한국경호경비학회 – 제27호(2011): 129–159
투고일 2011. 4. 30, 심사일 2011. 5. 11, 게재확정일 2011. 6. 20

보안디자인을 활용한 시설보안시스템 구축 방안

최 선 태

보안디자인을 활용한 시설보안시스템 구축 방안

최 선 태*

〈요 약〉

시설보안은 항상 보안영역에서 가장 중요한 부분을 차지하고 있다. 일반적으로 통합적 보안계획은 세 가지 요소로 구성된다. 여기에는 시설보안, 인사보안, 정보보안이 포함된다. 이 세 가지 요소는 상호간에 긴밀하게 연계되어 있고 보호하고자 하는 대상 시설과 기업의 유형에 따라 매우 다양하게 운영된다. 통합보안프로그램에서 시설보안요소는 대체적으로 정책과 절차, 사람, 방벽, 장비와 기록물로 구성된다.

인간은 선사시대부터 자신과 부족의 생명을 보존하기 위하여 쉼 없는 투쟁을 계속하였다. 그러나 선사시대의 인간들은 어떻게 견고한 집을 짓고 거주지를 어떻게 요새화하는지를 배우지 못하였기 때문에 자신들의 보호를 자연에 의존하였고 추운 날씨에는 동굴들을 보호나 피난처로 활용하였다. 인류사를 통하여 인간은 자신과 자신이 속한 부족의 생명과 자산을 보호하기 위하여 다양한 보호대책을 수립하여 왔다. 이러한 보안대책의 기본에는 시설보안대책이 자리하고 있다.

중세시대의 유럽의 대군주들은 성곽 둘레를 파내어 해자를 건설하거나 도개교를 만들어서 성 주위를 강화하고 거주자들에게 이러한 보호를 제공하고 경작된 농산물을 제공받았다. 20세기 들어 미국의 에드윈 홈즈는 미국의 보안산업발전에 혁신적인 전자경보서비스를 제공하기 시작하였다. 이것이 오늘날 전자보안시스템의 효시이며, 발전을 거듭하여 오늘날 해당 시설물에 다양한 전자보안시스템을 조합한 형태의 보안시스템이 보안시장의 대부분을 차지하고 있다.

이와 같이 인류는 태초부터 생명을 보호하기 위한 방법으로 다양한 보호대책을 수립하여 발전을 계속하고 있다. 오늘날 현대인은 생명과 자산의 보호와 다양한 사회병리현상에 대응하기 위하여 전국 방방곡곡 대부분의 시설물에 CCTV가 설치되어 현대인의 일상을 보호·감시하고 있다.

이러한 대부분의 시설보안시스템은 우리의 안전을 보장하기 위하여 설치되고 있으나 이에 대한 모든 비용 또한 우리가 지불하여야 한다. 따라서 효과적인 시설보안시스템의

* 경남대학교 경호비서학과 교수

구축은 매우 중요한 당면 과제이다. 이 연구에서는 현대사회의 필요성에 의해서 급속하게 증가하고 있는 시설보안시스템의 효과적인 구축방안에 대하여 보안디자인의 원리에 시스템 통합을 활용하여 효과적인 시설보안시스템 구축방안에 대하여 제시하였다.

주제어 : 보안디자인, 시설보안시스템, 시스템통합, 리스크평가, 시스템디자인

목 차

Ⅰ. 서 론

지난 수십 년 동안 그리고 최근 들어 더욱 급속한 성장을 계속하고 있는 보안산업의 성장은 눈부시다. 2000년 도 미국의 보안산업은 910억 달러에 달하고 여기에 전자장비 판매를 포함한 보안서비스 분야가 2/3에 달하며, 이러한 추세는 더욱 증가하여, 전 세계 보안장비의 시장규모는 2014년까지 1,000억 달러에 달할 전망이다.

전 세계 보안장비 시장규모는 연간 7.7%씩 성장하여 2014년까지는 거의 1,000억 달러에 달할 것으로 시장조사 전문업체인 The Freedonia Group이 밝혔다. 세계 보안장비 수요는 지난 2009년에 물리적 보안 제품은 전체 보안장비 수요의 60% 이상을 차지했는데 자물쇠 등 출입통제 제품과 다른 기계적 보안장치의 판매 또한 점차 늘어날 것으로 예측했다.[1)]

정부는 금년 1월부터 아파트에서 성추행 등 각종 범죄와 안전사고가 빈발함에도 방범시설 설치 규정이 미흡하다는 판단에 따라 의무관리 대상(300가구 이상, 또는 승강기가 있거나 중앙 난방하는 150가구 이상)인 신규 공동주택은 동별 주출입구, 승강기, 어린이 놀이터 등 주요 공간에 반드시 CCTV를 설치하도록 했다(주택건설기준 등에 관한 규정 제39조, 폐쇄회로 텔레비전의 설치). 2009년 우리나라의 CCTV

1) World Security Equipment to 2014, www.freedoniagroup.com, 검색일 2011. 4. 20.

시장규모는 7,200억 원대에 이른 것으로 조사되었다(인포더, 2010).

〈표 1〉 전 세계 보안장비 시장 규모(단위: 백만 달러)

지역/연도	2004	2009	2014
전 세계	52305	69600	99300
북미	12880	14510	21750
서유럽	18385	21300	26650
아시아태평양	12600	19970	29900
기타 지역	8440	13820	21000

* 자료 : World Security Equipment to 2014, www.freedoniagroup.com, 검색일 2011. 4. 20.

오늘날 보안산업은 현대인의 생활과 밀접한 관계를 가지고 있으며, 안전한 생활환경이 안락한 생활을 담보하고 있다. 이렇게 현대인의 삶에서 보안이 차지하는 비중이 점차적으로 확대되고, 보안비용이 증가하게 된다면 보안산업의 성장에만 관심을 기우릴 것이 아니라 과연 보안에 투자대비효과(ROI)에 대한 연구는 더욱 더 중요할 것이다. 그러나 보안산업관련 연구는 대부분이 보안산업의 발전방안과 경비원의 교육훈련 및 직무만족도, 그리고 보안업체와 경찰의 관계 등 구체적이고 실증적인 분석 중심이었다(이창무, 2009).

기존의 카지노, 항만을 포함한 시설보안시스템에 대한 연구도 운영과 제도개선에 대한 내용이 주를 이루고 있고 시설보안시스템의 효율성에 대한 연구는 찾아보기 힘들다(이호중, 2010: 김철영, 2009: 변용남, 2009).

선행연구를 일람하면 이호중(2010)의 연구는 주로 현재 사용 중인 기계경비시스템의 보완 필요성에 대하여 강조하였다. 더불어 건물의 시공과정에서 설치된 기계경비시스템은 관리자의 실무경험과 운영을 참고하여 설비의 부족함과 변경 또는 보완이 필요하고, 인력경비를 줄이고 기계경비시스템을 적극 활용해야 한다고 주장하였다.

김철영(2009)의 연구는 첫째, 카지노 보안시스템의 이원적인 운영의 문제점을 지적하고 서베일런스와 시큐리티를 통합하여 보안시스템을 구성하고, 둘째, 보안요원 교육의 문제점을 체계적이고 정기적인 교육을 실시함으로 극복하며, 셋째, 보안요원의 비정규직화의 문제점으로 소속감과 책임감의 부족을 야기함으로 비정규직화는 업무능력 저하로 이어진다고 지적하였다.

변용남(2009)은 현 항만관련 보안법령을 책임기관으로 일원화하여 장기적인 항만

보안계획의 수립하여야 하고, 항만시설을 포함한 내해까지 항만 보안관련 업무를 수행하는 Port Captain 제도의 도입을 주장하였다.

이와 같이 기존의 연구가 제한된 분야에서의 시설보안에 관한 운영의 효율화에 대한 연구가 대부분이었으므로, 국가와 국민생활에 밀접하게 관련된 보안산업, 이 중에서도 보안비용의 대부분을 차지하는 시설보안시스템의 디자인을 활용한 보안시스템의 효율성과 관련된 본 연구는 의미가 있다고 생각된다. 시설보안시스템의 구축에 디자인 개념의 활용은 인간공학과 행동공학적인 요소에 경제학의 기본개념을 보안시스템구축에 활용하는 것으로 매우 유의미한 방법론이다. 시설보안의 의미도 미국에서와 같이 각종 보안장비에 지정된 보안초소에서 보안업무를 수행하는 경비요원(guard)을 포함하였다. 구체적으로 시설보안에서 다루는 주요한 분야는 각종 방벽, 게이트, 출입문과 창문, 보안조명, 방탄유리, 자물쇠, 금고와 금고실, 출입통제장치, 방문자 관리, 경보시스템, 보안조사, CCTV, 인력보안서비스, 침입감지시스템, 보안취약성 평가, 요인보호, 주차장관리, 심지어는 경비견까지도 시설보안영역에 포함된다.

