국가 산업기술유출 대비 방안 연구

하 옥 현*

요 약

산업보안은 보안의 영역별 요소(물리적 보안도구, IT보안 도구, 융합보안도구)를 활용하여 기업의 산업자산을 보호하는 관리활동들로서 Hardware적 요소(보안을 위한 도구)의 운용은 물론 이를 활용하기 위한 Software적 측면(정책 및 전략수립, 유지운영, 사후 대응조치 등)을 포괄하는 개념으로 이해할 수 있다.

본 논문에서는 산업보안에 대한 정의와 관련 개념, 우리나라의 산업보안 관련 기관들의 역할과 관련 법규, 관리체계 및 실태 등을 살펴보고, 이에 따른 문제점을 파악하여 개선방안을 제시하려 한다. 아울러 우리나라 기업들이 효과적인 산업보안활동을 통하여 국가경쟁력을 제고하고 21세기 산업보안 선진국으로 진입하기 위한 향후 정책방향과 시사점을 제안하고자 한다.

A Study on Preparation Plan against National Industrial Technology Outflow

Ok Hyun Ha*

ABSTRACT

Industrial Security is a management activity protecting industrial asset of enterprise by application of security elements(physical, IP, conversion security tools) and can be understood as a comprehensive term including software aspect(establishment of policy and strategy, maintenance operation, post- response act, etc.) as well as the operation of hardware elements.

In this paper, after recognizing the definition and relative concept of industrial security, the role and its relative laws of the industrial security organizations, the management system and the reality, I will find some problems and submit a reform measure. Furthermore I would like to propose the policy direction to enhance the national competitiveness and to become one of the advanced nations in 21st industrial security through the effective industrial security activities of our enterprises.

Key words : Industrial Security

접수일 : 2009년 11월 23일; 채택일 : 2009년 12월 20일

* 호남대학교 경찰법행정학부 교수

1. 서 론

산업보안이란 “보호할 가치가 있는 산업자산의 안정성 유지를 위해 인위적·환경적 위험요소들을 관리하는 제반활동”을 의미 한다[1].

일반적으로 보안(security)의 핵심개념에는 안정성 유지와 위험관리라는 두 측면이 있으며 산업보안은 산업부문의 보안활동을 의미하는 폭넓은 개념이다. 세계최대 보안전문가 모임인 미국 산업보안협회(ASIS)에서는 보안(security)의 정의를 “사람, 자산 그리고 정보의 보호에 관한 업무”로 명시하고 있으며, “자산보호”, “화재와 안전”, “범죄예방과 통제”, “형사사법”의 의미를 포함하는 것으로 규정하고 있다. 지식정보 시대에 들어와서는 산업보안은 IT보안과 서로 개념적으로 혼용되고 있기도 하다. 이는 관점의 차이로 통상적으로는 IT보안이 산업보안보다 더 광범위한 개념들을 포함한다고 볼 수 있으나 보안의 객체를 산업자산으로 한정지을 경우 IT보안은 산업보안의 하위범주에 속하게 된다[2, 3].

우리나라에서는 아직까지 산업보안에 대한 명확한 개념이 정립되지 않고 있는데 그 이유로는 지금까지는 실용적 관리기술의 중요성이 강조되어 왔고 산업보안이 상황에 따라 변화하는 전략적인 성격이 강한 관리기법인 관계로 산업보안 관련 주변여건에 따라 그 영역과 관리기법등이 달라졌기 때문이다. 따라서 산업보안의 체계적인 연구 활동 활성화와 관리기술[4]의 발전을 위해 이에 대한 정의와 개념을 명확히 하는 것이 중요하다 하겠다.

2. 산업보안의 개념적 구성요소

산업보안에 영향을 주는 요인들은 국내외 산업환경, 정치·사회적 구조, 산업의 규모와 기술수준, 보안주체와 조직원들의 의식과 문화, 보안기술 등이 있으며 산업보안의 개념을 구성하는 요소들을 살펴보면

① 산업보안의 주체 : 산업기술의 개발·활용·보급에 관련된 모든 기관과 경영에 필요한 영업비밀 및 지식재산권을 보유한 국가기관·연구기관·기업·대학 등을 비롯한 법률상 영업상의 실체

② 산업보안의 목적 : 기업이 추구하는 최고가치인 이윤추구와 경쟁력확보를 위함이며 여기에 기업의 명예와 안전유지도 포함

③ 보호가치 : 산업경쟁력 확보 및 이윤창출에 유용한 기술이나 지식, 기업의 활동과 경영상에 필요한 정보 및 영업비밀, 노하우(knowhow), 지식재산권 등 유무형의 가치를 보호대상으로 함

④ 산업보안의 객체 : 보안관리 대상을 말하며, 보호해야할 가치를 지니고 있거나 비밀의 인지 또는 접근가능한 모든 인적·물적 요소들을 의미함.

