산업기술 보호 관리실태 및 발전방안에 관한 연구

A Study on the Real Condition and the Improvement Directions for the Protection of Industrial Technology

정 태 황* · 장 항 배**

〈목 차〉

〈요 약〉

본 연구는 산업기술 보호를 위한 관리적 발전방안을 마련하기 위하여 공공기관, 대기업, 중소기업 등을 대상으로 관리적 보안실태에 대해 조사·분석을 실시하였으며, 그 결과는 다음과 같다.

첫째, 보안정책을 효과적으로 실행할 수 있는 기반 구축이 필요하다. 조사대상 대부분이 보안규정을 잘 관리하고 있으나 보안규정을 지키거나 지속적으로 개선하려는 노력이 부족한 것으로 나타났다. 이를 개선하기 위하여 보안전담조직과 보안담당자 운영방법을 개선할 필요가 있으며, 보안규정을 모든 구성원에게 알리고 보안업무 수행을 위한 팀 간 업무 공조체계를 이룰 수 있는 조직문화를 활성화 할 필요가 있다. 이와 함께 지속적인 보안점검과 보안감사를 통해 보안의식을 향상시키고, 보안규정 준수 여부를 직원업무평가에 반영함으로써 보안정책을 가시화 할 필요가 있다.

둘째, 보안활성화를 위한 보안투자가 필요하다. 기술 유출경로와 수단이 다양화·첨단화 되어가고 있을 뿐 아니라 복잡하고 빠른 속도로 변화하기 때문에 관련 전문기관인 국가정보원, 한국인터넷진흥원, 정보보호 컨설팅 전문기업, 관련 대학 및 연구소 등과의 협조채널 유지하고, 필요에 따라서는 보안 전문기관으로부터 outsourcing 도입을 검토할 필요가 있다. 특히 공공기관이나 대기업에 비해 보안정책 운영실태가 미흡한 중소기업은 조직 규모나 재정적 여건을 감안하여 보안관리 능력을 보강할 수 있도록 국가적인 차원의 지원시스템을 증가할 필요가 있다.

셋째, 산업기술 유출의 주체는 사람으로 인력관리가 중요하다. 신규 입사자와 임직원을 대상

* 한서대학교 경호비서학과 교수, 제1저자
** 대진대학교 경영학과 교수, 교신저자(hangbae.chang@gmail.com)

으로 하는 정기적인 교육률은 높은 것으로 평가되나 핵심기술에 접근하는 임직원과 제3자로부터의 보안서약서 작성과 중요자산에 대한 접근권한이 변경될 때 접근권한 변경 적용과 같은 업무의 활성화가 필요하다. 중요기술을 다루는 사람에 한하여 신원조사를 실시할 수 있는 여건 조성이 필요하며, 퇴사자에 대한 보안서약서 징구와 정보시스템에 대한 접근권한 제거, 계정 삭제와 같은 퇴직자 관리를 강화할 수 있어야 한다.

넷째, 중요한 자산에 대한 관리와 통제를 강화해야 한다. 자산에 대한 목록과 관리기준은 비교적 잘 정리되어 있으나 자산의 중요성에 따른 등급화작업의 활성화와 자산의 유출 및 손상의 경우를 대비한 영향 정도를 평가할 수 있는 작업이 필요하다. 자산에 대한 중요도는 시간흐름 및 업무특성에 따라 변화되기 때문에 주기적인 자산평가 작업과 분류작업을 통해 사용자별로 권한을 설정할 수 있어야 한다.

주제어 : 산업기술, 보안수준, 보안정책, 인력관리, 자산

I. 서 론

첨단산업기술은 외부의 공격 또는 내부의 공격에 의해 외부로 유출되고 있으며, 유출 수단은 개인컴퓨터와 웹, 전자메일, 인터넷 메신저, 그리고 오프라인 문서인 경우 프린트와 복사, 팩스 등 다양한 경로를 이용하고 있다.

산업기술을 보호하기 위하여 '부정경쟁방지 및 영업비밀보호에 관한 법률' 도입과 '산업기술의 유출방지 및 보호에 관한 법률' 제정, 보안의식교육, 국가핵심기술보유기업 보안설비구축 지원사업 등 국가적 차원의 다양한 노력이 진행되고 있지만 산업기술유출 건수와 피해규모는 증가하고 있으며, 국내 핵심기술의 해외유출 또는 유출시도가 증가하고 있다.

〈표 1〉 산업기술 유출현황

연 도	2003	2004	2005	2006	2007	2008	계
발생건수	6	26	29	31	32	42	166

자료 : 국가정보원. 2008. 첨단산업기술보호동향.

산업기술의 유출은 일회의 유출로 그 피해가 지속적이면서도 방대하게 발생한다는 특징이 있으며, 유출을 시도하는 자는 주로 기술보유회사에 근무하는 자로서 지금까지 범죄경험이 전무한 경우가 대부분이다. 이러한 특징으로 인해 산업기밀 유출을 방지하기 위한 방법은 그 실효성을 거두기가 어려울 것으로 예측되고 있다(정진근, 2010).

기업적 차원에서도 산업기술보호를 위한 보안정책 및 보안조직 정비 등과 같은 관리적 활동이 추진되지만 아직 일부 대기업에 한정되어 있으며, 중소기업의 경우는 보안업무를 위한 기본 인프라 구축이 부족한 실정이다. 비록 보안전담조직이 있다 하더라도 물리적 보안시스템 구축이나 정보보호시스템구축 등에 한정되고 있는 실정으로 산업기술보호를 위한 보안관리 효과에는 한계가 있으며, 보안정책과 보안조직 관리, 보안업무 관리, 보안 투자 등과 같은 관리인 관점에서 대응방안을 마련하는 것이 필요할 것으로 인식된다. 특히 산업기술을 보호하기 위하여 다양한 노력에도 불구하고 산업기술 유출사고가 내부자에 의해 발생하는 비율이 높다는 것을 감안해 볼 때 관리적 방안의 중요성이 높다고 할 수 있다.