다양한 시설물에 설치된 시설보안은 인명보호나 정보보호대책에 대한 토대가 된다. 구성원과 정보시스템에 대한 보안은 고도로 치밀하게 디자인된 시설보안대책을 토대로 시작되며, 기업의 모든 자산보호의 핵심이 되므로 조직의 자산보호대책에 대한 전체적인 평가를 바탕으로 한 체계적인 시설보안디자인은 물리적 보안의 기초뿐만이 아니라 조직전체의 보호대책의 근간을 구성하므로, 첨단화된 물리적, 기술적인 보호대책이 서로 긴밀하게 연계되어 디자인되고 운영되어야 초기에 의도한 목적을 달성할 수 있을 것이다.

디자인이라는 용어는 '설계', '기획' 등의 용어와 뉘앙스의 차이가 있으며, 주어진 목적을 조형적으로 실체화하는 것의 의미로써, 지시하다·표현하다·성취하다의 뜻을 가지고 있는 라틴어의 데시그나레(designare)에서 유래한다. 디자인은 관념적인 것이 아니고 실체이기 때문에 어떠한 종류의 디자인이든지 실체를 떠나서 생각할 수 없다. 이러한 디자인은 주어진 어떤 목적을 달성하기 위하여 여러 조형요소 가운데서 의도적으로 선택하여 그것을 합리적으로 구성하여 유기적인 통일을 얻기 위한 창조활동이며, 그 결과의 실체가 곧 디자인이다.

어떤 조직에서건 보안업무에서 어떤 보호대상에 대하여 실시되는 모든 활동이나 시설물에 대한 효과적인 보안디자인을 적용하기 위해서는 몇 가지 중요한 원리가 적용되며, 사업장의 보안실무자들은 이러한 원리를 개발하여 사업장에서 적절하게 적용

하는 것을 통하여 해당 사업장의 베스트 프랙티스(Best Practices)를 수립하여야 한다.

보안디자인의 원리를 잘 적용하고 베스트 프랙티스를 잘 수립할 경우에는 현재 활용하고 있는 보안시스템의 효과성을 보장할 뿐만 아니라 동시에 잠재된 리스크를 감소시키게 한다. 그러나 여기에서 제시한 보안디자인의 원리가 모든 상황에 적용되는 것이 아니므로 궁극적으로 해당 사업장의 특성을 고려하고, 사고와 관련된 보안문제를 예방하고 리스크를 감소시키는 것과 같이 더 향상된 보안시스템을 구축하면 할수록 사용자에게는 더 많은 만족을 가져다 줄 것이다.

현대인의 안전욕구의 증대에 의하여 급속히 설치가 확대되고 있는 다양한 보안장비들의 효과에 대한 비판적 연구 없이 계속적으로 설치만 확대된다면 언제가 우리의 생활이 보안장비의 감시 속에 갇히게 될지도 모른다. 따라서 안전과 프라이버시가 조화를 이루는 최적의 보안디자인에 대한 연구는 보안시스템의 효용성 못지않게 중요하다. 본 연구는 국내에 시설보안디자인에 대한 참고 문헌이 제한적인 한계점으로 외국의 문헌(주로 영국)을 주로 하여 연구자의 기업체 시설보안컨설팅 경험을 활용하였다.

Ⅱ. 이론적 배경

1. 시설보안 개념

미군야전보안교범(US Army Field Security Manual)의 시설보안(physical security)이란 인명을 보호하기 위하여 디자인된 물리적 조치로써 장비, 설비, 물질 그리고 문서에 허가없이 접근하는 것을 방지하고 스파이, 사보타지와 절도를 방지하기 위한 보호대책을 의미한다고 하였으며, 월시(Timothy J. Walsh)는 출입통제와 운영활동의 방해요인을 예방하기 위하여 디자인된 유형적인 대응조치의 전반적인 시스템이라고 정의하였다(Walsh, 1994).

일반적으로 산업보안(Industrial Security)분야에서 포괄적으로 보안업무를 물리적, 전자적, 인사보호분야로 대별하며, 시설보안이라고 하면 물리적 보안분야를 의미하고, 시설보안은 보안의 가장 전통적인 영역이며 자산보호의 가장 기본적인 형태이다. 아무리 보안환경이 변화하고 첨단기술이 접목된다고 하더라도 인간이 생활하는 공간에 대한 시설보안의 중요성은 결코 간과되어서는 안 된다.

일반적으로 산업보안 선진국인 미국에서의 시설보안은 관리적인 보안업무를 수행하는 보안직능 이외에 순찰이나 입초근무를 수행하는 인력보안 영역까지도 시설보안 업무에 포함시킨다. 따라서 보안조직의 운영비 중에서 시설보안이 차지하는 비중은 절대적이다. 이러한 물리적인 통제를 통하여 경계구역, 사업장, 시설물, 건물을 보호하고 조직에 속하는 모든 물리적인 자산을 보호하는 임무를 수행한다. 물리적 보안은 허가되지 않는 출입, 위험요소, 자산의 파괴를 방지하기 위한 심층적인 시설보안대책을 활용하는 공정을 적용하므로, 필수적으로 손실이나 위험요소로부터 자산, 공장, 시설물, 건물, 사무실과 모든 기업자산을 보호하는 업무를 수행하여야 한다.

포괄적인 보안계획은 일반적으로 세 가지로 구성된다. 첫째, 일반적으로 시설보안은 접근방법을 통제하기 위한 유형적인 대응책을 디자인하고 운영상의 방해요인을 예방하기 위한 시스템이다. 둘째, 개인에 대한 안전조치는 업무를 수행하는 임직원이 업무수행에 대한 방해 없이 업무를 수행할 수 있도록 보장하기 위한 일련의 운영방법(a set of practices)이다.

셋째, 정보보안은 조직의 운영과 성장을 보증하도록 생산된 정보와 여러 가지 영업비밀인 고객명단과 마케팅계획, 재무통계와 다양한 형태의 재산적 정보의 보호를 다룬다.

이와 같은 세 가지 요소들은 서로 밀접하게 연관되어 있으며 보호되어야 할 시설물이나 조직의 유형에 따라 보호정도는 다양하다.

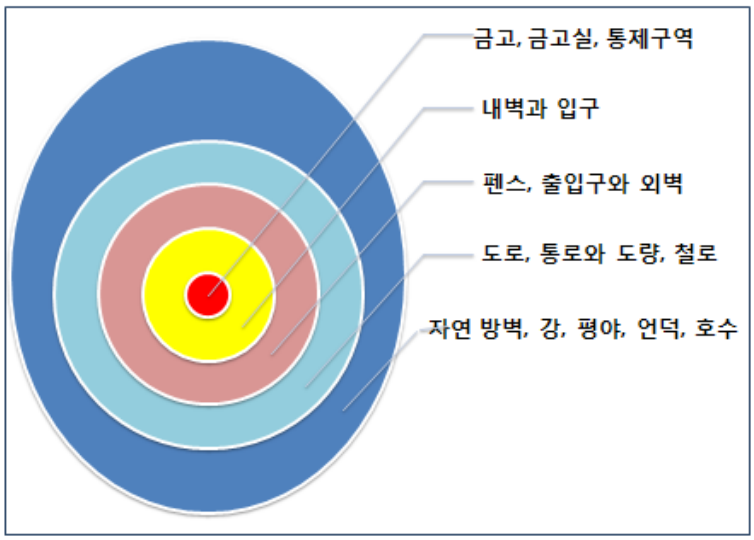
포괄적인 보안프로그램에서 시설보안의 구성요소는 대체적으로 다음의 5가지 구성요소로 첫째, 정책과 절차로 보안목표에 대한 선언서와 목표를 달성하는데 필요한 수단에 대하여 규정한다. 둘째, 인적구성으로 시스템을 시행·관리하기 위한 실무자를 의미한다. 셋째, 방벽으로 출입통제장치와 구조물을 말한다. 넷째, 장비로 감지, 경보, 교신과 통제시스템, 여기에는 하드웨어와 소프트웨어 모두를 포함한다. 다섯째, 기록물로 과거의 기록과 사고보고서, 출입통제에 대한 각종 기록, 업무처리 기록부 등으로 구성된다.

2. 심층보호

시설보안 프로그램의 주요한 목표는 목표물에 대한 접근을 통제하거나 어렵게 하여 지연시키는 것이다. 여기에서 사용되는 방벽(barriers)의 개념은 이러한 목표를 달성하기 위하여 그림 1과 같이 구성된다. 이러한 방벽에는 일반적으로 중심부로 접근

할수록 점차적으로 보안의 수준이 강화되는 동심테두리(concentric layer)로 구성된다. 각각의 층은 가능한 최대한 침입자의 침입을 지연시키는 역할을 수행하게 된다. 따라서 시설보안계획이 적절하게 수립된 경우에는 각각의 층에 의한 지연된 시간의 합은 침입자의 시도를 무력화하거나 보안시스템을 통제하는데 도움을 제공하게 된다. 그러므로 물리적 통제는 시설물 배치의 핵심적인 부분이 되어야 하고 이러한 시스템으로부터 최대한의 장점을 얻기 위해서는 전체적인 보안프로그램과 통합이 이루어져야 한다.