⑤ 침해요소 : 보안의 가장 취약요소는 내부인으로 산업기밀 유출 및 누설사고의 대부분이 전·현직 임직원에 의한 것이거나 이들과 연관된 산업스파이·경쟁업체 등의 인적침해가 가장 큰 실정. 그러나 보호가치를 파괴·훼손하는 위해요소에는 화재·홍수·태풍 등 자연재해와 방화·테러 등 인위적 재난도 포함됨.

⑥ 대응수단 : 보안활동의 목표는 예방관리에 있다. 위험을 예측하고 이를 예방하기 위해 물리적, 기술적 수단 외에 관리적 수단도 동원되어야 하는데, 이러한 대응수단은 사회 환경의 변화와 과학기술의 발전으로 계속 진화하고 있음

다음의 <표 1>에서 처럼 산업보안을 국가보안과 비교해 볼 때 보안의 주체와 목적, 가치판단기준 및 관리체계가 다를 뿐 보호객체와 침해요소가 상호 연결되어 있고 대응수단은 동일한 기술적 측면을 지니고 있으므로 산업보안은 국가보안의 하

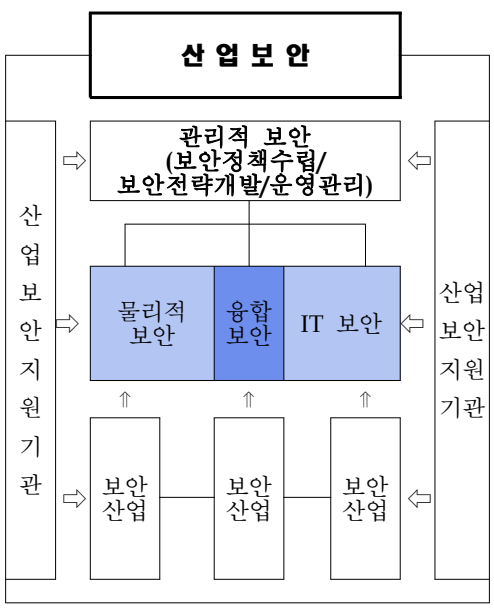
위개념으로 인식되어야 한다.

또한 산업보안의 객체가 국가경쟁력과 관련될 경우 공익성을 띠게 되어 산업보안이 국가와 기업의 공동목표가 되므로 국가는 비강제적·비법률적 성격의 행정지도를 통해 지도하는 것이 바람직 하다.

〈표 1〉 산업보안과 국가보안의 관련성

	산업보안	국가보안	관련성
추구 목표	산업자산 보호	국가기밀보호	상호의존적, 보완적
가치 기준	기업성 + 공익성	공 익 성	상호의존적
행위 주체	개별기업	국가기관	국가의 행정지도
관리 체계	자율적	통일성·일관성	국가의 행정지도

산업보안은 보호객체와 취급영역에 따라 다음과 같이 구분된다.



(그림 1) 산업보안 개념 체계화

- 관리적 보안 : 보안정책·보안전략의 수립과 운영을 위한 산업보안의 핵심역량[5]
- 물리적 보안 : 시설물, 유·무형 자산의 입·반출 통제에 의한 산업자산의 보호
- IT 보안 : 네트워크를 통해 유출 가능한 지식정보의 보호
- 융합 보안 : 지식정보보안과 물리적 보안의 방법들이 상호 결합된 형태의 산업자산보호 또는 제품자체에 보안기능이 탑재·내장된 형태의 산업자산 보호

이상의 영역별 산업보안 분야를 개념적으로 체계화 시켜 보면 (그림 1)과 같다.

물리적 보안·IT보안·융합보안의 영역은 관리적 보안을 위한 수단으로 이해가능하며, 각 산업보안의 영역별 활성화를 위해 보안 산업의 발전이 요구됨을 알 수 있다.

