한국경호경비학회 – 제39호(2014): 269–294
투고일 2014. 04. 29, 심사일 2014. 05. 26, 게재확정일 2014. 06. 18

지식정보보안 산업의 현황과 전망

최정일·장예진·이옥동

지식정보보안 산업의 현황과 전망

최정일* · 장예진** · 이옥동***

〈요 약〉

최근 우리나라는 카드3사의 개인정보 유출 등으로 보안 산업에 대한 관심이 높아지고 있다. 경영자들은 개인정보 유출 등 보안 사고에 의한 피해가 어떠한 재무적 위험보다도 더 위험한 요소로 인식하고 있다. 지식정보보안 산업은 과거 물리보안 및 네트워크 보안에서 최근에는 사회 안전 및 시설보안 등 융합 산업 보안으로 진화하고 있다. 관심분야도 방화벽이나 Anti-virus 등에서 스마트폰보안 및 지능형영상보안 등 융합보안 산업으로 변해가고 있다.

융합보안은 시설경비나 출입통제 중심에서 최근에는 공공기관 및 대기업을 중심으로 수요가 확대되고 있다. 금융, 교육, 유통, 국방, 의료, 자동차산업에 이르기까지 범위가 빠르게 증가하고 있다. 융합보안시장은 지능형차량 보안, U-헬스케어 보안, 금융 보안, 스마트 그리드 보안, 주력산업 보안 등 다양한 분야에서 제품 및 서비스가 개발되고 있으며 시장이 확대되고 있다.

지식정보보안 산업의 발전을 위해 시장중심의 인재를 육성하고 학계와 연계하여 교육과정의 신설 및 강화가 요구된다. 글로벌 기업과의 경쟁력 강화를 위해 교육의 질적 수준을 향상시키고 동시에 대국민 보안의식을 높이기 위한 노력이 병행되어야 할 것이다.

주제어 : 지식정보, 보안산업, 융합보안, 물리보안, 정보보안

* 성결대학교 경영학부 교수 (제 1저자)
** 국제대학교 경호학과 교수 (교신저자)
*** 성결대학교 부동산학과 교수 (공동저자)

목 차

Ⅰ. 서 론

지식정보보안 산업은 정보보호 산업의 차세대 버전으로 기존 정보보호 산업을 새롭게 정의한 것이다. 네트워크·시스템 기반의 정보보안, 안전·안심 생활을 위한 물리보안, 보안기술과 전통산업 간 융합으로 창출되는 융합보안으로 세분하고 있다.

지난 2014년도 초에 KB국민카드 5,300만 건, 롯데카드 2,600만 건, NH농협카드 2,500만 건 등 카드3사의 세계 3위 규모에 달하는 1억500만 건의 대규모 개인정보 유출에 이어 2차로 1,200만 명의 KT 고객정보 유출과 보험사, 소셜커머스, 인터넷쇼핑몰까지 유출사태가 나타났다.

이러한 개인정보 유출사태로 국민들의 불신이 높아지면서 정보보안이 기업 경영의 중요한 요소로 떠오르고 있다. 금융사고의 재발을 막기 위해 내부 통제를 강화하고 고객정보 보호 사각지대를 혁신해야 한다는 주장이 제기되고 있다.

빅 데이터 시대를 맞아 중앙집중식 데이터 수집·관리시스템이 일반화되면서 지식정보보안의 중요성이 더욱 커지고 있다. 지식정보보안에 대해 과거에는 방화벽을 세워 외부로부터의 침입을 막는 것이 목적이었지만 최근에는 내부자료 유출방지 등과 같은 새로운 기술을 더욱 필요로 하고 있다.

금융권에서는 정보 수집과 보유 제한, 정보공유 제한, 불법정보 수요 차단 등을 토대로 개인정보 유출 재발 방지 종합대책을 추진하고 있다. 또한 전자금융사기 방

지, 고객정보 보호 준칙, 정보보호 조직 신설 및 강화, 인터넷뱅킹 거래 보안 정비 등을 서두르고 있다. 고객정보 유출이나 국가기반시설에 대한 사이버공격 등을 방어하기 위해 일부에서는 국내 보안업체들이 해외 기업인수 등을 통해 부족한 기술력을 확보해야 한다는 주장도 제기하고 있다.

지식정보보안 산업은 과거 통신상의 정보보호에서 최근에는 개인 및 사회 안전의 개념으로 변해가고 있다. 인터넷과 모바일 등 네트워크를 기반으로 IT환경이 진화하고 다양한 보안 위협에 노출되면서 보안사고가 발생하는 경우 개인·기업·국가 등 사회 전 영역에 미치는 영향력이 커지고 있다(정수민, 2013).

지식정보보안 분야에서는 방화벽, 안티바이러스, 안티스팸 등의 시스템-네트워크 보안에서 사회 안전 및 시설보안으로 확장되고 있다. 정보보안 분야에서는 기존의 바이러스, 해킹, DDoS, CCTV 등과 같은 단순한 대응기술보다는 고도화되고 지능화된 보안기술들을 필요로 하고 있다(정수민, 2013).

최근 보안시장의 가장 이슈는 정보보안과 물리보안을 결합한 융합보안시장의 성장으로 융합보안관제시스템 영역이 활성화되고 있다. CCTV/영상보안시스템 등을 기반으로 기업 내부의 PC 사용정보, IP 및 네트워크 사용현황 등을 포함하는 보안관제시스템에 대한 수요 및 관심이 높아지고 있다. IT 및 모든 산업에 걸쳐 융합 과정에서 나타나는 보안수요 역시 융합보안의 개념에서 접근해야 하며 자동차, 의료, 금융 등의 분야에서도 보안 이슈에 관심을 가져야 할 것이다.

정보보안은 비 인가된 사용자로부터 보안을 보장하면서 동시에 정보를 공유 할 수 있는 본질적인 보호 프레임워크를 제공해야 한다. 따라서 본 연구에서는 정보보안의 침해로부터 예방하고 통제함으로써 조직에 대한 손실을 최소화하는 데 있다. 또한 지식정보보안 산업의 현황을 파악하고 향후 나아갈 방향에 대해 제시하고자 한다.

본 연구에서는 한국인터넷진흥원에서 2012년과 2013년도에 발표한 「국내 지식정보보안산업 실태조사」를 중심으로 관련 연구소 및 증권사에서 발표한 보안관련 자료를 토대로 작성하였다. 최근 정보보안시장의 현황을 파악하여 향후 지식정보보안 산업의 나아갈 방향을 제시하고 융합보안시장의 성장 가능성에 대해 조사하고자 한다.

Ⅱ. 이론적 배경

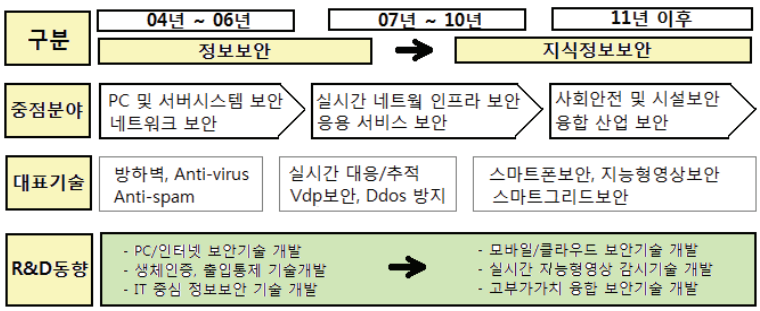
1. 지식정보보안 산업의 이해

지식정보보안 산업은 정보보호 산업의 차세대 버전으로 기존의 정보보호 산업을 새롭게 정의한 것으로 네트워크 및 시스템 기반의 정보보안, 안전 및 안심 생활을 위한 물리보안, 보안기술과 전통 산업 간 융합으로 창출되는 융합보안으로 세분화하고 있다.

