https://doi.org/10.33778/kcsa.2021.21.1.019

셉테드(CPTED)를 고려한 정보보안 관리시스템(ISO 27001)의 요구사항 개발★

임 헌 욱*

요 약

본 연구의 목적은 환경설계를 통한 범죄예방인 셉테드를 정보보안 영역에 추가하고자 하였다. 정보보안 관리시스템인 ISO 27001의 통제항목(11가지)과 셉테드(CPTED)의 적용원리(6가지)를 매핑하고 항목 간 관련성에 대해서 12명의 보안전문가를 통해 FGI 회의를 통해 검증 하였다. 조사결과 관련성이 평균 60% 이상인 통제항목으로 보안정책, 물리·환경적 보안, 사고관리, 준거성 등이 있었으며, 이는 포괄적인 정책으로 환경보안인 셉테드의 항목과 전반적으로 공유하였으며, 보안조직, 자산관리, 인원보안, 운영관리, 접근통제, 시스템유지, 연속성관리 등 전문적인 통제항목은 셉테드의 각각의 항목과 매핑이 이루어 졌다. 이를 통해 정보보호 인증과 셉테드는 관련성이 있다고 할 수 있으며, 이는 보안의 3대 영역인 관리적보안, 기술적보안, 물리적보안에 환경적보안을 고려할 수 있게 되었다.

Development of requirements for information security management system (ISO 27001) with CPTED in account

Heon - Wook, Lim*

ABSTRACT

The purpose of this study was to add CPTED to the information security area. The control items of ISO 27001 (11 types) and the application principles of CPTED (6 types) were mapped. And the relevance between the items was verified through the FGI meeting through 12 security experts. As a result of the survey, the control items with a relevance of at least 60% on average are security policy, physical and environmental security, accident management, and conformity. As a result, the comprehensive policy was shared with CPTED's items as a whole. The specialized control items are security organization, asset management, personnel security, operation management, access control, system maintenance, and continuity management. However, specialized control items were mapped with each item of CPTED. Therefore, information security certification and septed are related. As a result, environmental security can be added to the three major areas of security: administrative security, technical security, and physical security.

Key words : CPTED, ISO 27001, Management security, Technical security, Physical security, Environmental security

접수일(2021년 02월 28일), 게재확정일(2021년 03월 18일)

* 한세대학교 교양학부 조교수

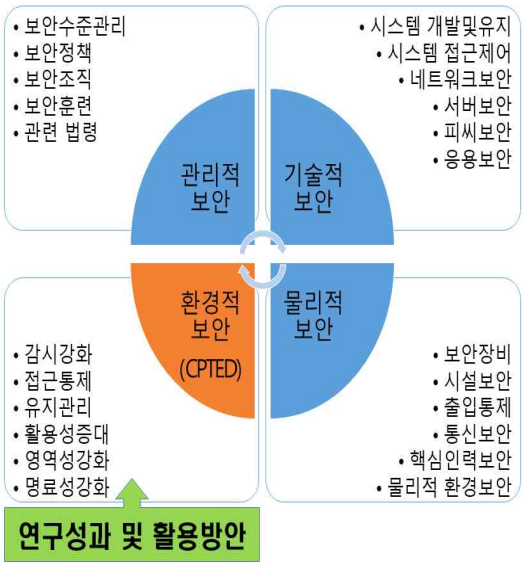
★ 본 연구는 2020학년도 한세대학교 교내학술연구비 지원에 의하여 연구되었음.

1. 서 론

1.1 연구목적

본 연구의 목적은 환경설계를 통한 범죄예방인 셉테드(CPTED, Crime Prevention Through Environmental Design)를 정보보안 영역에 추가하고자 한다.

