Journal of The Korea Society of Computer and Information
Vol. 20, No. 5, May 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.5.113

시스템경비 관제시설의 구축과 보안 및 경영대책

하 경 수*, 조 철 규**, 김 평 수***

Electronic Security Control Center Building Process and Security and Management Measures

Kyung-Su Ha*, Cheol-Kyu Cho**, Pyong-Soo Kim ***

요 약

이 연구는 국내 시스템경비업체의 보안관리 개선을 위한 경영대책의 일환으로 관제시설에 대한 구축 프로세스와 보안관리 방안을 제안한다.

관제시설은 시스템경비의 중추신경으로 현장의 대응체제가 아무리 잘 구축되어 있더라도 관제시설이 장애나 재해로 작동이 중단되거나 관제기계경비원이 위해를 입게 되면 본래의 기능을 수행할 수 없기 때문이다.

관제시설의 구축 프로세스는 공간구조, 기반시설, 관제장치, 관제 솔루션, 운영조직으로 구분하고, 보안관리 방안으로는 물리보안, 정보보안, 인적보안에 대한 대책을 제시한다.

▸ Keywords : 시스템경비, 관제시설, 장애, 재해, 보안대책

Abstract

This research suggests construction processes and security solutions for security control center as management measures for security management improvement in domestic electronic security companies. Security control center (SCC) is the central nerve of electronic security service, and no matter how well the on-site response system has been built, if SCC ceases to work due to an incident or disaster or security control personnel are harmed, the electronic security system cannot perform its proper functions. It is divided to a spatial structure, the infrastructure, control equipment, control solutions and operating structure in a construction process in the security control center. And a solution can be presented for physical security, information security, and personnel security in the way to security solutions.

•제1저자 : 하경수 •교신저자 : 조철규 •공동저자 : 김평수
•투고일 : 2015. 4. 16, 심사일 : 2015. 4. 28, 게재확정일 : 2015. 5. 9.
* (주)씨너스 SK broadband 마이캠 관제팀장(Synus SK broadband mycam)
** 경운대학교 경호학부(School of Protection Science, Kyungwoon University)
*** 전남도립대학교 경찰경호과(Dept. of Police & Security Service, Jeonnam Provincial College·Korea)

▸ Keywords : electronic security, security control center, incident, disaster, security measures

I. 서 론

관제시설은 시스템경비업무의 중추신경으로 계약상대방에 대한 이벤트정보 모니터링에 의한 상황관리와 다양한 관제 솔루션으로 관제기계경비원에게 과학적인 분석결과를 제공하는 기능을 수행한다[1]. 이러한 관제시설에 물리적인 위해나 기술적인 장애 등이 발생한다면 그에 따른 피해는 치명적인 수준으로 확대된다. 현장의 대응체제가 아무리 잘 구축되어 있더라도 관제시설의 작동이 멈추거나 관제기계경비원이 위해를 입게 되면 본래의 기능을 상실하게 된다. 그러나 현재 상당수 시스템경비업체의 관제시설은 화재를 비롯한 각종 자연재해, 전기·통신시설의 장애, 관제 솔루션의 이상 및 관제기계경비원에 대한 위해 등 각종 위협에 노출되어있다. 이러한 위협을 사전에 방지하기 위해서는 관제시설의 구축단계에서부터 보안을 고려한 설계가 선행되어야 한다. 또한 관제시설을 운용함에 있어 물리적인 위해와 기술적인 장애 그리고 관리적 측면에서의 보안대책이 마련되어야 한다.

관제시설의 장애나 재해는 시스템경비업체의 기업이미지 실추에 그치지 않고 시스템경비에 대한 신뢰하락으로 고객이탈, 피해보상, 기회비용의 손실로 이어져 기업의 위기를 초래할 수 있고, 계약상대방의 경영활동 및 금융시스템의 장애 등 국가적인 혼란과 직결되기 때문에 예방체계 구축은 안정적 운영을 위한 필수요소이다.

이 연구는 시스템경비업체의 보안관리 개선을 통한 경영상의 잠재적 기회이익과 손실관리의 일환으로 관제시설의 구축 프로세스의 정립과 위해방지를 위한 물리적, 기술적, 관리적 차원의 보안 및 경영대책을 모색하고자 진행되었다.

II. 관련 연구

1. 시스템경비 관제시설

시스템경비는 인력경비에 대응되는 경비 형태로서 기존의 인력에 의존하던 경비방식에서 벗어나, 첨단기계장비를 사용하여 경비대상시설에 사람 없이도 실시할 수 있는 경비형태를 말한다[2].