국내 카드3사의 개인정보 유출 등으로 보안 산업에 대한 관심이 높아지는 가운데 미국에서도 지난 2013년도 연말 대형 유통업체 "TARKET"에서 1억1천만 건에 이르는 고객정보 유출 사건이 발생하였다. 당시 미국 사회가 커다란 충격을 받았으며 이후 이를 방지하기 위해 보안 산업에 대한 관심이 높아지고 있다.

"TARKET"[1]은 개인정보 유출에 대비하여 AIG, Ace, Axis 등의 보험사를 통해 배상책임보험에 가입했지만 고객정보 유출에 따른 피해를 어느 정도 배상하게 될지는 모르는 상황이다. 경영자들은 개인정보 유출 등 사이버 공격에 의한 피해가 실적감소나 자산 가치하락 등의 재무위험보다 더 위험한 요소로 인식하게 되었다.

지식정보보안 산업은 <그림 1>에서 보듯이 과거 PC 및 서버시스템 보안 등 네트워크 보안에서 최근에는 사회 안전 및 시설보안 등 융합 산업 보안으로 변해가고 있다. 관심분야도 방화벽, Anti-virus, Anti-spam 등 네트워크 보안에서 스마트폰보안 및 지능형영상보안 등 융합산업 보안으로 진화하고 있다.



자료 : KISA, 하나대투증권

〈그림 1〉 지식정보보안 산업의 시기별 추이

1) 미국 대형 쇼핑몰 TARGET의 신용카드 정보 유출은 POS 단말기의 악성코드 감염이 원인인 것으로 지적됐다. POS 단말기가 보안에 취약하다는 것을 보여주는 전형적인 사례가 되었다.

최근 지식정보보안 산업은 산업의 적용 영역과 업종의 특성에 따라 정보보안, 물리보안, 융합보안으로 구분하고 있다. 금융 및 통신, 유통, 의료, 국방, 건설 등 모든 분야에서 사회 안전 및 시설보안을 강화하는 방향으로 발전해가고 있다. 암호·인증·감시 등의 보안기술을 활용하여 개인정보나 사회 안전을 보호하고 서비스를 제공하는 산업으로 인식하고 있다(Lazarica, 2011).

<표 1>에서 정보보안 분야는 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 보안기술이다. 과거 바이러스, 해킹, DDoS[2], CCTV 등 단순한 대응기술보다 방화벽, 디지털포렌식 툴(Digital Forensics Tool), DDoS 대응장비, Anti-Virus 등의 제품 등 고도화되고 지능화된 보안기술들이 개발되고 있다(정수민, 2013).

물리보안 분야는 공항, 항만, 발전소, 도로 등 국가 주요시설에서 개인의 정보, 인명, 시설 등을 보호하기 위한 보안기술이다. 테러나 재난·재해로부터 개인 및 사회를 안정하게 보호하기 위한 기술 및 서비스가 강조되고 있다. 과거 장비와 인력 중심의 보안에서 최근에는 영상감시 솔루션, 지능형 카메라, 바이오인식, CCTV, 보안관제 등 IT가 결합된 제품에 대한 관심이 증가하고 있다.

융합보안 분야는 <그림 2>와 같이 물리적 보안과 정보 보안을 융합한 보안기술이다. 각종 내·외부 정보 침해 대응과 물리적 보안 장비 및 각종 재난·재해 상황에 대한 관제까지 포함하고 있다. 향후 발전 가능성이 높은 분야로 통합보안관제시스템, 차량 블랙박스, U-헬스케어, 금융보안, 스마트그리드 보안 등에 대한 관심이 높아지고 있다.

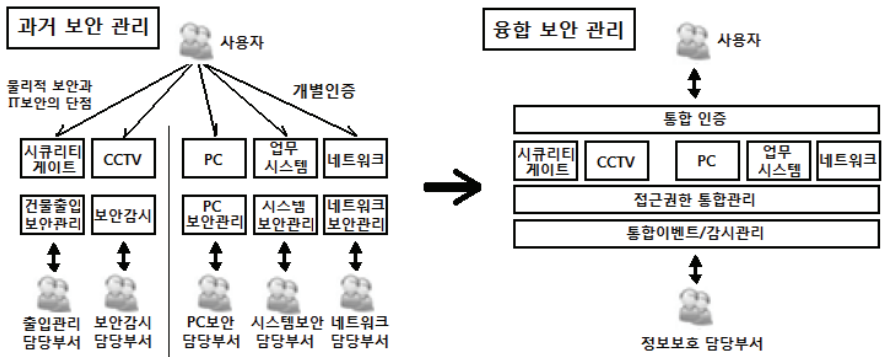
〈표 1〉 지식정보보안 산업의 정의

구 분	개 요	주요제품
정보보안	- 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 보안기술 - 공급자 측면 : 네트워크 및 시스템 등의 하드웨어, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호하기 위한 행위 - 사용자 측면 : 개인정보 유출과 남용을 방지하기 위해	방화벽 디지털포렌식 툴 DDoS 대응장비 안티바이러스

2) 분산서비스 거부 공격(Distributed Denial of Service attack)을 뜻하는 것으로 서비스 거부 공격 DoS(Denial of Service attack)에서 한 단계 파워업한 것이다. 인터넷상에서 사이트 공격을 하는 방법 중 하나로 사이버 테러의 대표적인 경우다.

구 분	개 요	주요제품
물리보안	- 개인의 정보, 인명, 시설 등을 보호하기 위한 보안기술 - 인가자/비인가자의 출입관리, 천재지변으로부터 시설보호, 방범관리 등 모든 물리적 위협에 대해 보안을 지키는 것을 의미	영상감시솔루션 지능형 카메라 바이오인식 CCTV, 보안관제
융합보안	- 물리적 보안과 정보 보안을 융합한 보안기술 - 각종 내·외부 정보 침해 대응과 물리적 보안 장비 및 각종 재난·재해 상황에 대한 관제까지 포함	통합보안관제시스템 차량 블랙박스 스마트그리드 보안

자료 : 하나대투증권



자료 : LG CNS, 하나대투증권

〈그림 2〉 차세대 융합보안 개념도

2. 국내 보안관련 기술과 기업

국내 보안관련 기업은 <표 2>와 같이 각 분야별로 네트워크, 시스템, 컨텐츠/정보유출방지, 암호/인증, 보안관리 등으로 분류하고 있다.

안랩은 세계적인 기술력을 보유한 국내 대표적인 정보보안업체로 모바일 악성코드 실시간 진단 및 치료 등 다양한 보안기능을 제공하는 통합시스템 업체이다. 아프리카TV는 보안솔루션 사업을 영위하고 있으며, 플랜티넷은 인터넷상의 유해사이트 차단 서비스 및 소프트웨어를 개발하고 있다.

넥스지는 VPN(Virtual Private Network)을 활용한 통합보안관제서비스사업과 사물지능통신(M2M) 보안솔루션에 이어 차세대 방화벽 출시로 사업다각화를 시도하는

업체이다. 이니텍은 정보보안과 금융IT서비스를 제공하고 있으며, 티모이앤엠은 보안사업 및 보안관련 솔루션사업 업체이다.