즉, 정보보안 관리시스템인 ISO 27001의 통제항목과 CPTED의 6가지 적용원리를 매핑하고 전문가를 통한 검증 후 보안컨설팅 등에 활용하고자 한다. 이를 통해 보안의 3대 영역인 관리적보안, 기술적보안, 물리적보안에 환경적보안 추가를 고려하고자 한다.[1][2]



(그림 1) 연구성과 및 활용방안

1.2 연구의 필요성

1.1.1 셉테드(CPTED)의 필요성

CPTED라는 단어는 1971년 레이 제프리(Ray Jeffery)가 “Crime Prevention Through Environmental Design”에서 도시 환경설계와 범죄와의 연계성에 대해 소개하였고, 미국·영국 등에서는 건축물 구조와 도로형태 등의 주택환경을 개선하여 침입절도 등 기회성 범죄를 감소시키기 위해 1980년대부터 도입하였다.[3] 경찰청 생활안전과(2005. 9.) 환경설계를 통한 범죄예방(CPTED)방안에서 범죄예방 활동은 경찰의 순찰력만 의존하였으나, 도시계획 수립과 건축설계 시작에서부터 범죄예방을 고려한 디자인 설계로 범죄기회를 사전에 차단하는「환경설계를 통한 범죄예방계획 (CPTED)」을 추진하게 되었다고 하였다. 이는 범죄로 발생하는 피해를 최소화하여 양질의 삶을 추구하는 것이다.[4] 셉테드의 목적은 물리적인 환경인 실배치, 창호설치, 공간구성, CCTV 등에 방범개념을 도입하여 시민들을 위한 안전지대를 조성하여 범죄 없는 환경에서 양질의 삶을 추구하는데 기여하는 것이다.[5][6]

셉테드는 6가지 적용원리는 공간배치와 시설디자인을 통해 자연스럽게 침입여부를 감시하는 ①자연감시(Surveillance), 보안설비(기술적, 물리적)를 통해 직접적으로 범죄를 차단하는 ②접근통제(Access Control), 특정 대상의 사적권리를 주장할 수 있게 경계를 표시하는 ③영역성 강화(Territoriality Reinforcement), 공간과 시설을 쉽게 인식하고 올바르게 이용할 수 있도록 계획하는 ④가독(명료)성 강화(Legibility Reinforcement), 공간과 시설을 활용하여 감시기회를 증대시키는 ⑤활용(활동)성 증대(Activity Support), 범죄예방 기능이 유지되도록 지속적 관리하는 ⑥유지관리(Maintenance & Management)로 나눈다.[7]

1.1.2 셉테드 추가에 따른 ISO 27001의 기대효과

첫째, 기존의 보안영역 확대이다. 그간 기술유출 방지를 위한 보안의 3대 분야는 관리적보안, 물리적보안, 기술적보안 이었으나 금번 연구를 통해 “환경설계를 통한 범죄예방인 셉테드(SPTED)를 도입하여 환경적 보안 까지 보안의 영역을 확대하고자 한다.

둘째, 국제인증(ISO27001)에 준하는 통제항목 도출이다. 정보보안인증(ISO 9001) 요구사항에 CPTED 6가지 적용원리인 감시, 접근통제, 영역성 강화, 가독성 강화, 활용성 증대, 유지관리를 매핑하여 신규 통제항목을 도출한다. 세째, 보안 컨설팅에 직접 활용 가능하다. 중소기업 기술보호 전문가 상담에서 보안역량 진단표에 환경적 보안을 추가하여 상담을 진행할 수 있다.

2. 본 론

2.1 국제표준화기구 ISO 인증의 이해

국제표준화기구 ISO(International Organization for Standardization)는 런던의 토목공학연구소에서 1946년 25개국 대표가 산업표준의 국제조정을 위한 통합기구를 만들기로 하고, 1947. 02. 23에 운영을 시작하였으며, 1998년에 제정된 BS 7799-2를 기초로, 2005. 10. 15에 제정되었다.[8]

ISO27001은 국제규격인 ISMS(Imformation Securiy Management System)에 적절한 정보보안경영시스템을 수행을 입증하는 것으로 단체의 경영시스템에 대한 인증이다.[9] 어느 조직이 정보 자산의 기밀성·무결성·가용성을 실현하기 위한 관리체계를 수립하고 운영할 때, 그 체계가 인증심사 기준에 적합한지를 인증하는 것인지 정의하고 있다.[10]

