복합적 보안위협에 따른 기계경비 개선방안 연구

공병석* · 황현석* · 김귀남**

요 약

현대사회는 IT기술의 급속한 발전으로 시·공간적 한계를 벗어나면서 사회적·경제적으로 변화를 가져오게 되었고, 단순히 정보 전달의 기능뿐만 아니라 정보를 가공하여 새로운 지식으로 창조할 수 있게 되었다. 이러한 새로운 지식의 창출은 기업 및 국가 경쟁력의 근간이 되었고, 국가 및 기업 간 경쟁이 심해지면서 신기술 개발에 대한 투자에 비해 기술을 보호하려는 인식부족으로 기술유출 사고가 끊임없이 일어나고 있다. 이러한 기술유출 사고는 국가 및 기업의 경쟁력을 저해시키는 가장 큰 원인으로 이에 대한 보안대책이 시급한 실정이다. 따라서 본 논문은 이러한 통합보안 환경에서 물리보안 영역의 제도 및 시스템 취약성을 분석한 다음 이에 대한 문제점을 도출하고, 그에 대한 개선방안을 제안하고자 한다.

A Study on a Plan for Improving an Unmanned Security System According to Security Threat

Byung Seok Kong* · Hyun Seok Hwang* · Kuinam J. Kim**

ABSTRACT

In modern society, a social·economic change is brought about, because time·space limitation regarded to be restrictive in times past was overcome owing to its rapid development on the basis of IT technology. The creation of new knowledge became the basis of competitiveness of nations and companies. As competition intensifies among nations and countries in relation to the development of core technology, companies make investment with placing much weight on the development of new technology, but on the other hand, technology leakage incident continuously occurs due to a lack of understanding to protect technology. This is the largest cause of impeding the competitiveness of nations and companies. And now, it is urgent to take security measures against this.

Therefore, this paper analyzes institution and system weakness in the physical security area in the integrated security environment, and then identifies all problems about this, and proposes a plan for solving these.

Key words : Machine Security, Security Layer, Security Management, Proxy, DDoS

접수일(2014년 2월 4일), 수정일(1차: 2014년 2월 16일), 게재확정일(2014년 2월 17일)

* 경기대학교 산업보안학과
** 경기대학교 융합보안학과(교신저자)

1. 서 론

현대사회는 IT 기술의 바탕 아래 급속하게 발전하여 과거 시·공간적 한계를 벗어나면서, 우리 생활 전반은 물론 여러 산업분야에서 업무영역 확대 및 새로운 인프라를 구축하는 등 사회적·경제적으로 변화를 가져왔고, 단순히 정보 전달의 기능뿐만 아니라 정보를 가공하여 새로운 지식으로 창조할 수 있게 되었다.

이러한 새로운 지식의 창출은 국가전반의 발전에 큰 영향을 줌은 물론, 과거 눈에 보이는 각종 생산품에 의한 발전 착도가 눈에 보이지 않는 핵심 기술 개발로 변화하면서 기업 및 국가 경쟁력의 근간이 되었다.

그러나 핵심 기술의 발전에 대하여 국가 및 기업간 경쟁이 심해지면서 기업은 신기술 개발에 대해 큰 비중을 두고 투자가 이루어지고 있지만 이에 반해 핵심 기술을 보호하려는 보안 인식부족으로 인하여 기술유출 사고가 끊임없이 일어나고 있다. 국가핵심기술에 대한 유출통계를 살펴보면 2005년부터 2012년까지 국내 첨단기술을 해외로 불법유출하였거나 유출을 기도한 사건이 매년 증가 추세로 나타났다[1]. 이는 국가 및 기업의 경쟁력을 저해시키는 가장 큰 원인으로 이에 대한 보안대책이 시급한 실정이다.

이와 같은 정보유출의 경로에 따른 보안 영역을 나누어 보면 정보보안 영역과 물리보안 영역으로 구분할 수 있지만, 최근 들어 보안 위협이 어느 한 영역에서 이루어지지 않고 통합적 영역으로 발전하면서 영역 구분이 무의미해졌다.