외곽의 보호테두리는 시설물을 둘러싸고 있는 모든 자연적인 방벽이나 시설물의 대지 경계선(property line)에서 설정된다. 가운데 테두리는 구조물의 외부에 설정하고 건물의 내부에는 내부테두리가 설정된다. 어떤 시설물에서는 전체적인 대지구역이 대지 경계선과 동일한 구조로 되어있어서 외부의 대지 경계선이 구분되지 않으므로 대지 경계선이 대지구역을 표시한다. 대신에 이러한 경우에 시설물에 대한 접근통제는 중간 보호 테두리나 구조물이 위치하고 있는 장소의 외부에서 시작되어야 한다. 각각의 보호 테두리의 역할과 개념은 다음과 같다.



〈그림 1〉 보안의 계층도

* 출처: Walsh, 1994: 19:2, 편집

1) 외부 보호 테두리

물리적인 통제는 담장이나 다른 방벽을 설치하는 것으로 구성하고 보안조명, 신호기, 경보기도 포함한다. 이 지점에서 통제는 일반적으로 경계선의 규정, 사람들이 출입하는 통행로, 차량의 접근지점을 지정하는 방법을 개괄적으로 디자인한다. 이러한 디자인을 통하여 침입자, 시위자가 경계선을 가로질러 진입하는 것을 방지하도록 한다. 또한 호기심으로 시설물에 접근하려는 사람들에게 경계선의 의미를 정확하게 전달할 수 있도록 표시하고 이러한 알림사항에 대하여 위반하는 경우에는 불이익을 당한다는 것을 잘 알 수 있도록 하여 이를 위반하는 사람들이 없도록 하는 역할을 한다.

2) 중간 보호 테두리

사업장 건물 외부의 중간보호 테두리는 대체적으로 보안조명, 경보기, 잠금장치, 출입문과 창문에 강력한 강도의 보조 금속막대, 신호기, 담장과 같은 방벽의 형태로 구성된다. 여기에 필요에 따라 추가적으로 외부의 보호 테두리보다 더 보강된 보호대책을 보강할 수 있다. 이 부분에서의 보호대책에는 출입문과 창문에 대한 물리적인 통제가 필수적이다. 더불어 방벽과 건축물의 외벽면에 대한 보호대책이 간과되는 경우가 많으나 실제적으로 이러한 취약성으로 인하여 보호대책이 잘 운영되지만 눈에 잘 보이는 부분에 대한 대책이 의미가 없어질 경우가 있다. 따라서 사업장의 보호대책은 보호객체를 하나의 지붕을 가진 상자로 생각하고, 바닥과 사면에 대한 균형있는 보호대책이 요구된다.

이러한 측면에서 항상 시설물의 지붕을 통한 침투에 대하여 고려하여야 하므로, 침입자가 채광창, 승강기 기계실, 환기구를 통하여 내부로 침투할 경우에는 침입 동선에 경보장치가 설치되거나 외부적인 침투를 어렵게 하는 보강장비가 설치되어야 한다. 더불어 맨홀, 하수구와 같은 지하통로를 이용한 침투는 의외로 대비에 소홀하므로 특히 침입자가 지하공간을 통하여 이동할 수 있는 충분한 공간이 있는 통로에 대한 점검과 이에 대비한 다양한 대응책도 강구되어야 한다.

3) 내부 보호 테두리

대체적으로 내부 테두리에는 중간이나 외부 테두리보다 더 강화된 보호대책이 수립된다. 침입자가 외부와 중간 테두리를 통과하였다 하더라도 아직 목표물이 어디에

있는지 알지 못하기 때문에 먼저 이러한 장소에 대한 구체적인 계획수립이 중요하다. 일반적으로 물리적 통제에는 창문과 출입문에 보강된 창살, 잠금장치, 방벽, 신호·경보기, 보안조명, 금고, 금고실, 통제구역이나 내부공간이 내부보호 테두리에 속하는 보호대책들에 포함된다.

내부 테두리에는 가치 있는 연구시설과 생산데이터, 장비와 공정, 현금과 유통증권, 조직의 각종 핵심적인 기록물들을 보관하고 있기 때문에 상당한 노력을 기울려 보호대책이 수립되어야 한다. 이 경우에 보호수준은 내부에 보관된 자료의 가치에 비례하여 결정되어야 한다. 이러한 과정을 리스크평가라 한다. 특히 중요한 연구시설에는 특별히 강화된 방벽, 다양한 종류의 경보장치, 조합잠금장치가 부착된 튼튼한 문, 출입에 필요한 서명의 요구, CCTV와 금고가 필요할 것이다. 더불어 잠금장치가 된 공간에 현금저장용 금고에는 제한된 수량만큼의 현금만을 보관하도록 하여 적절한 보호관리가 되도록 한다.

3. 보안디자인의 개념과 원리

1) 환경적으로 안전한 시설물 설계

새로운 시설물을 설계할 때 시설물의 안전성을 위하여 보안디자이너와 보안전문가의 협조가 필수적하며 여기에 지역 경찰과 소방 공무원의 협조도 중요하나 지금까지는 대부분 이러한 다양한 변수들에 대하여 간과되어왔다(최선태, 2008).

시설물 설계에 관한 다양한 전문적인 의견과 관점들의 수렴과정을 통하여 손실의 기회를 줄여서 시설물의 가치와 안전성을 향상시킬 것이다. 더욱이 실제로 시설물이 건축되기 전에 방어계획이 실시되면 차후에 시설물에 추가적인 보안대책을 추가할 필요가 없어질 것이다. 그러나 아직까지 우리나라에서 시설물을 설계할 때 보안대책을 설계에 반영하는 경우는 거의 없었으나, 최근 아산신도시와 수도권에 위치한 신도시 설계에 CPTED개념을 시범적으로 적용하였다. 이와 같이 기존 건물의 대부분이 구조적인 취약성으로 인하여 침입자가 쉽게 침입할 수 있으나 이러한 설계자체의 취약성을 물리적인 자물쇠와 감시카메라와 같은 안전대책으로서는 한계를 가지고 있으며 특히, 오늘날과 같이 공조기가 일반화되기 전까지는 건물의 적정한 환기를 위해서 많은 창문을 필요로 했으므로 이러한 개구부는 침입자에게는 더없이 좋은 기회를 제공하였다.

오늘날 대부분의 시설물도 불법침입 시 여러 가지 문제점을 가지고 있다. 예를 들면 매달려 있는 천장 타일은 천정과 바닥면 사이에 상당한 공간이 존재하므로 침입자가 쉽게 타일을 밀치고 천장사이 공간을 통하여 침입할 수 있으므로 타일 위의 공간은 한 사람이 기어서 같은 층의 다른 공간으로 이동할 수 있게 하는 침입통로가 된다. 또한 이웃하고 있는 건물의 지붕을 통한 침입은 오래된 건물이나 새로운 건물이나 마찬가지로 동일한 취약점이다. 이러한 많은 취약점은 적절한 시설보호대책에 의해 보완이 이루어지고, 지붕으로 통하는 개구부에는 자물쇠나 경보기가 설치되어야한다.

시설보안의 중요성이 대두됨에 따라 지난 40년 동안 미국 건축가들은 시설물의 기획단계에서 범죄예방 설계의 역할의 중요성을 증가하였고 환경적인 안전설계에 주차장이나 통행로의 자연적·전자적인 감시를 포함하여, 자연스럽게 거주자의 시계(視界)를 향상시키는 방법으로써 창문이나 조경, 밝은 조명, 기타 여러 건축적인 설계는 범죄예방 능력을 증진시켰다. 더불어 울창한 수풀과 같은 은신처는 침입자가 몸을 숨길 장소를 없애기 위해서 잘 정리되어야 하고, 바둑판식 도로는 침입자가 쉽게 도주하는 것을 방지하기 위해 통행차단을 위한 방호물을 이용하여 막힌 길의 개념으로 바꾸어야 한다.

1960년대 말부터 1970내 초 사이에 뉴먼교수(Oscar Newman)는 건축적인 설계와 범죄예방의 상관관계에 대한 혁신적인 연구를 시행하였으며 방어적 공간이란 개념을 만들어냈다. 뉴먼은 100개가 넘는 건축물 설계를 연구하였으며 설계적인 요소가 범죄를 방지한다는 것을 규명하였다. 예를 들면 뉴먼은 거주지의 창문을 통한 감시의 기회를 증가시키는 방법을 선호하였으며, 이러한 이웃을 통한 감시가 거주자나 이웃들의 안전에 영향을 준다고 인식하였다. 방어적인 공간의 가장 중요한 요소는 범죄에 대한 공포를 줄이기 위하여 거주자들이 사용하는 공공의 공간배치를 변경하는 설계를 하는 것으로, 이것은 상당한 기대효과를 갖게 하였다. 뉴먼교수는 공공을 위한 건물의 물리적인 설계의 모습이 거주자의 범죄에 의한 희생율과 그들의 안전에 대한 인식에 영향을 준다는 것을 알았다.