ISO27001(2013)의 전문(Foreword)에 의하면 국제표준화기구(ISO)와 국제전기표준회의(IEC)는 국제적인 표준화를 위한 전문가적인 체계를 구축하고 있다.[11]

ISO27001(2013)의 서문(Introduction)에 의하면 ISO/IEC 27000은 정보보호 경영시스템에 대한 표준 패밀리(ISO/IEC 27003, ISO/IEC 27004, ISO/IEC27005)에서 참고용으로 정보보호 경영시스템의 개요와 관련 용어 및 정의하고 있다. ISO27001(2013)의 부속서 A(Annex A)의 참조 통제 목적과 통제(Reference control objectives and controls)를 살펴보면 A.5에서 A.18까지 총14가지로 분류하였다.

A.5 정보보안 정책 : 정보보호를 수행하도록 경영방침과 제공
A.6 정보보안 조직 : 조직내에서 정보보호 구현과 운영
A.7 인원 보안 : 직원이 책임을 이해하고 역할을 보장
A.8 자산 관리 : 조직의 자산을 식별하고 책임을 정의
A.9 접근 통제 : 정보및 시설에 대한 접근 제한
A.10 암호화 : 정보의 기밀성, 무결성, 보호.
A.11 물리적 환경적 보안 : 정보및 시설에 대한 파손 및 간섭방지
A.12 운영 보안 : 정보처리 시설의 안전한 운영보장
A.13 통신 보안 : 정보처리 시스템의 보호
A.14 시스템 취득, 개발, 유지보수 : 정보시스템의 정보보호 보장
A.15 협력업체(공급자) 관리 : 공급자가 접근할수 있도록 보장
A.16 보안사고 관리 : 보안사고 관리의 효과적인 접근 보장
A.17 사업연속성 관리의 정보보안 측면: 정보보호 연속성을 포함
A.18 준거성 : 보안 요구사항의 위반방지

2.2 ISO27001의 통제항목 vs CPTED의 적용원리

ISO727001의 통제항목과 SPTED의 통제항목 매핑을 위해 <표 2>와 같이 CPTED의 6가지 적용원리와 ISO27001의 세부 통제 항목을 매핑을 통한 새로운 환경적 보안 통제항목을 도출할 것이다.

<표 2> 셉테드와 ISO27001 통제항목 매핑(예)

셉테드 관련			연계 사유	ISO727001의 통제항목 연계
적용원리	내용설명	적용사례		
①자연감시	공간배치와 시설디자인을 통해 자연스럽게 침입여부를 감시하는 것	시야, 조명, 공간설계	보안매뉴얼 및 스마트보안 관제와 연계	보안정책 마련, 보안조직 강화, 인원보완강화, 자산별 권한 관리
②접근통제	보안설비를 통해 직접적으로 범죄를 차단하는 것	고립·사각지역개선, 배치, 유도	통제구역 접근통제 및 보안설비와 연계	통제구역 출입통제, 네트워크 보안장비 운영, 시스템접근 권한 통제
③영역성강화	특정 대상의 사적권리를 주장할 수 있게 경계를 표시하는 것	대지의 사용증진, 활동성, 영역성 강화, 조경, 공동장소, 관리	특허 임치 등 자산 관리와 연계	보안조직관리, 보안책임자 및 운영 관리, 보안 거버넌스 준수
④명료성강화	공간과 시설을 쉽게 인식하고 올바르게 이용할 수 있게 계획하는 것	정확한 표시로 정보제공	법적경고 등 가시성 향상과 연계	정보보안 관리체계 준수, 보안 거버넌스 준수
⑤활용성증대	공간과 시설을 활용하여 감시기회를 증대시키는 것	활동의 활성화	자발적 활동강화 등 사이버감시와 연계	보안 관련 단체와 협업, 사업 연속성 강화
⑥유지관리	범죄예방 기능이 유지되도록 지속적 관리하는 것	폐쇄회로 텔레비전 안내판의 설치, 표지판 및 정보	사고대응 등 지속성 향상과 연계	보안시스템 유지리, 보안조직관리, 보안사고대응관리

출처 : 범죄예방디자인 연구정보센터 재구성

3. 실증연구

3.1 연구방법 및 내용

3.1.1 조사목적

환경설계를 통한 범죄예방인 셉테드의 6가지 적용원리와 정보보안 관리시스템인 ISO 27001의 14가지 통제항목을 연계하고자 한다.