3. 국내외 산업보안 현황

3.1 선진국의 산업보안 정책동향

3.1.1 미 국

9.11 테러 이후 美 연방 정부는 국토보안 강화를 위하여 법·제도를 대대적으로 정비하였다. 즉 국토안보법, 대테러감시법, 디지털 밀레니엄 저작권법, 전자서명법, 프라이버시보호법, 전자정부법 등 19개 보안 관련 법률들을 제정하였다.

이에 따른 보안 관련 정책 강화로 지식정보보안 제품 및 서비스 시장에 대한 유효 수요가 대폭적으로 증가하게 되었다. 또한 「Making the Nation Safer(2002)」의 일환으로 자연재해·재난·테러 등 국가재난 대응 R&D 프로젝트에 지속적 투자 하였고, 특히, 2009년 R&D 예산은 약 33억 달러로 전년대비 187.6% 증가(과학기술 예산의 2.2%) 하였다.

국토안보부 산하 '사이버보안R&D센터', 미국 국

방부 산하 'DARPA' 등에서 보안 관련 원천기술 개발을 중점 추진 중이다.

미국에서 영향력이 강한 정보보호관련 법규로는 Gramm-Leach-Bliley Act of 1999(금융기관의 고객 개인정보 보호를 강화하기 위한 가이드라인 등 규정), Health Insurance Privacy and Accountability Act of 1996(개인의료정보의 전자데이터 보호를 의무화하는 규정), Federal Information Security Management Act of 2002(연방정부의 정보보호를 확보하기 위한 체계 규정) 등이 있다.

정보보호에 관한 기본전략으로는 2003년 2월 수립된 국토안보부(DHS)의 'National Strategy to Secure Cyberspace'이 있으며 여기에는 국가 사이버 안보를 위한 민·관 협력관계 구축, 사이버안보 연속성확보, 범 국가적 정보보호 인식프로그램 등의 과제가 있다. 2008년 9월 9일 국토안보부는 국토안보 전략계획(2008년~2013년) 'One Team, One Mission, Securing Our Homeland'를 발표하였는데, 여기에는 정보보호 관련 국가 중요인프라와 자원보호를 강화하고 정부통신시스템의 연속성 확보 및 사이버 보안역량 강화전략 등의 내용을 포함한다. 2009년 오바마(Obama) 대통령의 지시로 60일간에 걸쳐 기존의 사이버안보관련 정책을 재검토하여 'Cyberspace Policy Review'를 내놓고 사이버안보를 최우선과제로 선정하였다. 전반적으로 사이버 보안정책의 중요성이 증대되면서 미국정부에서 사이버보안정책의 위상은 점진적으로 격상되고 있다.

3.1.2 E U

EU집행위원회 산하 "정보사회미디어이사회(ISMDG)"는 2006년 '안전한 정보사회 구현전략'을 기획하고 이해 관계자간 활발한 대화, 긴밀한 파트너십, 정부·기업역량강화라는 3대 정보보호전략을 제시했다. 정보보호 전담기구인 '유럽네트워크보안청(ENISA)'의 역할을 규정 하고 인터넷 등 유럽e-커뮤니케이션 네트워크 탄력성(Resilience) 향상시켰으며, 회원국의 정보보호 역량을 강화하고 상호협력 및 공조체계 강화하였다.

공공·민간의 다양한 포럼활용 등 미래 위험분석 프레임워크를 수립하고 2009년부터 안전한 인터넷 환경 및 이용자 보호계획을 추진하여 소셜 네트워킹(Social Networking), 불법 유해정보 차단을 위한 인식제고, 신고 및 보고체계, 자율규제 촉진, 지식기반 구축 등의 사업을 전개하고 있으며 최근 2013년 2월까지의 계획을 담은 '안전한 인터넷 프로그램(2009년~2013년)'을 수립하여 추진 중이다.

3.1.3 일 본

정보보호 정책은 내각관방에서 총괄하고 있으며, 산업정책은 경제산업성에서 주관하고 있다. 내각관방에서는 정보보호요구에 대응하기 위해 2006년 2월 국가 전반의 '제1차 정보보호 기본계획'을 수립하여 추진하고 있으며 2009년 현재 '제2차 정보보호 기본계획'을 마련 중이다.