시스템경비시스템은 경비대상시설에 경비업무용 기계장치

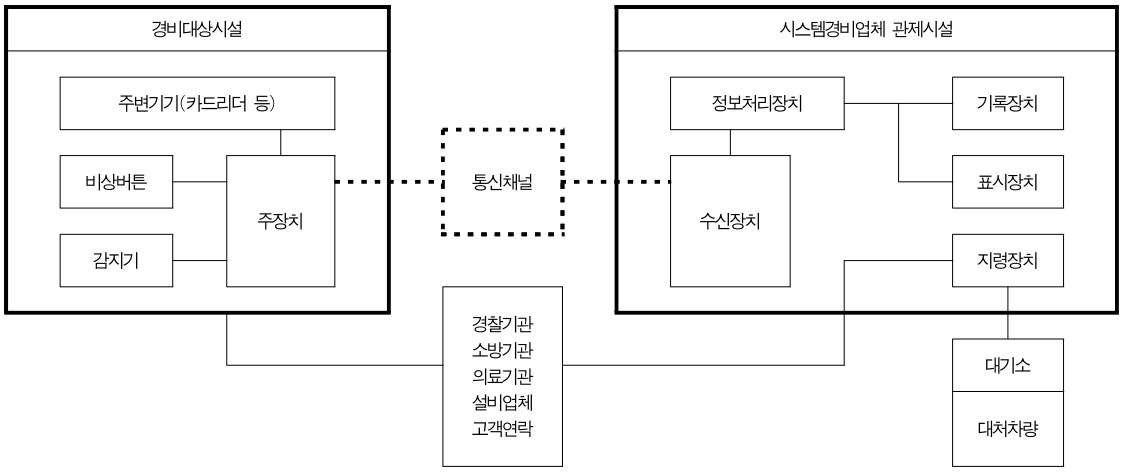

그림 1. 시스템경비의 구성
Fig. 1. Configuration of The Electronic Security System

를 설치하고 경비대상시설 이외의 원격지에 설치한 관제센터(SCC: Security Control Center)와 통신채널로 시스템을 구성한다. 그리고 관제센터에서 24시간 경비대상시설을 감시하며 이상정보가 수신될 경우 출동기계경비원을 대상시설에 급파하고 필요에 따라 경찰·소방·의료기관 또는 설비관리회사나 사용자 지정 연락선에 통보하여 경비대상시설의 피해의 확대를 방지하도록 시스템을 구축한다.

시스템경비는 경비대상시설의 도난·화재 등 위험발생을 방지하는 업무라는 목적을 달성하기 위해서는 지연(delay)·감지(detection)·감시(monitoring)·대처(response)의 기본기능을 갖추어야한다[3]. 이러한 시스템경비의 기본기능 중에서 감시기능에 해당하는 것이 관제업무이다.

관제시설에서는 24시간 네트워크를 통해 접수되는 정보를 원격감시하고, 경보나 장애신호를 확인하면 출동기계경비원에게 대처지시와 유관기관에 통보업무를 수행한다[4]. 또한 업무수행 중에 발생할 수 있는 출동기계경비원의 신변위험요소에 대한 안전조치를 취하여 계약상대방에게 제공하는 서비스의 품질을 최상의 상태로 유지하는 역할도 수행한다. 이러한 관제시설은 시스템경비업무의 중추신경과 같은 역할을 담당하므로 한순간이라도 그 기능이 중단되면 치명적인 결과를 초래할 수 있다.

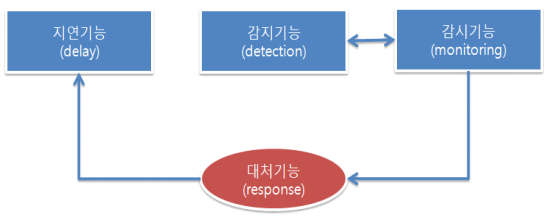

그림 2. 시스템경비의 기본 기능
Fig. 2. Basic Functions of The Electronic Security System

2. 시스템경비 관제시설의 구성요소

시스템경비 관제시설에서는 상황관리업무와 고객응대업무를 담당한다. 상황관리업무는 경비대상시설에서 이상신호가 접수되면 신속하고 정확한 판단으로 현장의 출동기계경비원에게 대처지시를 하여 계약상대방의 생명과 재산을 보호하는 일이며, 고객응대업무는 고객의 다양한 요구사항, 불만사항 접수와 초기대응의 역할을 수행한다.

관제시설에서 상황관리업무와 고객응대업무를 수행하기 위해서는 공간구조와 기반시설, 첨단의 관제장치와 다양한 시스템경비서비스를 제공하기 위한 기타 관제 솔루션, 그리고 관제기계경비원 등의 운영조직을 갖추어야 한다.

관제시설의 공간유형은 보안영역, 설비영역, 사무영역 및 공공영역으로 구분하여 설계하여야 한다. 기반시설에는 분전반, UPS, 축전지, 발전기, 접지 등의 전기시설과 전화, 인터넷 등의 통신설비와 관제시설의 항온항습을 유지하기 위한 공조설비를 갖추어야 한다. 관제장치에는 공중교환전화회선(PSTN central station data receiver), 전용회선(central station data receiver through direct line) 등의 관제수신장치를 비롯하여 데이터 다중화장치(data multiplexer) 및 경비용 지령통신장치(security communication system) 등이 구비되어야 한다.

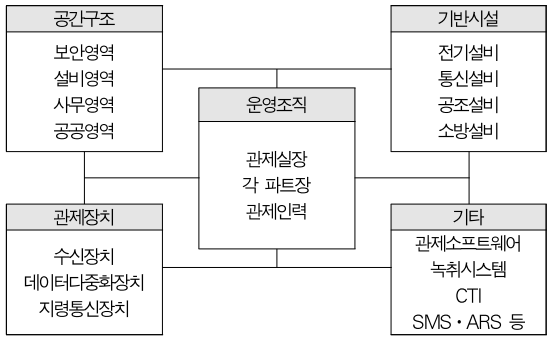

그림 3. 관제시설의 구성요소
Fig. 3. Components of the SCC

III. 관제시설의 구축과 보안대책

1. 시스템경비 관제시설의 구축

1.1 관제시설 구축 프로세스

시스템경비 관제시설의 구축을 진행하기 위해서는 계획, 설계, 구축, 운영의 4개 단계로 구분하여 절차를 수립한다.