2009년 9월 발생한 자동차 핵심기술 유출사건도 국내의 A자동차 회사의 전직 직원 5명이 현직 직원 2명으로부터 USB 메모리를 이용하여 사내 컴퓨터의 자동차핵심기술을 반출한 후 전자메일을 통해 넘겨받아 중국의 B자동차 회사에 기술이전 명목으로 유출한 사건이다.

그리고 대형조선업체 C사에 근무하던 L씨는 기술자료를 관리하는 총책임자의 권한을 이용하여 선박공정도와 설계완료 보고서 등 1,100여 개의 파일을 외장형 디스크에 저장하여 반출하려다가 적발되었다(장항배, 2010).

본 연구는 공공기관, 대기업, 중소기업을 대상으로 현재의 관리적 보안 실태를 조사·분석하여 산업기술을 보호하기 위한 관리적 발전방안을 제시하는 것을 목적으로 하며, 설문지 작성과 조사대상기관 선정과정에서 보안관련 협회, 보안관련 학과 교수, 보안관련 업계의 엔지니어 등으로부터 자문을 받았다. 선정된 조사대상 기관은 보호할 산업기술을 보유하고 있는 기관 68개로 많은 기관의 관리적 보안실태를 나타내는데 한계가 있을 것으로 생각한다.

Ⅱ. 연구 방법

1. 조사 대상

조사대상은 우리나라 전국에 있는 공공기관, 대기업, 중소기업을 대상으로 하였으며, 조사대상을 선정하는 과정에서 관련협회와 보안관련 학과 교수, 보안관련 기업의 엔지니어들과의 토의과정을 거쳤으며, 산업적으로 보호가치가 있는 중요한 기술 및 정보 등을 보유하고 있는 기관으로 선정하였다.

조사에 응답한 68개 기관에는 자동차 관련 기업이 가장 많고, 다음으로 전자·정보통신 관련기업과 조선·철강 관련기업이다.

〈표 2〉 조사대상 기관 구성

	공공기관	대기업	중소기업	계
자동차	4	13	9	26
조선·철강	1	14	3	18
전자·정보통신	2	5	12	19
기타(우주, 원자력)	3	0	2	5
계	10	32	26	68

2. 설문지 구성

연구에서 사용한 설문지는 연구목적에 맞게 작성하여 보안관련 학과 교수 및 보안관련 산업에 종사하는 엔지니어 등에게 사전 배포하고, 전문가 회의에서 토의를 거쳐 일부 수정 후 사용하였다.

설문지 문항은 보안 정책, 인적 자원 관리, 자산 관리 3개 부분으로 구성하였는데, 보안정책 부분은 10개 항으로, 보안규정 보유현황, 보안정책 및 지침절차 등의 내용에 대한 임직원 공지현황, 보안전담조직 현황, 조직의 주요정보 공유방법, 임직원 업무에 보안관련 내용 포함현황, 조직 내 보안업무 수행을 위한 팀 간 업무 공조체계 구성현황, 보안감사 실시현황, 정보 및 자산보호를 위한 비용투자 현황, 조직 내 보안업무 추진을 위한 전문기관 도움현황, 산업기술보안 컨설팅 경험에 관한 것이다.

인력관리 부분은 10개 항으로, 신규 입사자에 대한 보안교육 실시현황, 기존 임직원 대상 보안교육 실시현황, 임직원 보안의식 제고활동 실시현황, 신규 입사자에 대한 보안서약서 징구현황, R&D 프로젝트 참가자에 대한 보안서약서 징구현황, 보안규정 위반자에 대한 징계절차 마련 현황, 퇴사자에 대한 보안서약서 징구현황, 퇴사자 향후 진로 및 동향파악 현황, 협력업체 및 외국인 등 제3자에 대한 관리여부 현황, 사유발생시 조직의 정보자산에 대한 접근 권한 조정현황에 관한 것이다.

자산관리 부분은 7개항으로, 조직의 정보자산에 대한 관리기준 수립현황, 조직의 정보자산에 대한 등급구분 관리현황, 정보자산별 관리책임자 지정현황, 정기적인 정보자산 분류현황, 주요 기밀문서 관리현황, 지적재산권에 대한 관리방안 수립현황, 조직자산의 반출방법 현황에 관한 것이다.

3. 조사절차 및 자료처리

조사는 2009년 4월 20일부터 8월 10일 까지 실행되었으며, 설문지를 본 연구의 목적에 맞게 우편, 팩스, 이 메일로 보내고 응답하여 기재하는 방식을 선택하였다. 응답한 조사대상 기관은 68개이며, 응답받은 설문지는 응답오류 및 무응답 등에 관한 검토과정을 거친 후, 통계 프로그램인 SPSS ver.10.0을 이용하여 연구목적에 맞게 처리하였다.

Ⅲ. 결과 및 논의

1. 보안정책 관리 실태 분석

1) 보안규정 활용실태

조사대상기관의 79.4%가 보안규정을 보유하고 있고, 11.8%가 지시·지침으로 관리하고 있으며, 비교적 많은 대상이 보안규정을 관리하고 있으며, 보안규정은 조직의 경영목표에 부합하게 보안활동을 수행하는 구성원의 역할과 책임에 대해 설명하고 있다.

〈표 3〉 보안규정 보유현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안규정 보유	기업수	9	30	15	54
	비 율	90.0	93.8	57.7	79.4
지시·지침으로 관리	기업수	1	1	6	8
	비 율	10.0	3.1	23.1	11.8
보안규정 미보유	기업수	-	1	5	6
	비 율	-	3.1	19.2	8.8
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

그리고 보안관리 규정을 보유하고 있는 조사대상 기관의 67.7%가 실제로 규정을 시행하여 지속적으로 개선하고 있으며, 14.5%는 보안규정을 시행하고만 있는 것으로 나타나 보안규정의 이용도가 다소 미흡한 것으로 분석된다.