정부 주요 인프라, 민간(개인 및 기업)을 대상으로 정보보호 기본계획 주요대책을 2006년부터 2008년까지 3년간 추진하였고, 정부·지방공공단체, 주요기반시설, 기업, 개인영역으로 구분하여 매년 'Secure Japan 200X'를 수립하고 실행 성과를 평가하였다. 총무성에서는 U-Japan 정책을 통해 정보화 역기능에 관한 100대 과제를 정리한 'ICT 안심·안전 21 전략'을 추진 중이며, 경제산업성에서는 2007년 5월부터 정보보호 위협에 대한 국제적 대응, 국제경쟁력강화 기반마련, 국내·외 다양한 환경변화에 대응하기 위한 글로벌 정보보호 전략을 수립하여 추진했다.

3.1.4 영 국

2007년 정보보증관련 업무를 총괄하는 정보보증 중앙지원국에서 '국가정보보증전략(A National Information Assurance Strategy)'을 발표. 이를 통한 기관의 효율적인 위협정보 관리를 위해 임원급

의 책임과 의무를 강조하는 한편, 전문기술 인력양성 및 홍보를 통해 정보보증의 발전을 진행해 나가는 중이다.

2008년 내각부에서는 정부기관의 보안정책을 확산시키기 위한 정보보호 기본정책(Security Policy Framework)을 통해 정보보호 및 정보보증 관련정책을 발표 하였다.

2008년 총리의 지시에 따라 'Safer Children in a Digital World' 보고서를 작성하였는데, 보고서의 권고사항에 따라 세계 최초로 아동을 위한 아동인터넷안전위원회(UK Council for Child Internet Safety)를 창설하였다.

3.2 국내 산업보안 관리 현황

3.2.1 산업기술의 유출현황

〈표 2〉 연도별 산업기술 유출 적발실적[6]

구 분	계	2004년	2005년	2006년	2007년	2008년
건 수	160	26	29	31	32	42
예방액	253조 4,500억	32조 9,270억	35조 5,000억	13조 5,730억	91조 6,500억	79조 8,000억

<표 2>에서 발생건수가 연도별로 증가하는 추세이며, 유출분야도 전기·전자분야에서 다양한 산업분야로 확산 되고 있다. 기업규모별로는 대기업보다는 중소·벤처기업에서의 유출건수가 지속적으로 증가 했다.

〈표 3〉 기술유출 분야[6]

구분	계	전자	정보통신	정밀기계	생명공학	정밀화학	기타
건수	160	73	27	23	6	10	21
비율(%)	100	45.6	16.9	14.4	3.8	6.3	13.1

<표 3>에서 국가 전략산업인 전자·정보통신 부문의 유출사건이 62%를 차지했으며, 중소·벤처기업의 비중이 높아지는 가운데 기술유출 산업분야가 다양하게 확산 하였다.

<표 4>는 전·현직 직원을 통한 유출건수가 전체의 82.5%를 차지했다.

〈표 4〉 기술 유출 주체[6]

구분	계	전직원	현직원	협력업체	유치과학자	투자업체	기타
건수	160	89	43	16	6	3	3
비율(%)	100	55.6	26.9	10.0	3.8	1.9	1.9

〈표 5〉 기술 유출 유형[6]

구분	계	매수	무단보관	공동연구	위장합작	내부공모	기타
건수	160	89	30	9	6	17	9
비율(%)	100	55.6	18.8	5.6	3.8	10.6	5.6

<표 5>는 전·현직 직원의 금전적 매수를 통한 기술유출 유형이 전체의 55.6%를 차지하고, 내부공모에 의한 유출도 10.6%를 차지 했다.

〈표 6〉 기술유출 동기[6]

구분	계	개인영리	금전유혹	처우불만	인사불만	비리연루	기타
건수	160	68	52	16	11	4	9
비율(%)	100	42.5	32.5	10.0	6.9	2.5	5.6

<표 6>은 개인영리와 금전적 유혹의 비율이 75%를 차지하며, 조직에 대한 불만에 의한 기술유출 동기도 17%를 차지하는데, 이는 전체 유출사건의 92%를 차지하는 동기요인으로 작용했다.

4. 국가 산업보안 중장기 발전전략

5. 부분별 추진과제

5.1 정책부분

5.1.1 산업보안 유관 개념들의 재정의·재분류

산업보안 관련개념들의 조작적 정의 명확화가 필요하며, 산업기술의 분류체계 단일화를 통한 기업의 이해와 관리용이성 확보가 필요하다.

