한국경호경비학회 – 제48호(2016): 79–111
투고일 2016. 8. 19, 심사일 2016. 9. 13, 게재확정일 2016. 9. 20

ISO/TC 292에 의한 산업보안 분야 국제표준화의 동향

박 현 호

ISO/TC 292에 의한 산업보안 분야 국제표준화의 동향

박 현 호*

〈요 약〉

이 연구는 산업보안 관련 분야가 시스템 측면에서 국제표준기구인 ISO를 통해서 표준화되어 가는 추세를 분석한 것이다. 산업기밀 유출 방지와 같은 악의적 범죄공격에 의한 위험을 관리하고 손실을 방지하기 위한 산업재산권 보호 관련한 체계라는 범위를 벗어나서 공급사슬, 제품 및 문서 위조의 방지, 재난관리, 커뮤니티 회복력과 같이 폭넓은 분야를 다루었다. 이를 위해 산업보안 분야 표준화의 역사를 연혁적으로 분석하면서 ISO TC 292가 탄생된 역사적 배경과 표준화의 틀이 어떻게 변화되어 왔는지를 체계적으로 안내하였다. 또한 TC 292 안에서 워킹그룹 별로 개발되고 제정되어 온 보안 관련 표준들의 대략적인 내용들을 용어 정의(terminology) 및 일반적 보안 원칙(general standards)부터 공급사슬 보안경영시스템(supply chain security management)까지 상세하게 살펴보았다. 분석을 통해 도출된 주요 발견점은 보안의 대상(target)과 위협(threat)이 다양화되면서 기업 등의 조직이 보다 유연성 있게 보호하고 피해를 입고도 조속히 회복되는 적응력을 갖추기 위한 체계가 표준화되고 있으며, 산업보안 관련 국제표준화의 범위가 확장되고 있다는 점, 그 국제표준화는 공공 및 민간 보안의 홀리스틱(holistic) 접근의 중요성을 강조하고 있다는 점, 마지막으로 산업이 적절한 보안과 회복력을 갖추기 위해서 이러한 국제표준화를 통한 ISO 인증 요구사항에 시급히 대비 및 대응하여야 한다는 점이다.

주제어 : 산업보안, 표준, 국제표준기구(ISO), TC 292, 인증

* 용인대학교 경찰행정학과 부교수. ISO/TC 292(보안) WG4 프로젝트리더

목 차

Ⅰ. 연구 배경

미래학자 Alvin Toffler(1990)의 말대로 산업스파이 분야를 포함, 보안(security)은 '21세기 가장 큰 성장산업 중 하나'라는 점이 점차 가시화되어 가고 있고 국내외의 많은 전문가들도 공감하고 있다(유형창, 2014; 최진혁, 2010; 이성용, 2014 등). 산업보안연구학회(2012: 6)에서 발행한 교과서를 근거로 할 때 '산업보안(Industrial Security)'은 광의의 개념으로 '테러와 범죄 등 고의, 악의, 또는 과실에 의해 야기된 해(harm)로부터 산업의 손실을 예방하고 산업제반을 보호하는 활동이나 체계'로서 포괄적으로 정의될 수 있다.

이 연구는 산업보안 분야에서 진행되고 있는 국제표준화를 ISO 표준화를 중심으로 탐색한 것이다. 물론 국제표준기구(ISO)와 국제전기기술위원회(IEC)의 합동전문위원회인 ISO/IEC JTC 1나 IETF, ITU-T, 3GPP 등에서 산업보안 관련 글로벌 표준화가 수행되고 있기는 하지만 정보통신시스템에서 저장 및 유통되는 정보의 기밀성(정보누출 방지)과 무결성(데이터 위·변조 방지)을 보장하며, 정보통신 시스템의 안전성과 가용성을 향상시키는데 필요한 핵심기술을 지칭하는 소위 정보보호기술(IT security techniques)[1]에 치중하는 경향을 보인다. 물론 한국경호경비학회나 한국산업

1) 염흥열, 정보보호일반표준화로드맵 2006. TTA

보안연구학회 등을 통하여 산업보안의 개념과 범위, 그리고 그 유형론에 대하여 많은 문제가 제기되고 논의되어 보다 체계적이고 포괄적으로 정립이 되어 가고 있는 것은 다행스런 일이다.

이와 차별화하여 이 연구에서는 '보안 및 회복력[2](Security and Resilience)'을 타이틀로 하는 국제표준기구 기술위원회인 ISO/TC 292의 산업보안 분야 국제표준화를 분석하여 소개하고자 한다. 특히 표준화 차원에서 산업보안을 다룬 기존 연구가 많지 않은 관계로 여기서는 보안 분야 ISO 표준의 범위와 위치를 소개한 후 ISO/TC 292에 의한 산업보안 분야 표준화 동향을 기술한 후 그 시사점을 논하고자 한다. 다만, 이 연구에서는 테러와 범죄 등 고의적 공격에 의한 손실을 방지하고 위험을 관리하는 보안 영역을 중심으로 하되 미국, 영국 등에서 산업보안의 영역으로 포함하고 있는, 범죄 외의 영역(재난관리, 비상계획, 회복력 등)까지도 포괄적으로 논하고자 한다. 이는 범죄, 테러와 마찬가지로 지진, 쓰나미 등 재난에 의해 발생하는 해저드(hazard)와 위험(risk)은 그 특성은 다르지만 상당한 수준의 불확실성(uncertainty)의 시대에 예방, 대비, 대응, 복구 등의 프로세스 상에서 전반적인 리질리언스(resilience) 체계를 통한 사업연속성 확보 측면에서는 일맥상통하는 부분이 많아 이를 별개로 분리하기 보다는 같이 포함시켜 논하는 것이 의미가 있기 때문이다.

Ⅱ. 연구방법론

연구방법은 이 분야가 국내에서는 다소 생소한 분야라는 특성을 반영하고 다양한 방식의 연구조사의 기틀을 제공하기 위한 단초를 마련하기 위하여 주로 문헌분석과 전문가 인터뷰 기법 등 질적 연구방법을 활용하였다. 따라서 이 연구는 국내에서는

2) 분야 별로 복원력, 회복탄력성 등 다양하게 명명되고 있는 resilience는 '다시 뛰어 오르다(to jump back)'라는 라틴어 리실이오(resilio)에서 유래된 것으로 '자극이 가해지기 전의 상태로 돌아감'을 의미한다. 복원력의 개념은 생태학자 홀링(Holling)이 생태학적 관점에서 '생태시스템이 변화를 수용하면서도 지속할 수 있는 능력의 정도'로 사용하기 시작하여 이후 생태학, 물리학, 심리학을 중심으로 사용되었으나 최근에 와서는 사회과학 여러분야에서 사용되고 있다(김도균, 박재묵, 2012). 특히 TC 292에서 다루는 조직회복력(Organizational Resilience)이라는 개념은 Yossi Sheffi가 2005년 그의 저서 '회복력 있는 기업(Resilient Enterprise)'를 통해 사업연속성전략에 회복력이라는 개념을 확장시키면서 시작되었고 미국의 국토안보부(Homeland Security Advisory Council, 2008)는 회복력을 국토안보정책의 핵심요소로 삼았다

아직은 이 분야 선행연구가 매우 부족하여 국내 산업보안 분야에 대한 정책적 아이디어와 통찰을 얻기 위한 탐색적 연구(exploratory study)이다.

ISO/TC 292와 관련한 분야 선행연구로는 윤준영 외(2015)가 재난관리 표준 내용에 국한하여 관련된 국내 법·제도 동향을 소개한 논문이 있으며, 이슬기 외(2015)는 2015년 1월, TC 292에 편입된 ISO 28000 표준에 의한 물류보안경영시스템인증 확산을 시스템 다이내믹스 이론에 기초하여 모델화 하고 시뮬레이션 함으로써 인증확산의 양태를 규명하였다. 유병태(2014)는 우리나라 사회안전분야 표준화 정책을 살펴보고 재난 및 사회안전분야 국제표준(ISO/TC223) 동향 및 표준 제정현황에 대한 조사·분석, 국제표준의 도입 필요성을 제시한 바 있다. 이밖에는 TC 292를 직접적으로 분석하여 산업보안 관련 표준화를 설명하고 있는 연구는 발견되지 않았다.