이러한 환경적인 설계를 통한 범죄 예방(CPTED)은 거주자에게는 지역의 모습과 설계를 통해 관심을 이끌어내고, 이웃과의 빈번한 접촉을 가져오며, 더 나아가 지역의 환경개선을 이끌어내고 범죄의 통제와 감소를 위한 주민의 참여를 가능케 할 수 있다. 반대로 범죄자에게는 지역의 물리적인 환경개선과 관심을 통해 합법적인 거주

자의 존재에 의한 노출위험의 증가와 사용에 따른 감시수준의 증가, 그리고 범죄감소에 있어서의 지역사회의 관심에 대한 인상을 느끼게 되어 범죄 실행을 억제하게 되는 것으로 공공건축물뿐만 아니라 업무용·산업용·관공서·수송시스템·학교 등 모든 시설물에 적용이 가능하다. 더불어 새로운 시설물을 계획할 때 절대로 보안디자인의 중요한 요소로써 화재나 사고예방에 관한 산업안전에 관한 중요성을 간과하지 말아야 한다.

2) 보안관리와 균형유지

시큐리티는 연속되는 공정관리이므로 다음과 같은 여섯 가지 원칙이 유지되어야 한다.

첫째, 보안은 반드시 리스크와 균형을 유지하여야 한다. 따라서 보안시스템이 디자인되기 전에 전체적인 리스크분석이 시행되어야 한다. 이러한 결과물은 해당 자산에 잠재된 리스크에 대하여 결정하고, 자산에 어떤 위협요소가 있는지, 해당 위협요소가 실재로 구현될 가능성은 얼마나 되고, 발생할 경우에 비즈니스에 어떤 영향력이 있는지를 구체화할 수 있게 된다. 이러한 리스크분석의 결과로 대부분의 조직에서는 그동안 중요하지 않는 자산이 과잉보호되거나 중요한 자산이 잘못된 방법으로 보호되고 있는 것을 발견하게 된다. 따라서 보안전문가에 의한 리스크분석은 보안시스템을 디자인하기 전에 반드시 선행되어야 한다(ARC Training, 2006).

둘째, 가장 강력한 시설장벽은 목표물에 근접하여 설치한다. 우리는 가끔 경계시설의 펜스의 강도를 과신하는 경우가 있다. 일반적으로 외부장벽에 많이 사용되는 유형인 면도칼같이 날카로운 모양으로 된 2.4미터 체인링크펜스는 단지 30초 정도의 침입을 연장시키는 역할밖에 하지 못한다. 더군다나 경계시설은 매우 광범위한 영역을 보호하고 있으므로 비용효과적인 관점에서 분석되어야 한다. 이러한 비용효과적인 방법 중에 하나가 경계시설의 강도를 강화하기보다는 보호구역의 범위를 축소하여 귀중품을 금고에 보관하는 것이 더 향상된 보안대책이 될 것이다.

셋째, 최상의 경보시스템은 가장 먼저 경보를 울린다. 일반적으로 우리가 경보시스템을 설치하는 주요한 이유는 침입자가 목표물에 접근하는 시간을 지연시켜 경보가 울린 다음에 보안요원이 최대한 신속하게 침입자를 제지하거나 무력화하게 하는 시간을 확보하게 만드는 것이다. 그러나 여기에서 중요하게 고려하여야 할 것은 빠른 경보를 위하여 침입감지시스템을 목표물에서 너무 멀리 설치하는 경우에는 설치

범위가 넓어지게 되어 설치비용이 증가하고 침입경보를 받고 출동하는 대응팀이 침입자의 위치를 파악하기가 어렵게 된다. 따라서 침입감지시스템은 외부장벽에 가장 근접하게 위치한 곳에 설치하는 것이 적절하다.

넷째, 비용과 편익은 반드시 균형을 맞추어야 한다. "비용으로써 보안"이라는 용어는 비즈니스 환경에서는 난센스이다. 비즈니스 환경에서의 보안은 공공법집행 조직의 "어떤 희생을 치루더라도" 범죄를 방지해야하는 것과 같은 책임을 가지지는 않는다. 비즈니스에서의 주요한 보안의 관심을 반드시 조직의 자산을 보호하는 것이나, 이러한 자산을 보호하고자 하는 비용이 손실비용을 초과하는 경우에는 이러한 보안대책은 의미가 없으므로, 더 비용이 적게 드는 대안을 찾아야 한다. 이러한 원리는 모든 이윤을 추구하는 기업의 보안대책에 적용된다.

다섯째, 보안대책은 반드시 인간활동의 자유의 개념을 고려한다. 이러한 개념은 어느 나라에서 적용되든, 어떤 법적인 규제가 따르든 간에 기업보안운영을 할 경우에는 인간의 기본적인 권리 혹은 도덕성은 논쟁의 대상이 아니다. 어떤 보안대책이 통상적인 업무활동을 방해하는 경우에는 사람들은 이러한 방해물을 우회하는 방법을 찾게 되는 것은 매우 명확한 사실이다. 특히 특정한 보안지침이나 IT보안절차가 인간의 기본적인 특성들은 고려하지 않고 획일적으로 적용되는 경우에 이러한 상황이 발생한다. 그러나 일단 한번 이러한 상황이 발생하게 되면, 보안부서에서는 이러한 상황을 발견하기 어려우므로 매우 심각한 보안취약성이 노출되게 된다.

여섯째, 모든 보안시스템은 경고의 의미를 내포한다. 대부분의 전문적인 범죄자는 학습에 의하여 눈에 보이는 보안대책의 효과에 대하여 정확한 평가를 한다. 그러므로 보안대책들은 과장되거나 속임수의 수단을 포함하여 운영되는 것이 좋다.

3) 보안시스템의 통합

시큐리티시스템은 다음과 같은 여섯 가지 다양한 요소들의 조합에 의해서 이루어진다.

첫째, 최고의 보안시스템은 물리적, 전자적, 인적 그리고 절차적 대책들이 가장 적절하게 조화가 이루어져야 한다. 이러한 여러 가지 대책들의 조화의 내용은 비용과 편익의 상황에 관한 설명과 밀접한 관련이 있다. 우리는 때때로 어떤 보안대책에 필요한 절차가 타이트하게 적용될 경우에 전자감지장비에 막대한 금액을 투입하는 것이 의미 없다는 것을 알게 된다. 반대로 인건비가 높은 나라의 경우에는 많은 인력

의 순찰요원을 유지하는 것보다는 대응역할을 수행하는 인력을 최적으로 활용하고, 대신에 전자감지장치를 활용하는 것이 효과적이다.

둘째, 보안의 허점은 목표물의 존재가 노출될 경우에 시작된다. 대부분의 경우 보안장비가 존재한다는 것은 인근에 중요한 목표물이 있다는 것을 의미한다. 예를 들어, 현금운송용 차량에는 내부에 다량의 현금이 들어있다는 것을 의미한다. 또한 눈에 잘 띠지 않는 평범한 사람일지라도 주변에 검은 양복과 선글라스를 낀 사람들에 의해 호위되는 상황은 그 사람을 갑자기 중요한 사람으로 인식하게 만든다. 또한 새로운 전산장비를 구매하는 경우에는 장비뿐만 아니라 포장용기가 외부에 방치되어 절대로 사람들이 이러한 장비가 구매되어 내부에 설치된다는 생각을 갖지 않도록 해야 한다.

셋째, 보안대책은 보안취약점이 발생할 경우 즉시 발견이 가능하도록 설계한다. 우리는 가끔 보안시스템의 실패의 상황을 너무 늦게 발견하기도 한다. 이것은 특히 내부인에 의한 부정행위나 산업스파이가 발생하는 경우가 여기에 해당된다. 이러한 두 가지 범죄행위의 경우는 범죄자가 실제로 해당 목표물의 담당자인 경우가 대부분으로 매우 뛰어난 범행기법을 보여주거나, 대부분이 내부자이므로 상당기간동안 발견되지 않은 상태로 방치되어 결국에는 해당 조직이 파국적인 상황에 이르기도 한다.

넷째, 보호대상물은 반드시 자체적으로 보호되어야 한다. 보안대책들은 본질적으로 이러한 대책을 무력화시키려는 사람에게는 잠재적인 목표물이 된다. 보안업무를 수행하고 있는 보안요원은 구성원이나 대중의 공격에 노출되기 쉬운 위치에 있거나 CCTV장비는 반달리즘의 목표가 되기 쉽고 경보시스템은 침입자에 의해 무력화된다. 따라서 보안시스템을 디자인할 경우에는 보안대책 자체가 일정정도의 내구력을 보유하는 것은 필수적이다.

다섯째, 필요성의 원리를 적용한다. 일반적으로 대부분의 경계구역은 모든 사람들이 별다른 제한 없이 대부분의 장소에 접근이 가능하다. 이러한 잘못된 보안관행들은 모든 구성원이 건강에 위협이 되는 장소나 위험물질이 있는 장소에 접근하는 것을 제지하지 않는 경우와 마찬가지이다. 따라서 이러한 경우에는 명확한 절차를 적용하여 지정된 특정구역에는 구성원이 접근하지 못하게 하고 특정한 장소는 허가를 득한 요원만이 출입이 가능하도록 하고 출입 시에도 출입기록을 유지하며, 가능하다면 내부출입통제시스템이나 관리자가 직접 관리하도록 한다.