표 1. 시스템경비 관제시설의 구축절차
Table 1. Establish procedures for SCC

단계	구분	내용
계획단계	현황분석	내·외부현황 분석
	계획수립	유관부서와의 협의 및 의견수렴
설계단계	관제시설 구축 설계	공간구조, 기반시설, 관제장치, 관제 솔루션, 운영조직 설계
	발주	시공발주
구축단계	시공계획	실시설계 검토, 시공·감리 계획
	시공	관제시설 시공
	감리	관제시설 감리
	시험	관제시설 성능시험
	준공	준공검사 및 인수
운영단계	운영계획	관제조직 구성, 관제인력 산출, 운영관리

	수립	계획 작성
	운영관리	변경・장애・백업・시설관리

계획단계에서는 관제시설의 구축에 앞서 내・외부의 현황분석이 선행되어야 한다. 내부현황은 계약상대방의 규모, 제공업무, 관제시설의 설치장소, 운영부서 등에 대한 분석 등이 포함되며, 외부현황으로는 관제시설의 구축기간, 구축비용, 구성요소, 운영방법 및 조직 등에 대한 분석이 필요하다. 현황분석 후에는 예산, 기술지원 등을 담당하는 유관부서와의 협의를 거쳐, 관제시설의 구축목표, 구축방향, 운영방향, 기대효과 등을 포함하는 기본계획과 전문가나 관계자의 사전의 견수렴 등의 절차를 위한 계획수립 등이 필요하다.

설계단계에서는 효율적인 관제시설의 기능유지와 운영인력의 업무환경을 위한 공간구조, 쾌적한 근무여건과 시스템의 원활한 운용을 위한 기반시설, 제공업무별 기능을 수행하는 관제장치, 각종 부가서비스를 지원하는 관제 솔루션 및 운영조직에 대한 설계를 수행한다. 관제시설 구축을 위한 발주업무는 업체별 특성을 고려하여 시설공사 적격심사 또는 협상에 의한 계약으로 추진할 수 있다.

구축단계에서는 관제시설의 시공에 앞서 구성요소별 실시설계를 검토하여야 한다. 관제장치와 관제 솔루션의 검토사항으로는 하드웨어・소프트웨어・네트워크 아키텍처(network architecture), 단위시스템의 기능과 성능 및 운영・관리방안, 사용자 인터페이스 등이고, 공간구조 및 기반시설은 설계도면・시방서의 일치, 현실성 및 시공자의 이해 여부 등을 면밀히 검토해야 한다. 시공계획에는 공정계획, 원가관리계획, 안전관리계획, 품질관리계획 등이 포함되며, 정보시스템의 효율적 구축, 정보통신공사의 적합시공을 위한 감리계획을 검토해야 한다. 관제시설의 시공은 실시 설계서를 바탕으로 진행하며, 구축실무담당자는 주기적으로 전체 시공과정을 확인・검사하여야 한다. 성능시험은 사용자 요구사항에 따른 기능, 성능, 부하분산, 업무시나리오를 고려하여 시험기준 충족여부를 검증한다. 공사수행기관은 관제시설의 구축을 완료한 후 발주기관의 준공검사, 운영요원교육, 시험운전, 정상운영상태 확인 등의 과정을 거친 후 발주처에 결과물을 인도하여야한다.

운영단계에서는 관제시설의 구축 후에는 효율적 운영을 위하여 총괄부서, 운영부서, 유관기관, 유지보수인력 등의 운영조직을 구성한다. 운영인력은 관제기계경비원과 관제시설 운영인력으로 구분하며, 제공업무의 성격과 규모, 운영예산에 따라 결정한다. 관제시설 운영관리 계획은 시스템 변경관리, 장애관리, 백업관리, 시설관리 및 운영과정 중에 생성되는 각종 산출물과 양식 등의 내용을 포함하여 작성한다. 관제장치와 관제 솔루션의 변경관리는 표준화된 방법과 절차에 의하여 이루어지며, 단위 시스템들의 재설계 및 변경이 업무에 미치는 영향을 검토하고 모든 변경이 효율적이고 성공적으로 처리되는지를 확인한다.

1.2 관제업무 환경 구축

보안영역과 설비영역, 사무영역, 공간영역 등으로 구분되는 관제시설의 공간구조에는 각 영역에서 수행되는 기능에 따라 다시 세분화하여 다음과 같이 구성한다.

표 2. 시스템경비 관제시설의 공간 구분
Table 2. Space Division of SCC

공간구분	내용
보안영역	관제실, 장비실, 서버실, 회의실
설비영역	공조실, 전기실, UPS실
사무영역	사무실, 탕비실, 휴게실, 창고
공공영역	도입공간, 쇼룸

표 3. 활동유형에 따른 권장 조도(6)
Table 3. Recommended Illumination According to The Type of Activity

활동유형	권장조도(lx)	작업면 조명방법
어두운 분위기 중의 시식별 작업장 어두운 분위기의 이용이 빈번하지 않은 장소 어두운 분위기의 공공장소 잠시 동안의 단순작업장 시작업에 빈번하지 않은 작업장	4 10 20 40 100	공간의 전반조명
고휘도 대비 혹은 큰 물체 대상의 시작업 수행 일반휘도 대비 혹은 작은 물체 대상의 시작업 수행 저휘도 대비 혹은 매우 작은 물체 대상의 시작업 수행	200 400 1,000	작업면 조명
비교적 장시간동안 저휘도 대비 혹은 매우 작은 물체의 시작업 수행 장시간 동안 힘든 시작업 수행 휘도 대비가 거의 안 되며 작은 물체의 매우 특별한 시작업 수행	2,000 4,000 10,000	전반・국부조명을 병행한 작업면 조명

관제시설의 구축에 있어 계획단계에서부터 우선 고려되어야 할 사항은 공간구조와 환경디자인으로 능률적이고 쾌적한 사무환경을 목적으로 한다.

