유는 ISO/IEC 27701 프라이버시 관리체계 인증을 수행하는 인증기관을 지정하여 실제 프라이버시 인증을 수행할 수 있는 ISO 기반의 체계를 만들기 위해서였다. 또 한편으로는 시장에서는 27017에 기반한 클라우드 인증이 이루어지고 있었는데, 이는 인증기관이 자의적으로 진행하는 것이고 ISO 인증 체계를 기반으로 한 것은 아니었다. ISO/IEC 27006은 27001과 27002를 기준으로 한 것이고 다른 분야별 표준을 대상으로 포함하고 있지 않기 때문이다.

WG 1과 함께 ISO/IEC 27701 표준을 27009에 따라 인증이 가능한 표준으로 만든 WG 5에서는 이 표준을 기반으로 한 인증 제도를 실행하기 위해 27006 ISMS 인증기관에 대한 표준을 프라이버시 인증을 수행하는 인증기관에 대한 표준으로 확대하기 위한 표준을 개발하기 위해 2019년부터 심혈을 기울였다. WG 5는 이를 별개의 표준으로 제안하였으나 ISO는 이를 ISO 27006의 시리즈 표준으로 보고 27006-2로 만들도록 했다. 이에 따라 기존의 27006은 27006-1로 변경되어야 하는 상황이 되었다. WG 1 전문가들은 이 기회를 빌어 그간의 인증심사 경험과 대상 조직 환경의 변화를 반영하여 물리적 사무실이나 조직이 소유하고 관리하는 ICT 가 최소화된 가상 조직에 대한 심사 방법, 코로나 시대에서의 비대면 심사 등의 사항을 포함하여 기존 문서를 개선하는 한편, 분야별 인증이 가능한 인증기관 요구사항으로 만들기 위해 개정을 진행하고 있다.

프라이버시 관리체계 인증기관을 위한 ISO/IEC 27006-2는 올해 2월 최종 출판 되었으나, 27002의 개정을 반영하기 위한 개정 작업이 4월 시작된 상황이다. ISO/IEC 27006-1은 이번 회의에서 정식 개정이 시작되어 2023년 초까지 출판을 목적으로 작업 중이다.

이 외에도 ISO/IEC 27005 위험관리 표준 역시 2020년부터 개정이 시작되어 2022년 말 또는 2023년 초 출판을 목적으로 작업 중에 있다. 이 표준은 27002의 개정과는 상대적으로 관계가 적으나 분야별 인증기준이 위험관리에 관한 추가 요구사항을 포함하는 경우 이 표준에서 다루어 줄 필요가 있다. 단 27701에서 요구하는 개인정보보호 위험 관리는 WG 5에서 관리하는 ISO/IEC 29100 및 29134를 참조하므로 본 표준의 범위에는 해당되지 않는다.

Ⅴ. 결론: 대응 방안

지금까지 ISO/IEC JTC 1/SC 27 WG 1에서 관리하고 있는 정보보호관리체계 표준들을 소개하고 정보보호관리체계 인증의 핵심 표준인 ISO/IEC 27002의 개정 현황과 주요 변경 사항을 살펴 보았다.

또한 ISO/IEC 27002의 개정이 WG 1 및 기타 표준에 미치는 영향을 분석하고 이에 따른 SC 27 WG 1의 대응 계획과 ISO 인증 스킴에 따른 분야별 인증 제도 수립을 위한 개정 노력을 살펴보았다.

ISO/IEC 27002의 개정은 단일 표준의 개정으로 끝나는 것이 아니라 다수의 관련 표준에 영향을 미치며, 실질적으로 세계 각국에서 진행되어 온 ISMS 인증 심사에 영향을 미치게 될 것이다. 정보보호관리체계 수립, 운영 및 심사에 관련된 국내 전문가들도 이러한 변화를 파악하고 변경 사항을 습득하기 위해 노력할 필요가 있다.

한편 SC 27에서는 시장의 혼란을 최소화하기 위하여 기존 27001과 27002 Amd1의 활용 방법을 설명하기 위한 문서를 개발하기 위한 자원봉사자를 요청하는 한편, 단계별 표준 개정을 위한 에디터를 지속적으로 모집하고 있다. 이것은 국내 전문가의 국제 표준화 기구 진출에 매우 좋은 기회로서 적극적으로 활용할 필요가 있다.