여섯째, 보안은 모든 실행 가능한 대책들의 총량이다. 보안대책들은 서로 따로 떨

어져서 작동하지 않으므로 구역의 모든 시스템이 완전하게 서로 결합하여 작동하도록 구성한다. 이러한 시스템은 여러 가지 보호대책들이 서로 겹쳐지게 디자인하여야 한다. 그러나 좋은 경보시스템의 효율성도 경보가 발생하는 경우의 대응역량 뿐만 아니라 대응 팀의 대응절차에 의해서 급격하게 무력화될 수 있다.

Ⅲ. 보안시스템 설치환경과 고려요소

새로운 보안시스템의 디자인을 할 경우에는 언제나 해당 보안시스템이 적용되는 다양한 환경요인에 대하여 주의를 기울려야 한다. 따라서 어떤 조직이든 보안대책을 선정하는 경우에 고려될 물리적, 경제적, 기술적, 사회적, 정치적, 법적, 운영적인 환경, 핵심자산에 대한 심층적인 보호대책의 필요성들이 사전에 검토할 기본적인 요소들이다.

개별 유형의 보안시스템은 전체적인 시스템디자인에서 구체적인 기능을 수행하도록 구성된다. 디자이너가 최종적인 결과로써 고려하여야 할 실패요인으로는 반응이 없는 시스템, 비효과적인 시스템, 수용하기 어려운 오경비율과 귀찮은 경보의 발생 등이 있다. 이러한 기초적인 디자인에서 개별적으로 고려하여야 할 요인은 다음과 같은 보안환경을 전체적으로 검토한 다음 세부적인 디자인에 반영하여야 할 것이다.

1. 물리적 환경과 고려요소

우선 보안관리자는 최신의 전자보안시스템의 여러 가지 사양 중에서 최적의 제품을 선정할 수 있도록 디자이너에게 다양한 상품을 제시함으로써 소유자나 사용자가 수용할 수 있는 최상의 결과를 얻을 수 있도록 한다. 특히 센서와 CCTV는 개별 제품의 기술력이 업무수행의 저하나 과도한 귀찮은 경보를 발생하는 원인이 되므로 구체적인 환경적인 변수와 적용에 따른 요구조건을 신중하게 고려한 다음 선정한다. 더불어, 실제적인 시스템의 운영비용은 낮은 감지율과 평가에 대한 수용정도에 관련되어 있으므로 이러한 잘못된 적용으로 인한 수리비용과 구형장비의 한계와 같은 숨겨진 추가비용은 시스템에 대한 소유주의 신뢰를 잃게 하는 원인이 된다. 한편 보안시스템 디자이너는 전자장비의 운영에 악영향을 미치는 다양한 물리적인 환경변수에 관한

문서자료를 수집하여 실제적인 고려사항에 대한 주의 깊은 분석을 선행하여야 한다.

이때 필수적으로 확인하여야 할 외부적인 물리적 보안환경에는 바람과 온도, 안개와 주변의 무성한 나뭇잎, 염분, 강우와 고여 있는 수량, 펜스 구조물의 상태, 지하 유틸리티의 위치 등 구체적으로 운영에 제한요소로써 센서와 기술의 적용에 영향을 주는 환경적인 영향요소를 모두 고려한다. 또한 내부에서는 내부센서의 설치위치와 선정에는 반드시 난방, 통기, 공기 조절장치의 위치, 열원, 임시조명, 진동, 움직이는 기계, 먼지, 습기와 습도에 대하여 고려한다. 더불어 CCTV의 위치와 정렬은 반드시 햇빛의 눈부심과 보안조명의 충분한 배분, 온도, 바람, 모니터링 위치에 대하여 고려한다.

보안디자인을 하는 경우에 가장 핵심적인 고려요소는 전체적인 시스템을 운영함에 있어서 앞에서 언급한 다양한 환경적인 요인으로 인하여 발생할 수 있는 모든 잠재적인 악영향에 대하여 구체적으로 규명하기 위하여 시스템디자인 단계에서의 분석이 디자인 초기과정의 필수요소이다. 그런 다음 중요한 디자인 단계는 가장 적절한 기술수준의 제품의 선정과 환경적인 요인을 개량하기 위한 조치를 통하여 이러한 디자인을 수행하는데 제안요인을 반영하는 과정이다.

물리적인 환경에서 디자이너가 고려하여야 할 또 다른 요소는 환경적인 디자인을 통한 보안통제의 개념이다. 이 개념은 범죄행위에 이용되는 물리적인 환경요소를 제거하기 위한 시설물과 사업장 디자인개념을 활용하고 물리적인 환경에 의하여 보호조치를 향상시키기 위한 검토를 포함한다. 환경적인 디자인 전략은 보행로의 위치를 활용한 자연스러운 출입통제, 불안전한 구역을 제거함으로써 자연스러운 감시상황의 향상, 개선된 보안조명시설의 활용을 포함하게 된다. 환경적인 디자인 개념에는 개별적인 영역성, 효과적인 공간의 활용, 자연환경의 효과적인 조정을 통하여 잠재적인 위협요인을 방지하기 위함이다.

2. 경제적인 환경과 고려요소

모든 보안활동은 보안에 투자된 비용으로 최대한의 안전을 확보하는 것을 목표로 한다. 따라서 조직의 경제적인 상황에는 사업장과 국가적인 환경에서의 금융목표와 기업전체의 경제적인 현상 모두를 포함한다. 예를 들어, 한국의 어떤 통신기업의 지방 사업장에서 일 년에 2~3회의 원인을 알 수 없는 기지국 통신기기의 파손사고가 발생한 경우에, 이에 대한 대책으로써 서울본사의 보안관리자는 해당 사업장에 현재

의 벽돌형 담장을 보강하기 위해서 체인링크펜스를 추가적으로 설치하고자 경영진에게 보안예산을 신청하였다.

이에 따라 현재 해당 사업장의 부지 50M×50M의 보안을 강화하기 위한 경계구역 침입감지시스템과 CCTV와 더불어 가시철선을 상단에 부착한 체인링크펜스의 외곽 경계시설물의 설치가격이 5천만 원을 초과할 것이라고 예상된 경우, 해당 사업장의 연간 매출액이 200억 원이고 순이익이 5%인 경우에 해당 사업장의 경제적인 관점에서 체인링크펜스를 설치하는 것이 적절한가에 대한 판단은 보안시스템의 효과와 투입비용을 경제적인 요소를 포함한 다양한 관점에서 평가하여야 한다.

3. 운영적인 환경과 고려요소

보안시스템디자이너로서 보안시스템의 운영면에서 건축과 공학적인 측면에서의 제한요소는 크게 물리적인 요인과 소유주의 요구 두 가지가 있다. 앞에서 언급한 예와 같이 사업장의 경계구역은 반드시 현장에서의 독특한 제한요소, 재산의 가용성과 용도에 적합하도록 하여야 한다. 소유자의 요구에는 핵심적인 업무의 운영의 구획화, 장소와 출입통제를 위한 출입구의 디자인, 장애인 출입구의 위치 등이 포함된다. 사업장의 소유자들은 자신들의 안전과 효율성을 포함한 자신만의 독특한 업무운영을 유지하기 위하여 다양한 업무수행의 기준을 적용하기 위한 보안시스템을 요구한다.

이러한 개별적인 독특한 요구조건에 의하여 구체적인 보안시스템의 해결책들이 선정되거나 거부된다. 대체적으로 특정한 기술제품에 대한 거부는 보안시스템의 운영환경이나 통상적인 조직의 운영환경을 방해할 잠재성에 대한 우려의 결과로 효과적으로 보안시스템을 운영하기 어려운 경우이다. 이러한 상황에 대한 구체적인 예는 주출입구의 출입통제장비의 거부나 제조환경에서 CCTV 평가의 거부를 포함한다.

4. 사회적인 환경과 고려요소

오늘날 세계화의 진전에 따라 과거의 자급자족경제에 의존하던 자급형 경제시스템은 점차적으로 다국적기업을 앞세운 대량생산과 발달된 유통시스템에 제압되어 오히려 더욱 심한 빈부격차를 만들어 내고 있다, 이러한 빈부격차의 심화는 사회보장제도가 미숙한 저개발국의 경제시스템을 위태롭게 하고 사회불안의 원인이 되고

있다. 범죄의 주요한 원동력은 가난과 빈곤이라는 여러 가지 실증적인 연구가 존재한다. 이와 더불어 가진 자에 대한 못 가진 자들의 상대적인 박탈감과 경쟁에서 탈락한 집단의 열등감과 증오심은 사회안전망과 기업 비즈니스 활동에 가장 큰 리스크로 자리하고 있다.