연구자는 2001~2005년에 영국에서 범죄예방과 물리적 보안에 관련된 유럽표준(EN)과 영국의 국가(BS) 및 단체 표준들(LPS 등)[3]을 분석하면서 표준을 연구하게 되었고 본격적으로는 2008년부터 유럽표준 '물리보안 계획 및 설계' 분야 기술위원회(CEN/TC 325)에 국제옵서버로 참가하면서 표준전문가 활동을 시작하였다. 이후 2009년에 산업재산권 및 영업비밀 침해 방지와 보호를 위해 탄생한 ISO 프로젝트위원회(PC)인 ISO/PC 246 Anti-counterfeiting Tools에 전문가로서, 2010년에는 이를 확장하여 설립된 ISO/TC 247 워킹그룹(WG)의 리더인 컨비너와 프로젝트 리더[4]로서 TC247(및 이후 TC292)의 총회와 WG회의에 참석하고 2014년에는 직접 서울총회를 유치 및 주도하면서 각 국의 산업보안 관련 분야 전문가들을 면접 조사할 기회를 갖게 되었다. 이 연구는 이렇게 약 7년에 걸쳐서 10회 이상 참석한 ISO 국제회의를 통해 관찰 및 수집된 문헌자료와 참여한 해외 전문가들에 대한 면접조사 내용을 분석하여 정리한 것이다. 다만 이 글에서는 면담한 전문가의 수가 너무 많고(100명 이상) 응답에 중복이 상당히 많으며 또한 지문 분량의 한계로 면담한 전문가들의 코멘

3) 예를 들면: 유럽표준 EN 1627, 1628(창문, 출입문, 셔터, 침입 강도와 저항력, 측정 등급 및 테스트), 영국 BS 7958:2009 CCTV 관리운영(Closed–circuit television (CCTV). Management and operation. Code of practice), BS 8418:2010 센싱에 의한 영상감시시스템의 설치 및 원격모니터링(Installation and remote monitoring of detector–activated CCTV systems. Code of practice), 단체표준 LPS1175(손실방지인증위원회 승인을 받기 위한 요구사항 및 시험 절차와 침입도구 및 침입저항 건축자재 등의 리스트) 등

4) 연구자가 보안 분야 2개의 New Proposal을 제안하여 NP 프로젝트로 채택되었으며, 채택된 ISO CD 18641 위조사기방지–용어정의는 현재 ISO 22300에 Standing document형태로 통합 논의되고 있고, ISO 19564 제품위조사기방지의 일반원칙은 표준화 진행 중이다.

트를 일일이 직접 인용하기보다는 편의상 본문 안에서 이를 저자가 재해석하여 설명하는 방식으로 기술하였다.

Ⅲ. 보안 분야 ISO 표준의 범위와 그 위치

표준이 보안산업을 포함한 산업 경제와 기업성장을 견인하는 국가경쟁력의 핵심요소인 동시에 각종 테러 공격이나 범죄, 재난으로부터 국민의 편안하고 안전한 삶을 보장하는 국가인프라라는 전 세계적인 인식이 확산되고 있다. 이렇게 향상된 안전한 사회에 대한 요구 등을 만족시키고 기업의 생산경쟁력을 향상시키기 위한 표준화 정책을 펼 필요가 있으며 융·복합분야 등 신성장분야에 대한 표준을 개발하고 부처간 협력체계를 공고히 하여 신수요 분야에 대한 표준 확대 등을 지속적으로 추진해야 한다. 최근, 표준의 기능과 역할은 사회적 현상과 국민 욕구의 다양화로 인해 그 범위가 대폭 확대되고 있다(국가기술표준원, 2014).

헌법 제127조는 “국가는 국가표준제도를 확립한다”고 명시하고 있으며, 이를 위해 국가표준기본법과 산업표준화법 등을 운용하고 있다.「국가표준기본법」제7조에 따르면 정부는 국가표준 관련 계획과 시책 등을 종합한 제도의 확립 및 향후 5년간 우리나라의 국가표준 발전목표와 정책방향을 설정하고 이를 달성하기 위한 범정부적 정책과제를 제시하기 위하여 국가표준기본계획을 5년 단위로 수립하도록 규정하고 있다(유병태, 2014).

ISO/IEC Guide 2(표준화 및 관련 활동에 대한 일반용어 및 정의, 1991)에 따르면 “표준은 공통적이고 반복적인 사용을 위하여 합의에 의해 제정되고 인정된 기관에서 승인된 문서로서, 주어진 여건 아래서 최적의 질서 확립을 목적으로 하는 활동이나 그 결과에 대한 규칙, 지침 또는 특성을 제공한다”라고 정의되고 있다. 표준화는 표준을 개발하고 발간하며 이행하는 프로세스를 말하며, 표준의 보급과 이해 관계자들에게 관련된 정보를 제공하는 것 등을 포함한다(국가기술표준원, 2014). 이러한 표준은 다양한 산업 분야에서 채택되어 막대한 경제적 파급효과를 유발하고 있으며, 사회 발전에 의한 시대적 요구에 따라 표준의 니즈가 변화하고 있다. 1980년대에는 산업경쟁력 강화를 위한 전통기간사업 및 정보통신 중심에서 1990년대 산업화가 발달되면서 분야가 다양해졌고 1990년에는 환경, 2000년에는 식품안전 분야가 강화되

었다. 2010년에는 안전하고 행복한 국민생활 안전분야 및 사회안전에 대한 요구가 증대하고 있다(유병태, 2014).

이러한 추세에 맞추어 2010년 12월 제3차 국가표준기본계획에는「사회안전·보안 표준화」추진과제에 의해 사회시스템표준의 체계적 이행으로 안전한 사회구현을 위하여 사회책임경영, 환경보호, 범죄예방 대처, 재난으로부터의 안전, 도로교통 안전 시스템 및 인권보호 등을 위한 표준이행을 촉진하고자 하는 계획을 포함하고 있다. 여기에서 말하는 사회시스템 표준에는 보안 및 회복력(ISO/TC292), 사회적책임(ISO26000), 환경경영체계(ISO14000), 식품안전경영시스템(ISO22000), 도로교통안전 경영시스템(ISO/PC241), 범죄예방설계[5] 등이 포함되어 있다.

Ⅳ. ISO TC 292에 의한 산업보안의 국제표준화

1. 산업보안 분야 표준화의 역사

1) ISO 산업보안 표준화의 연혁

2015년 1월부터 기존의 국제표준기구 ISO/TC 223(societal security - 사회안전 및 재난관리)이 ISO/TC 247(fraud countermeasures and control - 제품/문서 위·변조 사기 방지), ISO/TC 284(Management system for quality of Private Security Company operations - 민간보안산업의 품질경영시스템) 등 3개의 기술위원회가 TC 292 Security and Resilience로 통합되어 운영되기 시작하였다. 아울러 ISO/TC 8(supply chain security - 공급사슬보안경영시스템)에서 표준화를 진행해 온 ISO 28000시리즈도 TC 292에 흡수되었다.

TC별로 살펴보면 첫째, ISO/TC223(Societal security, 사회안전) 총회는 지난 2001년 발생한 9·11테러 이후 각종 위기 및 재난 관리 능력향상을 목적으로 2001년 설립됐다. 이 총회는 2004년 인도양 쓰나미 이후 재난관리에 관한 국제공조의 인식에 따라 UN의 요청으로 진행됐다. 스웨덴을 의장국으로 각 국가의 재난 및 보안과 표준관련

5) 소위 CPTED(crime prevention through environmental design)라고 불리는 범죄예방설계 표준화는 연구자가 주도하여 2008년~2013년 사이에 총 6종의 국가표준(KS A 8800, 8801, 8802, 8803, 8804, 8805 방범설계의 원칙 및 프로세스, 주거시설, 상업업무시설, 학교, 공원, 대중교통시설 CPTED 가이드라인)을 제정 및 개발 완료한 바 있다.

공무원, 협회·단체, 기타 전문가들이 참석해 왔다. 2006년 5월 제1차 총회는 스웨덴의 스톡홀름에서 개최하였으며, 6개월에 1회씩 년2회 총회를 개최하였다. ISO/TC223의 총회는 ISO/22300 표준전반에 대한 개발 및 제·개정을 해온 기구로서, 공조직 또는 사조직이 의도적 공격(intentionally caused attacks) 및 비의도적 또는 자연적인 원인으로 발생하는 사고(Incident)와 파괴(Disruption), 비상(Emergency), 위기(Crisis), 재난(Disaster)에 대비하기 위해 필요한 요소와 절차를 고려하는 한편, 모든 형태와 다양한 규모의 적용 가능한 프레임워크를 개발하여 재난과 테러 등 범죄공격으로부터 국민의 생명 및 신체와 재산을 보호하고자 하는데 그 의의가 있다.

둘째로 ISO/TC 247(fraud countermeasures and control - 제품/문서 위·변조 사기 방지)의 배경은 개인적인 규모에서 조직범죄집단에 이르기까지 상품 위조로 인한 손실이 세계 무역(world trade)의 7%나 차지하고 있으며, 이는 6천억 US달러를 넘는 등 큰 해악과 손실 때문이다(International Chamber of Commerce, 2007). 더욱이 위조된 부품이나 의약품은 지구인의 안전, 생명과 건강을 위협 받고 있는 가운데 이러한 위협으로 인한 산업경영 리스크를 저감하기 위해 2009년 설립되었다. TC247은 신뢰성 있는 글로벌 공급망을 구축하고, 위조 제품/서비스 구매로 인한 리스크 및 비용을 경감시키고, 개인과 조직의 ID를 각종 사기적 공격으로부터 보호할 수 있게 해주며, 다양한 산업에서 엄격한 보안 및 인증 기술을 개발 및 활용케 하며, 제품 및 서비스의 안전을 도모하고, 보안보증(security assurance) 문제에 통일된 해결책을 제시하며, ID 사기·보안보증·상품위조·문서 위변조 사기 문제 등에 대한 예방과 대응을 위한 표준화를 추진해왔다.

셋째, ISO/TC 284(Management system for quality of Private Security Company [PSC] operations - 민간보안산업의 품질경영시스템)는 세계 민간보안업체 전체의 연간 사업 규모가 200억~1000억달러(약 22조~112조원)에 달하는 가운데 내전 중이거나 전후 복구 중인 코트디부아르, 이라크나 리비아 등에서 민간보안업체가 파견한 보안요원들(용병 포함)에 의한 인권 침해 행위가 발생하거나 그런 고위험지 안에서의 사업경영, 정부운영, 인프라 보호, 재난관리 및 구호기관 활동을 지원하는 보안서비스에 상당한 품질 저하 등의 문제가 발생하면서 표준화의 필요성이 UN과 미국을 중심으로 제기되었고 인정되면서 2013년에 탄생하였다. 표준 개발을 통하여 그러한 고위험 지역에서의 민간보안산업의 서비스는 품질 및 위험을 관리하고(www.securityinfowatch.com/news/11080951), 관련 국제 인권규정을 준수하기 위한

기준을 마련해 왔다.

