시큐리티 환경변화에 따른 융합보안의 대두와 물리보안업체의 대응★

안황권*

요 약

시큐리티환경이 급변하고 있다. 위협의 종류가 복합화되고 다양한 채널과 방법으로 발생하고 있으며, 신종위협이 발생하고 있다. 또 보안기술이 비 IT산업에 활용되고 있고 정보통신기술과 스마트폰의 등장으로 비즈니스 환경이 변화하고 있다. 이에 적절하게 대응하기 위해 융합보안이 대두고 있다. 융합보안은 융합관제, 통합인증, 출력물보안 등의 형태로 진전되고 있다. 융합보안 시대를 맞이하여 물리보안 사업자도 보안환경 변화 속에서 새로운 비즈니스 기회를 찾아야 할 것이다.

A Study on the Development of Convergence Security with the Changes in Security Environments

Ahn, Hwang Kwon*

ABSTRACT

As new technologies emerge and threats become increasingly complex and unpredictable, security professionals who are living in the age of information face an increasingly complex array of challenges. In recent, virtually all organizations with physical and IT assets protect those assets in a variety of methods. There are physical systems to protect facilities and their contents from unlawful trespassing.

It is important to note that the integration of physical and IT security is to be required: When done correctly, the integration starts with laws, strategies, policies and procedures. Integration of physical and IT security systems is done not for its own sake but in support of security policies and procedures. Significant security improvements can be made by integrating physical and IT security management without necessarily integrating physical and logical electronic security systems.

Up to now, the private security industries of the Republic of Korea have been operated and developed by the separation of physical security and industrial security. However, considering the fast changing security environments, physical security companies should turn their attention to security convergence field to cope with the new trends in the security matters. At the same time, governmental supports on the improvement of various laws, regulations and policies in such a way to meet the realistic needs of the industries should be followed.

Key words: convergence security, security environments, physical security, IT security, security policy

접수일(2011년 10월 04일), 수정일(1차: 2011년 10월 12일), 게재확정일(2011년 10월 13일)

★ 본 논문은 (사)한국경비협회 2011년 CEO 세미나 및 APSA 총회에서 발표한 논문을 수정한 것임.

* 경기대학교 경호보안학과

1. 서 론

지식정보사회는 우리에게 편리하고 유용한 초연결 사회를 만들어주고 있지만 한편으로 그 만큼 많은 위협이 내재되어 있고 보안 또한 사회 기반이 흔들릴 정도 취약한 실정이다. 그동안 보안체계가 수립되고 보안활동이 강화되었지만 실제 최근에 많은 보안사고를 통하여 정보자산과 고객정보, 개인정보 등이 큰 피해를 입었다.

그동안 많은 조직의 보안체계는 물리보안, 관리보안, 정보보안이라는 세 개의 영역으로 분리되어 운영되고 있다. 그러나 보안위협은 침입, 도난, 테러와 같은 물리보안 위협과 정보유출, 변조, 해킹 등의 정보보안 위협이 복합되고 융합된 형태로 발생하고 있다. 따라서 물리보안, 관리보안, 정보보안이 각각의 보안체계를 잘 수립하고 운영하더라도 하나의 영역에 취약점이 발생할 경우 복합적인 위협에 대비하거나 대응하는 것이 쉽지 않은 것이다.

물리보안과 정보보안 영역의 분리에 따른 보안사건, 사고는 새로운 정보보안 이슈로 부각되고 있다. 그 해결방안으로 대두된 것이 이를 융합, 복합한 융합보안의 등장이다. 또 폭넓은 고객의 보안니즈를 충족시키고 복합되고 융합된 보안사고를 예방하고 적절하게 대처하기 위해서는 세 가지 보안영역을 통합적인 관점에서 관리하고 운영하는 융합보안이 활성화되어야 할 것이다.

그동안 우리나라 민간경비(private security)산업도 경비업법에 따른 물리보안과 정보보호 또는 산업보안으로 분리되어 운영되고 발전되어 왔다. 그러나 이제 급변하는 시큐리티 환경변화를 감안하여 물리보안업체도 융합보안산업에 눈을 돌려 새로운 변화에 적극 대처해 나가야 할 때이다.

본 연구는 시큐리티의 유형과 법적 근거 및 시큐리티를 둘러싼 환경의 변화를 진단하고 보안산업의 새로운 메가트랜드로 등장한 융합보안의 가치와 현황 및 물리보안업체의 대응을 기술하는 것이 목적이다.

2. 시큐리티 유형과 법적 근거

2.1 시큐리티 유형

시큐리티의 유형은 많은 학자와 기관들에 따라 다양하게 분류되고 있다. 가장 광의의 분류이며 많은 지지를 받고 있는 것은 ASIS(American Society for Industrial Security)와 헐크레스트 보고서 등에서 분류한 물리 보안, 인적 보안, 정보보안의 유형이다.