또한 정부조직에서도 가난과 부패의 수준에 대한 범죄와의 상관관계는 매우 높게 나타나고 있다. 이에 관한 자세한 자료는 국제투명성기구 홈페이지[2]에 공개된다. 그러나 인간은 너무 다양하게 존재하기 때문에 단순하게 정직한 부류와 부정직한 부류로 이분화 하는 것은 도움이 되지 않으며, 범죄의 원인으로서 인간은 도덕심과 매우 다양한 상황과 상황요소에 의해서 통제된다.

Ⅳ. 보안디자인과 시스템통합 프로세스

1. 보안디자인 프로세스

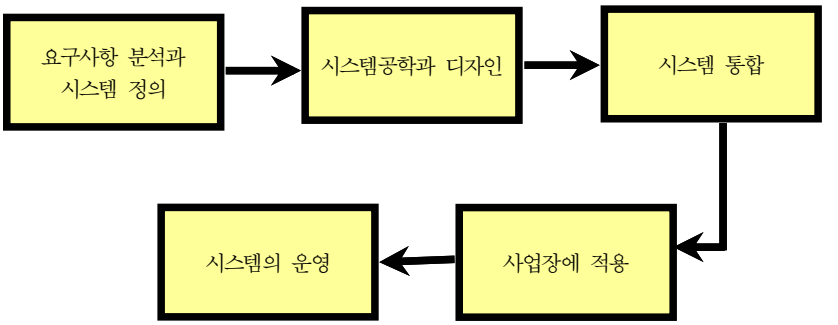
보안디자인과 시스템통합효과의 핵심은 보호목표에 대한 위협요인의 본질을 파악하는 것으로 손실의 파급효과는 대안이 없는 소규모기업의 경우에 중급수준의 위협요인으로도 핵심 비즈니스 자산이 위태롭게 되는 경우 기업이 파국이 이르기도 한다.

현대사회에서의 보안관리자는 역동적인 위협요인과 잠재적인 파국적 손실에 대응하기 위한 최대의 방어수단으로 신중하면서도 효과적인 건축시공, 기술적, 물리적 그리고 운영적인 요소들을 능동적이고 신속한 시스템으로 통합함으로써 핵심자산보호에 대한 안정성을 증대시키는 역할을 수행하여야 한다. 효과적인 디자인과 통합프로세스는 보안관리자가 효과적으로 위협요인에 대응하고 실제적으로 리스크나 손실로 인한 파급효과를 줄이는 핵심적인 역할을 한다. 이러한 효과적인 디자인 해결책에 도달하기 위하여 보안관리자가 자신의 보안문제점을 전반적으로 파악할 수 있도록 프로세스는 통합적、포괄적이어야 한다.

디자인의 핵심요소는 계획에 부합하도록 시스템의 구성요소와 세부사항을 순서대로 배열하는 것을 구체적으로 구현해내는 것이며, 보안 혹은 다른 기능이든 상관없이 모든 사례에서 시스템은 구체적인 목적을 위하여 디자인된다. 보안디자인의 경

2) http://www.transparency.org/.

우에 계획은 규명된 위협요소를 토대로 하여 이에 대한 취약성을 통제하거나 축소하기 위하여 통일된 시스템에 다양한 물리적인 요소, 인적요인과 절차를 통합하거나 선정하는 것을 의미한다.



〈그림 2〉 보안디자인 프로세스

대체적으로 공학적인 디자인에는 연구와 보고, 기초적인 디자인, 최종 디자인, 제안과 협상, 시공 그리고 운영의 여섯 단계의 프로젝트 과정이 포함된다. 이러한 공학적인 단계에서 보안관리자는 건축가 그리고 엔지니어와 긴밀한 관계를 유지하면서 공학적인 디자인의 기능뿐만 아니라 유·무형의 요소의 통합의 결과 위협에 대응하기 위한 보호시스템의 디자인을 포함한 프로세스의 목적을 성취하기 위한 조정의 필요성이 요구된다.

대부분의 공정에서 통합의 핵심은 따로 분리되어 운영되는 개별적인 부분을 한 군데로 모아서 하나의 완전한 운영체로 만드는 것이다. 따라서 보안관리자에게 시스템통합은 사후 대응보다는 사전 대응의 자산보호 방법을 만들어내는 것으로 보안장비, 시설과 인력, 그리고 절차를 유기적으로 융합하는 기법이다. 통합공정의 최종적인 결과는 전체적으로 통합된 보안시스템은 위기상황에서 역동적인 위협요소와 리스크에 효과적으로 대응함과 동시에 통상적인 상황에서 알아차릴 수 없을 만큼의 미세한 기능을 계속적으로 수행하여야 한다. 위협요소와 리스크에 대응하기 위한 다양한 보안과 관련된 요소의 결과가 디자인인 반면에, 통합은 효과적인 자산보호를 위한 매일의 전략과 실제적인 업무의 촉매제역할을 수행한다.

보안시스템의 디자인과 통합은 해당 공정을 통하여 추구하는 목표에 대한 분석과

구체적인 개념의 정의를 토대로 시작되고, 시설물과 사업장의 보호계획은 항상 개별적인 자산에 대해 가장 적합한 대응책에 대한 규명과 핵심자산에 대하여 필요한 보호대책이 무엇인가를 토대로 한다. 따라서 디자이너와 보안관리자는 보안시스템의 구성요소인 물리적인 장벽, 전자적인 하드웨어, 보안요원과 절차가 상호작용할 수 있도록 통합된 하부시스템의 보호계획을 설정하기 위하여 디자인 계획을 구성하는 것이 필요하다.

보안디자인을 구성하는 시스템의 개념은 개별적인 자산, 시설과 공통으로 경계구역을 공유하고 있는 시설물의 집합을 효과적으로 다루기 위하여 통합된 수집물을 통하여 형성된다. 조직에서 보안조직에 주어지는 다양한 임무를 수행하기 위한 보호대책과 자원들의 통합에는 고정된 환경상태를 포함하지 않는다. 왜냐하면 위협요소는 일반적으로 보호대책이 필요한 개별 자산이나 시설물에 대하여 역동적으로 작용하며, 전체적으로 통합된 시스템 개념에는 반드시 다양한 시나리오를 예상하고, 시스템의 용장성은 치명성을 토대로 하며, 최상의 달성 가능한 보호디자인을 통한 해결책을 성취하기 위해서 가능한 모든 자원의 집중관리를 필요로 하기 때문이다.

이러한 과정을 거쳐 최종적으로 승인된 개념을 토대로 공학적인 시스템과 디자인 단계는 예비단계에서 최종 디자인까지 단계별 디자인 단계를 거쳐 통합적으로 최종 시스템에 제공하며, 최종결과는 완전한 시스템에 대한 해결책을 제시하게 된다. 이러한 통합기능은 단순히 최종 디자인단계에서 디자인 검토과정으로 이어지므로 사전에 언급된 요구조건에 근거하여 통합솔루션은 보안관리자에 의해서 공식적으로 검토되어야 한다.

통합단계는 보안관리자에 의해서 사전에 요청한 모든 요구사항이 통합 디자인 솔루션에 반영되었는가를 확인하는 과정으로 가장 중요한 단계이다. 또한 하드웨어가 구매되고 난 다음 시공이 시작되기 전에 더욱 중요한 것은 디자인 솔루션의 인증이다. 따라서 한번 인증이 되고나면 해당 시스템은 사용자에 의해서 최종적인 운영과 시행의 최종 단계의 준비가 되었다는 의미이다. 그러므로 시스템의 효율성에 대한 재검토는 위협요소의 역동성과 변화된 임무에 근거하여 시행하고 계속적으로 최초의 요구사항 단계에 반영하도록 한다.

이러한 보호대책에는 반드시 통합적인 관점에서 해당 사업장의 개별적인 특성과 전체적인 시설물과 자산보호대책의 분포를 고려한다. 예를 들어, 선정된 건축물의 보호 장벽이 침입자를 지연시킬 수 있는 성능은 이와 관련된 감지기와 출입통제의

하부시스템의 구성요소에 대한 디자이너의 선택에 의해 조정된다. 이러한 경우에는 위협요소 시나리오에 가장 적합한 감지기를 선택하고 지연 시간동안에 충분히 대응팀이 출동하는 것과 연관된 보호 장벽의 지연성능에 대하여 측정하여야 한다. 따라서 대응팀의 가용성과 운영능력은 대응팀의 최상의 선발과 구성 그리고 다양한 보호대책의 배치가 핵심적인 요소이다.

예로서, 디자이너는 감지 가능성을 최대화하기 위하여 최신의 기술을 활용하여 극초단파와 적외선 감지기와 같은 구체적인 기술의 조합에 중점을 둔다. 이러한 방식에 따라 보안디자이너는 완전한 통합 시설보안시스템을 구축하기 위한 여러 가지 보호대책을 선정하고 서로 조화롭게 보호대책을 조합하기 위하여 사업장에 가장 적합한 방식을 선택할 수 있다.