국내 SC 27 전문위원회는 산업표준화법에 따라 구성된 조직으로써 전문위원은 20명으로 제한되어 있지만 참관인으로써 참여가 가능하고, 각 WG 별 표준 전문가 그룹 운영을 통해 국제 표준 검토, 기고, 회의 참여 등을 진행하고 있다. 전문위원회를 운영하고 있는 TTA 또는 전문위원을 통해 참여 요청을 할 수 있으며, 특히 코로나로 인해 온라인 회의를 진행하고 있는 현재는 해외 출장 없이도 국제회의에 참여가 가능하여 업무에 바쁜 전문가들에게 좀 더 유리한 상황이다. 다만 ISO 회원 기구로서 전문위원회를 관리하고 있는 국립전파연구원은 실제로 적극적인 참여와 기고를 수행할 수 있는 인력에게만 참여를 허용하고 있어 단순한 정보 수집을 위한 참여는 불가능하다.

SC 27에서 진행되는 표준 개정 작업은 이후 일정한 적응기간을 지나 국제 정보보호관리체계 인증 시장에 반영될 것이다. 이미 진행되고 있는 클라우드 인증은 물론, 프라이버시 관리체계 인증 등 현재 준비 중인 분야별 인증으로 다변화될 가능성이 높다. 또한 실질적인 IT 업무 환경 변화도 인증에 영향을 미칠 것이다. 이미 많은 기업들이 클라우드 기반의 IT 서비스를 이용하고 있으며 코비드 상황에서 재택 · 원격 근무 도입이 더욱 활성화 되면서 물리적 사무실의 경계가 모호해 지고 있다. IoT, AI, 블록체인 등의 신기술은 조직 간 경계를 넘어서는 기술 인프라와 이에 따른 새로운 보안 위협 및 대응 프레임워크를 요구하고 있다. 국내 보안 전문가들이 국제 표준화를 통해 이러한 새로운 환경 변화에 선제적으로 대응하고 글로벌 보안 시장으로 진출할 수 있는 기회를 잡을 수 있기를 바란다.

참 고 문 헌

[1] ISO/IEC 27000:2018 Information technology − Security techniques − Information security management systems − Overview and vocabulary, ISO 2018

[2] ISO/IEC 27001:2013 Information technology − Security techniques − Information security management systems − Requirements, ISO 2013

[3] ISO/IEC 27001:2013/COR 1:2014 Information technology − Security techniques − Information security management systems − Requirements − Technical Corrigendum 1, ISO 2014

[4] ISO/IEC 27001:2013/COR 2:2015 Information technology − Security techniques − Information security management systems − Requirements − Technical Corrigendum 2, ISO 2015

[5] ISO/IEC 27002:2013 Information technology − Security techniques − Code of practice for information security controls, ISO 2013

[6] ISO/IEC 27002:2013/COR 1:2014 Information technology − Security techniques − Code of practice for information security controls − Technical Corrigendum 1, ISO, 2014

[7] ISO/IEC 27002:2013/COR 2:2015 Information technology − Security techniques − Code of practice for information security controls − Technical Corrigendum 2, ISO 2015

[8] ISO/IEC TS 27006-2:2021 Requirements for bodies providing audit and certification of information security management systems − Part

2: Privacy information management systems, ISO 2021
[9] ISO/IEC 27006:2015 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems, ISO 2015
[10] ISO/IEC 27009:2020 Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements, ISO 2020
[11] ISO/IEC 27701:2019 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines, ISO 2019
[12] ISO 27799:2016 – Health informatics – Information security management in health using ISO/IEC 27002 (second edition), ISO 2016

〈저 자 소 개〉

오 경 희 (Kyeong Hee Oh)
정회원
1988년 8월 : 서강대학교 전산과 졸
1992년 2월 : KAIST 전산과 석사
2010년~현재 : 산업표준심의회 정보보안기술(ISO/SC27) 전문위원
2016년~현재 : 산업표준심의회 표준회의 의원
2017년~현재 : 산업표준심의회 블록체인(ISO/TC 307) 전문위원
2013년~2017년 : ITU-T SG17 Q3 Associate rapporteur
2017년~현재 : ITU-T SG17 Q14 Corapporteur
2019년~현재 : 한국정보시스템감사통제협회 연구책임자
<관심분야> 정보보안관리, 블록체인, 아키텍처, IT 감사, 거버넌스, 통제

김 호 진 (Hojin Kim)
1992년 2월 : 서강대학교 전산과 졸
2021~현재 : 한국정보시스템감사통제협회 연구원
2016~2021 : Xcolor International 대표
1992~2016 : 풀빛소프트, 한메소프트, 한글과 컴퓨터 등
<관심분야> blockchain, USB lockkey management, Secure execution environment, Device control, Image Processing