이로 인하여 물리보안 영역도 IT기술을 적극 활용한 무인시스템으로 빠르게 전환되면서 24시간 365일 감시가 가능하고 저장장치를 활용한 보안사고 발생 시 증거 수집이 용이하며, 네트워크 연결이 가능한 시스템 개발로 경제적 측면에서도 부담을 크게 줄일 수 있게 되었다.

하지만 무인경비 시스템은 실무적, 제도적, 서비스 취약점에 대한 문제점이 존재하고 있다. 따라서 본 연구는 통합보안 환경에서 무인경비 시스템이 갖고 있는 취약점을 분석하여 이에 대한 개선방안을 제안하고자 한다.

2. 관련연구

2.1 보안영역의 유형

Hallcrest Report 보고서에 따르면 보안영역의 분류를 물리적 보안(physical security), 인적보안(personnel security), 정보보안(information security) 등으로 분류하고 있다[2].

첫째 물리보안은 보호해야 할 대상을 물리적 방법이나 수단을 활용하여 물리적 보안 위협으로부터 인명 및 재산(정보·시설) 등을 보호하는 것을 의미한다.

둘째 정보보안은 정보 및 정보시스템을 보호하기 위하여 기밀성(confidentiality), 무결성(integrity), 가용성(availability)에 대하여 비인가자의 공격(위조, 변조, 유출, 훼손 등)을 방어하기 위한 일련의 보안활동이다[3].

셋째 인적보안은 보안 및 보안 위협을 행하는 주체인 사람에 대한 관리로 관리보안이라고도 한다. ISMS(Information Security Management System)에서의 통제항목인 인적보안은 정보보호 책임, 인사규정으로 한 관리체계를 정의하고 있다[4].

2.2 기계경비 시스템의 성장배경

오늘날 각종 범죄는 양적, 질적으로 증가하고 있는 추세로 국가의 공권력만으로는 범죄에 대응하는 것에 한계가 있다. 이로 인하여 전통적으로 치안서비스는 국가경찰이 독점적으로 제공하여 왔으나, 지식정보사회 및 치안서비스 수요의 다양화·고도화에 따라 종전의 집합재로만 여겼던 치안서비스의 일부분이 사적재의 성격을 띠게 되었으며, 그 결과 치안서비스 생산과정에 일반국민과 시민단체 및 민간경비업 등 민간부문이 적극적으로 참여하게 됨에 따라 치안서비스 생산주체의 다원화가 확산되고 있다[5].

그리고 민간 경비서비스형태는 과거 사람을 중심으로 한 인력경비 형태로 이루어지다가, 경비 절감효과와 장비의 운용으로 인한 정확성·신속성·계속성을 기대할 수 있는 기계경비시스템으로 전환되고 있다[6].

또한 기계경비 시스템은 전자·정보·통신 기술이 결합된 서비스로, 원격지에서 경보신호를 전달하기 위해 공중전화망, 전용망과 같은 통신매체 뿐만 아니라 인터넷망 등 기존 인프라의 활용과 디지털 기술을 적용

하게 되면서 보안관제의 구현을 가능하게 하는 등 정보통신기술의 변화와 밀접한 관계를 가지고 발전하였다[7]. 그리고 기업의 정보유출, 개인정보유출 등 다양한 형태의 정보유출 사고가 급증하여 기업과 개인의 정보보호에 대한 관심도 증가하고 있으며, 정보유출의 형태가 정보보안 측면뿐만 아니라 물리보안 측면과 결합된 형태의 보안위협이 증가하고 있기 때문에 보안위협의 패러다임 변화에 따른 무인경비 시스템의 발전을 가져올 수 있게 되었다.

3. 기계경비 시스템의 문제점

3.1 기계경비 시스템의 운용적 문제점

기계경비 시스템은 경제적·안정적·법적 측면에서 과거 인력경비 시스템경비에 드러난 단점들을 상당부분 보완하고 있고, 보안 경비를 절감하여 인력으로 수행하기 힘든 365일 24시간 감시를 통하여 보다 안정적인 보안형태로 운용할 수 있다. 또한 정확한 기록으로 인한 증거확보가 용이하고, 인력에 대한 인사사고의 발생 위험이 적다는 장점이 있다. 하지만 운용적 제한으로 인해 기계경비 시스템의 발전에 한계를 가져왔다.