3.1.2 조사기간

· 조사기간 : 2020. 8. 20 ~ 2020. 9. 20

3.1.3 조사대상 : 전문가 총 12명

· 정보보호전문가(6명), 산업보안전문가(6명)을 대상

조사대상을 셉테드와 정보보호인증을 이해하고 있는 보안전문가를 대상으로 정성적 조사 방법 특정한 경험을 공유한 사람들이 함께 모여 인터뷰를 진행하는 조사방법 FGI(Focus Group Interview) 방식을 사용하였다.

3.1.4 조사내용

설문조사는 <표 3> 셉테드와 ISO27001 통제항목 매핑을 설명 후 <표 3>과 같이 관련성에 따른 리커드 5점 척도가 일반적이나 본 연구는 셉테드와 정보보호인증의 연계성을 찾는 시도로 관련이 있으면(1) 없으면(0)으로 하는 더미변수를 사용하였다.

<표 3> 설문지 문항

CPTED 적용원리 \ ISO 27001 통제항목											
자연감시											
접근통제											
영역성강화											
명료성강화											
활용성증대											
유지관리											

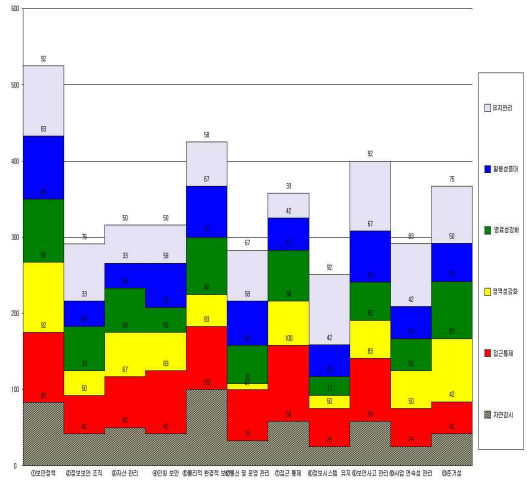
3.2 연구결과

3.2.1 기술통계(descriptive statistics)

기술통계란 조사한 데이터의 특성을 고려하고 요약하는 통계 기법으로 평균, 분산, 표준편차 등이 기술통계에 속한다. 기술통계 조사결과 <표 4> 셉테드와 ISO27001 통제항목 관련결과를 도출하였으며, 이중 응답자 모두(100%) 관련 있다고 한 경우는 ⑤물리적 환경적보안 & 자연감시, ⑦접근통제 & 접근통제, 90%이상인 경우는 ①보안정책 & 접근통제, 영역성강화, 유지관리, ⑧정보시스템유지와 유지관리, ⑨보안사고관리 & 유지관리로 나타났다. 또한 평균비교 분석결과 특이점으로 정보보호전문가와 산업보안전문가의 의견차이도 있었는데 4명 이상의 차이를 보인 문항은 자연감시 & 자산관리와 ⑥통신 및 운영 관리 & 접근통제, 3명 이상의 차이를 보인 문항은 ⑥통신및운영관리 & 활용성증대, ⑪준거성 & 명료성강화(6명)와 ② 정보보안 조직 & 유지관리로 조사되었다.