이글루시큐리티는 국내 1위의 통합보안관리 솔루션 개발업체로 250개 고객사에 종합보안관제 서비스를 제공하고 있다. 소프트포럼은 보안관련 토탈 솔루션 전문업체이고 윈스테크넷은 나우콤에서 네트워크 보안사업 부분이 분리되어 설립된 업체이다.

윈스테크넷은 IPS[3]와 DDoS 차단시스템 분야에서 국내 1위 보안업체이고, 라온시큐어는 국내 유일의 모바일 통합보안 기업이다. 파스닷컴은 국내 1위 전자문서보안 기업으로 DRM(Digital Rights Management) 기술을 기반하고 있는 업체이다. 이크레더블은 전자신용인증서비스를 제공하고 있으며, 인포뱅크는 모바일 결제서비스 전문업체로 휴대전화로 결제하는 솔루션 등을 제공하는 업체이다.

〈표 2〉 국내 보안관련 기업

	관련기업	내용
네트워크	윈스테크넷	IPS과 DDoS 차단시스템 분야에서 국내 1위 보안기업
	안랩	Firewall, IPS, VPN, Anti-Virus/Spam 등 다양한 보안기능을 제공하는 통합시스템
	넥스지	사물지능통신(M2M) 보안솔루션에 이어 차세대 방화벽 출시로 사업다각화
시스템	안랩	모바일 악성코드 실시간 진단 및 치료
	라온시큐어	국내 유일의 모바일 통합보안 기업
컨텐츠/정보유출방지	파스닷컴	국내 1위 전자문서보안기업 : DRM기술 기반
암호/인증	이니텍	국내 금융기관 대상 보안사업 M/S 1위
보안관리	이글루시큐리티	ESM 분야에서 국내 1위 250개 고객사에 종합보안관제 서비스 제공

자료 : 하나대투증권

3) 침입방지시스템(Intrusion Prevention System)은 인터넷 웜 등의 악성코드 및 해킹 등 침입이 일어나기 전에 실시간으로 침입을 막고 알려지지 않은 방식의 침입으로부터 네트워크와 호스트 컴퓨터를 보호하는 솔루션

Ⅲ. 지식정보보안시장 현황

1. 세계 지식정보보안시장 현황

세계적으로 지식정보보안시장은 2007년 이후 연평균 12.8%의 성장률을 보이고 있으며 <그림 3>와 같이 2012년에 3,301억 달러를 2016년에는 4,929억 달러 규모의 시장이 형성될 것으로 전망하고 있다.

지식정보보안시장은 과거 물리보안 및 정보보안에서 최근에는 <그림 4>에서 보듯이 융합보안 분야가 부각되면서 보안 산업의 성장을 주도하고 있다. 융합보안은 물리보안과 정보보안을 통합한 개념으로 각종 내·외부적 정보 침해에 대한 대응은 물론 물리적 보안과 각종 재난·재해 상황에 대한 관제까지 포함하고 있다.

지식정보보안 산업은 컴퓨터나 네트워크상 정보 유출 등을 방지하기 위한 정보보안과 재난 및 범죄 등을 방지하기 위한 물리보안으로 구분된다. 세계적으로 지식정보보안시장 규모는 2012년 기준 3,301억 달러로 반도체 3,080억 달러나 조선 2,500억 달러보다 더 큰 규모로 나타났다(KISA, 2013). 국가별 시장 비중을 살펴보면 미국이 41.9%의 점유율로 시장을 선도하고 있으며 유럽 33.5%, 일본 11.3% 등 주요 선진국이 90% 가까이 차지하고 있다(정수민, 2013).

미국의 오바마 정부는 사이버보안을 국가 핵심어젠더로 지정하고 강력한 정책수립과 투자 강화를 진행하고 있다. 2009년도 사이버 보안 중·단기 실행계획을 발표하면서 총 24개의 중점사업을 선정했다. 미 국방부의 2014년도 사이버사령부 예산은 2013년도 1억9,100만 달러에서 4억4,700만 달러(약 4757억 원)로 2배 이상 큰 폭으로 증가했다.

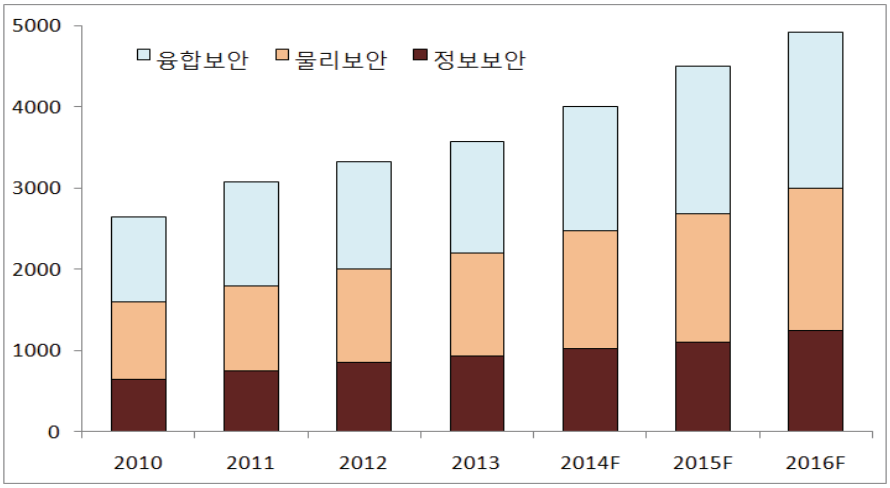
미국은 Symantec, McAfee, Cisco, Trend Micro, Check Point, IBM 등 글로벌 보안기업과 신생기업 팔로알토 네트웍스 등을 앞세워 전 세계 보안시장에 영향을 미치고 있다. 네트워크 접근통제, ID(Industrial Design) 접근제어, 컴퓨팅 리소스격리 방안, 보안관제 등을 강화하기 위해 방화벽 IPS 및 네트워크보안, OS보안, 서버보안 등을 중심으로 세계시장을 주도하고 있다.

프랑스는 사이버 방위능력 향상을 위해 향후 5년간 1조4,600억 원을 투입할 계획이며, 영국은 2013년도에 수백 명 규모의 사이버 방위부대를 개설했다. 유럽은 2013년에 사이버범죄대응 센터를 개설하여 회원국을 대상으로 인터넷 금융사기, 온라인

신분도용, 신용카드 개인정보유출, 금융 인프라 DDoS 공격 등의 사이버 예방에 나서고 있다.

이스라엘은 세계적인 보안강국으로 지난 2002년부터 사이버 전담부대를 창설해 대비책을 마련해 왔다. 또한 글로벌 시장점유율에서 4.1%를 차지하고 있으며 방화벽과 모바일보안, 국방보안관련 제품 등에서 높은 평가를 받고 있다. 중국은 활동 중인 해커만 30만 명이고 군 소속 정예 해커부대원이 1만3,000여 명에 달하고 있다[4]. 북한은 사이버 부대 인력이 3,000명에 이르는 것으로 추정하고 있다[5].