보안영역으로는 관제기계경비원이 업무를 수행하는 '관제실'과 관제업무를 수행하는데 필요한 전기·전자·통신장비 등이 운영되는 '장비실'로 구분할 수 있고, 규모에 따라 시스템경비 솔루션 및 전산시스템을 운용하는 '서버실'을 별도로 구성하기도 한다. 그리고 회의실·운영실 등의 공간으로 세분화할 수 있다.

보안영역의 구성에 있어서는 관제실과 장비실의 충분한 공간할당과 영역분리가 필수적이다. 관제실은 관제기계경비원이 쾌적하게 근무할 수 있는 환경을 우선 고려하여야 하고, 장비실은 각종 장비들이 최적의 상태로 가동될 수 있는 환경을 고려하여 설계하여야 한다. 관제시설은 사람과 기계장치가 공존하는 공간으로 그 중 24시간 교대근무가 이루어지는 관제실은 쾌적성이 요구되는 공간으로 일반사무공간과 특수공간으로서의 기능이 함께 고려되어야 한다.

관제시설의 업무환경 구축에는 사회적 환경변화에 따른 현대 사무공간이 갖추어야할 요소를 친환경적 관점과 환경심리학적 관점으로 구분하여 고려할 사항들이 있다[5].

친환경적 관점의 고려요소로는 빛 환경, 음 환경, 공조환경, 색채환경을 들 수 있다.

빛 환경은 조명에 관한 사항으로 관제실 설계의 중요한 인간적 요소가 된다. 관제실은 효율적이고 쾌적한 업무수행을 위하여 자연채광을 적극 사용하고 전반·국부조명을 병행하여 300~750lx의 적정조도를 유지하도록 설계하여야 한다.

음(音) 환경은 소음대책으로 쾌적한 사무공간의 창출과 사생활(privacy)의 확보, 업무능률의 향상을 위해 고려되어야 한다. 관제실은 관제 소프트웨어의 경보음과 전화통화, 무전교신 등으로 높은 수준의 소음이 발생하는 공간이다. 관제실의 소음수준은 추상적인 표현이지만 관제기계경비원이 평온함을 느끼는 정도를 제공해야한다. 소리는 데시벨(dB)로 측정되며 매 3dB 증가는 2배의 소음증가에 해당한다. 일상적인 관제업무를 수행 중인 관제실의 경우에는 80~90dB의 범위에 있다.

표 4. 소음도의 인체영향[7]
Table 4. Health Effects of Noise

dB	음원의 예	소음의 영향
20	나뭇잎 부딪히는 소리	쾌적
30	조용한 농촌, 심야 교회	수면에 거의 영향 없음
35	조용한 공원	수면에 거의 영향 없음
40	조용한 주택의 거실	수면깊이 낮아짐
50	조용한 사무실	호흡·맥박증가, 계산력저하
60	일상 대화, 백화점내	수면장애 시작
70	전화벨소리, 거리	TV·라디오 청취방해
	시끄러운 사무실	집중력 저하, 말초혈관수축
80	철로변 및 지하철 소음	청력장애 시작
90	소음이 심한 공장안	난청증상 시작, 소변량 증가
100	착암기, 경적소리	작업량저하, 일시적 난청

이러한 높은 소음 수준은 관제기계경비원의 피로요인이 되고 있다[8]. 관제실은 모든 소음원을 평가하여 설계되어야 하고, 소음을 최소로 하기 위해서 방음타일이나 천정, 바닥이나 벽체의 재질에도 소음감소기법을 포함해야 한다.

공조환경은 관제기계경비원의 건강과 밀접한 관련이 있는 공기질을 결정짓는다. 쾌적한 공조환경을 위해서는 데스크톱 개별공조시스템을 채택하는 것이 바람직하다.

색채환경은 사무공간에서 가장 시각적인 요소로 형태보다 인간의 감정을 무의식적으로 지배하므로 보다 나은 사무공간의 색채환경을 조성해야 한다.

환경심리학적 관점에서 고려되어야 할 사항으로는 소통·사생활과 영역성·상호작용과 자율성 등이 있다. 관제실의 소통이란 관제기계경비원의 활동이 조정·통합되고 출동기계경비원과의 정보교환과정으로 볼 수 있다. 워크스테이션은 소통과 업무효율을 증진시키는 직접적인 상관관계가 있으므로 레이아웃을 형성할 때 독립성과 정보공유에 장애가 없도록 설계한다. 관제업무에는 구성원간의 상호작용이 원만해야 업무능률이 오르는 일도 있고 조용하고 폐쇄적인 공간에서 오랫동안 혼자 집중해야 할 일도 있다. 다양한 업무의 성격을 체계적으로 구분하기 위하여 관제실은 상호작용과 자율성의 두 가지 변수를 모두 수용해야 할 것이다. 변화되는 사회환경과 근무형태에서의 관제기계경비원의 건강을 유지하는 친환경적 요소와 환경심리학적 관점에서도 고려한 관제실의 구축에 관심을 기울여야 할 것이다.