개별적인 보호대책을 평가할 경우에 대응책들은 핵심적인 자산을 완전하게 보호하는 방법은 거의 없으나, 자산보호를 위한 통합적인 접근법을 활용하여 보호대책들의 서로 다른 장점들이 조합하게 되면, 시설물과 해당 사업장에 적합한 구체적인 대책들의 조합을 신중하게 선정할 수 있을 것이다. 디자이너의 개별적인 결정과 성능, 신뢰도, 유지가능성, 비용, 취약성의 축소 가능성을 종합적으로 검토하여 최상의 보호대책을 선정한다.

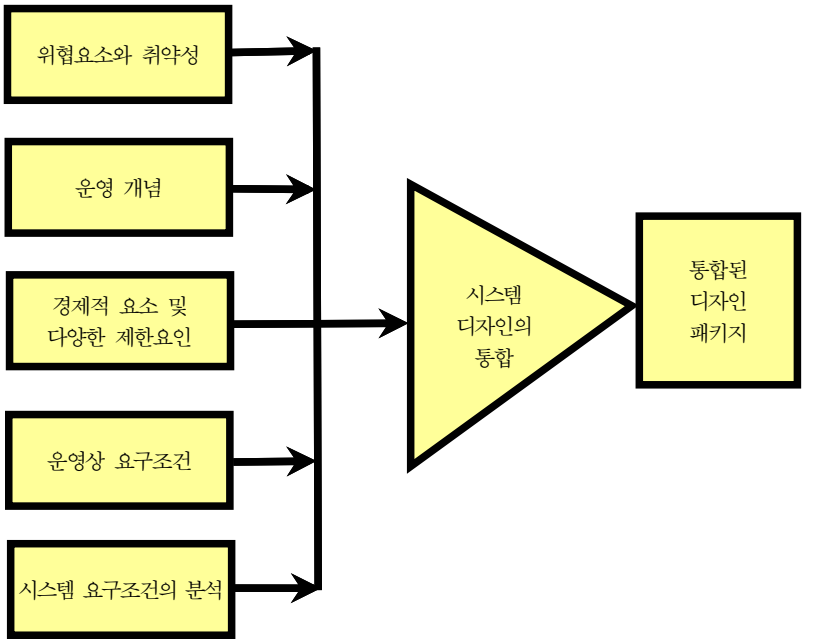
모든 시스템디자이너의 기본적인 기능은 다양한 구성요소와 하부시스템의 선정과 통합을 통하여 완전한 시스템 디자인을 구성하는 것이다. 따라서 모든 경우에 사업장마다 개별적으로 독특하게 인식된 위협요소에 따른 자산보호대책의 조합의 선정과 균형, 그리고 의도된 결과를 달성하는 것이 디자인통합의 핵심이다.

2. 시스템통합 프로세스

최근 인건비 상승과 빌딩자동화에 따라 대부분의 자동제어시스템의 통합화가 가속화되고 있고, 건물의 방제실에 소방설비, 가스제어, 보안시스템이 동일한 공간에 배치되는 것이 일반화되었다. 시스템 통합은 사업장이나 시설물 각각의 분야에 산재된 보안업무와 관련된 모든 보안기능을 하나의 시스템으로 인식하고 보안관리자가 종합적으로 운영·통제하는 것을 말한다(Walsh, 1994). 일반적으로 빌딩의 라이프 사이클을 건축 후 약 5~6십년이라 할 때, 라이프 사이클 비용을 분석해 보면 건축에 드는 비용과 운영비용으로 구분됨을 알 수 있으며, 이러한 비용의 비율은 통계적으

로 건축에 드는 비용이 약 17%, 운영비용이 약 83% 정도로 나타난다(에스원, 1997에서 재인용).

시스템디자인과 통합은 보안관리자와 보안설계자에 의해 이루어지며 완성된 공정으로 제시된다. 비록 통합기능이 공정의 모든 단계에 공통으로 적용되기도 하나 디자인과 실제적인 운용사이의 주요한 단계가 시스템통합 과정이다. 이전 단계인 공학적인 시스템디자인 단계를 마친 다음에 보안관리자와 디자이너는 디자인된 시스템에 대하여 주의 깊게 검토한 다음 핵심적인 통합공정에 대한 결과물로 선택된 보호대책과 구성요소가 전체적인 시스템의 효율성을 다함께 달성하기 위해서 운영상의 최적상황을 달성하는데 필요한 요소가 무엇인가를 도출한다.



〈그림 3〉 시스템통합 프로세스

시스템통합 구축공정은 많은 비용이 들어가는 실제적인 시공과 운영 단계 이전에 정당하게 인정된 요구조건과 제한요소에 따라 검토의 중요성을 부각하며 공학적인 디자인의 균형감을 강조하기 위한 중요한 하나의 단계로써 취급되어야 한다. 실제로

통합단계에서는 디자인공정의 중요한 단계로 공식적으로 세부적인 최종 디자인을 검토하고 평가한다.

그러나 실무에서는 아직도 시스템통합 단계를 주요한 디자인 단계로써 인식하지 못하는 경우가 있는데, 시스템통합은 최종디자인과 시행 사이에 보안관리자가 사전에 확립된 요구조건에 의거하여 시스템디자인을 검증하는 매우 중요한 공정이다. 이러한 관점에서 보안관리자는 사전에 결정된 위협요소와 취약성, 보안운영에 관한 보안관리자의 개념, 경제적 요인 등 여러 가지 제한 사유, 조직운영, 전체적인 시스템에 대한 요구조건을 근거로 하여 완성된 최종적인 시스템디자인 솔루션의 적합성을 고려한다.

시스템통합 구축단계에서는 자산보호를 위한 통합공정을 만들어 내기 위한 인적 요인과 절차적 요인과 더불어 다양한 하부시스템의 요소인 물리적인 장벽, 감지기, 데이터 전송기기, 통제기, CCTV 등을 통합하기 위하여 이전의 디자인공정의 주요한 목적을 확정한다. 이러한 통합과정에서 이와 관련된 구성요소와 더불어 개별적인 하부시스템은 취약성의 감소와 전체적인 시스템의 보호효과에 대한 기여정도에 대하여 보안관리자와 디자이너에 의해서 평가되어야 한다. 이러한 개별적인 측정치는 비용과 편익의 관점에서 가역관계(trade-off)를 야기한다. 이와 같은 하부시스템의 통합은 개별적인 자산보호결정에 적절한 선택의 최고점(optimal point)을 의미하는 것으로 최종적인 디자인에 반영된다. 공학적인 디자인단계의 최종적인 결과는 다양한 하부시스템과 이와 관련된 고도의 신뢰도와 확신을 가진 집합체로서 다양한 부정적인 환경에 대응하는 요소들로 구성된 완전하게 통합된 보안시스템으로 구현된다.

V. 결 론

시설보안은 자산보호의 가장 기본적인 형태이다. 모든 시설물은 물리적인 통제를 통하여 경계구역, 사업장, 시설물, 건물을 보호하고 조직에 속하는 모든 유·무형 자산을 보호하는 임무를 수행한다. 따라서 보안디자인 원리를 활용하여 체계적으로 잘 구현된 시설보안시스템을 통하여 목표로 하는 자산의 대부분을 효과적으로 보호할 수 있다.

기본적으로 시설보안은 허가되지 않는 출입의 통제, 위험요소, 자산의 손괴를 방

지하기 위한 심층적인 시설보안대책을 활용하는 공정을 적용하므로, 필수적으로 손실이나 위험요소로부터 자산, 공장, 시설물, 건물, 사무실과 모든 조직자산을 보호하는 중요한 기능을 수행한다. 또한 시설보안은 인명과 정보호호대책에 대한 토대가 된다. 구성원과 정보시스템에 대한 보안은 고도로 치밀하게 디자인된 시설보안대책을 토대로 시작되며, 모든 자산보호의 핵심이 되므로 조직의 자산보호대책에 대한 전체적인 평가를 바탕으로 한 체계적인 시설보안디자인은 시설보안의 기초뿐만이 아니라 조직전체의 보호대책의 근간을 구성하므로 첨단화된 물리적, 기술적인 보호대책이 서로 긴밀하게 연계되어 디자인되고 운영되어야 초기에 의도한 목적을 달성할 수 있을 것이다.

보안에 대한 비용과 관련하여 시설보안시스템에 대한 구축은 전체적인 보안시스템 구축비용의 50% 이상의 많은 투자를 필요로 하므로 어떤 조직에서건 중요한 투자결정사항이다. 그러나 지금까지 우리는 관행적으로 구조물을 설치한 다음 필요에 따라 보안시스템을 추가적으로 부가시키는 방법으로 시설보안시스템을 구축하였다. 이런 결과 실제적인 보호효과에 대한 분석이나 구조물을 특징을 반영하거나 보안시스템의 효과를 극대화하기 위한 어떠한 사전적인 계획이나 시나리오도 없이 시설보안시스템을 구축하고 운영하는 것이 보편적인 방법이었다. 그러나 필요에 따른 사후적인 보안시스템의 구축에는 추가적인 비용이 요구되고 실제적인 효과는 반감되며 시설물의 외관이나 특징을 훼손하는 경우가 많이 발생하였다. 따라서 이러한 낭비적인 요소를 제거하고 보호효과를 극대화하기 위해서는 보안디자인에 대한 고려는 모든 시설물의 시공초기에 고려하여야 할 필수적인 공정이다.