〈표 4〉 보안규정 개선현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
실제로 실시, 지속적인 규정 개선	기업수	9	28	5	42
	비 율	90.0	90.3	28.6	67.7
수립되어 있으며, 지켜지고 있음	기업수	1	2	6	9
	비 율	10.0	6.5	23.8	14.5
수립되어 있으나, 지켜지지 않음	기업수	-	1	10	11
	비 율	-	3.2	47.6	17.8
합 계	기업수	10	31	21	62
	비 율	100.0	100.0	100.0	100.0

〈표 3〉과 〈표 4〉에서 보안규정을 보유하지 않은 기관은 6개 기관 8.8%로 비교적 낮게 나

타났지만 중소기업이 공공기관이나 대기업에 비해 보안규정을 보유하지 않은 비율과 보안규정을 잘 지키지 않는 비율이 각각 19.2%와 47.6%로 전체 평균비율 보다 훨씬 높다는 것을 보여준다. 이는 중소기업이 보안에 취약할 수 있다는 것을 나타내는 것으로 재정적으로 취약한 중소기업의 보안규정 관리와 활용도를 높이기 위한 지원시스템을 강화할 필요가 있다.

〈표 5〉 보안규정 공지현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
임직원 공지	기업수	10	32	18	60
	비 율	100.0	100.0	69.2	88.2
임직원 미공지	기업수	-	-	8	8
	비 율	-	-	30.8	11.8
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 5〉에서 보유하고 있는 보안정책, 지침, 절차 등의 내용에 대한 임직원 공지는 보유기관의 88.2%가 수행하고 있는 것으로 나타났는데, 설계된 보안정책, 지침, 절차 등은 적절한 절차와 방법으로 모든 구성원에게 알림으로써 이를 준수할 수 있어야 보안규정의 목적을 효과적으로 달성할 수 있다.

2) 보안전담조직 운영실태

보안전담조직은 51.5%가 보안전담조직과 보안담당자를 보유하고 있으며, 39.7%가 보안담담자만을 39.7%가 지시·지침으로 관리하고 있다. 조직이 보안활동을 체계적으로 실행하기 위해서는 조직특성에 적합한 보안전담조직을 구성해야 하는데, 기관의 규모에 따라 보안전담조직을 구성하기 어렵다는 현실적 인식을 반영한 것으로 볼 수 있다.

〈표 6〉 보안전담조직 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안전담조직과 보안담당자가 존재	기업수	6	25	4	35
	비 율	60.0	78.1	15.4	51.5
보안담당자만 존재		4	6	17	27
		40.0	18.8	65.4	39.7
보안전담조직과 보안담당자 모두 미존재	기업수	-	1	5	6
	비 율	-	3.1	19.2	8.8
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

3) 보안업무 및 주요정보 관리실태

〈표 7〉에 의하면 임직원의 업무에 보안관련 내용 포함여부는 조사대상 기관의 91.2%가 포함되어 있고 8.8%가 포함되어 있지 않는 것으로 나타났는데, 임직원의 업무 특성상 많은 정보를 처리하기 때문에 보안을 고려한 업무처리 절차가 설계되어야 한다.

〈표 7〉 보안업무분장 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안내용 포함	기업수	10	31	21	62
	비 율	100.0	96.9	80.8	91.2
보안내용 미포함	기업수	-	1	5	6
	비 율	-	3.1	19.2	8.8
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 8〉 정보접근 권한체계 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
업무담당자 등 소수만이 접근 가능	기업수	9	29	20	58
	비 율	90.0	96.0	76.9	85.3
핵심정보를 제외하고 직원 열람 가능	기업수	1	3	5	9
	비 율	10.0	9.4	19.2	13.2
대부분의 정보에 대해 직원 열람 가능	기업수	-	-	1	1
	비 율	-	-	3.8	1.5
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

그리고 〈표 8〉에 의하면 조직의 주요정보 공유방법으로 85.3%가 업무담당자 및 관계자 등 소수만이 접근 가능하고, 13.2%가 핵심정보를 제외한 정보에 대하여 직원이 열람 가능한 것으로 나타났다. 이는 중요한 정보에 접근할 수 있는 권한은 비교적 잘 구분되어 있는 것을 보여주는 것으로, 조직의 중요정보에 대한 접근 및 열람 등의 권한은 개인의 보직 및 임무에 따라 상이하게 부여하여야 하며, 권한 남용을 방지하기 위하여 사용내역을 확인할 수 있어야 한다.

〈표 9〉 보안업무 공조체계 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
공조체계 구성	기업수	10	29	10	49
	비 율	100.0	90.6	38.5	72.1
공조체계 미구성	기업수	-	3	16	19
	비 율	-	9.4	61.5	27.9
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 9〉에 의하면 조직 내 보안업무 수행을 위한 팀 간 업무 공조체계는 조사대상 기관의 72.1%가 구성되어 있고 27.9%가 구성되어 있지 않은 것으로 나타났다. 보안업무는 특정개인이나 부서만의 노력으로는 이루어질 수 없으며, 전사적인 관점에서 보안업무 수행을 위해 관련 부서간의 협력체계가 필요하므로 보다 높은 공조체계가 필요하다.

4) 임직원 보안감사 실태

조사대상 기관의 54.4%가 정기적인 보안감사를 실시하고 있으며, 29.4%가 필요할 때마다 수시로 보안감사를 실시하고 있는 것을 나타났다. 공공기관의 경우 관련지침에 따라 매년 1회 이상 자체적인 보안감사를 실시하고 있으며, 지속적인 감사활동을 통해 순차적으로 보안수준 개선을 위한 노력이 필요하다.