2. 시스템경비 관제시설의 보안대책

최근 보안 분야는 클라우드 컴퓨팅(cloud computing)이나 사물 인터넷(internet of things) 등과 같은 다양한 기술들이 등장하면서 중요성이 더욱 부각되고 있다. 이러한 가운데 국내에서는 보안 분야를 정보 보안(information security)과 물리 보안(physical security), 융합 보안(convergence security)으로 분류하고 있으며, 이와 같은 국내 보안 분류체계는 산업 분야별 현황 분석 및 통계와 로드

맵 등에 매우 중요한 기준이 되고 있다[9].

시스템경비 관제시설의 안정적 기능유지를 위해서는 철저한 보안대책을 수립해야 한다. 시스템경비업체에서는 회사의 이미지실추와 사회적 영향을 우려하여 엄격한 보안을 유지하기 때문에 외부로 공개되는 경우는 드물지만 악천후, 정전, 화재, 천재지변을 비롯하여 인재에 의한 사고, 이상정보의 집중 또는 관제장치의 장애, 계약상대방이 예탁한 열쇠의 분실 등으로 인해 통상적인 시스템경비업무가 불가한 상황이 빈번하게 발생한다.

관제시설의 위해(危害)는 시스템경비업무의 공백으로 이어지므로 이에 대한 물리적, 기술적, 인적보안대책을 수립하고 운영해야 한다. 관제시설의 물리적 보안대책으로는 출입자통제와 소방대책, 기술적 보안대책은 주로 관제시설의 정보보호대책, 그리고 관제시설의 구성원에 대한 인적대책이 요구된다.

2.1 물리적 보안 대책

물리적 보안이란 사람과 차량 등에 대한 접근통제와 감시, 불법침입자의 예방과 탐지, 재산의 보호를 말하며 관제시설의 물리적 보안설비에는 CCTV, 침입감지센서 그리고 출입통제장치(access control system)가 포함된다.

이러한 물리보안 장치들은 TCP/IP 기반 인터넷 기술을 사용하여 더 이상 거리 혹은 공간의 제약을 받지 않고 있다. 즉 특정 보안영역을 출입하는 사람들을 감시하고 추적하여 원격지 보안관제 센터까지 실시간으로 관련 물리보안 이벤트를 전송하고 보안관제센터에서는 물리보안 장치로부터 수신된 다양한 보안이벤트를 통합 관리할 수 있는 환경을 마련하였다. 영상 감시시스템의 경우, 보안 담당자에 의해 24시간 실시간 영상을 감시하고 대응하는 것이 사실상 불가능하기 때문에 지능화된 영상감시 기술이 매우 중요하다[10].

관제시설의 물리적 보안 대책으로 먼저 출입통제대책을 들 수 있다. 관제시설은 수신장치를 비롯하여 전산장비, 통신설비와 네트워크 장비 등 시스템경비업무를 수행하기 위한 설비들이 설치되어 있으므로 비인가자의 출입이 엄격히 제한되어야 한다. 이러한 설비와 장치는 외부의 위협으로부터 보호되어야 하며, 이를 위해 엄격한 출입통제를 필요로 한다. 관제시설의 출입통제는 출입자에 대한 통제는 물론 위험물질의 반입이나 정보의 유출 또는 반출되는 정보자산에 대한 안전을 보장하는 제반 업무를 의미한다.

출입자관리는 허가되지 않은 자의 출입을 제한함으로써 주요 장비나 시설 및 관제기계경비원을 외부의 위협으로부터 보호하는 것을 목적으로 한다. 출입자 관리를 위해서는 출입자에 대한 신원확인 및 용무를 확인하는 절차로부터 자동화된 개폐시설, 그리고 무단침입을 예방하고 감시할 수 있는 각종 보안장치들을 설치·운영하여야 한다. 출입자에 대한 식별과 단계적 접근을 위한 출입통제장치(access control system)를 구성하여야 한다.

표 5. 출입통제 식별방식[11]
Table 5. Identify How The Access Control

구분	내용
식별 Identification	• 접근주체가 자신임을 확인하는 방법 • 이름, ID, 개인식별번호(PIN), 스마트카드, 전자서명, 계좌번호 등
인증 Authenticatio n	• 인증을 요하는 사용자가 본인임을 증명하는 과정, 즉 신원확인방법 • 지식기반 신원확인 : 패스워드, 암호 키 등 • 소지기반 신원확인 : IC카드, 배지, Key 등 • 생체특성기반 신원확인 : 지문, 홍채 등
권한부여 Authorization	• 사용자가 요구하는 작업을 허용하게 할 것인가를 결정하는 과정 • 기본적으로 접근금지로 설정하고, 특정 사용자만 접근하게 함

관제시설에는 보안이 요구되는 장소 즉 장비실이나 전산실 등을 통제구역으로 설정하여 출입자를 식별하고 기록할 수 있는 장치를 설치하여야 한다. 통제구역에는 '통제구역'이란 표식을 부착하여 주요 장비와 시설이 설치되어 있음을 표시하고 출입문에는 잠금장치나 자동화된 개폐장치의 설치 및 통제구역 출입관리대장을 비치한다.