마지막으로 TC 8은 안전한 국제공급망 체제를 구축하기 위해서뿐만 아니라 공급 흐름에 대한 진일보한 모니터링과 밀수와 테러, 해적 등의 위협에 맞서기 위해 고안되었다. 국제무역거래시스템이 직면한 주요 문제들 중 하나가 세계공급망의 보안관련 위협인데, ISO는 두 가지 참조 문서를 통해 이 문제에 해결책을 제시하고 있다. ISO 28000 패밀리규격은 보안 관련 사고에 대비하고 수송수단을 비롯한 인력, 상품, 기반구조를 보호하며 사고 시 잠재적인 부정적 영향을 예방하고자 만들어진 규격이다. 기존의 일부 법률 및 기준은 특정 공급사슬의 보안만 다루는데 공급사슬 전반의 보안리스크를 줄이기 위해 공급사슬전반에 적용 가능한 물류보안 경영시스템 기준이 필요한데 이러한 문제들을 해결하기 위해 국제표준화기구(ISO)에서 2007년 공급사슬보안경영시스템 'ISO28000' 시리즈 규격을 제정해 온 것이다(임준영, 2006).

이렇게 ISO/TC 223의 경우 2001부터 설립 및 운영되어 왔고, ISO/TC 247는 2009년부터, ISO/TC 284는 2013년부터 설립 및 운영되어 오는 등 각 TC마다 시작점이 달랐으며 참여하는 국가 별 전문가들도 약간의 중첩도 있었지만 상호 독립적인 상태를 유지하여 왔다. 하지만 ISO에서는 security라는 용어와 영역에 대해 각각의 기술위원회마다 서로 다른 목소리와 정의를 내리면서 조화되지 못하고 상호 충돌하는 양상이 발생하자 2014년 6월에 ISO 산하 기술관리위원회(TMB)에서 위원회 간 조화와 통일성 향상을 위해 security와 연관된 모든 TC들을 통합하여 하나의 TC를 설립하는 결정을 내림으로써 이루어진 것이다. 특히 ISO가 주로 산업과 기술에 관한 표준을 다룬다는 점에서 이러한 결정은 산업보안 관련 영역을 전체적이고 효율적으로 융합시켜 표준화하려는 의도로 해석될 수 있다.

총 50여개 회원국이 참여하고 있는 ISO TC 292는 산업보안과 관련된 다양한 전문영역들 간에 서로 업무의 중복을 피하고 용어정의의 충돌을 막으면서 동시에 산업의 보호와 손실방지라는 같은 목표와 방향을 향해서 서로 조정하고 조화를 추구하고 있다.

2) ISO TC 292 워킹그룹 틀의 변경

TC 292는 2015년 1월 시작단계에서는 TC의 타이틀을 '보안(security)'으로 하였으나 전 세계적으로 각종 테러공격이나 재난 등의 위험(risk)으로 인해 불확실성(uncertainty)이 높아가고 보안 실패의 상황이 빈발하는 가운데 국가, 기업, 개인의

사업연속성(public private business continuity)과 회복력(resilience)의 중요성을 강조하면서 '보안 및 회복력(security and resilience)'로 변경되었다(표 1 참조).

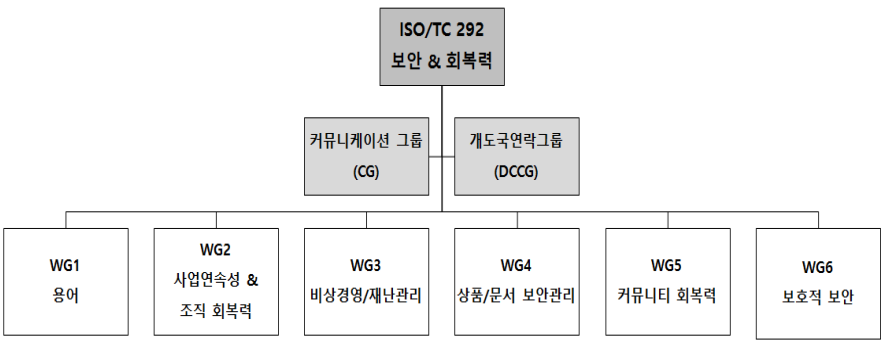
〈표 1〉 ISO TC 292 워킹그룹 틀의 변천

WG	WG 명칭
WG1	공급망 보안관리 시스템 (Security management systems for the supply chain)
WG2	사회적 보안관리 프레임워크 기준 (Framework standard on societal security management)
WG3	용어 - 사회적 보안 (Terminology - Societal security)
WG4	비상경영 및 재난관리 (Emergency management)
WG5	회복력 및 연속성 (Resilience and continuity)
WG6	대규모 대피 (Mass evacuation)
WG7	보안 보증 (MSS for security assurance)
WG8	용어 – 위조사기 대책 (Terminology - Fraud countermeasures & control)
WG9	위조 및 불법 거래를 방지하기 위한 상호운용성 및 인증 시스템 가이드라인 (Guidelines for interoperable object and related authentication systems to deter counterfeiting and illicit trade)
WG10	제품 위조사기 방지대책 (Product Fraud Countermeasures and Controls)
WG11	문서 위조사기 방지대책 (Document Fraud Countermeasures and Controls)
WG12	민간보안 운영을 위한 경영시스템 - 지침과 요구 사항 (Management system for private security operations - Requirements with guidance)
	⇩
WG	WG 명칭
WG1	용어 (Terminology)
WG2	사업연속성 및 조직회복력 (Continuity and organizational resilience)
WG3	비상경영 및 재난관리 (Emergency management)
WG4	제품/문서의 정품성, 무결성과 신뢰성 (Authenticity, integrity and trust for products and documents)
WG5	커뮤니티 회복력 (Community resilience)
WG6	보호적 보안 (Protective security)
특별그룹	커뮤니케이션 그룹 (communication group) 개발도상국콘텍그룹 (Developing country contact group)
태스크포스	UN기구와의 협력을 위한 TF (Cooperation with UN agencies)

산업보안 분야 별로 표준 개발 추진을 위한 작업반인 워킹그룹(WG)은 1회 모리오카 총회에서 주제별로 12개였으나 대표단 회의(2015년 8월 30일, 9월 31일, 제네바)와 2015년 12월 총회를 거치면서 6개의 WG과 2개의 특별그룹, 그리고 1개의 Task Force으로 재편되었다.

2. TC 292 표준화의 전반적 프레임

전체적인 TC 292의 표준화 내용의 모습은 민간 산업보안과 공공 재난관리 요소들이 다소 혼합되어 있다고 볼 수 있다. 그러나 제정되었거나 개발 진행 중인 TC 292 내의 표준들은 대부분 산업보안이나 보안산업 분야에 그 성격 상 직접 적용해야 하거나 직·간접적으로 활용할 수 있는 것들이다. 크게 보면 TC 292는 사업연속성경영, 비상경영 및 재난관리, 회복력, 지식재산권(IPR) 보호를 위한 제품과 문서의 보안, 영상감시 등 물리적 보안과 보안서비스 품질경영, 물류보안관리 등으로 구분될 수 있다. 공식적으로 TC 292 홈페이지 www.isotc292online.org에서 제시된 WG 별 보안 분야 표준화의 틀은 <그림 1>과 같다.



〈그림 1〉 ISO/TC 292의 워킹그룹 별 표준화의 틀

여기서 TC292는 산업보안 분야에서 다루는 일반적인 주제들과 크게 다르지 않지만 재난관리, 회복력, 물류보안 등은 산업보안과 연관성은 있으되 다소 특화된 보안 영역들을 포괄하고 있는 것으로 분석된다. 실제로 2015년 12월 발리 TC 292 총회에서도 보안 분야의 새로운 워킹그룹의 설립을 권고한 바 있고 그만큼 향후 TC 292

안에서 산업보안 관련 표준화의 영역이 넓어지고 확대되는 방향으로 나아갈 수 있다는 것을 시사한다.

TC 292에서 제정된 표준은 총 20개이며 현재 개발 진행 중인 표준은 총 11개로 집계되었다. 이 중에서 개발(제정) 진행 중인 각 표준의 진행단계는 <표 2>와 같다.