〈표 10〉 임직원 보안감사 실시현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
정기적으로 실시	기업수	8	27	4	39
	비 율	80.0	84.4	15.4	54.4
필요할 때 수시로 실시	기업수	2	5	13	20
	비 율	20.0	15.6	50.0	29.4
실시하지 않음	기업수	-	-	9	9
	비 율	-	-	34.6	13.2
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

5) 보안 지원 및 투자 실태

〈표 11〉에서 보여주는 것처럼 조직의 보안업무 추진을 위하여 외부 전문기관의 도움을

받고 있는 조사대상 기관은 64.7%로 조사되었다. 〈표 12〉에서 산업기술보호문제를 진단하고 대책방안을 마련하기 위하여 전문기업체나 기관에서 보안컨설팅을 받은 경험이 있는 조사대상 기관은 62.9%이며, 보안 컨설팅 분야로는 정보보호 관리체계 구축에 집중되어 있는 것으로 나타났다.

〈표 11〉 외부 보안전문기관 도움요청 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
도움 받음	기업수	8	26	10	44
	비 율	80.0	81.3	38.5	64.7
도움 받지 않음	기업수	2	6	16	24
	비 율	20.0	18.8	61.5	35.3
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 12〉 보안컨설팅 경험현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
컨설팅 경험 있음	기업수	4	7	11	22
	비 율	66.7	77.8	55.0	62.9
컨설팅 경험 없음	기업수	2	2	9	13
	비 율	33.3	22.2	45.0	37.1
합 계	기업수	6	9	20	35
	비 율	100.0	100.0	100.0	100.0

기술을 유출할 수 있는 경로와 수단이 다양화・첨단화 되어가고 있을 뿐 아니라 유출기술도 상대적으로 복잡하고 빠른 속도로 변화하기 때문에 관련 전문기관인 국가정보원, 한국인터넷진흥원, 정보보호 컨설팅 전문기업, 관련 대학 및 연구소 등과의 협조채널을 유지하고 확인하는 작업이 요구되며, 필요에 따라서는 보안 전문기관으로부터 outsourcing 도입을 검토할 필요가 있다.

〈표 13〉 보안투자 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
기술적, 물리적, 관리적 보안을 위해 매년 일정비용 투자	기업수	5	24	2	31
	비 율	50.0	75.0	7.7	45.6
특정 보안분야에 대해 필요시 비용투자	기업수	4	8	17	29
	비 율	40.0	25.0	69.2	42.6
보안분야에 대한 투자 미실시	기업수	1	-	7	8
	비 율	10.0	-	23.1	11.8
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 13〉은 정보 및 자산보호를 위한 비용투자 형태를 보여주는 것으로, 매년 일정비용 이상을 꾸준히 투자하는 기관은 45.6%, 특정 보안 분야에 한정하여 필요에 따라 비용을 투자하는 기관은 42.6%로 나타나 다른 보안수준 항목에 비하여 상대적으로 낮은 상태임을 보여준다. 무응답을 제외한 조사대상 기관 43개의 매출금액 대비 평균적으로 차지하는 보안투자 금액 비율은 약 0.34%로 집계되었다. 정보 및 자산보호를 위한 비용은 보안시스템 도입과 이에 대한 유지보수 및 컨설팅 등에 소요되는 예산을 의미하는데, 〈표 13〉에서 보여주는 것처럼 낮은 보안투자율은 보안수준을 보여주는 것으로 보안투자를 위한 인식전환이 필요하다.

2. 인력관리 실태 분석

1) 보안교육 실태

〈표 14〉에 의하면 신규 입사자에 대한 보안교육은 조사대상 기관의 80.9%가 시행하고 있는 것을 나타났다. 보안교육에는 조직의 보안정책과 절차, 정보 서비스 인증 절차, 응용 프로그램 사용, 요구되는 보안사항, 법적 책임, 업무통제 수단 등을 포함할 수 있어야 한다.

〈표 14〉 신규입사자 보안교육 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안교육 실시	기업수	9	31	15	55
	비 율	90.0	96.9	57.7	80.9
보안교육 미실시	기업수	1	1	11	13
	비 율	10.0	3.1	42.3	19.1
계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 15〉에 의하면 기존 임직원 대상 보안교육은 조사대상 기관의 54.4%가 정기적으로 실시하고 있으며, 30.9%가 필요할 때마다 교육을 실시하고 있는 것으로 나타나 비교적 양호한 교육실태를 보여준다.

〈표 15〉 임직원 대상 보안교육 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안교육을 정기적으로 실시	기업수	7	27	3	37
	비 율	70.0	84.4	11.5	54.4
보안교육이 필요할 때만 실시	기업수	3	4	14	21
	비 율	30.0	12.5	53.8	30.9
보안교육을 실시하지 않음	기업수	-	1	9	10
	비 율	-	3.1	34.6	14.7
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 16〉은 보안교육 방법을 보여주는 것으로, 조사대상 기관의 75.0%가 자체적으로 실시하고 있으며, 외부강사 초빙 42.6%, 온라인 콘텐츠 활용 32.4% 등의 순으로 조사되었다. 보안수준을 높이기 위하여 정기적인 보안교육이 필요하며, 전문가에 의한 체계적인 보안교육 기회를 증가시킬 필요가 있다.