2.1.1 물리보안

물리보안이란 ① 사람과 차에 대한 접근 통제 감시, ② 불법침입자의 예방과 탐지, ③ 재산(정보, 건물, 자재, 장비 등)의 보호를 말한다. 물리보안은 순찰활동과 경비실에서의 전통적인 경비활동뿐 아니라 물리적 장벽(담장, 출입문, 벽, 자연방벽), 잠금장치(locking system), 방범조명, CCTV, 침입감지센서 등이 포함된다. 그리고 접근통제장치(access control system)인 열쇠관리시스템부터 고급화된 통제장치(지문, 홍채인식, 카드식 감식장치 등)가 포함된다.

우리나라 경비업법에 분류된 시설경비, 기계경비 등이 물리보안에 포함되는 것이다. 따라서 물리보안에서는 경비대상시설의 내부공간을 보호하기 위한 전형적인 장치인 경보기(alarms), 잠금장치, 전자적 접근통제, 감시시스템 등이 개별적으로 또는 결합되어 사용되는 형태이다[12].

2.1.2 인적 보안

인적 보안(personnel security)은 인적 보안관리라고도 한다. 이것은 조직이 안전과 이익을 위해 업무와 관련된 사람을 관리하는 기술적 과정이라고 할 수 있다 즉 “보호가치”를 지니고 있거나 접근이 필요한 사람은 적극적으로 보호·관리하고, 위해 가능성이 있는 사람은 접근을 차단하기 위해 물리적, 과학적 수단을 활용한다[3].

인적 보안의 범위는 신규채용자의 경력조사, 조직구성원들의 안전의식 고양, 종업원에 대한 성실의무계약, 주요 경영간부 등 요인경호의 업무를 포함한다. 많은 조직에서 관심을 가지는 요인경호는 사무실 접근통제, 통신통제, 자택의 안전관리, 통근 및 여행 시 특별경호, 훈련된 운전기사와 경호원을 배치하는 것이다[5].

따라서 인적보안은 우리나라의 경비업법상의 신변보호업무뿐 아니라 폭넓은 관련 업무를 포함하고 있다. 그런 점에서 인적 보안은 업무과정에서 각 단계별로 업무가 차단되어 연속성과 일관성이 있어야할 뿐 아니라 사람의 정신적·심리적 구조와 환경을 중심으로 관리제도와 기술이 강구되어야 한다[3].

2.1.3 정보보안

정보보안(information security)이란 사람, 기술, 사고, 재난 및 이들의 복합으로부터 야기될 수 있는 광범위한 위협을 고려하여 폭넓게 기초되고 잘 계획된 창조적 전략 프로그램을 통하여 조직의 정보자산을 지키는 것이다[17]. 따라서 정보보안을 하기 위해서는 정보 및 정보시스템을 허가되지 않은 접근, 사용, 공개, 손상, 변경, 파괴 등을 보호하여 기밀성, 완전성, 가용성을 제공하는 것이다.

이런 면에서 정보보안은 기밀성(confidentiality), 완전성(integrity), 가용성(availability)의 3요소를 확보하는 것이다. 이것이 국제적으로 공식무대에서 처음 등장한 것은 1992년의 OECD 정보보안 가이드라인이다. 이어서 영국 표준규격 'BS7799'에도 같은 내용이 등장하였다. 이것은 두 개의 파트로 나눠졌는데 하나는 국제표준규격 'ISO/IEC 17799'가 되고 또 하나는 로컬규격이 되었다.

OECD는 1980년에 공표한 프라이버시 가이드라인은 '안전보호의 원칙'을 강조하고 있다. 이 내용이 1992년의 OECD의 시큐리티 가이드라인을 사실상 이어 받아 정리한 결과 이 3요소를 중심으로 한 개념이 탄생한 것이다. 이후 OECD 시큐리티 가이드라인은 2002년에 개정되었다[11].

정보보안 3요소의 내용은 다음과 같다.

첫째, 기밀성(confidentiality)이란 내부의 정보처리 과정을 외부에서 보거나 확인할 수 없도록 하는 것이다. 따라서 내부자료 또는 전송자료에 대해 접근이 인가된 자만이 정보에 접근할 수 있도록 하는 것이다. 침해의 사례는 정보의 누출이다.

둘째, 완전성(integrity)이란 내부정보가 인가된 사용자 이외에는 내용의 변경이 불가능하도록 하는 것이다. 이것은 정보 및 처리방법이 완전하고 확실하다는 것을 보호하는 것이다. 침해의 사례는 정보의 훼손 및 고치는 행위이다.

셋째, 가용성(availability)이란 내부의 정보자원에 대해 허가된 이용자가 필요할 때에 정보 및 관련 자산에 접근하고 사용하도록 허가하는 것이다. 침해의 사례는 정보의 훼손·멸실 등이다.

2.2 법적 근거

2.2.1 물리보안 관련 법

물리보안에 관한 대표적인 법률은 경비업법이다. 형식적 의미의 경비업무 즉, 실정법상에서 경비업무를 시설경비업무, 호송경비업무, 신변보호업무, 기계경비업무, 특수경비업무로 분류하고 있지만 이를 대별하면 시설경비업무와 호송경비업무, 기계경비업무, 특수경비업무는 물리경비에 포함된다.