〈표 2〉 ISO/TC 292에서 제정 진행 중인 표준 별 단계

워킹 그룹	표준 번호	제정 단계*	표준명(프로젝트)
WG1	ISO 22300	개정 중	용어 (Terminology)
WG2	ISO 22316	DIS	사회안전- 조직 회복력 가이드라인 (Societal security - Guidelines for organizational resilience)
	ISO 21272	NP	사업연속성전략 지침(BCMS-Guidelines for business continuity strategy)
	ISO 22330	NP	사업연속성의 인적 자원 지침(BCMS-Guidelines for people aspects on business continuity)
WG3	ISO 22325	DIS	비상경영-역량 평가 지침(Emergency management-Guidelines for emergency management capability assessment)
	ISO 22326	AWI	비상경영-확인된 위험요인 모니터링 지침(Guidelines for monitoring of facilities with identified hazards)
WG4	ISO 34001.3	DIS	사기위조방지를 위한 보안경영시스템(Security management system - Fraud countermeasures and controls)
	ISO 19998	NP	소비세 소인의 내용, 보안, 발급 요구사항(Requirements for the content, security and issuance of excise tax stamps)
	ISO 19564	AWI	상품사기방지의 일반 원칙(Product Fraud Countermeasures and Control - General Principles)
	ISO 20229	WD	위조·불법거래 방지를 위한 상품식별시스템 간 상호운용성 지침 (GuideLine for establishing interoperability among object identification systems to deter counterfeiting and illicit trade)
WG5	ISO 22319	CD	긴급 자원봉사자 지침(Guidelines for spontaneous volunteers
	ISO 22325	NP	취약한 사람들을 돕기 위한 공동체의 대응 지침(Security and resilience – Community resilience - Guidelines for supporting community response to vulnerable people)
	ISO 22396	NP	조직 간 정보교환 지침(Guidelines for information exchange between organizations)
WG6	ISO 22311	개정 중	보안 영상감시-송출 상호운용성 (Societal security - Video-surveillance - Export interoperability - revision)

* 표준개발 절차 : PWI(예비) → NP(제안) → WD(준비) → CD(위원회) → DIS(질의 및 승인) → IS(출판)
* AWI : Approved Work item(승인된 작업 항목)

3. 워킹그룹 별 표준화의 내용

TC 292의 사업 범위는 크게 보면 사회의 안전과 회복력 제고를 위한 보안분야 표준화이다. 하지만 ISO/TC 262 리스크관리나 ISO/PC 278 반부패(뇌물수수) 경영시스템 등 분야 별로 크게 차별화되거나 별도로 표준화되어야 할 만큼 비중이 큰 영역의 표준은 제외하고 있다. 통합된 지 얼마 되지 않은 TC의 성격 상 아직 TC 292의 전략적 비스지스 플랜(strategic business plan)과 목표는 설정이 완료되지 않았고 논의 중에 있다. 여기서는 TC 292의 공식 웹사이트(www.isotc292online.org)에서 제시하는 바대로 워킹그룹 별 표준화 주제를 따라 (1)용어 정의(terminology) 및 일반적 보안 기준, (2)사업연속성 및 조직회복력(Continuity and organizational resilience), (3)비상경영 및 재난관리 (Emergency management), (4)제품·문서의 보안관리(Authenticity, integrity and trust for products and documents)[6], (5)커뮤니티 회복력(Community resilience), (6)보호적 보안 (Protective security), (7)공급사슬보안경영시스템(Supply chain security management)의 순으로 표준화 내용을 각각 설명하고자 한다.

1) 용어 정의(terminology) 및 일반적 보안 원칙(General standards)

용어 정의 및 일반적 보안원칙 분야에서는 다음과 같이 3개의 표준이 제정 완료되었다(표 3 참조).

〈표 3〉 용어 정의 및 일반 보안원칙 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 22300 Societal security – Terminology	용어
	ISO/TR 22312 Societal security – Technological capabilities	기술적 역량
	ISO 22398 Societal security – Guidelines for exercises	훈련을 위한 지침

ISO 22300 Societal security – Terminology은 TC 223 사회안전 분과에서 2012년에 제정되었다. 그러나 TC 292로 기존 TC에서 개별적으로 진행하던 용어정의 표준화가 통합되면서 보다 폭넓은 보안 분야를 다루야 하는 상황이 되면서 이를 개정하는 작

6) 직역하면 '제품·문서의 위조방지를 위한 정품성, 무결성과 신뢰'이나 WG4의 작업 범위가 전체적으로 보면 제품/문서의 보안에 해당하여 이렇게 의역하였다.

업이 진행되고 있다. Security라는 개념에 대하여 포괄적으로 정의하는 것을 어려운 일이다. 가령 ISO 28000:2007 공급사슬보안경영시스템 표준에 의하면 'security'란 '물류에 대하여 혹은 물류에 의해 손상이나 해를 야기하도록 계획된 고의적, 비인가된 행위에 대한 저항능력'이라고 정의하고 있다. 물류라는 분야에서만 이렇게 정의되고 있는 것인데 그 밖의 여러 보안 분야에 포괄적으로 적용되는 개념정의를 수립하고자 하는 것이다.

또한 일반적인 보안 원칙으로는 ISO/TR[7] 22312 기술적 역량과 ISO 22398 훈련을 위한 지침이 제정되었다. ISO/TR 22312는 보안 분야 내에서 기술적 표준을 개발하는 것으로서 실제 보안 장비, 보안 솔루션, 보안 시스템 등 구체적인 기술적 기준을 제시하는 것이다. 한편 ISO 22398은 표준화된 훈련·테스트 프로그램을 제시하고 있으며 모의훈련과 테스트로 구분되어 사건·사고 시나리오는 목적에 따라 훈련형태를 선택하도록 되어 있다. 현재 다른 WG를 통해 제시되는 더 많은 용어를 포괄하기 위한 개정 작업이 진행 중이다.

2) 사업연속성 및 조직회복력(Continuity and organizational resilience)

사업연속성 및 조직회복력 분야에서는 다음과 같이 5개의 표준이 제정 완료되었고, 현재 3개의 표준이 개발 진행 중에 있다(표 4 참조).

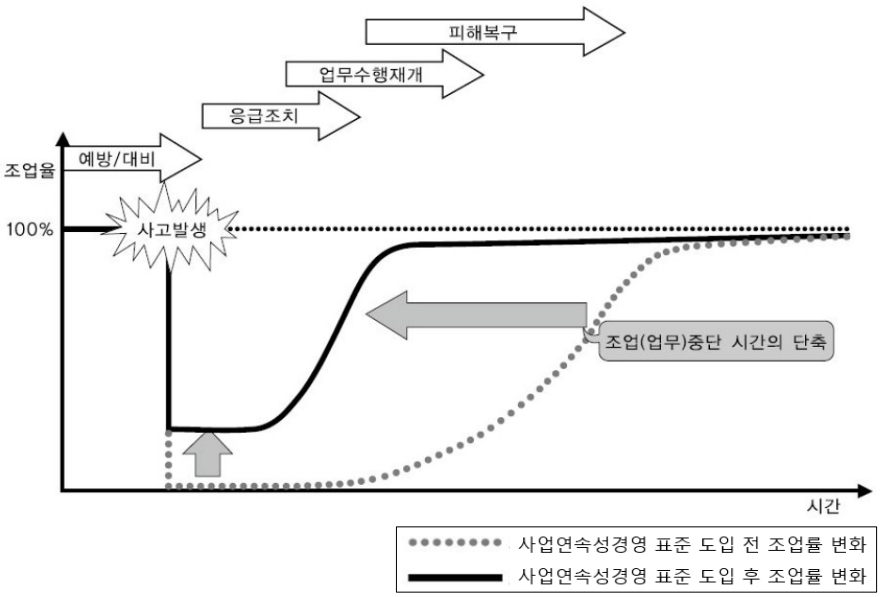
〈표 4〉 사업연속성 및 조직회복력 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 22301 Business continuity management systems [BCMS] – Requirements	사업연속성경영시스템 요구사항
	ISO 22313 BCMS – Guidance	사업연속성경영시스템 지침
	ISO/TS 22317 BCMS – Guidelines for business impact analysis(BIA)	사업영향분석(BIA) 지침
	ISO/TS 22318 BCMS – Guidelines for supply chain continuity	공급사슬 연속성 지침

7) 국제표준은 제정 시 작업제안 단계부터 최종 규격의 발간까지 평균 5–7년이 소요됨에 따라 첨단기술과 같이 급변하는 기술에 대한 요구를 만족시키는데 어려움이 있다고 판단, TR/TS/PAS 등 유연한 형태의 기준 문서를 발간하고 있는데 TR은 기술보고서로서 관련 정보를 제공하는 문서이며, TS는 기술시방서로서 향후 규격으로 발간될 가능성이 있는 문서이며, PAS는 WG(작업반)차원의 합의를 반영하는 규범적 문서로서, 신규작업항목 등록 시 TC/SC 차원에서 논의를 거쳐 규격으로 제정할지 또는 PAS로 제정할지를 결정하게 된다(www.iso.org).

	ISO/IEC/TS 17021-6 Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 6: Competence requirements for auditing and certification of business continuity management systems	적합성 평가를 위한 사업연속성경영시스템 인증심사를 위한 역량 요구사항
진행 표준	ISO 22316 Societal security - Guidelines for organizational resilience	사회안전- 조직 회복력 가이드라인
	ISO 22330 BCMS-Guidelines for people aspects on business continuity	사업연속성의 인적 자원 지침
	ISO 21272 BCMS-Guidelines for business continuity strategy	사업연속성전략 지침

먼저 ISO 22301 사업연속성경영시스템 요구사항은 사업연속성을 확보하기 위해 사업에 대한 위협을 이해하고 우선순위를 결정하는 하는 것으로서 파괴적인 사건·사고로부터 사업을 복구하고, 사건·사고 가능성을 줄이며, 사업을 보호할 수 있도록 경영시스템 요구사항을 명시하고 있다(그림 2 참조).



〈그림 2〉 사업연속성경영 시행의 효과[8)]

8) 그림 출처 : 소방방재청(2012)

ISO 22301에서 규정하는 요건은 조직의 형태, 규모 및 특징에 관계없이 모든 조직들 또는 조직들의 일부에 일반적으로 적용되도록 하는 목적으로 만들어졌으며 이러한 요건들에 대한 적용의 범위는 조직의 운영환경과 복잡성에 따라 좌우된다. 이러한 요구사항은 법적, 규정적, 조직적 및 산업의 요구사항, 제품 및 서비스, 채택된 프로세스, 조직의 규모 및 구조, 조직의 이해관계자들의 요구사항에 의해서 모습을 갖추게 된다.