〈표 16〉 보안교육방법 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
자체적으로 실시	기업수	5	29	17	51
	비 율	50.0	90.6	65.4	75.0
외부강사 초빙	기업수	8	17	4	29
	비 율	80.0	53.1	15.4	42.6
온라인 콘텐츠 활용	기업수	4	16	2	22
	비 율	40.0	50.0	7.7	32.4
외부교육 참석(공공기관)	기업수	4	12	5	21
	비 율	40.0	37.5	19.2	30.9
외부교육 참석(민간기관)	기업수	-	6	2	8
	비 율	-	18.8	7.7	11.8

2) 보안활동 실태

〈표 16〉에 의하면 임직원의 보안의식을 재공하기 위한 활동으로서, 퇴근 또는 자리를 이탈할 경우 PC 전원 Off 확인 82.4%, 화면보호기 설정확인 85.3%, 노트북 방치 여부 확인 70.6%, 출입문, 개인서랍 잠금 여부 확인 80.9%, 문서 및 도면 방치여부 확인 83.8%, USB, 노트북, 문서 등 무단 방출여부 확인 72.1% 등이 수행되고 있는 것으로 나타났다. 보안의식을 재고하기 위하여, 보안관리 규정에 따른 생활수칙 준수여부를 지속적으로 점검할 수 있어야 한다.

〈표 16〉 임직원 보안활동 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
PC 전원 Off 여부 확인	기업수	8	27	21	56
	비 율	80.0	84.4	80.8	82.4
자리이탈시 화면보호기 설정여부 확인	기업수	10	31	17	58
	비 율	100.0	96.9	65.4	85.3
노트북 방치여부 확인	기업수	10	26	12	48
	비 율	100.0	81.3	46.2	70.6
출입문, 캐비넷, 잠금여부 확인	기업수	10	32	13	55
	비 율	100.0	100.0	50.0	80.9
문서 및 도면방치 여부확인	기업수	9	31	17	57
	비 율	90.0	96.9	65.4	83.8
반출여부 확인	기업수	7	28	14	49
	비 율	70.0	87.5	53.8	72.1

〈표 17〉은 보안서약에 관한 현황을 보여주는 것으로, 신규 입사자에 대한 보안서약서와 근로계약서를 별도로 징구하는 조사대상 기관은 88.2%이며, 고용 계약서에 보안책임을 명시하는 조사대상 기관은 5.9%이다. 직원 선발 시에는 개인이 작성한 신원증명서 확보, 이력서 검토, 신원 확인(여권 또는 유사서류), 보안 서약서 징구 등의 신원조사 활동을 수행할 수 있도록 지속적인 관심이 필요하다.

〈표 17〉 보안서약방법 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안 서약서와 근로계약서 별도 징구	기업수	9	29	22	60
	비 율	90.0	90.6	84.6	88.2
고용 계약서에 보안책임 명시	기업수	-	2	2	4
	비 율	-	6.3	7.7	5.9
징구하지 않음	기업수	1	1	2	4
	비 율	10.0	3.1	7.7	5.9
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 18〉은 R&D 참여인력에 대한 보안서약 징구 현황을 보여주는데, 주요 R&D 프로젝트 참가자에 대한 보안서약서에 대해 조사대상 기관의 72.1%가 징구하고 있다. 조직의 지적자산을 생성 또는 취급하는 직원에 대해서는 지적자산이 기밀 또는 비밀사항이라는 것을 환기시키기 위하여 보안서약서를 징구하여야 하며, 직원들은 이러한 사항을 고용조건의 일부분으로 인식하고 서명할 수 있어야 한다.

〈표 18〉 R&D 참여인력 보안서약서 징구 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안 서약서 징구	기업수	8	26	15	49
	비 율	80.0	81.3	57.7	72.1
보안 서약서 징구하지 않음	기업수	2	6	11	19
	비 율	20.0	18.8	42.3	27.9
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 19〉 제3자 관리방안 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
관리방안 마련, 대상자 보안서약	기업수	8	26	4	38
	비 율	80.0	81.3	15.4	55.9
관리방안 미 마련, 대상자 보안서약	기업수	1	4	11	16
	비 율	10.0	12.5	42.3	23.5
둘 다 하지 않음	기업수	1	2	11	14
	비 율	10.0	6.3	42.3	20.6
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 19〉에 의하면 제3자(협력업체, 외국인 등)에 대한 관리에 있어서는 조사대상 기관의 55.9%가 관리방안을 마련하고 대상자로부터 보안서약서를 징구하고 있으며, 23.5%는 단순히 외부 인력으로부터 보안서약서만을 받고 있는 상태이다. 조직의 정보자산에 대한 개발, 운영, 관리업무 등을 외부에 위탁할 경우 보안에 관한 책임사항, 책임범위, 보안대책 등을 계약서에 반영하여 신뢰성 있는 보안관리 업무가 수행되어야 한다.

3) 보안규정 위반자 징계실태

〈표 20〉에 의하면 보안규정 위반자에 대한 징계절차가 마련되어 필요시 징계조치가 이루어지는 조사대상 기관은 67.6%이며, 징계절차는 마련되어 있으나 실제로 실시되고 있지 않고 있는 조사대상 기관은 20.6%로 조사되었다. 조직의 보안정책이나 절차를 위반한 직원에 대하여 공식적인 징계 절차가 있어야 하고, 규정준수 여부를 직원업무평가에 포함하고 이를 실행할 수 있는 인식이 필요하다.

〈표 20〉 보안규정 위반자 징계 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
징계절차 마련, 필요시 징계조치	기업수	7	29	10	46
	비 율	70.0	90.6	38.5	67.6
징계절차 마련, 징계조치 거의 미실시	기업수	3	2	9	14
	비 율	30.0	6.3	34.6	20.6
징계절차 마련되어 있지 않음	기업수	0	1	7	8
	비 율		3.1	26.9	11.8
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

4) 퇴사자 보안관리 실태

〈표 21〉에 의하면 퇴사자 보안관리를 위해 필요한 보안서약서는 조사대상 기관의 85.3%가 징구하고 있다. 신규 입사자뿐만 아니라 퇴사자에 대해서 보안서약서를 징구하고 주요 정보시스템에 대한 접근권한을 제거하고, 계정을 삭제할 수 있어야 한다.