5.1.2 산업보안 관리 · 지원조직 정비

산업보안관련 업무를 총괄할 관리·지원조직 정비하고, 산업보안 통합인증을 통한 관리효율성 제고 및 유관기관·기구와의 유기적 협조체계 구축이 필요하다.

5.1.3 법제 정비 및 홍보

미래지향적 산업보안 법률 및 제도 정비가 필요하고, 산업자산의 등급화 기준 및 자산가치 산정기준 설정하여, 산업보안의 중요성 對기업·對국민 홍보·전파가 필요하다.

5.1.4 산업보안 패러다임 선도 및 산업보안 구축기업에 대한 지원

국내외 동향분석을 통한 지원부문·보안산업부문 활동방향 제시가 필요하며, 산업보안 체계구축 기업에 대한 자금 및 세제 등의 정책적 지원과 산업보안 평가인증을 통한 인센티브 제시가 필요하다.

5.2 지원부문

5.2.1 정책과제 발굴 및 수행

정부 주무부처와의 협의체 구성을 통한 과제 발굴 및 선정 및 미래지향형 전략과제 수행이 필요하다.

민·관 협력의 효율적 중재 역할수행 과 국내외 동향분석팀 운영을 통한 정책방향 제시가 필요하다.

5.2.2 기초 인프라 구축

“산업보안 상용화 센터” 설립을 통한 중장기적 장비구축과 산업보안 집적화를 위한 산업보안 특구 조성 및 운영, 중소기업 산업보안 관제센터 운영이 필요하다.

5.2.3 제품기술 표준화 및 상용화 지원

산업보안 분야별 핵심기술 개발 선도 및 산업보안 표준화를 통한 핵심기술 일관성 유도와 기술 상용화를 위한 기업별 특화서비스 제공이 필요하다.

5.2.4 산업보안 통합인증체계 구축

인증기관 운영을 통한 산업보안체계인증 및 제품인증과 산업보안성평가 인증 컨설팅 사업지원 필요하다.

5.2.5 인력양성 체계 구축

산업보안 전문인력 양성과 산업보안 최고위과정 개설 및 운영, 산업보안 전문가 자격제도 운영이 필요하다.

6. 결 론

산업보안은 보안의 영역별 요소(물리적 보안도구, IT보안 도구, 융합보안도구)를 활용하여 기업의 산업자산을 보호하는 관리활동들로서 Hardware적 요소(보안을 위한 도구)의 운용은 물론 이를 활용하기 위한 Software적 측면(정책 및 전략수립, 유지운영, 사후 대응조치 등)을 포괄하는 개념으로 이해 가능함을 알 수 있다.

이상을 통해 산업보안의 정의와 관련 개념, 우리나라의 산업보안 관련 기관들의 역할과 법률, 관

리체계 및 실태 등을 살펴보았으며, 이에 따른 문제점을 바탕으로 개선방안을 설정하고 향후 우리나라 기업들이 효과적인 산업보안활동을 통하여 국가경쟁력을 제고하고 21세기 산업보안 선진국으로 진입하기 위한 정책부문, 지원부문, 보안산업부문의 역할을 중심으로 향후 정책방향과 시사점을 제안하였다.

산업보안은 정부, 지원기관, 보안산업활성화, 기업의 보안의식강화를 통해서만 실현가능하기 때문에 부문별 유기적 협력관계가 무엇보다 중요하다 하겠다.

참 고 문 헌

[1] 최선태, “21세기 산업보안론”, 2009.
[2] 최선태, “한국산업보안발전방안”, 2007.
[3] 최순호, “경찰의 산업보안활동 강화를 위한 체계적 접근 방안”, 2008.
[4] 조안 마그레타, 권영설 외1명 옮김, “경영이란 무엇인가”, 2004.
[5] Booz Allen Hamilton, ″Convergence of Enterprise Security Organizations, Novermber 2005.
[6] 한국산업기술보호협회, “산업기술 보호를 위한 실태조사 보고서″, 2008.

하 옥 현

1978년 성균관대학교 정치외교학과(정치학사)
1980년 서울대학교 행정대학원(행정학석사)
1998년 프랑스 사회과학대학원(EHESS) 박사과정(DEA 취득)
2005년 고려대학교 정보보호대학원(공학박사)
2008년~현재 호남대학교 경찰법행정학부 교수