경비업법은 경비업의 건전한 육성 및 발전과 그 체계적인 관리에 관하여 필요한 사항을 정함으로써 경비업의 건전한 운영에 이바지할 목적으로 1976년 제정되었다. 경비업법상 경비업무는 시설경비업무, 호송경비업무, 신변보호업무, 기계경비업무, 특수경비업무이지만 이중 신변보호업무를 제외한 나머지는 물리보안에 속한다고 볼 수 있다. 특히 경비산업에서 대표적인 물리경비인 시설경비업무와 기계경비업무의 업체 수, 매출액 등에서 차지하는 비중은 80%가 넘는다.

2.2.2 정보보안 및 산업보안 관련 법

2.2.2.1 부정경쟁방지 및 영업비밀보호에 관한 법률

부정경쟁방지 및 영업비밀보호에 관한 법률(이하 영업비밀보호법이라 함)은 국내에 널리 알려진 타인의 상표·상호 등을 부정하게 사용하는 등의 부정경쟁행위와 타인의 영업 비밀을 침해하는 행위를 방지하여 건전한 거래질서를 유지할 목적으로 제정되었다. 이 법은 1961년 12월 30일 부정경쟁방지법으로 제정된 것을 우리 기업의 기술수준이 향상되고 국제교류가 증대됨에 따라 핵심기술의 유출 등 영업비밀 침해행위의 증가가 우려되어 이를 효율적으로 대처할 수 있도록 관련 규정을 보완하는 등 영업비밀의 보호에 관한 내용의 비중이 커지면서 법명을 부정경쟁방지 및 영업비밀보호에 관한 법률로 1998년 12월 31일 변경하였다.

이 법에서 영업비밀이란 공공연히 알려져 있지 아

니하고 독립된 경제적 가치를 가지는 것으로서 상당한 노력에 의하여 비밀로 유지된 생산방법, 판매방법, 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다(법 제2조 제2호).
영업비밀보호법의 보호를 받는 영업비밀의 대상은 크게 기술상의 정보와 경영상의 정보로 나눌 수 있다.

첫째, 기술상의 정보는 ① 제품 및 장비, ② 설계도, 시설배치 및 제조공정, ③ 연구개발보고서 및 실험데이터, ④ 물질의 배합방법, ⑤ 컴퓨터 프로그램 등, 기타 기능성이 있는 디자인, 아이디어, 공개 전의 특허출원정보 등이다.

둘째, 경영상의 정보는 ① 고객명부, ② 기업의 주요계획, ③ 매뉴얼, ④ 아이디어, ⑤ 기타 경영상 정보이다.

2.2.2.2 산업기술의 유출방지 및 보호에 관한 법률

산업기술의 유출방지 및 보호에 관한 법률(이하 산업기술유출법)은 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지할 목적으로 2006년 10월 27일 제정되었다.

기업이 아닌 정부출연 연구소 및 대학 등에서 개발된 첨단기술의 해외 불법 유출을 규제할 수 없고, 국부인 핵심기술에 대한 예방적 차원의 보호를 충분히 수행할 수 없다는 문제점이 있다. 이에 정부는 2006년 10월 27일 지정된 국가핵심기술의 수출승인 및 사전신고를 골자로 하는 '산업기술의 유출방지 및 보호에 관한 법률'(법률 제8062호, 2007. 4. 28 시행)을 제정하여 산업기술에 대한 종합적인 보호체계를 마련하였다[8].

2.2.2.3 개인정보보호법

개인정보보호체계는 그동안 부문별 개별법 체계로 규정되었으나 2011년 3월 29일 제정·공포된 개인정보보호에 관한 법률(이하 개인정보보호법이라 함)이 단일한 법으로 통일되어 2011년 9월30일부터 시행되었다. 그동안 개별법령을 보면 공공행정기관은 공공기관의 개인정보보호에 관한 법률, 금융·신용은 신용정보의 이용 및 보호에 관한 법률, 의료는 의료법, 교육은 교육정보시스템의 운영 등에 관한 규칙, 정보통신은 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에 분산되어 있었다.

개인정보보호법은 개인정보처리자가 반드시 알아야 할 개인정보보호 내용을 기본이념과 원칙, 수집·이용, 민감정보·고유식별정보 처리와 개인정보 암호화 등의 안전조치 강화, 영상정보처리기기의 설치·운영 제한, 개인정보 유출대응에 대한 벌칙 등을 규정하고 있다.

2.2.2.4 기타 산업보안관계법

산업보안과 관련 법률은 발명진흥법, 특허법 등 지적재산권법, 대외무역법, 외국인투자촉진법, 산업발전법, 형법, 대·중소기업 상생협력 촉진에 관한 법률 등이 있다.