(단위 : 억 달러)

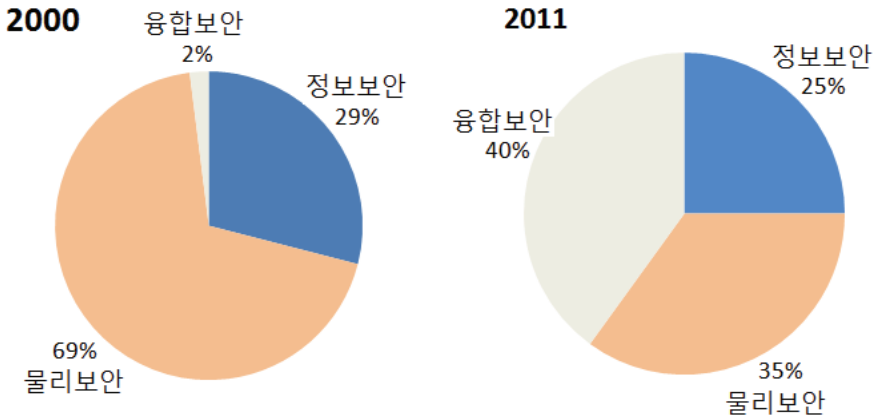


자료 : IDC & RNCOS, 하나대투증권

〈그림 3〉 세계 지식정보보안 시장 규모

4) 중국 정보보안시장은 정부, 통신, 에너지 군을 중심으로 발달해왔으며 최근 금융, 교통, 교육, 제조 분야에서 연평균 20% 성장률로 빠르게 시장이 확대되고 있다. 물리보안시장은 2112년 3,200억 위안에서 2115년 5,000억 위안을 돌파할 것으로 전망되며 이 중 영상감시 장치시장이 가장 빠른 성장세를 보여, 2115년도 전체 시장의 23%를 차지할 전망이다.

5) 우리나라는 2013년도 최정예 사이버보안인력 양성사업을 시작해 2017년까지 전문가 5,000명을 양성한다는 계획을 세웠다. 현재 국내 사이버보안전문 인력이 200명 수준인 것을 감안할 때 미국, 중국, 북한 등과 비교해 10분의 1수준에 불과한 상황이다. 유럽은 사이버범죄대응센터(EC3)에서 금융사기, 온라인신분 도용, 신용카드 개인정보유출, 금융 인프라 디도스 공격 등 사이버 범죄 예방에 나서고 있다. 글로벌 보안 강국들은 정부차원에서 강력한 사이버 보안 정책을 취하고 있으며 탄탄한 보안 산업이 뒤를 바치고 있다.



자료 : IDC, 하나대투증권

〈그림 4〉 지식정보보안 산업 비중의 변화

2. 한국 지식정보보안시장 현황

KISA(한국인터넷진흥원)에 의하면 한국의 지식정보보안 산업 규모는 2012년도 5조8,417억 원이고 2013년도 6조6,870억 원으로 연평균 15.5% 성장해 <그림 5>과 같이 2015년에는 10조3,094억 원 수준에 이를 것으로 기대하고 있다.

국내 기업들의 해외시장 수출금액은 <표 3>에서 2012년 1조4,574억 원이고 2013년 1조 5,487억 원으로 전년 대비 6.3% 증가한 것으로 조사되었다. 전체 수출금액 중 정보보안 분야의 실적은 6,986억 원이고 물리보안 분야의 실적은 1조4,789억 원으로 약 95.5%의 압도적인 수치를 나타내고 있다(정수민, 2013).

수출금액에서 물리보안이 정보보안을 압도적으로 앞서는 것은 정보보안 부문의 성장성이 사실상 국내시장에 한정되어 있으며 국내 230개가 넘는 국내 보안업체들이 국내시장에서만 치열하게 경쟁하고 있기 때문이다. 해외진출에 어려움을 겪으며 <그림 6>에서 보듯이 주로 일본과 동남아시아를 중심으로 매출을 올리고 있을 뿐 보안시장의 중심지인 미국시장으로의 진출은 어려운 상황이다.

정보보안제품의 경우 보안관리, 웹 방화벽, 네트워크(시스템) 방화벽 등에서 높은 비중을 나타내고 있다. 그 이유는 보안관리 분야가 아프리카시장으로 진출하였고, 웹 방화벽, 네트워크(시스템) 방화벽 분야가 일본시장으로 수출이 증가하였기 때문

으로 분석된다.

물리보안제품의 경우 기타 분야에서는 블랙박스 제품이 크게 증가했다. 또한 바이오인식 분야 등에서는 기존의 RF카드(ID카드) 위주의 출입보안장비에서 복제가 더 어려운 지문·홍채·얼굴인식 등의 장비로 교체되었기 때문으로 분석된다.

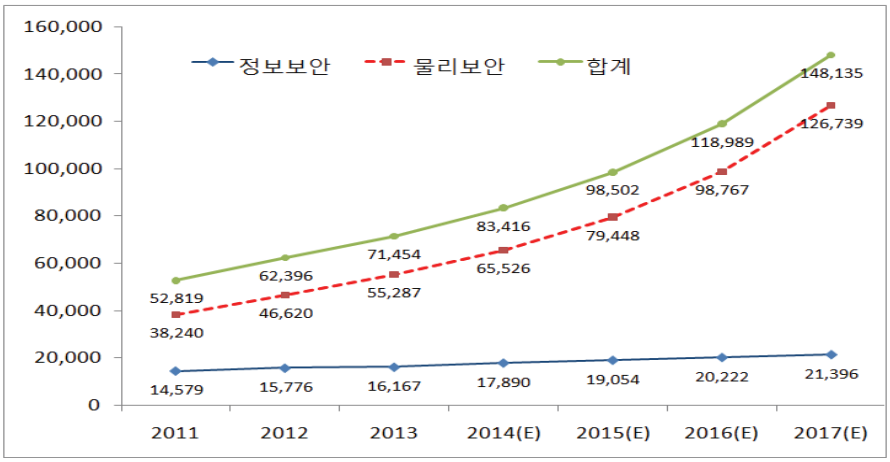
최근 인터넷 사용량의 증가와 스마트폰의 급속한 보급으로 인해 통신사 네트워크 보안의 중요성이 더욱 커지고 있다. 스마트폰 등 모바일 기기는 네트워크 위험은 물론이고 상대적으로 보안에 약한 무선랜이나 비인가장치 등을 이용하고 있어 보안상 위험이 높아지고 있다(정수민, 2013).

최근 IBM이 130여 개국 3,700여 고객사를 분석해 발표한 사이버 보안지수라는 보고서에 따르면 사이버 공격은 전 세계적으로 하루 38만 건, 연간 1억4,000만 건이 발생했으며 분야별로는 의료, 사회보장서비스, 운송서비스, 금융 및 보험 산업 순으로 나타났다.

KISA에 접수된 국내 개인정보 침해사고 건수는 2006년 2만3,333건, 2007년 2만5,965건, 2008년 3만9,811건, 2009년 3만5,167건, 2010년 5만4,832건, 2011년 12만2,215건, 2012년 16만6,801건(전년대비 26.7% 증가)로 최근 급속히 증가하고 있다. 이를 방지하기 위해 국내기업들의 원천기술 확보는 물론이고 일부 선진국들의 높은 기술력이나 특허권을 인수하거나 구매할 필요성이 제기되고 있다.

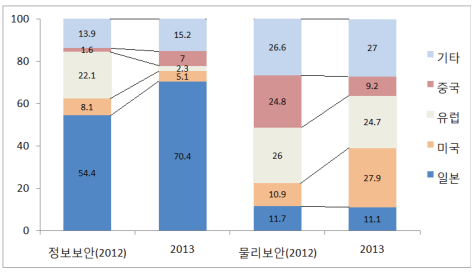
참고로 우리나라 사이버사령부의 2014년도 예산이 10억 원에 미치지 못하며 2013년에 처음으로 최정예 사이버보안인력 양성사업을 시작해 2017년까지 전문가 5,000명을 양성한다는 계획이다. 현재 국내 사이버보안 전문 인력이 200명 수준인 것을 감안할 때 미국, 중국, 북한 등과 비교하면 1/10 수준이다.