<표 4> ISO27001과 셉테드의 연관성 기술통계 (단위 %)

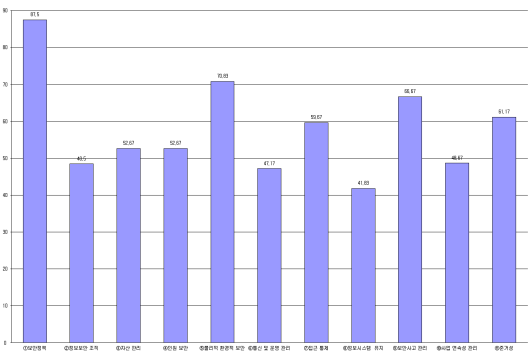
CPTED 적용원리 \ ISO 27001 통제항목							
①보안정책	83	92	92	83	83	92	87.50
②정보보안 조직	42	50	33	58	33	75	48.50
③자산 관리	50	67	58	58	33	50	52.67
④인원 보안	42	83	50	33	58	50	52.67
⑤물리적 환경적 보안	100	83	42	75	67	58	70.83
⑥통신 및 운영 관리	33	67	8	50	58	67	47.17
⑦접근 통제	58	100	58	67	42	33	59.67
⑧정보시스템 유지	25	50	17	25	42	92	41.83
⑨보안사고 관리	58	83	50	50	67	92	66.67
⑩사업 연속성 관리	25	50	50	42	42	83	48.67
⑪준거성	42	42	83	75	50	75	61.17



(그림 2) ISO27001과 셉테드의 연관성 기술통계 (단위 %)

3.2.2 셉테드와 ISO27001 통제항목 관련도

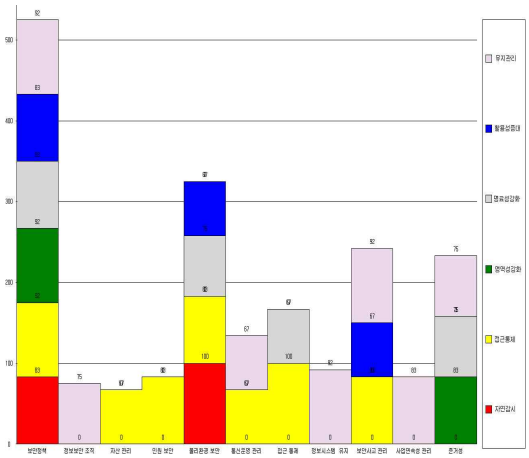
(그림 3)과 같이 셉테드와 ISO27001 통제항목의 관련도 평균비교를 살펴보면 평균 60점 이상인 ①보안정책(87.50), ⑤물리적 환경적 보안(70.83), ⑨보안사고 관리(66.67), ⑪준거성(61.17)과 나머지 항목이 차이가 있다.



(그림 3) ISO27001과 셉테드의 연관성 평균비교

응답자의 60%이상 관련이 있다고 응답한 결과는 (그림 4)와 같이 1)정보보호를 수행하도록 경영방침과 지원을 제공 하도록 하는 정보보안정책은 접근통제>영역성강화>유지관리>자연감시>명료성강화>활용성증대 순으로, 2)조직 내에서 정보보호 구현과 운영하는 정보보안 조직은 유지관리, 3)조직의 자산을 식별하고 책임을 정의하는 자산 관리는 접근통제, 4)직원이 책임을 이해하고 역할을 보장하는 인원 보안은 접근통제, 5)정보 및 시설에 대한 파손 및 간섭을 방지하는 물리·환경적 보안은 자연감시>접근통제>명료성강화>활용성증대 순으로, 6)정보처리 시스템의 보호하는 통신 및 운영 관리는 접근통제>유지관리 순으로, 7)정보 및 시설에 대한 접근 제한하는 접근 통제는 접근통제>명료성강화 순으로, 8)정보시스템의 정보보호를 보장하는 정보시스템 유지는 유지관리, 9)보안사고 관리의 효과적인 접근 보장하는 보안사고 관리는 유지관리>접근통제>활용성증대 순으로, 10)정보보호 연속성을 포함하는 사업 연속성 관리는 유지관리, 11)보안 요구사항의 위반을 방지하는 준거성은 영역성강화>명료성강화 >유지관리 순으로 조사되었다.