반출입관리는 관제업무의 산출물이나 관제장치 등의 불법유출과 위험물질의 반입에 의한 관제시설의 장애 및 훼손을 예방하기 위한 목적이다. 관제시설의 반출입 관리대상은 관제업무의 각종 산출물(고객정보, 신호정보 등), 정보기록매체, 개인용(휴대용) 컴퓨터, 관제장치 및 기타 비품 등이 해당한다.

소방대책으로는 관제시설에서 화재가 발생하면 수신장비, 전산장비 등 각종 관제장치뿐만 아니라, 건물구조에도 심각한 손상을 입게 되어 돌이킬 수 없는 재앙을 초래하게 된다. 따라서 화재로 인한 손실을 예방하기 위해서는 철저한 소방시설의 구축이 필수적이다.

소방시설은 화재감지기의 설치와 소화설비의 구축을 들 수 있다. 화재감지기는 신속한 화재경보로 관제시설에 설치된 수신장비 및 전산장비와 건물의 훼손을 방지하고, 관제장치의 가동 중단으로 인한 기능 마비를 사전에 차단하기 위하여 설치·운영한다. 화재감지장치는 화재가 발생하면 열이나 연기를 이용하여 조기에 감지하는 장치로써 감지기, 음향장치, 시각경보기 및 수신기로 구성된다.

소화설비는 화재발생시 신속한 진압으로 관제시설과 건물의 훼손을 최소화하고, 관제장치의 가동중단으로 인한 시스템 경비업무의 중단을 최소화하기 위하여 설치하고 운영한다.

화재발생시 손실을 최소화하기 위해 방화문을 설치하고, 신속한 화재 진압을 위해 이동식 소화기와 자동소화설비를 설치하고, 소화약제는 관제장치에 영향을 미치지 않도록 전기적으로 비전도성이며 사용 후 잔유물이 남지 않는 할로겐화합물 소화약제나 청정소화약제를 사용한다.

2.2 정보보안 대책

정보보안(information security)이란 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다. 이러한 정보보안은 정보를 제공하는 공급자 측면과 사용자 측면에서 이해할 수 있다.

공급자 측면은 내·외부의 위협요인들로부터 네트워크, 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호·운영하기 위한 일련의 행위를 말하고, 사용자 측면은 개인정보 유출·남용을 방지하기 위한 일련의 행위를 말한다. 정보보안은 정보에 대한 위협으로부터 보호하기 위한 것으로 전통적으로 기밀성, 무결성, 가용성이 주요한 목표가 된다.

정보보안 사고를 줄이기 위해서는 보안정책, 정보유출방지, 사업연속성, 접근제어 및 기타 많은 정보보안 이슈들이 고려되어야 한다[12].

관제시설의 정보보안 대책은 관제전산시스템에 대한 정보보호활동 및 절차를 체계적으로 관리하여 기밀성, 무결성, 가용성을 확보함으로써 내·외부의 무단사용자에 의해 불법 유출·파괴·변경되는 것으로부터 안전하게 보호하고, 관제전산시스템의 운영환경과 소프트웨어를 안전하고 신뢰성 있게 운영하여 관제기계경비원에게 원활한 서비스를 제공하는데 필요하다. 관제전산시스템의 보안관리를 효과적으로 수행하기 위해서는 관리대상이 적절히 분류되어야 하고 각 대상들에 적합한 보안관리 기능이 설정되어야 한다.

관제시설의 정보보안 대책으로 다음 사항들을 고려하여야 한다.

첫째, 보안수칙, 보안등급, 보안점검 및 보안사고의 처리에 대한 기준마련이 선행되어야 한다. 관제시설에는 정보보안 수칙과 보안등급을 제정하여 주기적으로 주요 정보보호자원에 대한 보안점검을 실시하여야 한다. 보안사고가 발생했을 경우에는 절차에 따라 처리하고 관제기계경비원을 대상으로 정보보안 교육을 수행한다.

둘째, 관제기계경비원은 관제정보시스템 사용에 있어 적절성을 유지하여야 하고 정보보안 담당자는 부적절한 사용사례를 정의하여 이를 위반할 경우 적절한 제재조치를 취해야 한다.

셋째, 관제시설의 네트워크는 물리적으로 광범위하고 경로가 다양하며, 많은 사람에게 이용되고 있기 때문에 여러 가지 보안문제를 야기하고 있다. 따라서 중요한 정보자산에 영향을 미치는 불법시도를 사전에 감지하고 보호하기 위해서는 특히 전산망과 방화벽에 대한 보안관리 활동이 요구된다.

넷째, 관제서버는 인터넷의 발달과 개방화에 따라 많은 부분에서 보안의 취약성을 가지고 있다. 이러한 보안 취약성으로부터 주요 운영시스템에 대한 보호를 위해 운영관리, 보안점검, 계정관리 등을 수행해야 한다.

다섯째, 관제시설의 정보자산에 대한 위험요소를 식별하고 적절한 통제를 구현하기 위하여 자료에 대한 관리, 보관, 파기에 대한 보안활동이 요구된다. 자료관리에 있어서는 데이터베이스 로그인 계정관리 기준을 정의하고, 비밀번호는 암호화된 형태로 관리하며 데이터베이스의 수정은 인가자에 의해서만 이루어져야 하며, 주기적으로 백업을 실시해야 한다. 중요자료로 분류된 자료에 대한 자료보관과 재해 및 비상사태를 대비한 소산 계획을 수립하여 운영한다.