(단위 : 억 원)



자료 : KISA 2013, 하나대투증권

〈그림 5〉 한국 지식정보보안 산업 전망



자료 : KISA 2013, 하나대투증권

(단위 : 억 원, %)

구분	정보보안		물리보안	
	2012	2013	2012	2013
일본	54.4	70.4	11.7	11.1
미국	8.1	5.1	10.9	27.9
유럽	22.1	2.3	26	24.7
중국	1.6	7	24.8	9.2
기타	13.9	15.2	26.6	27

〈그림 6〉 국가별 수출 현황(2013년 기준)

〈표 3〉 지식정보보안 산업 수출 현황

(단위 : 억 원, %)

구분	정보보안			물리보안			합 계		
	2011년	2012년	2013년	2011년	2012년	2013년	2011년	2012년	2013년
수출액	450	587	699	11,450	13,987	14,788	11,900	15,574	15,487
증가율	30.4		19.0	22.2		5.7	30.9		6.3

자료 : KISA 2013, 하나대투증권

3. 보안 서비스시장의 성장

지난 2013년도 국내 지식정보보안 산업의 매출액은 7조1,454억 원으로 2012년 대비 14.5% 증가하였다. 이 중 정보보안 분야는 2.5% 증가한 1조6,168억 원, 물리보안 분야는 18.6% 증가한 5조5,287억 원으로 나타났다. KISIA(지식정보보안산업협회)는 지식정보보안 산업의 향후 매출액이 오는 2017년도까지 연평균 18.9%(정보보안 6.3%, 물리보안 22.1%) 성장할 것으로 전망하고 있다.

<표 4>에서 정보보안제품의 경우 네트워크보안제품 4,778억 원과 콘텐츠/정보유출방지제품 2,804억 원으로, 서비스의 경우 유지보수 769억 원과 보안관제 1,422억 원으로 높은 매출액을 보여주었다. 지난 2013년도 '3.20 전산망해킹'과 '6.25 사이버테러' 그리고 개인정보 대량유출사고 등으로 내부통제 강화와 보안 관리의 중요성이 강조되고 있기 때문으로 분석된다.

정보보안제품 규모를 보면 네트워크 보안 분야가 전체의 약 25%로 가장 큰 규모를 차지하고 있으며 개인정보 유출 등으로 콘텐츠/정보유출방지 분야에서 연평균 18%가 넘는 높은 성장세를 나타내고 있다. 시스템보안 및 암호/인증보안 분야의 규모와 성장세도 관심을 가지고 지켜보아야 할 것이다.

절대적인 규모에서 보안제품시장이 보안서비스시장을 월등히 앞서고 있지만 향후 보안서비스 분야가 성장 가능성이 높을 것으로 예상된다. 최근 정보보호시장은 보안관제 및 기업 보안에 대한 맞춤형 컨설팅을 제공하는 보안컨설팅 분야에서 각각 연평균 35%와 19%의 높은 성장률을 보이고 있다. 또한 교육훈련 분야는 아직 규모는 작지만 연평균 100%가 넘는 높은 성장세를 보이고 있다.

<표 5>에서 물리보안제품의 경우 블랙박스 등 기타제품에서 2,516억 원을, 출동보안서비스에서 1조2,880억 원으로 높은 매출액을 보여주었다. 최근 차량용 블랙박스가 대중화되면서 새로운 수요 증가는 물론이고 기존의 저화소 카메라와 아날로그 영상장비를 고화소 디지털 장비로 전환하는 수요가 증가하고 있기 때문으로 보인다(정수민, 2013).

물리보안제품 분야에서 IP 영상장치 및 바이오인식 분야가 높은 성장세를 보이고 있는데, 그 이유는 주차관제나 출입통제, 무선영상전송시스템 등 새로운 보안관련 서비스의 규모가 커지고 있기 때문으로 보인다. IP 영상장치는 약 80%에 가까운 성장세를 보이고 있어 각종 범죄 및 사고를 미리 예방하고 생활주변을 보호·감시하기

위해 영상보안서비스에 대한 관심이 높아지는 것으로 보인다.

<표 6>에서 정보보호 산업의 인력현황은 총 34,707명(2013년 기준)이며 이 중 정보보안관련 인력은 9,446명이고 물리보안관련 인력은 25,261명으로 조사되었다. 또한 정보보안기업 618개 중 340개(55%) 기업이 기업부설연구소를 운영하고 있으며 70개(11%) 기업이 연구개발 전담부서를 보유하고 있다(KISA, 2013).

〈표 4〉 정보보안 산업 분류별 매출 현황

(단위 : 억 원, %)

구 분		2009	2010	2011	2012	2013	평균성장률
정보보안 제품	네트워크보안	2,863	3,513	3,945	4,670	4,778	13.35
	시스템보안	1,008	1,168	1,705	1,684	1,701	15.4
	콘텐츠/정보유출방지	1,502	1,812	2,498	2,758	2,804	18.57
	암호/인증	588	685	1,125	1,126	1,136	20.18
	보안관리	901	1,092	1,255	1,179	1,197	8.03
	기타제품	708	898	811	1,090	1,097	12.78
정보보안 서비스	보안컨설팅	470	595	1,055	780	803	19.48
	유지보수	535	632	780	714	769	10.38
	보안관제	421	527	870	1,324	1,421	35.57
	교육훈련	29	30	55	277	425	134.83
	인증서비스	279	362	480	447	457	14.57

자료 : KISA 2013

〈표 5〉 물리보안 산업 분류별 매출 현황

(단위 : 억 원, %)

구 분		2011년	2012년	2013년	평균성장률
물리보안 제품	DVR	5,550	6,111	6,468	5.03
	카메라	8,030	10,405	12,592	25.30
	IP영상장치	1,560	3,699	4,512	79.64
	엔진/칩셋	960	1,009	1,157	0.10
	Solution	1,750	2,249	2,984	30.59
	주변장치	870	664	899	0.06
	Access Control	2,410	3,023	3,549	21.40

구 분		2011년	2012년	2013년	평균성장률
	바이오인식	1,250	1,716	2,062	28.73
	알람/모니터링	1,630	1,655	1,867	6.41
	기타	1,070	1,381	2,516	55.59
물리보안 서비스	출동보안서비스	10,280	11,347	12,880	11.96
	영상보안서비스	2,260	2,398	2,736	10.10
	기타보안서비스	620	961	1,063	32.81

자료 : KISA 2013

〈표 6〉 정보보호 산업 인력현황(2013년)

(단위 : 명, %)

구분	정보보안	물리보안	합 계				
			특급	고급	중급	초급	총합계
인원수	9,446	25,261	5,008	6,867	9,079	13,753	34,707
비 중	27.2	72.8	14.4	19.8	26.2	39.6	100

자료 : KISA 2013

4. 융합보안시장의 성장

지식보안시장은 정보보안과 물리보안의 기술이나 서비스를 결합한 융합보안시장의 성장에 관심이 높아지고 있다. 최근 미국은 중국의 해킹을 공개적으로 비난하고 있으며 중국 역시 자국의 해킹 피해 중 60% 이상이 미국 소행이라고 발표하면서 정보보안이 국가적인 관심사로 부각되고 있다.