3. 시큐리티의 환경변화

3.1 복합위협과 신종위협의 대두

기업의 정보유출, 개인정보유출 등 다양한 형태의 정보유출 사고가 급증하고 있어 기업과 개인의 정보보호에 대한 관심도 증가하고 있다. 심각한 것은 정보유출이 단순하게 증가되고 있을 뿐 아니라 위협의 종류가 갈수록 복합화 되어 다양한 방법과 채널로 발생하고 위협에 대한 결과 또한 점점 심각해가고 있다[4].

즉, 침입·도난·테러와 같은 물리적 위협과 정보의 유출, 변조, 해킹 등과 같은 정보적 위협이 복합적 형태로 발생하고 있다. 또한 미래적 관점에서 산업기술의 진화로 인한 편리성과 더불어 이들의 생산에서부터 폐기까지의 과정은 환경에 부정적 역할을 하게 되고, 미래에 현재의 주에너지원의 자원고갈로 인한 대체에너지의 개발 필요성과 현재 대체에너지로써 태양열과 풍력 등의 친환경적 에너지 R&D가 이루어지고 있지만 현재의 기술로 인류가 필요로 하는 에너지를 공급하는 것은 불가능하므로 핵 발전에 의한 대체에너지에 의존하게 되면서 환경안전과 에너지의 안전과 에너지 고갈 등의 신종 위협이 등장하고 있다.

이와 같이 위협의 다변화, 다채널화 되는 상황에서 대안으로 등장한 것이 융합보안이다.

3.2 보안기술의 非IT산업에 활용추세

사용자의 인증 및 암호화 등의 보안기술이 자동차, 헬스케어, 에너지 등의 비(非) IT산업에 활용되는 추세를 포함되는 추세이다. 구체적으로는 운송보안(자동차, 항공, 조선 등), 로봇보안, 금융보안, 의료보안, 건설보안, 국방보안, 산업보안 등에서 보안기술이 적용되고 있는 추세이다.

3.3 정보유출사고의 증대와 정보보호관심 증대

(그림 1)에서 보는 바와 같이 국가정보원 산업기밀보호센터(2011. 11. 5 검색)의 기술유출통계를 보면 2004년부터 2010년도까지의 국내 첨단기술을 해외로 유출하였거나 기도한 사건 244건을 적발하였다. 이를 연도별로 보면 2004년 26건, 2005년 29건, 2006년 31건, 2007년 32건, 2008년 42건, 2009년 43건으로 꾸준히 증가하였고, 2010년 에는 41건으로 다소 감소하였다.

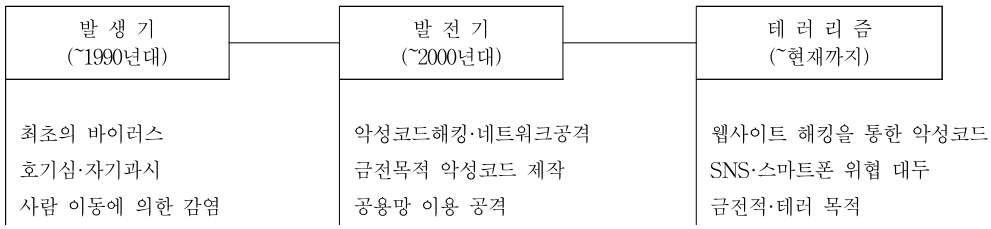
또한 대형 금융보안사고의 발생도 증가하고 있다. 2011년에 발생한 금융 보안 사고는 현대캐피탈, 솔로몬 신용정보, NH증권, 리딩증권 등이다.

형태로써 사무실에 출근하지 않고 자택에서 정보통신망을 이용하여 일을 하고 스마트폰을 이용하여 현장업무를 수행하거나 영상회의 시스템을 이용하여 원격근무를 하는 형태이다.

이와 같이 사무환경의 경계가 파괴되어 개방형 환경으로 변화되고 다양한 통신채널과 휴대 장치의 등장과 같은 기술변화는 기존 보안시스템에 있어서는 새로운 위협이 될 수 밖에 없다. 따라서 이러한 비즈니스 환경변화로 새로이 등장하는 위협에 대한 대안으로 융합보안이 대안이 될 수 있다[4].

3.5 다양한 위협과 피해의 대량화

1980년대에 컴퓨터 바이러스가 처음 발생하고 1990년대에 인터넷의 보급이 증가하게 되면서 본격적으로 정보에 대한 피해가 발생하게 되었다. 초기에 호기심과 자기 과시적 목적에서 2000년대에 들어서면서 테러와 금전적 목적으로 그 형태가 바뀌었다.



(그림 1) 정보보안 위협의 발전과정

이와 같은 정보유출은 금전적 거래와 밀접하게 관계되어 있기 때문에 대형화되어 증가하고 있다. 따라서 정보유출의 심각성이 대두되면서 기업뿐만 아니라 개인도 정보보호에 대한 관심이 증대되고 있다.