ISO 22313 사업연속성경영시스템 지침은 ISO 22301 요구사항에 대하여 보다 자세하고 명료한 안내서로의 역할을 한다. ISO/TS 22317 사업연속성경영시스템-사업영향분석(BIA) 지침은 ISO 22301이 요구하는 사업영향분석을 수행하기 위한 지침을 제공한다. 사업영향분석은 사업연속성과 복구 우선순위, 목표 그리고 대상을 결정하기 위한 프레임워크를 제공한다. 사업영향분석의 목적은 파괴적인 사건·사고가 조직이나 기업에 주는 영향을 분석하는 것이다.

ISO/TS 22318 사업연속성경영시스템-공급사슬 연속성 지침은 외부의 상품 및 서비스 공급망과 기업 내부 서비스에 대한 평가와 관리에 대한 기준을 제공한다. 특히 공급망의 차단에 따른 사업의 차질에 대비하여 소비자와 공급자의 양 측면에서 이를 보호하기 위한 적절한 대책을 제시한다.

ISO/IEC/TS 17021-6 적합성 평가를 위한 사업연속성경영시스템 인증심사를 위한 역량 요구사항은 인증기구가 갖추어야 할 구체적인 기능에 맞춘 일정한 유형의 지식과 기술을 반영하는 ISO/IEC 17021 : 2011의 현행 요구사항의 보충적 기술시방서이다. 사업연속성경영시스템과 ISO 22301을 위한 인증 프로세스에 참여하는 심사원(auditors) 등 관련 인력의 구체적 역량 요구사항을 제시한다.

한편 개발 진행 단계의 표준인 ISO 22316 사회안전 - 조직 회복력 가이드라인은 사업연속성경영 외에도 TC 292 전체에 적용되는 포괄적인 내용을 다루고 있다. 조직의 회복력이란 복잡하고 (급)변화하는 불확실성의 위협과 기회의 환경에서 기업이나 조직이 이를 예측하고 대응하면서 복원 및 적응할 수 있는 유연성과 역량을 갖추기 위한 거버넌스(governance)[9] 원칙과 전략을 제시한다. ISO 22330 사업연속성의 인적

9) 일반적으로 거버넌스는 공공문제 해결을 위해 정부부문과 민간부문 간에 이루어지는 협력적 체계로 정의된다. 따라서 보안경영 및 재난관리 거버넌스 또한 시민의 안전한 생활을 위하여 정부, 기업, NGO, 시민 등 다양한 행위주체들이 의사결정권을 공유하고, 상호의존과 협력의 네트워크를 구성하여 보안관리정책(재난 포함)을 집행해나가는 체계로 정의될 수 있다(이재은 · 양기근, 2004 참고).

자원 지침는 파괴적인 사건 · 사고에 의해 영향을 받거나 관여가 될 수 있는 사람들에 대한 니즈(needs)를 강조하는 기준으로서 이러한 상황 하에서의 사업운영을 하는 인적 자원 관리책임자를 위한 기술적 지침을 제공한다. ISO 21272 사업연속성전략 지침은 ISO 22301이 요구하는 사업연속성전략의 선택 및 결정을 위한 지침을 제공한다.

3) 비상경영/재난관리(Emergency management)

공공분야에서는 재난관리로 산업보안에서는 비상경영 등으로 해석될 수 있는 emergency management 분야에서의 표준화는 다음과 같이 4개의 표준이 제정되었고, 2개의 표준 개발이 진행되고 있다(표 5 참조).

〈표 5〉 비상경영 / 재난관리 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 22320 Societal security – Emergency management –Requirements for incident response	비상경영-사고대응 요구사항
	ISO 22322 Societal security – Emergency management – Guidelines for public warning	비상경영-공공 예 · 경보
	ISO 22324 Societal security – Emergency management – Guidelines for colour coded alert	비상경영-컬러 경고 코드
	ISO/TR 22351 Societal security – Emergency management – Message structure for exchange of information	비상경영-정보 교환을 위한 메시지 구조
진행 표준	ISO 22325 Security and resilience - Emergency management - Guidelines for capability assessment	비상경영-역량평가지침
	ISO 22326 Security and resilience - Emergency management - Guidelines for monitoring of facilities with identified hazards	비상경영-확인된 위험 시설 모니터링 지침

제정 완료된 ISO 22320 비상경영-사고대응 요구사항은 “효과적인 사고대응을 위한 최소한의 요구사항[10]”을 규정하며 사고대응 조직의 내부에서 지휘통제, 운영정보, 조정 및 협력을 위한 기본사항을 제공한다. 이것은 지휘통제 조직체계 및 절차,

10) minimum requirements for effective incident response

의사결정 지원, 추적가능성, 정보 관리와 상호운영을 포함한다. ISO 22320은 국제적, 국가적, 지역적 또는 지방 차원에서 사고에 대한 대비 또는 대응에 참여하는 어느 조직(민간, 공공, 정부 또는 비영리)에라도 적용 가능하며 관련된 조직들을 포함한다(소방방재청, 2012).[11]

ISO 22322 비상경영-공공 예·경보 지침은 재난, 테러 공격이나 대형 사고 발생 시 생명을 구하고, 손실을 경감시키기 위하여 빠르고 효과적인 예보와 경보 체계를 갖추어야 하는데, 리스크를 커뮤니케이션하기 위한 시간이 매우 제한적이기 때문에 실제 행동을 요구하는 구체적인 메시지를 많은 사람들에게 효과적으로 전파하기 위한 지침을 제시한다.

ISO 22324 비상경영-컬러 경고 코드 위기에 처한 상태에서 관련된 사람들에게 그 상태를 수준 별로 효과적으로 전달하기 위해 적색(Red), 노랑색(Yellow), 녹색(Green) 등 컬러로 경고를 안내하는 것에 대한 지침이다. ISO/TR 22351 비상경영-정보 교환을 위한 메시지 구조는 비상경영에 관련된 조직 간 정보교환을 위해 상호운용성을 제고하는 메시지 구조를 설명하고 있다.

현재 개발 진행 중인 ISO 22325 비상경영-역량평가지침은 비상경영 역량을 평가하고 개선하기 위해 비상경영역량 평가 방법론과 프로세스의 지표를 제공한다. 또한 ISO 22326 비상경영-확인된 위험 시설 모니터링 지침은 위험에 처한 시설에 대한 모니터링 프로세스인 계획, 개발, 실행, 관리, 지속적 개선 등에 대한 지침을 제공한다.

4) 제품·문서의 보안관리[12](Authenticity, integrity and trust for products and documents)

제품·문서의 보안관리를 위한 정품성(진위), 무결성 인증과 신뢰 분야에서는 다

11) 다음 분야에 관련된 조직들이 ISO22320을 적용할 수 있다(소방방재청[2012]에서 인용)
- 사고 예방과 회복력 대비에 대한 책임 및 참여
- 사고 대응에 대한 지침과 관리 제공
- 지휘통제를 위한 규정과 계획 개발
- 사고 대응을 위하여 다수 기관/조직의 조정 및 협력 개발
- 사고 대응을 위한 정보 및 커뮤니케이션 체계 개발
- 사고 대응, 정보와 통신 및 데이터 상호운용성 모델 분야 연구
- 사고 대응에서 인적 요소(human factor) 분야 연구
- 공공과의 커뮤니케이션 및 상호작용에 대한 책임

12) '제품·문서의 위조방지를 위한 정품성, 무결성과 신뢰'는 제품/문서의 보안경영을 위한 요체이다.

음과 같이 2개의 표준이 제정되었고 4개의 표준이 제정 진행되고 있다(표 6 참조).

〈표 6〉 제품 · 문서의 보안관리 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 12931 Performance criteria for authentication solutions used to combat counterfeiting of material goods	유형제품의 위조방지에 사용되는 진품입증솔루션의 성능기준
	ISO 16678 Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade	상호운용 가능한 상품식별과 위조 · 불법거래 방지를 위한 입증 시스템 지침
진행 표준	ISO 34001 Security and resilience - Security management system - Fraud countermeasures and controls	제품/문서 위조방지 보안경영시스템
	ISO 19564 Security and resilience - Product fraud countermeasures and control - General principles	상품사기방지의 일반 원칙
	ISO 19998 Security and resilience - Requirements for the content, security and issuance of excise tax stamps	소비세 소인의 내용, 보안, 발급 요구사항
	ISO 20229 Security and resilience - Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade	위조 · 불법거래 방지를 위한 상품식별시스템 간 상호운용성 지침

WG4에서 제정하고 개발되고 있는 '제품 · 문서의 정품성(진위), 무결성 인증과 신뢰' 표준들은 주로 산업재산권[13]과 영업비밀 등의 지식재산권의 침해 방지와 보호를 목표로 하고 있다. 이 중에서 제정된 ISO 12931 유형제품의 위조방지에 사용되는 진품입증솔루션의 성능기준은 유형상품의 라이프 사이클에 걸쳐 제품이 진품임을 확인하기 위해 사용되는 진품입증솔루션의 성능 기준과 평가방법을 자세히 기술하고 있다(박현호, 2014).