융합보안은 시설경비나 출입통제 중심에서 최근에는 공공기관 및 대기업을 중심으로 수요가 확대되고 있다. 또한 보안의 중요성과 산업 간 융합이 확대되면서 금융 및 교육을 비롯하여 유통, 국방, 의료, 자동차산업에 이르기까지 범위가 신속하게 증가하고 있다(이홍표, 2013).

향후 보안시장의 성장률은 물리보안 10.3%, 물리보안 9.6%, 융합보안 20.9%로 예상되고 있어 융합보안시장의 높은 성장세가 기대되고 있다. 냉장고나 TV 등 가전제품이나 자동차까지 양방향 통신이 가능해지고 전기, 가스, 플랜트 등 국가 기간산업들이 모두 네트워크로 연결되면서 융합보안제품의 많은 성장이 전망된다.

융합보안관제시스템 분야가 확대되면서 <그림 7>과 같이 CCTV 및 영상보안시

스템 등을 기반으로 네트워크 사용현황, 네트워크 인증관리, 문서보안 관리 등을 포함하는 보안관제시스템에 대한 수요가 높아지고 있다. 스마트워크 환경이 증가하면서 스마트폰에 의한 정보유출 방지와 출입보안, 전자주민증 등의 분야에서 제품 및 서비스 개발이 진행되고 있다(조억래, 2013).

<표 7>에서 에스원은 대표적인 물리보안 기업으로 네트워크 보안장비인 UTM을 설치하여 해킹, 침입탐지 및 차단, 바이러스 스팸 차단, 원격 관제 및 제어 서비스를 제공하고 있다. ADT캡스는 무인경비서비스, 고화질 CCTV에 의한 영상감시, 출입통제, 도난방지솔루션, 빌딩 통합관리 솔루션 등을 통합적으로 제공하는 서비스로 시장에 진출하고 있다.

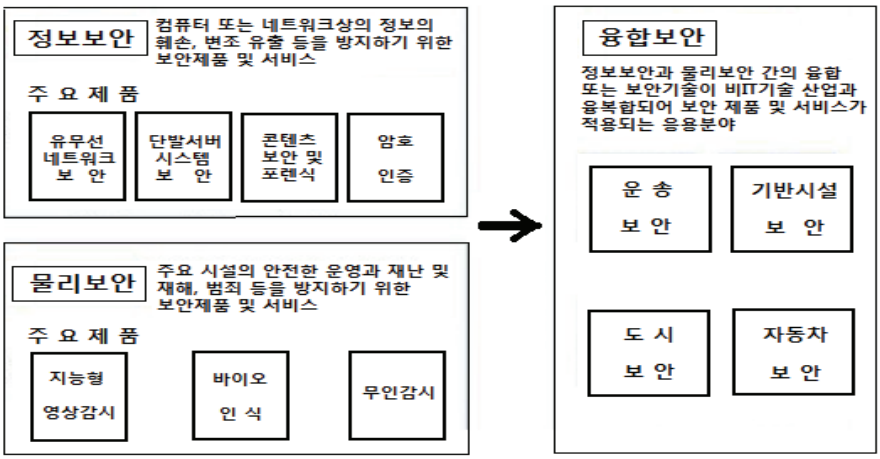
이글루시큐리티는 차세대 융복합 보안 선도기업으로 보안 솔루션 및 관제 서비스 전문기업이다. 차세대 통합 보안관리 플랫폼인 IS-CENTER를 통해 주력제품인 IS-ESM을 공급하고 있으며 국내 ESM(Equipment Service Management) 시장의 80% 이상을 점유하고 있다. 롯데정보통신은 시스템관리, 시스템통합, IT 컨설팅, e-Biz 등 체계적인 IT서비스를 제공하는 IT서비스 전문기업이다.

안랩(Ahnlab)은 한국 정보보안업계 1위로 컴퓨터 바이러스 백신 소프트웨어 V3로 잘 알려진 기업이다. 주요 제품으로 V3 365 클리닉(개인용 백신 소프트웨어), V3 Internet Security 9.0(기업용 백신), TrusGuard(기업용 방화벽 시스템) 등이 있으며 바이러스, 스파이웨어, 해킹차단, 보완관리, V3, 디도스 전용 백신 다운로드 안내로 알려져 있다.

〈표 7〉 국내 주요 보안기업의 융합보안사업 및 서비스

기업명	솔루션	주요 내용
에스원	에스원엑세스	관제 상황실, 종합건물관리 시스템, 통합 보안 시스템 등 다양한 빌딩통합관리시스템
ADT캡스	ADT Calm	침입감지, 영상모니터링 등 보안과 가스, 조명제어, 누수감지 등 에너지관리까지 스마트폰을 통해 모니터링 제어가 가능한 첨단보안솔루션
안랩	차세대 원격관제 서비스	APT 공격의 시도, 내부 침투 성공, 악성코드 확산, 정보유출 등 각 단계에서 정교하게 모니터링하여 정보 유출을 방어
롯데정보통신	제주도 스마트그리드 실증단지 토탈 보안서비스	다양한 모델의 전기차 충전 스탠드와 차량인식 등 고객서비스 제공과 복합 통신망의 실시간 대용량 정보처리 및 보안기술을 접목
이글루시큐리티	라이거원	방화벽, 해킹탐지, 가상 시설망 개설 등 여러 종류의 인터넷 기반 보안솔루션을 통합한 시스템

자료 : 하나대투증권



자료: KISA 2012, 우리투자증권

〈그림 7〉 융복합 보안의 정의

5. 융합보안시장의 주요 이슈

최근 금융권에서 개인정보가 대량으로 유출되면서 개인정보보호관련 컨설팅서비스나 E-DRM[6], DLP[7] 등 보안관련 솔루션에 대한 관심이 높아지고 있다. 스마트그리드 보안은 통신단말 자동인증 및 대규모 복합통신망 보안키 관리, 지능형 임베디드 시스템 보안, 유무선 연계통신망 보안, 전력망 보안 사전진단 및 분석에 대한 수요가 증가하고 있다(정수민, 2013).

자동차산업에서는 블랙박스를 포함하여 지능형 CCTV 시스템에 대한 수요자들의 기대가 기존 CCTV 통합관제 시스템보다 더 획기적인 시스템으로 예상하고 있다. 최근에는 CCTV 통합관제 시스템이 일정 반경 이내의 상황을 실시간으로 인지하여 경보를 발령하는 방식으로 시스템 기술이 진화하고 있으며 사생활 침해 같은 사회문제도 해소되는 방향으로 개발되고 있다(정수민, 2013).

6) 암호화 솔루션을 DRM(Digital Rights Management)이라 하고 기업에서 사용하는 정보유출방지 솔루션을 E-DRM이라 한다. 문서나 도면을 자동 암호화 해주고 암호화된 상태로 유통시키므로 보안성이 높다.

7) Data Loss Prevention(기업데이터 유출방지)은 사용자가 사무실, 집, 현장, 등 업무 중에 사용자의 PC에서 기업 내 기밀 자료가 외부로 반출되는 것을 항시 감시하고 기록하며 유출을 차단시키는 것을 구현한 솔루션이다.