3.4 비즈니스 환경 변화

정보통신기술의 발달과 스마트폰의 등장으로 비즈니스 환경측면에서도 변화가 일어나고 있다. 효율적으로 업무에 종사할 수 있도록 하는 미래지향적 업무형태로 스마트워크 방식이 대두되었다. 스마트워크는 시간과 장소의 제약 없이 업무를 수행하는 유연한 근무

정보에 대한 공격동향을 초기, 발생기, 발전기, 테러리즘으로 구분하여 살펴보면 (그림 1)과 같다.

4. 융합보안의 대두와 물리보안업체의 대응

4.1 융합보안의 의의

융합 및 융합보안에 대한 정의는 <표 1>에서 보는 바와 같이 많은 학자나 기관들이 다양한 관점에

서 제시하고 있기 때문에 아직 표준화되거나 통합된 내용은 없는 실정이다.

<표 1> 융합 및 융합보안에 대한 정의

학자 또는 기관명	정 의
ASIS(American Society for Industrial Security	융합이란 기업 내에 존재하는 비즈니스 기능과 프로세스 사이의 상호의존성 및 보안 위험을 식별하고, 이를 적절하게 관리할 수 있는 비즈니스 솔루션을 수립하는 것
OSE(The Open Security Exchange)	융합이란 물리적 보안과 IT보안이 동일한 개체(objective), 프로세스, 아키텍처를 향하여 이동하는 것
Nicole S. Latimer-Livington	융합보안이란 물리보안과 정보보호가 IT위험을 관리하기 위하여 비슷하거나 연계되거나 혹은 동일한 프로세스와 기능을 갖추는 것
COSO online	융합보안이란 비용 효율적으로 전사적 차원의 위험을 관리하기 위하여 전통적인 운영적 위험관리의 기능을 통합하는 것
김정덕・김건우・이용덕	융합보안이란 비용감소, 운영의 효과성 및 효율성 향상, 전사적 차원의 위험을 관리하기 위하여 조직의 보안 요소들이 점진적으로 통합되고 상호협력하는 체계

자료: 김정덕・김건우・이용덕(2009: 70-71)가 기술한 내용을 정리

우리나라에서 융합보안이라는 용어는 2008년 지식경제부에서 발표한 'Securing Knowledge Korea 2013'에서 기존 정보보호산업을 지식정보보안 산업으로 재정의하면서 지식정보 보안산업을 정보보안, 물리보안, 융합보안으로 세분화하는 과정에서 태생된 용어이다[4]. 정보보안은 방화벽, 안티바이러스, Forensic 툴, 물리보안은 보안관제, CCTV, 영상보안, 바이오 인식, 융합보안은 차량불랙박스, RFID 보안칩 등이 대표적인 제품이다.

이상을 종합해 보면 융합보안이란 조직의 보안을 위하여 모든 관련 보안체계가 통합되고 복합한 형태로 협동하는 체계를 말한다.

4.2 융합보안의 가치

4.2.1 정보가치의 증가에 따른 보안 환경의 변화 측면

국내의 기술경쟁력이 세계적으로 높아지면서 정보의 가치가 증가하고 IT기술이 발전함에 따라 정보의 위협이 질적·양적으로 발달하고 있다. 국가정보원 산업기밀보호센터의 통계자료를 보면 2004~2010년 사이에 기술유출 사건이 무려 244건 적발되었고 금융보안사고 또한 증가되고 있는 추세이다. 보안 영역별(물리·정보·관리·인적보안) 위협을 분석해 보면 복합적으로 사건이 일어나고 있다. 이러한 보안위협 환경에 대한 대응으로 효과적이고 효율적인 보안의 수단으로 융합보안을 고려해야 하는 것은 필연적이다.

4.2.2 보안 운영 환경의 변화 측면

복합적 보안 위협에 따른 대응으로 이원적 형태의 시스템이 네트워크화 되면서 물리보안 시스템에 IT기술을 접목한 보안 컨버전스가 이루어지고 이에 따르는 보안 운영 환경의 변화가 일어나게 되었다. 이원적 형태로 운영되어지던 보안의 형태가 융합관제와 같은 물리보안과 정보보안의 융합으로 보안운영의 효율성 증가와 원가 절감이 이루어지게 된다.

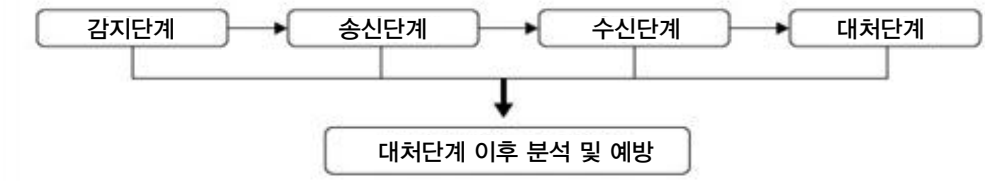
4.2.3 보안영역의 확대로 인한 사용자의 유연성 제고 측면

보안위협으로부터 정보를 보호하기 위한 보안 체계로 대두된 융합보안은 보안영역(물리·정보·관리·인적보안)의 통합으로 보안 수준을 높이는데 목적이 있다. 따라서 기존의 단일적 보안 솔루션에서 통합적 보안 솔루션으로 변화함에 따라 사용자의 편의성을 제고해야 한다. 보안 수준의 강화 될수록 사용자의 불편함을 초래하기 때문에 초보 사용자도 쉽게 사용할 수 있고 보안대상자가 인식하지 못하는 유연성 있는 보안 솔루션 기술이 발전하는 추세이다.