〈표 21〉 퇴사자 보안서약서 징구 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
보안 서약서 징구	기업수	8	30	20	58
	비 율	80.0	93.8	76.9	85.3
보안 서약서 징구하지 않음	기업수	2	2	6	10
	비 율	20.0	6.3	23.1	14.7
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 22〉에 의하면 모든 퇴사자의 동향을 파악하는 조사대상 기관은 10.3%, 주요 임직원에 한하여 동향을 파악하고 있는 기관은 72.1%로 조사되었다. 산업기술 유출사고의 대부분이 전(현)직 임직원에 의하여 발생하였기(81%) 때문에 퇴사자에 대한 철저한 관리가 필요하다.

〈표 22〉 퇴사자 동향 파악 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
모든 퇴사자의 동향 파악	기업수	2	4	1	7
	비 율	20.0	12.5	3.8	10.3
주요 임직원에 한하여 동향 파악	기업수	5	24	20	49
	비 율	50.0	75.0	76.9	72.1
전혀 파악하고 있지 않음	기업수	3	4	5	12
	비 율	30.0	12.5	19.2	17.6
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

5) 정보자산 접근권한 관리

〈표 23〉에 의하면 정보자산 사용자에 대한 접근권한은 변경이 생길 때마다 즉시 조정하는 조사대상 기관은 69.1%이며, 변경사유 발생 후 1주일 이내로 조정하는 기관은 16.2%조사되었다.

〈표 23〉 정보자산 접근권한 관리 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
사유발생 즉시 조정	기업수	8	28	11	47
	비 율	80.0	87.5	42.3	69.1
사유발생 1주일 이내 조정	기업수	1	3	7	11
	비 율	10.0	9.4	26.9	16.2
조정이 지연되거나 이루어지지 않음	기업수	1	1	8	10
	비 율	10.0	3.1	30.8	14.7
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

정보자산에 대한 접근권한 변경이 즉시 반영되지 않을 경우, 기존에 직원이 가지고 있던 정보시스템 접근권한이 남용되어 정보가 유출될 가능성이 있으므로 정보자산에 대한 접근권한이 변경될 때 접근권한 변경이 같이 이루어 질 수 있어야 한다.

3. 자산관리 실태 분석

1) 정보자산 관리 실태

〈표 24〉에 의하면 조사대상 기관의 83.8%가 정보자산에 대한 목록관리를 통하여 관리기준을 수립하고 있으며, 〈표 25〉에 의하면 조사대상 기관의 70.6%가 정보자산의 중요성에 따라 등급화(극비, 대외비, 일반 등)작업을 수행하고 있다.

조직 내 정보의 생산, 유통, 이용과 관련된 자산을 정보자산이라고 정의할 수 있는데, 이에 대한 분류 및 관리규정이 필요할 뿐 아니라 정보자산에 대한 효율적인 보호를 위하여 조직의 특성에 맞는 정보보호 등급체계를 설계하고 유출 및 손상되는 경우를 대비한 영향 정도를 평가를 실시하여야 한다.

〈표 24〉 정보자산 관리기준 수립 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
정보자산 관리기준 수립	기업수	10	31	16	57
	비 율	100.0	96.9	61.5	83.8
정보자산 관리기준 미수립	기업수	-	1	10	11
	비 율	-	3.1	38.5	16.2
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 25〉 정보자산 등급관리 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
정보자산을 등급화하여 관리	기업수	7	31	10	48
	비 율	70.0	96.9	38.5	70.6
정보자산을 등급화 하지 않음	기업수	3	1	16	20
	비 율	30.0	3.1	61.5	29.4
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 26〉는 정보자산 관리책임자 지정 현황을 보여주는 것으로, 정보자산에 대한 특정한 관리책임자를 조사대상 기관의 82.4%가 이를 지정하여 수행하고 있다. 정보자산별 업무프로세스에 따라 관리자를 두어 주기적으로 점검할 수 있어야 한다.

〈표 26〉 정보자산 관리책임자 지정 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
정보자산 관리책임자 지정	기업수	10	31	15	56
	비 율	100.0	96.9	57.7	82.4
정보자산 관리책임자 미지정	기업수	-	1	11	12
	비 율	-	3.1	42.3	17.6
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 27〉 정보자산 반출승인 수행현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
반출에 대한 사전인가 필요	기업수	10	32	21	63
	비 율	100.0	100.0	80.8	92.6
반출에 대한 사전 인가절차가 없음	기업수	-	-	5	5
	비 율	-	-	19.2	7.4
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 27〉은 정보자산 반출승인 현황을 보여주는 것으로, 장비, 정보, 소프트웨어 등을 반출할 경우, 조사대상 기관의 92.6%가 사전인가가 있어야만 가능한 상태이다. 정보자산은 허가 없이 외부로 옮겨져서는 안 되며, 외부로 반출해야 할 경우에는 그 사실을 기록하고, 다시 반입 때에도 기록되어야 한다.

2) 정보자산 분류 실태

〈표 28〉에 의하면 정보자산의 분류작업은 조사대상 기관의 41.2%가 정기적으로 실시되고 있으며, 44.1%가 필요할 때마다 정보자산을 분류하고 있다. 정보자산에 대한 중요도는 시간흐름 및 업무특성에 따라 변화되기 때문에 주기적인 자산평가 작업이 필요하다.