2.3 인적보안 대책

관제시설의 보안업무를 실행하고 유지하기 위해서는 관제기계경비원에 대한 책임과 역할을 정의해야 한다.

관제기계경비원의 채용·재직·퇴직 등에 있어서는 단계별로 구분하여 적절한 보안대책을 강구해야한다. 이들은 관제시스템을 통해 고객정보나 회사의 기밀정보 등 민감한 정보를 처리하는 인원으로 반드시 적성검사·이력서 점검·및 경력확인 등을 통한 신용점검이 필요하다. 관제기계경비원을 채용할 때에는 "재직 중 취득한 회사 기밀을 누설하는 경우 손해배상은 물론 민·형사상 책임을 지겠다."는 내용의 보안 서약서를 받고, 보안에 대한 경각심을 주도록 한다. 재직 중인 핵심인력에 대해서는 정기적으로 면담을 실시하고 금전적 문제와 근무여건 등 제반 애로사항을 수시로 파악하여 불만이 없도록 사전에 조치하고 정기적으로 보안교육을 실시하는 한편, 정기 또는 불시 보안점검을 실시하여 경각심을 제고하는 것도 좋은 방법이 될 수 있다.

관제기계경비원은 정보보안의 위협을 인식하고 일상 업무 중에 적절한 교육을 받아야 한다. 보안사고나 관제시스템의 장애가 발생했을 경우에는 사고보고→사고조치→피드백→전파의 보고와 사고대응절차에 따라 대응하여야 하고 관제시스

템이나 관련 장비에 취약점을 인식했거나 의심스런 요소를 발견했을 경우에는 반드시 정보보안 관리자에게 보고하도록 교육하여야 한다.

관제시설의 보안정책과 절차를 위반한 직원에게는 공식적인 징계처리가 수행되어야 하며, 이는 보안절차를 경시하는 직원이 보안관리 규칙을 준수하게 하는 목적이 있다. 관제기계경비원이 퇴직할 때에는 재직 중에 담당하였던 업무내용, 연구·개발 및 영업비밀과 관련된 서류 등 일체를 반납하도록 하고 이를 확인하도록 한다. 업무상 정기적으로 출입하는 협력업체 직원은 최소한으로 제한하고 출입지역도 일정한 한계를 두어 핵심시설에는 일체 접근하지 못하도록 엄격하게 통제한다. 관제시설에 대한 A/S업체 등과 기술자문, M&A 업체 직원에게 제공한 자료는 반드시 회수하고 별도의 보안대책을 수립하여 시행하고 하청 및 부품업체와 제품판매업체 직원에 대해서도 중요정보에 접근하지 못하도록 사안별로 적절한 보안대책을 강구한다.

관제시설의 모든 정보는 영업비밀로 분류 하고 비인가자는 접근하지 못하도록 물리적·기술적 보안대책을 강구해야 한다. 중요자료를 외부에 제공하거나 열람시키는 것은 엄격히 제한하되 부득이하게 제공해야 할 경우에는 관련인원을 최소한으로 제한하고 보안서약서를 받는 등 적절한 보안대책을 강구한다. 기술이전이나 하청계약 체결 시 자료를 제공할 때에는 반드시 비밀유지의무조항을 포함시키고 이를 위반하였을 경우 책임소재를 명시한다[13].

IV. 결 론

1980년에 귀금속점이나 전당포 등을 대상으로 시작된 한국의 시스템경비산업은 지난 30여 년간 비약적인 발전을 거듭하여 현재는 국가중요시설을 비롯하여 금융기관, 관공서, 외국공관에 이르기까지 경비대상이 확장되어 현대인의 일상과 밀접한 관계 속에 있다. 그러나 시스템경비업무는 사람과 경비용기계장치의 상호작용이 요구되는 특성으로 물리적, 기술적, 인적 위해의 우려가 상존하고 있다. 우려는 현실로 나타나 화재나 대규모 정전으로 인한 시스템경비업무의 중단사태도 발생했었다. 이제는 시스템경비업무가 중단되면 국가중요시설이나 관공서 등은 안전을 담보하기 어려운 실정이며 금융기관은 자동화기기를 운영하기 어려운 현실에 이르렀다.

관제시설은 시스템경비의 핵심적인 구성요소로 현장의 대응체제가 아무리 잘 구축되어 있더라도 관제시설의 작동이 중단되거나 관제기계경비원이 위해를 입게 되면 시스템경비는 본래의 기능을 할 수 없게 된다. 기업의 이미지실추를 경계하기 위하여 외부로 공개되지 않았을 뿐 현재도 시스템경비업체 관제시설에서는 전기나 통신, 각종 전산장애로 시스템경비업무의 중단이 발생하고 있다.

관제시설의 장애나 재해는 기업이미지 실추에 그치지 않고 시스템경비에 대한 신뢰하락으로 고객이탈, 피해보상, 기회비용의 손실로 이어져 기업의 위기를 초래할 수 있고, 계약상대방의 경영활동뿐만 아니라 금융시스템의 운영에도 장애를 초래하는 등 국가적인 혼란과 직결되기 때문에 예방체계 구축은 안정적 운영을 위한 필수요소이다.