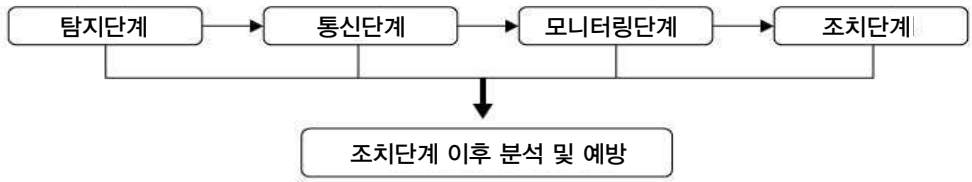
4.3 융합보안의 진전

4.3.1 물리보안과 정보보안간의 융합

4.3.1.1 융합관제



(그림 2) 물리보안 관제의 구성 단계



(그림 3) 정보 보안관제 구성 단계

융합관제는 물리보안관제와 정보보안관제를 통합하여 운용하는 형태이다. 우선 물리보안 관제체계는 (그림 2)에서 보는 바와 같이 경비대상시설에 설치한 기기에 의하여 감지·송신된 정보를 관제시설의 기기로 수신하여 분석한 후 대처하는 것이다.

정보보안 관제도 (그림 3)에서 보는 바와 같이 해킹·불법침입을 탐지하는 탐지단계, 이에 대한 신호를 전송하는 통신단계, 전송된 신호를 분석하여 이상신호를 분석하여 이상상황을 파악하는 모니터링 단계, 이상상황으로 파악된 경우 원격접속 등을 통하여 사이버 대응을 하는 조치단계, 조치 이후 위협에 대한 분석 및 예방으로 구성되어 있다.

물리적 보안관제와 정보보안 관제는 구성 단계가 유사하기 때문에 전체 보안체계를 통합하는 경우 시너지 창출이 가능하다.

365일 24시간 이루어져야 하는 보안에 있어 통합적 보안관제는 상시모니터링을 통해 장애조기 발견 및 대응을 통해 최소 비용으로 물리보안 위협과 정보보안 위협을 한꺼번에 해결할 수 있는 솔루션이 될 수 있다[4].

4.3.1.2 통합인증

통합인증은 물리보안과 정보보안의 융합사례로 가장 대표적인 사례이며 가장 먼저 시도되는 분야이다. 통합인증(Single Sign-On, SSO)이란 '단 한번의 로그인만으로 기업의 각종 시스템이나 인터넷 서비스에 접속하게 해주는 보안 응용 솔루션이다[9]. 각각의 시스템마다 인증 절차를 밟지 않고도 1개의 계정만으로 다양한 시스템에 접근할 수 있어 ID, 비밀번호에 대한 보안 위험 예방과 사용자 편의 증진, 인증 관리비용의 절감 효과가 있다는 것이다. 따라서 양자의 인증수단이 통합되면 보안관리가 강화됨은 물론, 사용자 정보의 등록 및 갱신이 단일화 되어 효율성이 제고되며, 운용비용 또한 절감되는 효과가 있다.

출입관리에서의 카드, 지문, 생체인식 등으로 출입을 위하여 사용자를 인증하는 물리보안 체계와 컴퓨터 로그인과 사내 인트라넷의 접속을 위한 ID, 패스워드를 입력하는 정보보안 체계를 통합하는 것이 통합인증이다. 이것은 단계적으로 볼 때 단순히 사용자가 누구인가를 인증하는 사용자인증 체계의 통합인 통합인증체계(single sign on)로부터 통합계정관리, 계정 및 권한 관리의 통합에 이르기까지 확대가 가능하다[4].

통합인증요소는 통합된 인증, 통합된 권한, 통합적 관리이다.

첫째, 통합인증은 물리적인 출입부터 컴퓨터 로그인, 경영정보시스템(MIS), 인사관리시스템 등을 접근

할 때 필요한 아이디와 패스워드를 입력하는 것을 사용자는 인증을 위한 크리덴셜을 제출하는 것이고, 사용자임을 확인하는 것이다.

둘째, 통합된 권한이란 사용자의 권한을 부여하는 인가이다. 이것은 아이디와 패스워드를 입력하고 인증을 성공적으로 받게 되면 그 후부터 사용자의 등급에 맞는 권한을 부여받아 서비스를 이용할 수 있다.

셋째, 통합적 관리는 사용자에 대한 관리자의 관점에서 보는 인증과 권한을 통합 관리하는 부분이다. 보안융합을 통하여 사용자의 계정, 패스워드를 통합적으로 관리한다.