〈표 28〉 정기적 정보자산 분류작업 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
정기적으로 정보자산 분류작업 실시	기업수	7	19	2	28
	비 율	70.0	59.4	7.7	41.2
정보자산 분류작업을 필요할 때마다 실시	기업수	3	12	15	30
	비 율	30.0	37.5	57.7	44.1
실시하지 않음	기업수	-	1	9	10
	비 율	-	3.1	34.6	14.7
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

3) 문서 접근권한 설정 실태

〈표 29〉 사용자별 문서 접근권한 설정 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
사용자별로 권한설정	기업수	9	27	11	47
	비 율	90.0	84.4	42.3	69.1
사용자별 일부 권한설정	기업수	1	4	9	14
	비 율	10.0	12.5	34.6	20.6
사용자별 권한 미설정	기업수	-	1	6	7
	비 율	-	3.1	23.1	10.3
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

〈표 29〉에 의하면 주요 기밀문서의 경우 조사대상 기관의 69.1%가 사용자별로 권한을 설정하고 있으며, 20.6%가 사용자별 일부 권한이 설정되어 있다. 인사조직 단위가 아닌 업무 프로세스 중심의 권한설정이 필요하다.

4) 지적재산권 관리 실태

〈표 30〉은 지적재산권 관리형황을 보여주는 것으로, 특허, 실용신안, 디자인 등과 같은 지적재산권에 대한 관리방안에 대해서는 조사대상 기관의 64.7%가 관리출원 및 대응전략이 모두 마련되어 있으며, 17.6%가 일부만 마련되어 있는 상태이다. 조직의 핵심역량을 정리되어 있는 지적재산권 문서도 기밀문서와 같이 업무절차 및 보안대책을 수립할 수 있어야 한다.

〈표 30〉 지적재산권 관리 현황

		기업규모별			전 체
		공공기관	대기업	중소기업	
권리출원 및 대응전략 모두 마련	기업수	10	28	6	44
	비 율	100.0	87.5	23.1	64.7
권리출원 및 대응전략 일부만 마련	기업수	-	3	9	12
	비 율	-	9.4	34.6	17.6
권리출원 및 대응전략 모두 마련되어 있지 않음	기업수	-	1	11	12
	비 율	-	3.1	42.3	17.6
합 계	기업수	10	32	26	68
	비 율	100.0	100.0	100.0	100.0

IV. 결 론

최근 산업기술유출사건이 심각한 문제로 대두되면서 '산업기술의 유출방지 및 보호에 관한 법률' 제정과 산업기밀보호센타 발족 등 산업기밀유출 방지를 위한 국가적 차원의 노력이 진행되고 있으며, 이와 함께 기업도 보안시스템 구축과 보안정책 수립・개선 등 자체적인 노력을 보이고 있다. 그럼에도 불구하고 산업기밀 유출사건이 지속적으로 발생하고 있는 것을 감안해 볼 때 산업기밀 유출을 방지하기 위한 일은 쉬운 일의 아닌 것으로 보인다.

산업기술보호를 활성화하기 위하여 물리적인 보안시스템과 기술적인 보안시스템 구축과 함께 관리적 보안업무를 강화할 필요가 있는데, 본 연구에서는 국가핵심기술을 보유하고 있는 기관을 대상으로 관리적 보안업무 실태를 조사・분석하여 다음과 같은 대응방안을 제시할 수 있다.

첫째, 보안정책을 보다 효과적으로 실행할 수 있는 기반 조성을 강화하는 것이 필요하다. 국가핵심기술을 보유한 기관 대부분이 보안규정을 관리하고 있으나 보안규정을 지키고 지속적으로 개선하는 노력이나 보안업무를 전담하는 조직과 보안담당자를 보유하고 있는 정도가 다소 부족하다. 보안규정은 적절한 절차와 방법으로 모든 구성원에게 알릴 수 있고, 조직 내 보안업무 수행을 위한 팀 간 업무 공조체계를 이룰 수 있는 조직문화가 필요하다. 이와 함께 지속적이고 현실적인 보안감사를 통해 순차적으로 보안수준을 개선하고 보안정책을 보다 효과적으로 실행할 수 있을 것이다.

둘째, 보안활성화를 위해 보안투자의 증가가 필요하다. 산업기밀 유출경로와 수단이 다양화・첨단화 되어가고 있을 뿐 아니라 복잡하고 빠른 속도로 변화하고 있기 때문에 관련 전문기관인 국가정보원, 한국인터넷진흥원, 정보보호 컨설팅 전문기업, 관련 대학 및 연구소 등과의 협조채널을 유지하고 확인하는 작업이 요구되며, 필요에 따라서는 보안 전문기관으로부터 outsourcing 도입을 검토할 필요가 있다. 이를 위해 보안 투자를 증가할 수 있어야 하며, 공공기관이나 대기업에 비해 보안정책 운영실태가 미흡한 중소기업은 조직 규모나 재정적 여건을 감안하여 보안관리 능력을 보강할 수 있도록 국가적 차원에서 지원할 수 있는 시스템 확장이 필요하다.

셋째, 산업기밀 유출의 주체는 사람이므로 인력관리가 중요하다. 신규 입사자와 임직원을 대상으로 하는 정기적인 보안교육률은 높은 것으로 평가되나, 보다 효과적인 교육을 위하여 콘텐츠 활용도와 전문가에 의한 체계적인 보안교육 기회를 증가시킬 필요가 있다. 임직원 뿐 아니라 핵심기술에 접근하는 제3자로부터도 보안서약서 징구받고, 핵심기술을 다루는 사람에 한하여 신원조사를 실시할 수 있는 여건 조성이 필요하다. 그리고 정보자산에 대한 접근권한이 변경될 때 접근권한 변경 설정도 같이 이루어 질 수 있어야 하며, 퇴사자에 대한 보안서약서 징구를 비롯하여 주요 정보시스템에 대한 접근권한 제거와 계정을 삭제하는 적극적인 보안활동이 요구된다. 그리고 평상시 컴퓨터 관리와 출입문, 문서관리, 개인서랍 관리 등을 지속적으로 점검하여 보안의식을 향상시킬 필요가 있으며, 보안정책이나 절차를 위반한 직원에 대하여 공식적인 징계 절차가 있어야 하고, 규정준수 여부를 직원업무평가에 포함하고 이를 실행할 수 있는 인식이 필요하다.