U-헬스케어는 미국이나 유럽 등에서 이미 비즈니스로 활발히 진행되고 있어 위험도의 임산부, 만성질환자, 심장질환자 등을 대상으로 지속적인 환자 모니터링을 통해 질병 판단 및 예측, 응급상황 대처 등의 서비스를 제공하고 있다. 암과 같은 질병의 환자들에게는 집에서 원격 모니터링 및 진단 서비스를 받을 수 있으며 의료 케어 및 환자의 이동 등의 데이터를 실시간으로 의료기기에 전송하는 RFID (Radio-Frequency Identification) 센서 응용연구가 진행되고 있다. 따라서 의료산업 분야에서는 센서 간 통신 및 데이터 송수신을 위한 유무선 네트워크, 바이오 데이터 분석과 건강 피드백을 담당하는 의료정보서버 등에 대한 환자의 정보에 대한 보안 및 프라이버시를 보호하기 위한 보안관리 기술의 개발이 요구된다.

금융 산업에서는 최근 인터넷뱅킹 및 스마트폰뱅킹의 가입자가 증가하고 이용금액이 증가하면서 이에 대한 보안관련 기술수준이 가장 높게 요구되고 있다. 최근 발견된 '하트블리드' 보안 취약점으로 정보기술 및 보안업계가 긴장하고 있으며 안드로이드 스마트폰과 태블릿에도 결함이 있는 것으로 나타나 사용자들의 주의가 요구되고 있다(Gueguen, G., 2009).

구글 온라인보안 블로그에 따르면 안드로이드 4.1.1 젤리빈은 하트블리드 보안 취약점을 가지고 있어 앞으로 해커들이 등장할 가능성이 제기되고 있다. 금융기관의 개인정보 유출이나 서버 마비, 악성코드 침투, 해킹 등은 심각한 수준의 금전적인 피해를 야기하면서 신용도를 떨어뜨릴 수 있어 관련 보안기술에 대한 높은 관심이 요구된다.

〈표 8〉 융합보안의 다양한 범위

	종 류	주요 기술
융합보안	지능형 차량 보안	라우팅 테이블 및 LDM의 변조 공격 방어, 차량 통신 메시지의 도청 공격 방어, 프라이버시 보호 등
	U-헬스케어 보안	시스템 오류나 결함 등으로 일어날 수 있는 의료사고로부터 환자의 건강을 지키기 위한 표준기술
	금융 보안	전자금융사기 방지, 고객정보보호 준칙, 인터넷뱅킹 거래 보안, 모바일 뱅킹 보안 등
	스마트그리드 보안	지능형검침인프라(AMI) 암호인증, 해킹이나 바이러스 침투 방어, 차세대 전력 시스템 보안
	주력산업 보안	금융/유통/국방/반도체/통신/조선 산업 등 보안

자료 : 하나대투증권

Ⅳ. 지식정보보안 산업의 육성방안

국내 지식정보보안 산업을 육성하기 위해서는 보안정책과 법을 만들어 정보보호 산업을 발전시키고 예산을 확보해 보안 산업을 육성시키는 동시에 우수한 인재 양성에 많은 노력을 기울어야 할 것이다.

최근 정보기술(IT) 산업에 대한 의존도가 커질수록 개인정보유출 등 사이버 보안 사고는 개인·단체·기업을 넘어 IT 산업 전체에 큰 위협으로 다가오고 있다. 최근 나타난 보안 사고는 IT산업 분야의 빠른 발전에 비해 상대적으로 정보보안 산업이 발전하지 못했기 때문으로 보인다. 앞으로 보안 산업에 대한 법과 제도를 정비하고 정보보안 인재양성을 통해 핵심기술을 개발할 수 있는 여건을 조성해야 할 것이다(손경호, 2010).

정보보안 산업은 향후 개인의 사생활뿐만 아니라 국가의 안보를 책임지는 중요한 분야이므로 국민과 국가의 자산을 보호하기 위해 외부 공격을 방어하는 것은 중요한 역할이다. 이를 위해 전문적인 보안전문가를 양성하기 위한 교육기간이 필요할 것이며 도덕성을 갖춘 전문가로 성장할 수 있도록 기반여건을 조성해야 할 것이다(전효정·김태성, 2013).

우리나라는 전 세계에서 정보기술의 의존도가 가장 높아 사이버 보안 사고의 빈도가 가장 빈번하게 나타나고 있다. 이를 방지하기 위해 지식정보보안 산업 발전을 위한 정책 제안과 신규 사업 발굴, 인재양성, 네트워크 형성 등을 위한 노력이 필요해 보인다. 정보기술의 수준은 세계적인 수준이지만 보안 제품 및 서비스와 관련해서는 미국이나 유럽의 글로벌기업에 비해 경쟁력이 미약한 수준이어서 국가적인 차원에서 기술력 지원이 요구되는 시점이다.

정보보안 강화 및 보안시장 확대를 위해서는 일정부분 정부의 규제강화와 육성정책이 필요해 보인다. 정보보안 산업의 인프라조성을 위해 산·학·연 연구협력을 통해 지식정보보안 조직의 확대가 요구된다. 수출경쟁력 제고를 위해 업체가 공동으로 참여하는 수출컨소시엄을 구성하고 해외 로드쇼 개최 등 수출마케팅 전략이 필요하다(정태근, 2010).

지식정보보안관련 핵심기술 개발을 위한 연구 개발의 예산 확대가 정부차원에서 이루어지고 해외 수출지원 및 홍보활동에 노력해야 한다. 또한 여러 산업과의 연계강화를 통해 신규 융합보안시장을 창출하고 이를 위해 공동 플랫폼화 및 커스터 마

이징 강화를 통한 여러 산업의 응용보안기술을 확보해야 한다.

지식정보보안 산업의 발전을 위해 시장중심의 인재를 육성하고 학계와 연계하여 교육과정의 신설 및 강화가 요구된다. 글로벌 기업과의 경쟁력 강화를 위해 교육의 질적 수준을 향상시키고 대국민 보안의식을 높이기 위한 노력이 병행되어야 할 것이다.

최근 정부에서는 정보보호시장 확대 기반조성, 기술경쟁력 강화 촉진방안 마련, 정보보호 전문 인력양성 지원, 글로벌 정보보호기업 육성 등의 「정보보호산업진흥법」을 마련하여 정보보호 산업의 기반을 구축하고 경쟁력을 강화하고자 시도하고 있다. 정보보호 산업 활성화를 위해 정보보호 제품과 서비스의 수요 증대를 위한 규정을 마련하고 민간기업의 정보보호 책임 강화를 위해 융합형 정보보호 기술 및 서비스 개발을 위한 정책을 수립하고자 한다.

또한 정보보호 산업 전문 인력양성을 위한 시책을 수립하고 정보보호 제품과 서비스 등에 대한 품질인증 제도를 도입하고 체계적인 사업 지원을 위해 전담기관을 운영할 계획으로 있다. 정보보호 기업이 생산한 제품 및 서비스에 대한 영업이익 침해 금지 규정을 만들어 정보보호 산업관련 제품 및 서비스의 이용자 기본 권익 보호를 위한 대책도 마련할 계획으로 있어 조속한 실행이 요구된다.

지식정보 보안시장의 규모를 증대시킬 수 있도록 관련 규정들이 제정되어야 하며 기술과 서비스의 향상은 물론 정보보안전문 인력양성과 보안의식 제고에 더 많은 관심을 가지는 방향으로 나가야 할 것이다. 국내 정보보안 기업들의 글로벌시장 진출을 위해 규모의 확대가 필요하며 이를 위해 정보보안업체 간 M&A가 촉진될 수 있도록 관련 제도의 정비가 필요해 보인다.