기계경비 시스템은 상주경비의 형태가 아닌 출동경비의 개념이기 때문에 신속한 대응이 어렵고, 예정된 범위에 한하여 감시가 이루어지기 때문에 해당 범위 이외의 지역에 대한 탐지가 불가하다.

또한 네트워크 취약점으로 인한 서비스 중단을 막고 보다 높은 서비스를 제공하기 위하여, 메인 관제실과 서브 관제실을 운영하여야 하지만 서브 관제를 운용하는데 실시간 데이터 업그레이드와 관리 비용을 투자해야 하므로 효율성 및 비용성에 대한 문제점이 있어, 대부분의 서브 관제를 백업(backup)형태로 운용하고 있다.

3.2 기계경비 시스템의 기술적 문제점

감지 장치의 결함 및 SP(Security Planning)를 바탕으로 한 설계 및 시공이 이루어지지 않고, 사용자가 시스템의 원리나 장비의 작동원리를 몰라 오경보가 발생할 수 있는 취약점으로 무인경비 시스템의 발전의 한계를 가져왔다. 그리고 무인경비 시스템의 각 서비스 지점의 Main Control(각종 감지센서, 출입통제)과 CCTV 영상장치와 보안관제실의 각 서버를 인터넷망과 공중회선망으로 연결하여 운영되면서 단선의 문제점뿐만 아니라 정보통신과 관련된 보안 취약성에 노출되어 있다.

4. 기계경비 시스템의 발전방향

4.1 기계경비 시스템의 운용적 개선방안

4.1.1 보안 계층화

보안 계층화는 보안 위협으로부터 정보 및 자산을 보호하고 더 나아가 예방하기 위한 보안영역을 4단계로 구분한 것이다. 단계별 요소로 1계층 '환경보안', 2계층 '출입보안', 3계층 '감지보안', 4계층 '응용보안'으로 각 계층 영역에 맞는 보안설정을 하여 운용하게 된다. 각 계층별 세부내용을 살펴보면 다음과 같다.

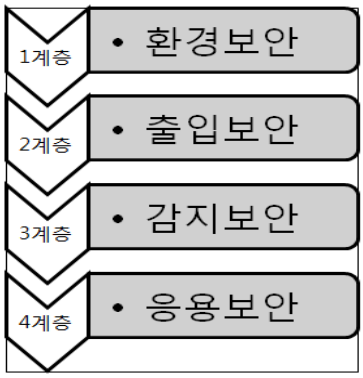
첫째 '환경보안'은 외부의 환경을 개선하여 자연스러운 감시가 이루어지도록 설계하여야 한다. 이를 위해 개방형 개구부로 인해 보안 시스템이 아닌 내·외부인의 이동만으로 자연스러운 감시가 이루어지도록 가시범위를 최대화해야 한다. 그리고 외부공간의 감시에 있어 음폐·엄폐 할 수 있는 공간의 확보는 범죄행동을 이롭게 하기 때문에 이러한 사각지대를 최소화해야 한다. 또한 적절한 조도와 간격의 조명과 CCTV의 설치로 범죄자의 행위를 위축시킬 수 있도록 야간의 가시성을 극대화해야 한다.

둘째 내부 보안이 시작되는 계층인 '출입보안'은, 출입을 위해 일정한 공간으로 내·외부인을 유도하여, 허가받지 않은 인원의 출입을 차단하고 범죄행동의 노출위험을 증가시켜 범죄를 예방하게 된다. 이를 위해서는 출입구 수를 최소화해야 하고, 출입통제 시스템을 통한 관리가 이루어져야 한다. 출입통제 시스템의 기능은 단순히 출입통제만을 수행하는 것이 아니라, 출입자의 이동 동선을 파악할 수 있어야 한다.

셋째 내부 시설에 대한 보안 계층인 '감지보안'은, 각종 센서를 이용하여 내부 주요 시설을 보호하게 된다. 이는 외부인원에 대한 보안뿐만 아니라, 허가 받은 내부인원의 보안 위협에 대해서도 감시가 이루어

질 수 있다. 업무시간에는 CCTV를 활용한 감시가 이루어지고, 그 외의 시간은 CCTV와 더불어 각종 감지센서를 활용한 보안시스템을 운용하게 된다.