ISO 16678 상호운용 가능한 상품식별과 위조 · 불법거래 방지를 위한 입증 시스템 지침은 상품 식별과 위조 및 불법 거래 방지를 위한 관련 시스템의 상호운용을 위한 표준화를 통해 신뢰하는 조사자가 상품의 진품 입증을 하는데 있어서 정확한 식별 정보 접근과 전달을 용이하게 하기 위해서 제정되었다. 또한 사용편리성 향상을 통해 정확한 정보를 가지는 다수의 시스템 참여를 촉진하여 위조 탐지 증가와 위조사

13) 산업재산권은 특허권, 상표권, 실용신안권, 디자인권으로 세분화된다(국가지식재산위원회, 2013).

기에 의한 손실 감소를 도출하려는 목적도 가진다. 이에 연관되어 개발 중인 ISO 20229 위조·불법거래 방지를 위한 상품식별시스템 간 상호운용성 지침은 ISO 16678이 제시하고 있는 상호운용성에 대한 시스템적 틀과 방법론을 제시하고자 한다.

현재 개발 진행 중인 또 다른 ISO 34001 제품/문서 위조방지 보안경영시스템은 제품·문서의 위조나 사기를 방지하기 위한 일반적인 보안경영시스템 기준을 제시하고 있다. 또 ISO 19564 상품사기방지의 일반 원칙은 제품 위조나 위화(adulteration)를 포함한 다양한 제품사기 공격 유형과, 제품사기범죄자(개인, 집단, 조직 등)의 다양한 수준을 제시하고 그 위험에 대한 평가방법과 맞춤형 위험관리 대책을 제시하고 있다. 한편 진행 중인 ISO 19998 소비세 소인의 내용, 보안, 발급 요구사항은 상품이 물품세나 소비세 등을 납부해서 합법적으로 시장에 나와 있다는 것을 증명하거나 표시해 주는 물리적 또는 非물리적 소인(stamps)의 내용, 보안 그리고 발급에 대한 요구사항들이 제시된다.

5) 커뮤니티 회복력(Community resilience)

커뮤니티 회복력 분야에서는 다음과 같이 2개의 제정 표준과 3개의 진행 표준이 있다(표 7 참조).

〈표 7〉 커뮤니티 회복력 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 22315 Societal security – Mass evacuation – Guidelines for planning	대규모 대피 계획 지침
	ISO 22397 Societal security – Guidelines for establishing partnering arrangements	파트너쉽 협정 지침
진행 표준	ISO 22319 Security and resilience - Community resilience - Guidelines for spontaneous volunteers	긴급 자원봉사자 지침
	ISO 22325 Security and resilience – Community resilience - Guidelines for supporting community response to vulnerable people	취약한 그룹을 돕기 위한 공동체의 대응 지침
	ISO 22396 Security and resilience - Community resilience - Guidelines for information exchange between organizations	조직 간 정보교환 지침

제정된 ISO 22315 대규모 대피 계획 지침은 비상 시 대규모 대피를 준비하기 위한 계획 수립, 실행, 모니터링, 검토 그리고 개선에 관한 지침을 제시하고 있다. 테러 등 비상 시 체계적으로 단계적인 대규모 대피를 성공시키기 위한 프레임을 제시하고 효과적인 평가를 받기 위한 증거에 기초한 계획으로 기업이나 조직이 인명을 구조하고 고통을 최소화하기 위한 의무사항을 제공한다.

ISO 22397 파트너쉽 협정 지침은 비상 시 관련된 지역이나 국가, 글로벌 공동체 수준에서 정부, 기업, 조직, 부서 간 다양한 업무 영역에서의 충돌이나 프로세스 상의 중복을 방지하기 위한 명료한 파트너십 체계에 관한 계획의 수립, 실행, 모니터링, 검토 그리고 개선에 관한 지침을 제시한다.

진행되고 있는 표준인 ISO 22319 긴급자원봉사자(SV) 지침은 테러 등 재난 사고 발생 시에 소방, 경찰 등 구호기관과 요구호자 등을 돕기 위해 편성되는 긴급자원봉사자(SV)들을 구호작업에 참여시키고, 협업 계획을 수립하고, 이들의 안전을 위해 위험관리를 하는 책임을 지는 기업, 지자체, 정부, NGO 등의 조직들이 활용하는 지침을 제공한다. 또한 ISO 22325 취약한 그룹을 돕기 위한 공동체의 대응 지침은 사건·사고의 발생으로 가장 취약한 집단(아동, 장애인, 노약자 등)을 우선적으로 구호하고 보호하기 위해 기업을 포함한 다양한 공동체의 구성요소들이 실행 및 유념해야 할 지침을 설명한다. ISO 22396 조직 간 정보교환 지침은 근래의 사건 · 사고 위험의 양태가 개인, 기업, 공공/민간 조직 등 영역에 관계없이 점차 상호 연결되고 상호 의존적으로 변하면서 이러한 위험관리에 참여하는 조직, 기업 간 상호 정보교환의 필요성이 증가하면서 제시된 것이다. 이 표준은 그러한 조직 간 정보교환 협정의 원칙, 프레임워크 및 프로세스에 대한 지침을 제공한다.

6) 보호적 보안(Protective security)

현재 Preventive Security(예방적 보안[14])으로 그 타이틀 개정을 논의 중인 WG6 보호적 보안에서는 다음과 같이 2개의 표준이 제정되었고 그 중에 1개는 개정이 진행 중이다(표 9 참조). 물론 WG6 보호적 보안은 최근에 발표된 개발로드맵(TC292 N 265 TC292 Draft Road map from ISO/TC 292/WG 6 Protective security)을 볼 때 향

14) 공공이든 민간이든 보안 분야에서는 전 세계적으로 대응보다는 예방력 강화를 강조하는 추세이다. 체계적인 예방을 통한 손실방지가 대응과 복구에 의한 접근방법에 비하여 훨씬 비용효과성이 높기 때문인 것으로 판단된다.

후 TC292 안에서 큰 비중을 차지할 것으로 예측된다. 그 로드맵의 틀을 보면 <표 8>와 같다.

〈표 8〉 WG6 '보호적 보안' 표준개발 드래프트 로드맵[15]

항목	세항목	관련 표준	향후 개발 분야
보안 프로그램 및 시스템의 관리 및 경영	- 보안경영 - 민간보안 - 보안감사 및 리뷰 - 적합성평가 - 보안리스크관리 - 보안리포팅	ISO 18788 ISO 28000 ISO 28001 ISO 28002 ISO 28003 ISO 28004 ISO 14298[16] ISO 34001	보안경영시스템(SMS) 보안리스크관리(TC262 연계) 민관 보안 파트너쉽 민간보안서비스 가이드라인 ISO 18788 적합성평가 취약성평가 및 위협평가 보안 정보관리 다중운집시설(교통, 주거, 상업)의 보안 대형행사 등 혼잡경비보안 대중교통시설 보안 총기사고 등에 대한 공격대응(attack response) 관리 중요시설붕괴 보안대응 관련 표준의 적합성 툴
사건·사고 (Incident) 관리	- 보안조사 - 대응 및 복구 - 사건·사고 분류 - 완화		사건·사고 보안조사 사건·사고 대응 및 복원(remediation) 사건·사고의 분류(ISO/IEC JTC1/SC 27 정보통신보안 연계) 사고 영향 완화(mitigation) 케이스관리 복구(recovery)
물리적 보안	- 보안 계획 및 설계 - 접근통제시스템 - 물리적 자산 보호		보안 및 방범 계획/설계 실행 가이드라인 물리적 자산보호의 가이드라인

15) 출처 : TC292 N 265 TC292 Draft Road map from ISO/TC 292/WG 6 Protective security

인적 보안	- 조사 - 입사 신원조사, 스크리닝, 인사평가 - 보안 인식 및 교육 - 신분확인 및 접근 - 보안문화		보안조사 신원조사, 스크리닝, 인사평가, 보안지도 보안 인식 제고 교육 신분확인 및 접근 보안문화 인적 고위험요소 관리 가이드라인 소셜미디어와 verbal 커뮤니케이션 보안 가이드라인 보안 테스트 가이드라인
정보보안	- 정보평가 - 유형정보의 관리 체계 - 전자 및 오디오 대응과 조사	ISO 27000	민감문서의 보안관리 문서 전송 보안통제 전자 및 오디오 보안 대응과 조사
감시 (surveillance)	- 정적 감시 - 이동 감시 - 데이터 감시 - 영상 감시	ISO 22311	정적 감시, 이동 감시, 데이터 감시, 영상 감시의 관리 및 시스템 가이드라인

그 중에서 ISO 22311 영상감시 송출의 상호운용성 표준은 전술한 바와 같이 위험관리를 위해 조직 간 상호 영상 정보교환의 원활한 실천을 위한 것이다.

〈표 9〉 보호적 보안 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 22311 Societal security – Video-surveillance – Export interoperability	영상감시 송출의 상호운용성
	ISO 18788 Management system for private security operations - Requirements with guidance for use	민간보안서비스 경영시스템의 사용 지침 요구사항

즉, 이것은 정보수집, 위험관리, 법과학 수사를 수행하는 수사기관 등 end-user들이 디지털 영상에 접근하여 필요한 업무를 수행하는 것을 돕기 위하여 교환성 있는 데

16) 문서 보안 관련 보안프린팅(인쇄)

이터 저장장치 미디어에 의한, 또는 네트워크를 통한 영상감시 콘텐츠 집적시스템으로부터 추출하는 공통적 출력파일 포맷에 대한 시방을 제시하고 있다. 異기종 CCTV 간의 신속한 영상자료의 공유 사용을 위한 최소한의 기술적 요구사항(비디오, 오디오, 메타데이터, 출력파일 보호, 데이터 접근 보안, 개인프라이버시 보호 등)을 제공하는 것이다. 요구사항의 기술적 진화 내용을 업데이트하기 위하여 2016년 5월 현재, 이 표준의 개정이 진행 중이다.