Ⅴ. 결 론

최근 우리나라는 카드3사의 개인정보 유출 등으로 보안 산업에 대한 관심이 높아지고 있으며, 미국도 대형 유통업체 "TARGET"의 고객정보 유출 사건 등으로 보안 산업에 대한 관심이 높아지고 있다. 경영자들은 개인정보 유출 등 보안 사고에 의한 피해가 어떠한 재무적 위험보다도 더 위험한 요소로 인식하게 되었다.

지식정보보안 산업은 과거 PC 및 서버시스템 보안 등 네트워크 보안에서 최근에는 사회 안전 및 시설보안 등 융합 산업 보안으로 진화하고 있다. 관심분야도 방화벽

이나 Anti-virus 등 네트워크 보안에서 스마트폰보안 및 지능형영상보안 등 융합보안 산업으로 변해가고 있다.

융합보안은 시설경비나 출입통제 중심에서 최근에는 공공기관 및 대기업을 중심으로 수요가 확대되고 있으며 금융, 교육, 유통, 국방, 의료, 자동차산업에 이르기까지 범위가 빠르게 증가하고 있다. 향후 보안시장의 성장률은 물리보안 10.3%, 물리보안 9.6%, 융합보안 20.9%로 예상되고 있어 융합보안시장의 높은 성장세가 기대되고 있다.

융합보안시장은 지능형차량 보안, U-헬스케어 보안, 금융 보안, 스마트그리드 보안, 주력산업 보안 등 다양한 분야에서 제품 및 서비스가 개발되고 있으며 시장이 확대되고 있다. 특히 금융기관은 개인정보 유출이나 서버 마비, 악성코드 침투, 해킹 등은 심각한 수준의 금전적인 피해 및 신용도를 떨어뜨릴 수 있어 관련 보안기술에 대한 높은 관심이 요구되고 있다.

지식정보보안 산업은 향후 개인의 사생활뿐만 아니라 국가의 안보를 책임지는 중요한 분야이므로 국민과 국가의 자산을 보호하기 위해 외부 공격을 방어하는 것은 매우 중요한 일이다. 이를 위해 전문적인 보안전문가를 양성하기 위한 교육기간이 필요하고 전문가로 성장할 수 있도록 교육여건을 조성해야 할 것이다.

우리나라는 전 세계에서 정보기술의 의존도가 가장 높은 반면 보안 사고도 가장 빈번하게 발생하고 있다. 이를 방지하기 위해 지식정보보안 산업 발전을 위한 정책 제안과 신규 사업 발굴, 인재양성, 네트워크 형성 등을 위한 노력이 필요해 보인다. 국내기업의 보안 제품 및 서비스 수준이 미국이나 유럽 등 글로벌기업에 비해 경쟁력이 미약하므로 국가적인 차원에서 기술력 지원이 요구되는 시점이다.

지식정보보안 산업의 발전을 위해 시장중심의 인재를 육성하고 학계와 연계하여 교육과정의 신설 및 강화가 요구된다. 글로벌 기업과의 경쟁력 강화를 위해 교육의 질적 수준을 향상시키고 동시에 대국민 보안의식을 높이기 위한 노력이 병행되어야 할 것이다. 개인정보보호에 대한 중요성을 인식시키고 자신의 사이버 공간을 보호할 수 있는 능력 향상과 민간부문지원을 확대시켜 나가야 할 것이다.

지식정보 보안시장은 창조경제의 핵심으로 앞으로 중요성은 더욱 커질 것으로 보인다. 하지만 정부의 정보보안정책은 통제하고 관리하는 방식의 사후 보완대책으로 일관해 왔다. 앞으로 지식정보보안 산업의 발전을 위해서는 새로운 사업을 발굴하고 전문인력 등을 양성해야 한다. 이를 위해 학계와 산업계 등 다양한 의견을 반영할 수 있는 전문기관의 필요성을 제기해 본다.

참고문헌

1. 국내문헌

손경호(2010), "정보보안 산업 혁명 및 전망", 정보과학지, 제28권 11호, 한국정보과학회, pp.72-78.

안황권·박영만(2009), "민간 경비 산업의 경영환경(SWOT) 분석과 활성화 전략", 한국경호경비학회지, 제20호, 한국경호경비학회, pp.229-248.

이홍표(2013), "융합이 대세 - 스몰캡-보안 산업 진화하다", 한경비즈니스, 통권 915호, pp.50-51.

이창무(2010), "우리나라 보안 산업의 역사적 기원에 관한 연구", 한국경호경비학회지, 제22호, 한국경호경비학회, pp.91-111.

전효정·김태성(2013), "가치사슬을 통한 지식정보보안 산업의 애로사항 분석", 한국IT서비스학회, 제12권 제1호, 한국IT서비스학회, pp.229-245.

정수민(2013), "보안산업, 진화하다", 스몰캡 Issue Report, 하나대투증권, pp.1-19.

정태근(2010), "지식정보보안 산업 살린다! : 인터넷, 스마트폰, 웹뷰어 등 사이버세상은 더 이상 안전지대가 아니다", 중소기업을 살린다. 제10호, pp.1-30.

정태황(2009), "RFID의 보안업무 적용환경과 적용방안에 관한 연구", 한국경호경비학회지, 제21호, 한국경호경비학회, pp.155-175.

정태황·소승영(2010), "기계경비의 발전적 대응방안에 관한 연구", 한국경호경비학회지, 제22호, 한국경호경비학회, pp.145-168.

조억래(2013), "빈틈없이 막는 융합보안이 뜬다.", Weekly Issue, 우리투자증권, pp.9-12.

최진혁(2010), "산업보안의 제도적 발전방안 연구", 한국경호경비학회지, 제22호, 한국경호경비학회, pp.197-230.

한국인터넷진흥원(2012, 2013),「세계 지식정보보안 산업 비교 분석 : 지식정보보안 산업 심층 분석보고서」, 연구자료, pp.1-61.

2. 국외문헌

Gueguen, G.(2009), "Coopetition and business ecosystems in the information technology sector : The example of intelligent mobile terminals", International Journal of Entrepreneurship and Small Business, Vol.8, No.1, pp.135-153.

IDC(2010), Korea Security Software 2010-2014 Forecast and Analysis 2009 Year End Review

IDC.

Lazarica(2011), M., 'Business ecosystems vs business digital ecosystems", EIRP(International Conference on European Integration-Realities and Perspectives) Proceedings.

3. 기타자료

www.csokorea.org : 한국CSO협회

www.kisa.or.kr : 한국인터넷진흥원

www.kisia.or.kr : 한국지식정보보안산업협회

【Abstract】

Status and prospects of Knowledge Information Security Industry

Choi, Jeong-Il
Chang, Ye-Jin
Lee, Ok-Dong

Korea is concerned with information security industry due to recent leak-out private information of 3 card companies. Executives are aware of damage from breach of security such as personal data spill, is more dangerous than any other financial risks.

The information security industry, which was limited in physical security and network security formerly, is evolving into convergence security of public and facility security industry. The field of interest has also been changed into security of smart phone and intelligence image recently, from firewall or Anti-virus.

The convergence security is originally about access control of facility, but recently its demand has been increased mostly by public institutions and major companies. The scope of the industry also varies from finance, education, distribution, national defense, medical care to automobile industry.

The market of convergence security has been expanded and new various products and services of security of intelligent vehicle, 'U' healthcare, finance, smart grid and key industries are also developed.

It is required to create and enhance of new curriculum and cultivate human resources for the development of knowledge information security industry. Raising standard of education and security consciousness of the nation is also necessary to strengthen the global competitiveness.

Key words : Knowledge information, Security industry,
Convergence security, Physical security, Information security