넷째, 중요한 자산에 대한 통제와 관리를 강화해야 한다. 자산에 대한 목록과 관리기준은 비교적 잘 정리되어 있으나 자산의 중요성에 따른 등급화(극비, 대외비, 일반 등)와 관리규정의 보완 작업이 필요할 뿐 아니라 중요한 자산이 유출되거나 손상되는 경우에 대비한 영향정도를 평가를 실시와 함께 자산에 대한 주기적인 점검을 활성화 할 수 있어야 한다. 그리고 자산에 대한 중요도는 시간흐름 및 업무특성에 따라 변화되기 때문에 주기적인 자산평가작업과 분류작업을 통한 사용자 권한 설정이 필요하다.

참 고 문 헌

1. 국내문헌

국가정보원 산업기밀보호센터(2008).「산업기술유출방지법 요해」.

김경규・최서윤・허성혜(2009). "산업기술보호를 위한 기술적 보안의 탐색적 연구". 한국항행학회지 제34호.

김동복(2007). "첨단산업기술유출의 방지대책과 법적동향". 한국콘텐츠학회지 제5권 2호.

김민배(2009). "일본의 기술보호동향과 전망". 산업기술보호 창간호.

김민배・김경준(2007). "산업기술의 유출방지 및 보호에 관한 법률과 쟁점". 한국산업재산권법학회지 제23호.

김정덕・홍기향(2007). "정보보호 거버넌스 이슈 및 연구과제". 정보보호학회지 제4호

김정덕・정태황・장항배・권태종(2008). "산업기술보호를 위한 보안기술 개발정책 연구", 한국산업기술보호협회 보고서.

노호래(2008). "산업기술유출범죄에 대한 정책적 대응방안". 한국공안행정학회보 제17권 1호

오흥룡・오세순・김선・염홍열(2005). "정보보호표준화 항목 정의 및 로드맵". 정보보호학회지 제15권 5호.

유다혜・윤신숙・오수현・김한구(2007). "국내정보보호시스템 평가기관 승인자격기준 개발". 정보보호학회지 제17권 3호.

육소영(2008). "산업스파이에 대한 법적 고찰". 충남대학교 법학연구소 법학연구 제19권 2호.

이대성(2010). "정보유출방지 연구기술동향". 정보보호학회지 제20권 1호.

이정덕(2007). "산업스파이범죄에 대한 대응방안에 관한 연구". 한독사회과학논총 제17권 3호.

이준승(2010). "국가연구개발사업 보안과제 활성화 방안". 산업보안 연구논집 제6호.

이창무(2010). "범죄자 프로파일링기법을 활용한 산업기밀 유출방지의 필요성". 산업보안연구논집 제6호.

임채호(2006). "효과적인 정보보호 인식제고". 정보보호학회지 제16권 2호.

장항배(2010). "비즈니스 관점의 산업보안 발전방향 연구". 산업보안연구논집 제6호: 179.

정진근(2010). "산업기밀 유출범죄의 효율적 규제를 위한 법적 개선방안". 산업보안연구논집 제6호: 285.

조용순・홍영서(2007). "산업기술유츨규제에 관한 법적고찰". 한국산업재산권학회지.

주일엽(2008). "외국정보기관의 인간정보(HUMINT) 활동에 대응한 산업기술 보호방안". 한국경호경비학회지 제17호.

지식경제부(2009).「산업보안실무 가이드북」.

_____(2009).「산업기술의 유출방지 및 보호에 관한 법률」.

_____(2008).「유비쿼터스 환경에서의 정보보호 정책방향」.

한국산업기술보호협회(2010).「산업보안시스템구축 사례집」.

_____(2010).「산업보안시스템 구축전략설명회」.

한국정보사회진흥원(2008).「국가정보화백서」.

홍도원(2006). "정보보호기술의 현재와 미래" 정보보호 제40호.

홍성혁・박종혁・서정택(2008). "국내환경에 적합한 정보보호관리체계 평가방법론". 한국한행학회지 제12권 4호.

Abstract

A Study on the Real Condition and the Improvement Directions for the Protection of Industrial Technology

Chung, Tae-Hwang · Chang, Hang-Bae

This study is to present a improvement directions for the protection of industrial key technology. For the purpose of the study, the survey was carried out on the administrative security activity of 68 enterprises including Large companies, small-midium companies and public corporations. survey result on the 10 items of security policy, 10 items of personal management and 7 items of the assets management are as follows;

First, stable foundation for the efficient implement of security policy is needed. Carrying a security policy into practice and continuous upgrade should be fulfilled with drawing-up of the policy. Also for the vitalization of security activity, arrangement of security organization and security manager are needed with mutual assistance in the company. Periodic security inspection should be practiced for the improvement of security level and security understanding.

Second, the increase of investment for security job is needed for security invigoration. Securing cooperation channel with professional security facility such as National Intelligence Service, Korea internet & security agency, Information security consulting company, security research institute is needed, also security outsourcing could be considered as the method of above investment. Especially small-midium company is very vulnerable compared with Large company and public corporation in security management, so increase of government's budget for security support system is necessary.

Third, human resource management is important, because the main cause of leak of confidential information is person. Regular education rate for new employee and staff members is relatively high, but the vitalization of security oath for staff members and the third party who access to key technology is necessary. Also access right to key information should be changed whenever access right changes. Reinforcement of management of resigned person such as security oath, the elimination of access right to key information and the deletion of account. is needed.

Forth, the control and management of important asset including patent and design should be tightened. Classification of importance of asset and periodic inspection are necessary with the effects evaluation of leak of asset.

Key Word : Industrial Technology, Security Level, Security Policy, Human Resource Management, Asset.

논문투고일 2010.07.30, 논문심사일 2010.08.18, 게재확정일 2010.09.24