ISO 18788 민간보안서비스 경영시스템의 사용 지침 요구사항은 민간보안산업을 위하여 보안운영관리 체계를 수립, 실행, 운용, 모니터링, 리뷰, 유지, 개선하기 위한 프레임워크를 제공한다. 즉, 이 표준은 보안운영관리시스템(security operations management system)의 원칙과 요구사항을 제시하며, 특히 테러나 재난 등으로 인하여 거버넌스 체계가 약화된 지역 환경에서 운영되는 다양한 형태의 보안기업의 서비스에 적용된다.

7) 공급사슬 보안경영시스템(Supply chain security management)

국제적으로 테러 위협이 증가하여 물류 보안의 중요성이 날고 커져가면서 항공기, 국제 선박 및 시설에 관한 보안검색이 강화되면서 세계 각국이 다양한 물류보안제도를 시행하고 있는 가운데 탄생된 ISO 공급사슬보안경영시스템 표준들은 다음과 같이 총 5개의 표준이 제정되어 있다(표 10 참조).

〈표 10〉 공급사슬 보안경영시스템 표준

구분	표준명(영문)	표준명(한글)
제정 표준	ISO 28000 Specification for security management systems for the supply chain	공급사슬 보안경영시스템 시방 – ISO 28000 실행지침
	ISO 28001 Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance	공급사슬보안경영시스템 - 공급사슬 보안의 실행, 평가, 계획의 모범경영
	ISO 28002 Security management systems for the supply chain - Development of resilience in the supply chain - Requirements with guidance for use	공급사슬보안경영시스템 - 공급사슬 회복력 개발 사용지침 요구사항
	ISO 28003 Security management systems for the supply chain - Requirements for bodies providing audit and certification of supply chain security management systems	고급사슬보안경영시스템 - 심사 및 인증기관 요구사항
	ISO 28004 Security management systems for the supply chain - Guidelines for the implementation of ISO 28000 (Part 1-4)	공급사슬 보안경영시스템 – ISO 28000 실행지침

ISO 28000시리즈는 공급사슬을 관리하는 조직과 공급사슬에 포함된 제조, 서비스, 보관 및 운송 관련 조직에서 적용할 수 있도록 개발된 경영시스템으로서 공급사슬의 보안에 대한 리스크와 위협에 대한 관리를 하도록 요구한다. 화물의 흐름에 대한 효과적인 모니터링을 포함하며 밀수를 방지하고 해적의 위협이나 테러리스트의 공격에 대응하도록 할 뿐만 아니라 안전한 국제적인 공급사슬시스템을 만들도록 설계되었다. 조직이 공급사슬의 보안을 보장하는데 필요한 핵심적인 측면을 포함하여 보안경영시스템을 수립, 이행, 유지 및 개선하도록 하는 요구사항을 담고 있는 것이다. 이러한 핵심적인 측면은 재무회계, 제조, 정보보안, 그리고 상품의 포장, 보관 및 수송시설을 포함한다.

보안경영시스템 구조 및 적용 범위는 프로세스 접근방식(Process Approach)을 채택하고 있는 ISO 28000은 PDCA(Plan-Do-Check-Act) cycle을 기반으로 하며, 이미 효과가 충분히 입증된 ISO 14001규격을 모델로 하고 있다. 그러므로 위험요소에 기초한 접근방법(Risk Based Approach)에 의해 공급사슬의 보안 위험성 및 위험요인을 분석할 수 있다. 이 표준은 단독으로 사용할 수 있으며, ISO 9001 또는 ISO 14001 규격과 통합시스템으로 운영할 수도 있다.

ISO 28000은 공급사슬에 포함된 제조, 서비스, 보관 및 운송의 각 단계에 위치한 대, 중, 소규모의 어떠한 조직에도 적용이 가능하다. 현재 및 미래의 보안관련 법규를 파악하여 충족하게 하도록 체계적인 접근 방법을 제공한다. 이를 통해 물류보안 관련 리스크에 대한 효과적인 관리가 가능하고 조직이나 기업의 방침에 대한 실행의지를 확인하며 목표 달성을 위한 지속적 개선을 유도한다. 또한 원자재의 효율적인 사용과 성과 개선을 통하여 비용이 절감되고 독립적인 심사를 통한 신뢰도가 증진하며 다른 경영시스템 규격인 ISO 9001, ISO 14001, ISPS Code[17] 등과 병행하여 사용할 수 있으며 이는 품질, 환경, 안전, 보안 시스템이 하나의 경영시스템에서 운용될 수 있음을 의미한다.

17) 선박 및 항만시설 보안규칙(International Code for the Security of Ships and of Port Facilities)

Ⅴ. 시사점 논의

1. 보안 대상(target)과 위협(threat)의 다양화

TC 292가 다른 TC들을 통합하여 탄생 된 배경 중 하나는 개인, 기업, 조직, 지역공동체가 의존하여 살아가고 언제 그리고 어디에서나 원활하게 생산적 활동을 수행하기 위한 안전환경을 대규모로 위협하는 요소들이 점차 다양화되어 가고 있다는 점이다. 이에 대해 ISO 보안분야 전략자문그룹(Strategic Advisory Group on Security)인 SAG-S는 공격의 대상이 되는 보안 타겟과 위협의 목록(Inventory of security-related standards: www.iso.org/sites/sags)을 체계적으로 제시하고 있다.

먼저 보안 대상(targets)은 식품 및 농산물, 수자원(물공급과 하수 포함), 에너지(전기, 원자력, 가스, 파이프라인), 정보통신인프라(ICT), 제조산업시설(침입 방지/탐지/센서, 소방시설, 난방 · 환기 · 냉방시설), 공공안전 · 응급의료 시설, 교통인프라, 다중운집시설(대형행사장, 퍼레이드, 스포츠아레나 등)로 제시하고 있다. 보안 위협(threats)은 생화학 · 핵 · 폭발물(CBRNE) 위협, 사이버보안 위협, 범죄공격(제품 · 문서 위조사기, ID사기 등) 위협, 자연재난 위협 등으로 구분하고 있다.

이렇게 다양해지는 각종 산업과 도시시설 환경의 보안 위협들의 유형들도 표준화하여 대응하려는 국제사회의 움직임으로 이해될 수 있다.

2. 산업보안 관련 표준화 범위의 확장

다양해지고 지역적으로도 넓어지며 글로벌화 되어 가는 보안 공격의 대상과 위협의 확산으로 인하여 기존의 분야 별, 영역 별 보안 표준의 개발과 제정 등 표준화도 각종 산업의 제품과 서비스의 연구개발, 제조, 생산, 판매, 물류 유통 등의 활동이 그러한 위협과 공격으로부터 침해되지 않고 보호를 받아 안전하고 원활하게 이루어지도록 지원해야 한다. 21세기 산업보안 표준화가 그런 시대적 상황과 환경에서 보안관리와 위험관리를 제공할 수 있도록 범위가 확장되는 것은 당연한 현상일 것이다.

보다 중요한 것은 이러한 위협 수준에 맞는 위험평가 기반의 보안관리 표준들이 어떤 틀과 방법론, 그리고 절차적 체계성과 엄격성을 가지고 제안되고 논의되어 산

업의 손실을 경감 및 방지하고 위험관리에 도움을 줄 수 있을지를 파악하여 국내에서도 적극적으로 이를 적용 및 활용하는 것이다. 더불어 점차 표준 강국이 되어 가고 있는 한국이 이러한 산업보안 분야 국제표준화에 보다 적극적으로 참여하여 Good Practice를 전파하고 리드할 필요가 있다.

3. 공공 및 민간 보안의 홀리스틱(holistic) 접근 필요성

TC 292에서 제정되고 있는 표준들의 전반적인 특징을 살펴보면 개인, 비즈니스, 공공기관, NGO 조직 등 다양한 이해관계자들이 활용할 수 있는 범용성을 갖추고 있다는 점이다. 그 이유는 각종 보안 공격과 위협들의 불확실성이 커지고 보안실패 사례가 증가하면서 보안사고 및 재난 관리 기관 등 단일한 주체에 의존한 보안 확보와 실현이 매우 어려워지고 있기 때문인 것이다. 따라서 이 TC 292에서 강조되는 표준화의 방향은 산업이 보안관련 예방, 대비, 대응 복구, 그리고 업무연속에 이르는 전 과정에 보안 관련 교육훈련, 보안 장비 및 시설 구축, 상호 커뮤니케이션 체계 확보, 사고관리, 대인보호장구 비치 등의 노력과 투자를 하고 공공기관들, 자원봉사자, 소비자 등과 협업하고 정보를 교환하며 소통하는 홀리스틱 접근을 통해 소비자 및 지역공동체와 함께 보다 효과적이고 신속한 회복력을 확보해야 한다는 것이다. 이는 보안 사건·사고 관련한 공공기관 간 협력체계와 민관 협력파트너쉽이 선진국에 비하여 취약한 우리나라에 제도 및 정책 면에서 시사하는 바가 크다고 할 수 있으며 향후 그 표준화의 내용들은 한국 실정에 맞는 파트너쉽의 모델과 시범운영 사례를 개발 및 실험하는데 많은 도움이 될 것으로 기대 된다.