그러나 시설보안시스템 뿐만 아니라 모든 보안시스템을 구축하는데 어려움은 보안시스템의 방어정도와 강도는 가장 취약한 부분의 강도로 결정된다는 점이다. 아무리 잘 디자인되고 시공된 경계펜스라도 펜스 근처에 나중에 새로운 건물이 설치된다면 경계펜스의 효율성은 반감되게 된다. 이와 유사하게 첨단 전자보안장비라 할지라도 이를 운영하는 보안요원의 전문성과 자세에 따라 첨단장비는 무용지물이 되기도 한다. 따라서 보안디자인에 참여하는 전문가들은 이러한 부가적인 문제에 대한 고려도 공정에 중요하게 포함하여 반영하여야 한다. 더불어 보안은 보안장비와 절차에 투입된 비용과 불편함의 합이므로 적은 비용과 적은 불편함이 좋은 보안디자인의 근간이 되어야 한다. 모든 건축물의 시공초기부터 잘 디자인되고 효과적으로 운영되는 보안활동은 적은 비용으로 많은 효과를 창출하게 된다.

잘 디자인된 보안시스템의 효과적인 통합공정에는 보안 하드웨어와 소프트웨어의 선택과 적용뿐만 아니라 현재 운영 중인 절차, 건축물의 대책, 보안재원 모두를 포함한다. 또한 여기에는 시스템디자인과 통합공정에 대한 전체적인 이해와 더불어 프로젝트팀 개별 구성원의 책임과 역할을 요구한다. 무엇보다도 운영단계에서의 충실한 업무수행이 효과적인 시스템디자인과 운영을 위하여 핵심적인 사항이다.

그러나 무엇보다도 중요한 것은 보안관리자는 보호가 필요한 자산을 전문적인 보안조사를 통하여 선정한 다음 리스크분석 프로세스에서 핵심적으로 고려할 사항은 반드시 잠재적인 위협요소와 특징, 위협요소에 대한 핵심자산의 유인성, 잠재적인 공격 형태와 공격의 치명성에 관하여 체계적으로 고려한 다음 리스크분석 전문가와 디자이너가 다 같이 디자인 프로세스를 참여하여야 한다. 마지막으로 프로젝트팀의 도움을 바탕으로 가장 효과적이며, 유연성 있고, 경제적인 보안시스템에 대한 적용과 이해는 환경적요인, 인적요인, 절차, 기술을 적절히 조합하여 통합된 보안시스템을 디자인하는 것이다.

결론적으로 어떠한 보안시스템이나 대책도 완벽하지는 않으며, 완벽한 보안시스템은 실용적이지 못하며, 현실적으로도 부적절하다. 대부분의 보호장벽과 같은 시설보호대책의 목적은 완벽하게 자산을 보호하는 것이 아니라 침입자의 침입시간을 지연시켜 경보가 울린 다음 대응팀이 침입자를 찾아내거나 대응하는데 필요한 시간을 확보하는데 목적이 있으므로, 리스크평가분석법을 활용한 목표물의 보호가치와 투자비용과의 균형이 요구된다. 따라서 어떤 의미에서는 구축된 보안시스템의 성능보다는 잠들지 않는 보안실무자의 태도가 실제적인 시설보안시스템의 성능을 결정짓게 될 것이다.

참고문헌

1. 국내문헌

김철영 (2009). **카지노 보안 시스템 운용방안 : 외국인전용 카지노를 중심으로**, 석사학위논문, 경기대학교 대학원.

변용남 (2009). **항만보안위협의 효율적 대응을 위한 보안관리시스템 개선에 관한 연구**, 석사학위논문, 한국해양대학교 해사산업대학원.

에스원 (1997). **Security Management, 통합 시큐리티 디자인 방법과 사례**, 서울: 정출판사.

이창무 (2010). 우리나라 보안산업의 역사적 기원에 관한 연구. **한국경호경비학회지**, 23, 91-111.

이창무 (2009). 형사사법 민영화에 관한 정치이념적 고찰, **한국공안행정학회보**, 18(4), 291-318.

이호중 (2010). **시설경비 운영시스템의 개선방안에 관한 연구 : 기계경비시스템이 설치된 상업용 임대빌딩을 중심으로**, 석사학위논문, 극동대학교 경영행정대학원.

인포더 (2010). **시큐리티월드**, 156, 2010년 2월호.

최선태 (2009). **21세기 산업보안론**, 서울: 진영사.

최선태 (2008). **기업보안핸드북**, 서울: 진영사.

2. 국외문헌

ARC Training. (2007), *security management stage I (core skills)*, Principles of Security Design, 22-27

Bruce Schneier. (2003), *Beyond Fear-Thinking Sensibly About Security in an Uncertain World*-, Copernicus Books.

Carl A. Roper. (1999). *Risk management for security professionals*, Boston: BH.

Charles A. Sennewald. (2003). *Effective Security Management*, Boston: BH.

George D. Haddow & Jane A. Bullock. (2005). *Introduction to Emergency Management*, 2nd ed, Boston: BH.

James F. Broder. (2006). CPP, *Risk Analysis and The Security Survey*, 3rd ed, Boston: BH.

John J. Fay. (1993). *Encyclopedia of Security Management -Techniques & Technology*, Boston: BH.

John Nolan. (1999). *Confidential, Business secrets, Getting theirs -keeping yours*, 2nd ed, Yardley-Chambers.

Mary Lynn Garcia. (2006). *Vulnerability Assessment of Physical Protection Systems*, Elsevier: BH.

Philip P. Purpura. (1998). *Security and Loss Prevention*, Boston: BH.

Robert J. Fisher & Gion Green. (1998). *Introduction to Security*, sixth ed, Boston: BH.

Russell L. Bintliff. (1992). *The Complete Manual of Corporate and Industrial Security*, Prentice-Hall.

Steven Fink. (2002). *Sticky Fingers, Managing The Global Risk of Economic Espionage*, Dearborn.

Dennis DeConcini. (1994). "The Role of U. S. Intelligence in Promoting Economic Interests," *Journal of International Affairs*. vol. 48, no.1.

Thomas E. Cavanagh & Meredith Whiting. (2003). Corporate Security Management: Organization and Spending Since 9、11.

Timothy J. Walsh. (1994). *Protection of Assets*, Volume Ⅲ, The Merritt Company.

3. 인터넷자료

www.freedoniagroup.com, World Security Equipment to 2014. 검색일 2011. 4. 20.

http://likms.assembly.go.kr/law/jsp/main.jsp, 국회법률지식정보시스템. 키워드/ 주택건설기준 등에 관한 규정. 검색일 2011. 3. 20.

http://100.naver.com/100.nhn?docid=52671, 네이버 백과사전. 일반검색/키워드:디자인. 검색일 2011. 4. 20.

【Abstract】

A Study on the construction of physical security system by using security design

Choi, Sun-Tae

Physical security has always been an extremely important facet within the security arena. A comprehensive security plan consists of three components of physical security, personal security and information security.

These elements are interrelated and may exist in varying degrees defending on the type of enterprise or facility being protected. The physical security com-ponent of a comprehensive security program is usually composed of policies and procedures, personal, barriers, equipment and records.

Human beings kept restless struggle to preserve their and tribal lives. However, humans in prehistoric ages did not learn how to build strong house and how to fortify their residence, so they relied on their protection to the nature and use caves as protection and refuge in cold days. Through the history of man, human has been establishing various protection methods to protect himself and his tribe's life and assets. Physical security methods are set in the base of these security methods.

Those caves that primitive men resided was rounded with rock wall except entrance, so safety was guaranteed especially by protection for tribes in all directions. The Great Wall of China that is considered as the longest building in the history was built over one hundred years from about B.C. 400 to prevent the invasion of northern tribes, but this wall enhanced its protection function to small invasions only, and Mongolian army captured the most part of China across this wall by about 1200 A.D.

European lords in the Middle Ages built a moat by digging around of castle or reinforced around of the castle by making bascule bridge, and provided these protections to the resident and received agricultural products cultivated. Edwin

Holmes of USA in 20 centuries started to provide innovative electric alarm service to the development of the security industry in USA. This is the first of today's electrical security system, and with developments, the security system that combined various electrical security system to the relevant facilities takes charging most parts of today's security market.

Like above, humankind established various protection methods to keep life in the beginning and its development continues. Today, modern people installed CCTV to the most facilities all over the country to cope with various social pathological phenomenon and to protect life and assets, so daily life of people are protected and observed.

Most of these physical security systems are installed to guarantee our safety but we pay all expenses for these also. Therefore, establishing effective physical security system is very important and urgent problem. On this study, it is suggested methods of establishing effective physical security system by using system integration on the principle of security design about effective security system's effective establishing method of physical security system that is increasing rapidly by needs of modern society.

Key words : Security Design, Physical Security System, System Integration, Risk Evaluation, System Design