1) 보안정책 : 접근통제 > 영역성강화 > 유지관리 > 자연감시
2) 정보보안 조직 : 유지관리
3) 자산 관리 : 접근통제
4) 인원 보안 : 접근통제
5) 물리·환경적 보안 : 자연감시 > 접근통제 > 명료성강화 > 활용성증대
6) 통신 및 운영 관리 : 접근통제 > 유지관리
7) 접근 통제 : 접근통제 > 명료성강화
8) 정보시스템 유지 : 유지관리
9) 보안사고 관리 : 유지관리 > 접근통제 > 활용성증대
10) 사업 연속성 관리 : 유지관리
11) 준거성 : 영역성강화 > 명료성강화 > 유지관리



(그림 4) 셉테드와 ISO27001 통제항목 관련도(60%이상)

4. 결 론

4.1 연구결론

본 연구의 목적은 셉테드를 정보보안 영역에 추가하고자 하였다. 이를 위해 정보보안 통제항목(11가지)에 셉테드 적용원리(6가지)를 매핑하고 이를 증명하고자 하였다. 이에 결론으로 정보보호인증의 통제항목 중 보안정책, 물리·환경적 보안, 보안사고관리, 준거성 등은 포괄적인 정책은 환경적보안인 셉테드와 전반적으로 공유하였으며, 보안조직, 자산관리, 인원보안, 운영관리, 접근통제, 시스템유지, 연속성관리 등 전문적인 관리는 셉테드의 각각의 항목과 매핑이 이루어 졌다. 이를 통해 정보보호 인증과 셉테드는 관련이 있다고 할수 있다.

4.2 연구의 한계

본 연구의 목적대로 정보호호 인증과 셉테드의 통제항목 간에 상관성과 신뢰성을 밝혀야 하는데 본 연구의 시도만으로 많은 의문이 따른다. 이에 연구의 한계는 ISO27001과 셉테드의 연관성에 관한 기술통계의 부분에 있어서 상관성과 신뢰성을 밝히지 못하는 것이 한계이다. 다만 정보보호 인증에 환경적 보안인 셉테드를 통제항목으로 접근한 것을 본 연구의 의의로 두고자 한다.

참고문헌

[1] 임헌욱, “산업보안 패러다임 변화에 따른 보안 교육 방안 고찰”, 보안공학연구논문지, 12권 제6호, pp.597-608, 2015.

[2] 임헌욱, “융합보안 설비구축 원인에 대한 근거이론적 접근”, 융합보안논문지, 16권, 제7호, pp.69-75, 2016.

[3] 경찰청, 생활안전과, “환경설계를 통한 범죄예방(CPTED) 방안”, 2005.

[4] 강용길, 박민영, “CPTED 제도화를 위한 법령정비 방안에 관한 연구”, 경찰학연구, 14권, 제2호, pp.3-28, 2014.

[5] 조진일, 박성철, 최형주, 박희원, “학교범죄예방을 위한 디자인(CPTED) 평가모형 개발”, 한국교육 40권, 3호, pp.133-154, 2013.

[6] 임헌욱, “정보보호 산업의 기술성숙도에 따른 비즈니스 모델 상관성 분석”, 융합보안논문지, 19권, 제4호, pp.165-171, 2019.

[7] http://www.cpted.kr 범죄예방디자인 연구정보센터

[8] 임헌욱, “국제표준화기구(ISO)의 인증기준에 준하는 「국가중요시설」의 요구사항 개발”, 융합보안논문지, 17권, 제3호, pp.65-71, 2017.

[9] https://www.kab.or.kr/

[10] 임헌욱, “정보보호 관리체계의 마케팅 전략 수립” 보안공학연구논문지, 12권, 4호, pp.305-318, 2015.

[11] 임헌욱, “정보보호 관리체계의 마케팅 전략 수립”, 보안공학연구논문지, 12권, 제4호, pp.305-318, 2015.

〔저 자 소 개〕

임 헌 욱 (Heon Wook Lim)
인하대 경영학 박사
현) 한세대학교 조교수
email : 3795879@hanmail.net