통합인증은 사용자 측면에서는 편리하며, 관리자 측면에서는 일관된 보안정책을 적용할 수 있어 보안관리가 강화됨은 물론, 운영 효율성이 제고되고, 운영비용 또한 절감되는 효과가 있다.

4.3.1.3 보안기술이 비 IT 기술과 융복합되어 창출되는 보안제품 및 서비스

융합보안의 한 형태로 보안기술이 비 IT기술・산업이 융복합되어 창출되는 보안제품 및 서비스로 자동차나 항공기의 운송보안, 조선・의료・건설・국방의 보안, 방범보안로봇 등이 해당된다[6].

이를 융합보안이 적용되는 분야별로 나누어 살펴보면 다음과 같다.

첫째, 운송(자동차・항공・조선)분야에서는 차량 지능키, 차량전자번호판, 차량불랙박스, 차량 간 통신보안모듈, 차량통합보안관리, 승객용 스크리너, 조선보안 등의 형태로 적용된다.

이것은 자동차와 IT가 융합됨에 따라 IT기술에 대한 다양한 공격들을 통해 야기될 수 있는 자동차 사고, 교통환경 위조, 차량정보 위조, 교통흐름방해, 위치정보노출로 인한 프라이버시 침해 등을 방지할 수 있다.

둘째, 로봇분야에서는 보안로봇, 네트워크로봇 보안 등의 형태로 적용될 수 있다. 현재의 보안로봇은 침입자의 공격에 대해 경고하고 긴급상황을 관제센터에 알리는 '움직이는 센서'로서의 역할을 수행하지만 점차 상황에 따라서 판단하고 행동을 하는 보안로봇을 예상하고 있다.

셋째, 금융분야에서는 금융ATM기기, OTP, 금융IC카드 등에 적용될 수 있다. 특히 최근 모바일뱅킹, IPTV, VoIP 기반의 전자금융서비스 제공환경의 다양화와 스마트폰 등 신규 채널의 취약점에 따른 주요 정보유출 가능성의 증가, 무선랜 사용 증가 등으로 정보보안이 취약해지는 실정이다.

넷째, 의료분야에서는 의료영상보안제품, 의료DB공유보안시스템 등에 적용되고 있다.

다섯째, 건설분야에서는 지능형건물, 오피스 침입감지, 홈네트워크보안 등에 적용되고 있다.

여섯째, 국방분야에서는 다양한 국방보안장비에 적용되고 있다.

일곱째, 산업분야에서는 산업용 기기 보안에 적용되고 있다.

4.3.1.4 출력물보안

산업기밀보호센터의 통계자료와 중소기업 산업기밀관리 실태조사 보고서에 의하면 기술유출 은 내부자(전직, 현직 직원)에 의한 유출이 80% 이상이며, 출력물에 대한 유출이 약 40%이다.

출력물보안에서 가장 중요한 이슈는 출력물의 무단반출을 막기 위한 솔루션이 출력물 보안솔루션이다. 출력물보안을 위해 인쇄시 전자감응 특수용지를 사용하여 출입통제에서 출력물에 대한 무단 반출을 탐지하는 솔루션의 적용과 복합기 등에 카드리더를 연동하여 인쇄시 사용자를 인증하는 체계, 인쇄물에 출력자의 신상정보 및 워터마크를 자동 인쇄하도록 하는 방안 등이 적용되고 있다[4].

4.4 융합보안의 대두에 대한 물리보안업체의 대응

보안 산업은 그동안 두 개의 축을 형성하면서 발전되어 왔다. 하나는 출입통제, CCTV, 주차시설 관리, 영상보안 등을 통한 시설경비, 기계경비와 같은 물리보안이다. 한국 경비업법에서는 기계경비를 비롯한 시설경비, 호송경비, 신변보호, 특수경비 등이 모두 여기에 속한다고 볼 수 있다.

또 하나는 컴퓨터와 네트워크상의 정보를 보호하는 IT 정보보안과 정보보호의 형태로 발전되어 왔다. 이것은 우리나라에서 그동안 정보보호, 산업보안 등으로 불리면서 발전되어 온 것이다.

그동안 보안에 대한 잘못된 인식 중의 하나는 흔히

보안의 목적이 시설보호나 신변보호에 초점이 맞춰져 있으면 물리보안이라고 생각하고 정보보호나 사이버 상의 정보자산을 보호하는데 있으면 별개의 영역이라고 생각한 것이다. 그러나 보안위협이 복잡화, 변형화, 다양화되면서 이분적인 시각의 보안으로는 해결하기 어려운 점이 대두되면서 융합보안이 등장하게 된 것이다.

이제 기술력이 요구되는 정보보안의 가치가 높아지고 부가가치가 커지면서 상대적으로 물리보안은 위축되고 점점 그 영역을 정보보안에 빼앗기는 양상이 나타나고 있는 것이다. 결과적으로 융합보안이 대두되면서 물리보안은 정보보안영역으로 흡수되거나 잠식되는 양상을 점차 보이게 될 것이다.