이 연구에서는 시스템경비의 관제시설의 구축과 보안 및 경영대책을 제시하였다.

관제시설의 구축을 위해서는 먼저 구성요소와 절차 등의 프로세스를 정의하여야 한다. 관제시설의 구성요소로는 공간구조, 기반시설, 관제장치, 각종 관제 솔루션 및 관제시설의 운영조직 등이 있다. 공간구조에는 보안영역, 설비영역, 사무영역, 공공영역으로 구분하고 각 공간의 특성에 맞는 환경을 구축하여야 한다. 전기·통신·공조 등의 기반시설과 수신장치, 데이터다중화장치, 지령통신장치 등의 관제장치와 관제업무를 위한 소프트웨어와 부가서비스를 위한 관제 솔루션을 구축하여야 한다. 관제시설의 구축은 계획단계, 실시단계, 구축단계, 운영단계의 절차로 진행되며 각 단계별 고려사항을 포함하여야 한다.

관제시설은 사람과 기계장치가 공존하는 공간으로 그 중 24시간 교대근무가 이루어지는 관제실은 일반사무공간과 특수공간으로서의 기능이 함께 수행할 수 있어야 한다. 친환경적 관점에서 조명, 소음, 공조, 색채환경을 고려하여야 하고, 환경심리학적 관점에서는 소통, 프라이버시와 영역성, 상호작용과 자율성을 고려한 공간구축이 이루어져야 한다.

관제시설의 보안대책으로는 물리적 보안, 정보보안, 인적보안으로 나눌 수 있다.

물리적 보안대책으로는 출입통제대책과 소방대책을 수립하여야 하고, 정보보안대책으로는 보안수칙, 보안등급, 보안점검 및 보안사고의 처리기준 제시를 비롯하여 관제시스템과 네트워크, 서버와 데이터베이스에 대한 보안대책을 강구하여야 한다. 인적보안대책으로는 내·외부인원의 채용·재직·퇴직에 관한 사항과 정보보안에 대한 교육훈련 등이 있다.

시스템경비업체에서는 관제시설의 가동중단을 예방하고 가용성 있게 운영하기 위해서는 현재의 운영 상태를 철저히 모니터링하고 데이터를 누적해야 한다. 그 결과를 토대로 관제시설의 운영을 개선하여 시스템경비업무에 대한 성능향상, 재해나 장애의 예방, 보안서비스의 개선 등을 모색해 나가야 할 것이다.

REFERENCES

[1] Young-Kwan Kwon. *"Security System and Services"* Jinyoungsa, pp. 92, January 2013.

[2] Berger, David L. "*Industrial Security*" Boston: Butterworth Publishers. Inc. pp. 11-12, February 1999.

[3] John Sanger. "*Basic Alarm Electronics*" Boston: Butterworth Publishers. Inc. pp. 11-12, January 1988.

[4] Robert J. Fischer & Gion Green. "I*ntroduction to Security*" Boston: Butterworth-Heinmann Publishers. pp. 211-212, April 1998.

[5] Park, Kyung Hwan · Kim, Kang Soo. "A study on modern office environment in accordance with social changes" Architecture & Urban Research Information Center, Vol. 8, No. 1, pp. 49-52, August 2008.

[6] Korea Standards & Certifications. "Recommended Level of Illumination" KS A 3011. December 1998.

[7] National Noise Information System. "Effects of noise", http://www.noiseinfo.or.kr, May 2015.

[8] Robert L. Pearson. "*Electronic Security Systems, A Manager's Guide to Evaluating and Selecting System Solutions*" Boston: Butterworth-Heinmann Publishers. pp. 167-168, December 2006.

[9] Jeong-Hoon Jeon. "A study on the classification systems of domestic security fields" Journal of The Korea Society of Computer and Information Vol. 20, No. 3, March 2015.

[10] Koo-Hong Kang. "An Implementation Strategy for the Physical Security Threat Meter Using Information Technology" Journal of The Korea Society of Computer and Information Vol. 19, No. 7, July 2014.

[11] National Information Society Agency. "*Integrated control center building guidelines*" pp. 42, February 2011.

[12] Sangsoo Yeo, Suchul Hwang. "A Safe Operating Strategy for Information System of Small and Medium Enterprises" Journal of The Korea Society of Computer and Information Vol. 14, No. 7, July 2009.

[13] National Industrial Security Center. Security Diagnosis. May 2015. http://service4.nis.go.kr

저 자 소 개

하 경 수

1996: 계명대학교
일어일문학과 문학사.
2011: 용인대학교
경호학과 경호학 석사.
2015: 용인대학교
경호학과 경호학 박사
현 재: 주)씨너스 SK broadband
마이캠 관제팀장
관심분야: 기계경비, 영상보안
Email : hiroppong@empas.com

조 철 규

2009: 경운대학교
경호학부 체육학사.
2011: 용인대학교
교육학과 교육학석사.
2015: 용인대학교
경호학과 경호학박사.
현 재: 경운대학교 경호학부 교수
관심분야: 민간경비, 기계경비
Email : cck1001@nate.com

김 평 수

2000: 용인대학교 경호학과 체육학사
2002: 용인대학교 경호학과 경호학석사
2005: 경기대학교
경호학과 경호안전학박사.
현 재: 전남도립대학교
경찰경호과 교수
관심분야: 경호학,
시큐리티 행정 및 경영
Email : kimkps@hanmail.net