4. 산업보안 ISO 인증시장 확대에 대한 대비

글로벌 기업과의 경쟁은 심화되고 있으나, 교역 증가와 시장 개방으로 시험인증시장은 급성장하고 있고, 특히 한국은 1조불 무역규모(세계 8위)로 풍부한 시험인증 수요를 갖고 있으며, 우수하고 풍부한 전문 인력, 가격대비 신속한 서비스, 정보화 능력, 시장 변화에 대한 빠른 적응력 등이 강점이다.

ISO 경영시스템 인증시장의 활성화를 위해 신규 인증제도 도입, 인증산업에 대한 지원정책 등이 추진되어 가고 있으나 FTA 확산에 따른 교역 증가와 시장개방으로

시험 및 인증 시장이 꾸준히 성장하는 가운데 글로벌 기관과의 경쟁도 심화되고 있다. 이러한 상황에서 국내 시험인증기관은 신규 내수시장을 확보하거나 해외시장을 개척하려는 노력이 부족한 실정으로 국제시장변화에 신속히 대응하고 글로벌기관과 경쟁하기 위한 전략마련이 필요하다(국가기술표준원, 2014).

즉, 이러한 산업보안 관련 표준화에 제대로 대응하거나 대비하지 못하면 무역기술장벽(TBT) 통보 건수가 증가하여 수출기업의 해외 기술규제에 큰 애로가 발생하기 때문에 해소를 위한 효율적인 TBT 대응체제의 구축이 필요하다. 범부처 참여형 국가표준 운영체계 도입('14.5)과 관련하여 산업통상자원부가 범부처 표준에 대한 총괄·조정 역할을 수행하면서 국내외 인증제도 총괄관리체제 등 운영체계를 고도화할 필요가 있다.

Ⅵ. 결론

지금까지 산업보안 관련 분야가 시스템 측면에서 국제표준기구인 ISO를 통해서 표준화되어 가는 추세를 살펴보았다. 산업기밀 유출 방지와 같은 악의적 범죄공격에 의한 위험을 관리하고 손실을 방지하기 위한 산업재산권 보호 관련한 체계라는 범위를 벗어나서 공급사슬, 제품 및 문서 위조의 방지, 재난관리, 커뮤니티 회복력과 같이 폭넓은 분야를 다루었다. 이를 위해 산업보안 분야 표준화의 역사를 연혁적으로 분석하면서 ISO TC 292가 탄생된 역사적 배경과 표준화의 틀이 어떻게 변화되어 왔는지를 체계적으로 안내하였다. 또한 TC 292 안에서 워킹그룹 별로 개발되고 제정되어 온 보안 관련 표준들의 대략적인 내용들을 (1) 용어 정의(terminology) 및 일반적 보안 원칙(General standards), (2) 사업연속성 및 조직회복성(Continuity and organizational resilience), (3) 비상경영/재난관리(Emergency management), (4) 제품·문서의 보안(Authenticity, integrity and trust), (5) 커뮤니티 회복성(Community resilience), (6) 보호적 보안(Protective security), (7) 공급사슬보안경영시스템(Supply chain security management)의 순으로 설명하였다. 각 표준들은 서로 독립된 면도 있으며 상호 의존적인 면도 있는데, 예를 들면 용어 정의 표준은 모든 WG에서 생산하는 용어정의들을 규합하고 같은 용어에 대하여 WG 간 정의(definition)가 충돌되거나 혼란스럽지 않고 서로 조화가 될 수 있도록 유도하는 중요한 역할을 하고 있다. 또한 WG2에서 작업 중인 조직 회복력

관련 표준인 ISO 22316은 TC 292 전체를 아우르는 조직 회복력 확보를 위한 일반적이고 원칙적인 지침을 제공한다.

분석을 통해 도출될 주요 발견점은 이러한 보안 분야의 국제표준화는 보안의 대상(target)과 위협(threat)이 다양화되면서 기업 등의 조직이 보다 유연성 있게 보호하고 피해를 입고도 조속히 회복되는 적응력을 갖추기 위한 체계가 표준화되고 있다는 점이다. 그리고 산업보안 관련 국제표준화의 범위가 확장되면서 정보보안의 영역보다 포괄적인 모습을 그려가고 있다는 점이다. 이러한 표준화를 통해서 기업들은 글로벌화와 로컬화를 동시에 추진하면서 겪게 되는 많은 보안 위협과 손실에 보다 비용효과적으로 대비하고 대응할 수 있게 되는 것이다. 보안 문제는 비단 기업만의 문제가 아니고 산업 혼자서 해결할 수 있는 문제는 더욱 아니다. 따라서 이러한 국제표준화는 공공 및 민간 보안의 홀리스틱(holistic) 접근의 중요성을 크게 강조하고 있다는 점이다. 마지막으로 산업이 적절한 보안과 회복력을 갖추기 위해서 이러한 국제표준화를 통한 ISO 인증에 대비하여야 한다는 점이다. 이 분야 국제표준화에 산업계가 시의적으로 적절히 대응하지 못할 경우 대외 무역과 수출입에서 우리나라가 무역장벽에 걸리고 경제적으로 손실을 입을 가능성이 있기 때문이다.

이 연구는 최근의 산업보안 분야의 국제표준화를, 특히 시스템표준 분야에 대한 동향을 심도 있게 다루면서 산업보안 학계에 소중한 정보와 지식을 제공하여 기여하였다고 생각된다. 그러나 제한된 자료와 연구 기간의 한계로 인해 보다 심오하고 정교하며 치밀한 분석이 이루어지지 않은 점이 아쉽다. 향후 이 글을 통해 제시된 산업보안 관련 분야 국제표준들의 내용들이 산업보안학에서 어떻게 해석되고, 응용되고, 활용될 수 있을 지를 확인하기 위한 추가적 연구가 이어지길 바란다.

참고문헌

1. 국내문헌

국가기술표준원 (2014). 국가기술표준백서.

국가지식재산위원회 (2013). 2013년도 지식재산 침해대응 및 보호집행 보고서.

김도균, 박재묵 (2012). 허베이 스프리트호 기름유출사고 이후 재난관리 거버넌스 구축 실패와 재난 복원력의 약화. 환경사회학연구 ECO, 16(1), 7-43.

박현호 (2014). 상품위조방지 기술의 성능평가 표준 이행을 위한 가이드라인 개발, 산업통상자원부 국가기술표준원 용역연구보고서.

소방방재청 (2012). ISO 22320·22300·22301에 관한 사회안전 분야 국제표준의 효율적인 국내 도입방안.

염흥열 (2006). 정보보호일반표준화로드맵 2006. TTA

유병태 (2014). 재난분야 국제표준(ISO/TC223) 현황분석 및 효율적 대응방안, 대한안전경영과학회지. v.16 no.1.

유형창 (2014). 산업보안관리에 관한 뉴패러다임의 정립: 글로벌 비즈니스를 중심으로, 38, 57~82.

윤준영, 민금영, 정덕훈 (2015). 재난관리 관련 국제표준별 국내 법·제도 동향 - ISO/TC 292 중심으로, 한국재난정보학회논문집 제11권 2호.

이성용 (2014). 독일의 산업보안 정책과 시사점, 한국경호경비학회지, 38, 57~82.

이재은, 양기근 (2004). 재난관리의 효과성 제고방안: 시민참여와 거버넌스, 현대사회와 행정, 14, 53-81.

임준영 (2006). ISO 공급망보안(Supply chain security) 관한 모범사례지침, ISO Bulletin.

최진혁 (2010). 산업보안의 제도적 발전방안 연구: 미국 사례를 중심으로, 한국경호경비학회지, 22, 197-230.

2. 국외문헌

Homeland Security Advisory Council (2008). *Top Ten Challenges Facing the Next Secretary of Homeland Security*.

International Chamber of Commerce (2007). Counterfeiting Intelligence Bureau. *Overview of Counterfeiting*.

TC292 N 265 TC292 Draft Road map from ISO/TC 292/WG 6 Protective security.

Toffler, A. (1990). *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, Bantam.

3. 웹사이트

www.securityinfowatch.com/news/11080951/asis-ansi-looking-for-stakeholders-to-participate-in-technical-advisory-group-for-new-iso-standard

www.dhs.gov/xlibrary/assets/hsac_dhs_top_10_challenges_report.pdf

www.iso.org

www.iso.org/sites/sags/

【Abstract】

Trend of standardization in the field of Industrial Security through ISO/TC 292

Park, Hyeon-Ho

This study aims at analyzing the global trend of standardization in the field of Industrial Security through ISO/TC 292. It covers broad areas from risk management for industrial property protection and loss prevention through supply chain security, product and document fraud and counterfeiting countermeasures and control and community resilience. It also explores the historical background of the standardization in the security field, how ISO TC 292 came out as a leading group in order to standardize relevant security management systems. TC 292 deals with terminology, general security-related standards and supply chain security management.

One of the major findings from this analysis is that security targets and threats are diversified and so organizations like enterprises should have proper flexibility to adapt themselves to new security environment and take appropriate resilience system to cope with the threats and incidents. Also the ISO standardization requires public or private entities to take holistic approaches in security management. Finally, it was found that South Korea has to prepare for this global trend of standardization in this field so that ISO certification market demand and the requirements for transnational trades can be well met.

Key words : industrial security, standard, International Standard Organization, TC 292, certification