IT환경의 개방화로 네트워크경제와 글로벌 기업화의 추세 속에서 세계의 보안시장은 통합화, 대형화로 나가고 있다. 융합보안의 시대를 맞이하여 물리적 보안 사업자도 기존의 사업영역만을 고수할 것이 아니라 시큐리티 환경 변화 속에서 새로운 비즈니스 기회를 찾아야 할 것이다.

5. 결 론

정보화사회에서 보안서비스가 복잡 다단해짐에 따라 보안의 취약성은 급증하고 있다. 이러한 보안위협에 대한 예방과 적절한 대응은 부분적인 영역의 보안만으로는 한계가 있다. 우리의 민간경비(private security)는 그동안 경비업법에 따른 물리보안과 정보보안 또는 산업보안으로 분리되어 발전되어 왔다. 그러나 물리보안의 한계, 복합위협과 신종위협의 대두, 보안기술의 비 IT산업에 활용추세, 정보유출사고의 증대와 정보보호관심 증대, 다양한 위협과 피해의 대량화, 비즈니스 환경 변화로 인하여 시큐리티 환경이 급변하고 있다.

물리보안과 정보보안을 융합하는 경우 그 가치가 훨씬 커지는 장점이 있다. 즉 정보가치의 증가에 따른 보안 환경의 변화 측면, 보안 운영 환경의 변화 측면, 보안영역의 확대로 인한 사용자의 유연성 제고 측면 등이다.

융합보안은 다양한 형태로 진전되고 있다. 우선 물리보안과 정보보안과의 융합형태이다. 대표적인 사례는 융합관제와 통합인증의 형태로 발전되고 있다.

둘째는 보안기술이 비 IT 기술과 융복합되어 창출되는 보안제품 및 서비스 형태이다. 이것은 자동차나 항공기의 운송보안, 조선・의료・건설・국방의 보안, 방범보안로봇 등의 산업과 연결되어 발전되고 있다. 셋째는 출력물보안이다. 이것은 내부자의 정보유출을 막고 출력물의 무단방출을 막기 위한 것이다. 그리고 출력물보안의 융합형태이다.

보안산업의 메가트랜드는 융합보안이다. 융합보안의 시대를 맞이하여 시설경비, 신변보호, 기계경비 등 물리 보안 사업자도 시큐리티 환경 변화에 적절하게 대응하면서 사업영역의 외연을 넓히는 새로운 비즈니스 기회를 찾아야 할 것이다.

참고문헌

[1] 김정덕・김건우・이용덕, “융합보안의 개념 정립과 정립방법”, 정보보호학회지, 제19권 제6호, pp. 68-74, 2009.

[2] 김홍, “정보보안의 필요성과 방향”, 국회도서관보, 제46권 제9호, pp. 40-45, 2009.

[3] 민병설, “인원보안 관리의 한계와 발전과제”, 산업기술보호 issue, 제4호, pp. 40-41, 2011.

[4] 보안뉴스 미디어, 2010. 10. 05

[5] 안황권, 민간경비학, 인천: 진영사, 2009.

[6] 이필재,“유비쿼터스 환경과 국가사이버위기관리 법・제도의 문제점 및 개선방안”, 국가위기관리학회, 국가위기관리학회보, 제1호, pp. 123-139, 2009.

[7] 한국산업기술보호협회, 산업보안관리사, 서울: 크라운출판사, 2010.

[8] 한국산업기술보호협회, 국가핵심기술 보호 실태조사보고서, 미간행물, 2010.

[9] 한국정보화진흥원, http://word.tta.or.kr/terms/terms.jsp, 검색일: 2011. 9. 22.

[10] 東倉洋一 外, 情報セキュリテイと法制度. 東京: 丸善ライブラリ, 2005.

[11] (社)全國警備業協會, 警備業法解說, 2009.

[12] Cunningham, Willam C., John J. Stauchs, Cliffor

d W. Van Meter. (1990), Private Security Trends 1970 To 2000, The Hallcrest Report Ⅱ. MA: Butterworth-Heinemann.

[13] Fischer, Robert J., Edward Halibozek, Gion Green, Introduction to Security, 8th edition, MA: Butterworth-Heinemann, 2008.

[14] Johnson, Brian R, Principles of Security Management. NJ: Pearson Prentice Hall, 2005.

[15] Khairallah, Michael, Physical Security Systems: The Design and Implementation of Electronic Security Systems, MA: Butterworth-Heinemann, 2006.

[16] Norman, Thomas, Integrated Security Systems Design: Concepts, Design, and Implementation, MA: Butterworth-Heinemann, 2007.

[17] Purpura, Philip P, Security and Loss Prevention, 5th edition. MA: Butterworth-Heinemann, 2008.

[저 자 소 개]

안 황 권 (Ahn, Hwang Kwon)

1981년 경기대학교
법정대학(행정학사)
1989년 경기대학교
대학원(행정학박사)
현재 경기대학교 경호보안학과 교수

e-mail : ahk@kgu.ac.kr