넷째 최종 보안 계층인 '응용보안'은 이중 보안관제 운영을 바탕으로, 앞서 1, 2, 3계층에 대한 모든 이벤트를 수집·분석하는 보안관제이다. 응용보안에서는 아웃소싱을 통한 외부 관제실에서 이벤트를 이용한 이동동선의 변화·오경보 등을 수집하여 보안 이벤트로 분석하여 보다 효과적이고 개선적인 보안 업무수행을 수립하게 된다.



(그림 1) 보안 계층화

4.1.2 지역 포인트의 통합화

우리나라는 물론 세계 경제의 장기 침체 등으로 경제상황이 악화되고 실업률 상승이 범죄현상에도 반영되는 등 경제적 이익을 목적으로 하는 경제범죄가 최근 몇 년간 증가하였다. 범죄의 증가는 경찰인력의 수급 부족을 가져왔고 사회구성원인 국민의 안전의식 증대, 정보보안 영역과의 결합으로 통합보안 형태의 보안업무로의 전환, 보안성 강화, 편리성 제고, 비용절감의 효과를 가져 오면서 무인경비 시스템의 수요가 늘어나고 있는 실정이다.

이러한 보안 수준을 더욱 향상시키기 위해서는 무인경비업체들의 보안지역에 대한 업무협력이 우선되어야 한다. 보안관제를 중심으로 지역 포인트에서의 신속한 출동과 유기적 순찰은 범죄예방효과도 가져올 수 있다.

4.2 기계경비 시스템의 기술적 개선방안

4.2.1 시스템의 표준화

기계경비 시스템의 표준화 측면은 기계경비 시스템 설치에 대한 기준과 기계경비 시스템 기술에 대한 기준으로 구분할 수 있다.

첫째, 기계경비 시스템에 대한 우리나라의 설치규격 표준화 실태는 한국표준협회(KSA)에 등록되어 있으나, 강제성이 없어 적극적으로 반영하기보다 각 업체별 기존의 사용방식을 사용하고 있다.

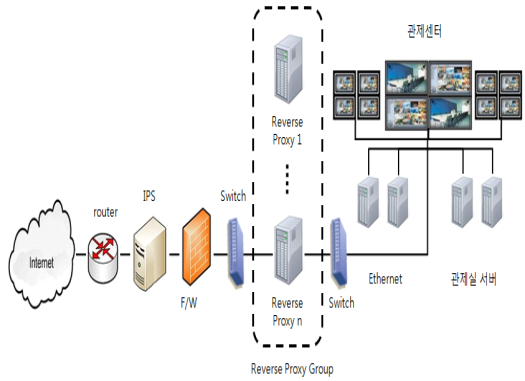
둘째, 기계경비 시스템 기술에 대한 기준은 일부 업체의 경우, 자체적으로 IEC(International Electrotechnical Commission) 61000-4 인증기준[8]에 적합한 수준으로 기기에 대한 신뢰성기준을 정하여 무인경비 시스템에 적용하고 있다.

기계경비 시스템에 대한 표준화를 위해서는 보안계층화를 기준으로 각 계층에 대한 설치 표준과 오경보를 줄이기 위한 장비 개발이 이루어져야 한다.

4.2.2 가상화를 통한 보안

일반적으로 네트워크에 연결된 보안관제는 침입차단시스템인 방화벽을 기본으로 침입방지시스템인 IPS(Intrusion Prevention System) 등을 활용하게 된다.

하지만 일반적인 보안형태는 관제시스템을 마비시키려고 악의적인 DDoS 공격을 받기 되면 관제센터는 각종 감지기 및 CCTV의 정상적인 서비스 및 백업 기능을 수행하기 힘들게 된다.



(그림 3) 가상화를 통한 보안관제 보안

(그림 3)은 Reverse Proxy서버를 그룹화한 구조로, DDoS 공격으로부터 관제시스템을 보호하기 위해 Reverse Proxy서버 그룹을 이용한 방어기법을 사용하게 된다. Reverse Proxy는 관제센터의 실 서버보다 앞에서 마치 실서버처럼 동작하기 때문에 공격자의 DDoS 공격을 Proxy 서버가 받게 되면 Proxy 서버가 다운되더라도 관제실 서버는 공격에 노출되지 않기 때문에 시스템 구성정보만 변경하여 서비스 계속 운영할 수 있게 된다.

5. 결 론

IT 기술의 발전으로 과거 제한적으로 여겨졌던 시·공간적 한계를 벗어나면서, 여러 산업분야의 업무영역 확대 및 새로운 인프라 구축 등의 변화를 가져오게 되었다. 이는 물리 보안분야에도 적용되어 과거 이원적으로 다루어졌던 보안영역이 물리 보안과 IT 기술이 융합된 통합보안영역으로 확대되면서, 기계경비 시스템의 급속한 발전이 이루어지고 있다. 하지만 통합보안적 형태로 발전함에 따른 현재 우리나라의 물리보안 영역의 무인경비 시스템에의 취약점들이 나타나고 있다.

첫째 기계경비 시스템의 운용적 취약점은 이 시스템이 상주경비의 형태가 아닌 출동경비의 개념이기 때문에 관제실에 이상 신호가 발생하게 되면 신속히 대응하기가 어렵고, 예정된 범위에 한하여 감시가 이루어지기 때문에 해당 범위 이외의 이상현상에 대한 탐지가 어렵다. 그리고 보안관제센터는 주 관제와 서브 관제를 운용하면서 보안위협에 의한 주 관제의 업무수행이 어려워질 경우 서브 관제를 운용될 수 있도록 이중 보안관제를 실시하야 하지만, 서브 관제를 운용하는데 실시간 데이터 업그레이드와 관리 비용을 투자해야 하므로 효율성 및 비용성에 대한 문제점이 있어 대부분의 서브 관제를 백업(backup)형태로 운용하고 있다.

둘째, 기계경비 시스템의 기술적 취약점으로 오경보에 대한 취약점으로 기계경비 시스템의 발전의 한계를 가져왔고, 기계경비 시스템의 각 서비스 지점의 Main Control(각종 감지센서, 출입통제)과 CCTV 영상장치와 보안관제실의 각 서버를 인터넷망과 공중회선망으로 연결하여 운영되면서 단선의 문제점뿐만 아니라 정보통신과 관련된 보안 취약성에 노출되어 있다.

이를 개선하기 위한 방법으로 보안영역을 환경보안, 출입보안, 감지보안, 응용보안으로 계층화하여 각 계층 영역에 맞는 보안설정을 하여 운용하여야 한다.. 또한 보안관제를 운용함에 있어 관제서버 공격에 대비하기 위해 Reverse Proxy Group을 이용한 방어와 더불어 이중 보안관제를 실시하여 운용해야 한다.

마지막으로, 보안 수준을 더욱 향상시키기 위해서는 기계경비업체들의 보안지역에 대한 포인트 통합화로 인한 업무협력과 더불어 시스템의 표준화가 이루어져야 할 것이다.

참고문헌

[1] http://service4.nis.go.kr/page?cmd=preservation&cd_code=outflow_1&menu=AAA00

[2] William C. Cunningham, John J. Strauchs, Clifford W. Private Security Trends: 1970 to 2000 The Hallcrest Report(MA: Butterworth Heineman), pp.125-132, 1990.

[3] NIST, SP 800-55 Performance Measurement Guide for Information Security, 2008.

[4] http://isms.kisa.or.kr/kor/main.jsp

[5] 이준형, “치안서비스 공급주체의 다원화 방안에 관한 고찰”, 경찰대학교, Vol.5, pp.74-99, 2003.

[6] 손영경 외, “효율적 범죄예방을 위한 기계경비시스템의 활용방안”, 한국화재소방학회, Vol.2003, No.10, pp.393-399, 2003.

[7] http://www.cctvnews.co.kr/atl/view.asp?a_id=700

[8] http://www.iec.ch

[저 자 소 개]

공 병 석 (Byung Seok Kong)

2011년 경호학사
2013년 산업보안학석사

email : kong6371@hanmail.net

김 귀 남 (Kuinam J. Kim)

미국 캔자스대학(학사)
미국 콜로라도주립대학(석사)
미국 콜로라도주립대학(박사)
현재 경기대학교 융합보안학과 교수

email : harap123@daum.net

황 현 석 (Hyun Seok Hwang)

2003년 컴퓨터공학사
2011년 정보보호학석사
2014년 현재 경기대학교
산업보안학과 박사과정

email : nicepolice@police.go.kr