기밀유출방지를 위한 융합보안 관리 체계

이창훈* · 하옥현**

요 약

정보통신의 눈부신 발전은 생활의 편리함과 더불어 산업기술 발전을 도모하였다. 국가 간의 기술 경쟁 시대에 돌입한 현 시점에 국가 뿐만 아니라 기업 간의 기술 확보와 기술 경쟁이 치열하게 이루어지고 있다. 이렇게 산업기밀의 유출로 인한 피해는 그 회사나 국가의 존폐를 위협할 정도로 위협적이기 때문에 이를 효과적으로 예방하고 관리하는 기술이 국내·외적으로 이루어지고 있다. 현재 산업기밀 유출을 방지하기 위한 연구는 크게 물리적 보안 기술과 정보보호 보안 기술로 구분되어 연구되고 있다. 산업기밀 보호에서의 물리적 보안 기술은 출입통제시스템, 접근권한시스템, 도난방지 시스템과 같은 물리적 공간이나 물리적 장치의 접근과 사용을 보안 관리하는 것이며, 정보보호 보안 기술은 네트워크 트래픽 모니터링, 이메일 모니터링, USB 사용 모니터링, 기밀 파일 접근 통제 모니터링 등의 통신이나 소프트웨어 및 전자문서의 접근과 사용을 보안 관리하는 기술이다. 본 논문은 산업기밀 보호 체계에 있어서 물리적 보안과 정보보호의 이런 이분화 된 보안 체계의 문제점을 도출하고 이를 효과적으로 해결하고 융합할 수 있는 방안을 제시한다.

A Study on Convergence of Cyber Security Monitoring and Industrial Security

Chang Hun Lee* · Ok Hyun Ha**

ABSTRACT

Information communication the dazzling development life was convenient with to join in and planned an industrial technical advance. Not only the nation with technical security of the enterprise between the description competition keenly in the present point of view which rushes to technical competitive time of the nation between is become accomplished. The damage which is caused by with outflow of industrial secrecy that company prevents this effectively because is threatening at the degree which will threaten the existence of the nation and the technique which manages is become accomplished with the domestic foreign enemy. Prevents an industrial secret outflow the research for on a large scale with physical security technique and information security to be divided, is researched.

Key words : Industrial Security, Convergence Security

접수일 : 2010년 11월 1일; 채택일 : 2010년 12월 15일

* 경기대학교 정보보호기술공학과

** 교신저자, 호남대학교 경찰법행정학부

1. 서 론

정보통신과 산업기술 발전으로 인하여 국가 간의 기술 경쟁 시대에 돌입하게 되었고, 국가 뿐만 아니라 기업 간의 기술 확보와 기술 경쟁이 치열하게 이루어지고 있다. 이런 기술 무한 경쟁시대로 인하여 기술의 가치와 중요성은 날로 높아지고 있으며, 국가 및 기업의 상호간 핵심 기술을 확보하고 보호하려는 노력이 지속적으로 이루어지고 있다.

향후 10년 간 피해액은 5,000조 이상에 이를 것으로 예상되며, 산업기술보호 전문 인력, 장비, 그리고 기술이 취약한 현 상태를 그대로 지속된다면 향후 3~5년 후에는 국가경쟁력 저하 및 국가 경제에 심각한 파탄 상태에 이를 수 있는 상황이다[1].

지식정보보안 시장은 전 세계적으로 빠르게 성장하고 있으며, 미국, 유럽, 일본을 중심으로 미래 융합보안 시장선점을 위한 원천기술 R&D 경쟁력이 가속화 되고 있다.

따라서, 본 논문은 산업기밀 보호 체계에 있어서 물리적 보안과 정보보호의 이런 이분화 된 보안 체계의 문제점을 도출하고 이를 효과적으로 해결하고 융합할 수 있는 방안을 제시한다. 이렇게 함으로써 국내·외의 산업체 뿐만 아니라 국가의 융합된 산업기밀 보호체계를 정립할 수 있으며, 이를 통하여 국가와 기업의 산업기밀 유출로 인한 경제적 피해를 최소할 할 수 있다.

2. 관련 연구

2.1 산업기밀 유출 실태 조사

가. 산업기밀 유출 적발 실적

산업기술 불법유출 발생건수는 연도별로 증가하는 추세이며, 건당 평균예방액도 큰 폭으로 증가하는 추세.

나. 산업기밀 유출 현황

기업 규모별로는 대기업보다는 중소기업과 벤처기업에서의 기술유출 시도가 각 각 전체의 63%를 차지.

〈표 1〉 2004~2008년 분야별 산업기술 해외 유출사건 적발건수

구 분	전기 전자	정보 통신	정밀 기계	생명 공학	정밀 화학	기타	계
대기업	21	7	13	0	0	6	47
중소기업	47	19	10	3	10	14	103
기 타	5	1	0	3	0	1	10
계	73	27	23	6	10	21	160

2.1.1 기술유출 주체

전·현직 직원을 통한 유출건수가 전체의 82.5%를 차지하고 그 다음이 협력업체, 유치과학자, 투자업체의 순으로 나타남.

〈표 2〉 2004~2008년 분야별 산업기술 해외 유출주체별 비중(국정원 산업기밀보호센터)

구 분	계	전직원	현직원	협력 업체	유치 과학자	투자 업체	기타
건수	160	89	43	16	6	3	3
비율 (%)	100	55.6	26.9	10.0	3.8	1.9	1.9

유출주체별 비중(국정원 산업기밀보호센터).

2.1.2 기술유출 유형

전·현직 직원의 금전적 매수를 통한 기술유출 유형이 전체의 55.6%를 차지하고, 내부공모에 의한 유출도 10.6%를 차지.

〈표 3〉 2004~2008년 기술유출 유형별 산업기술 해외 유출주체별 비중(국정원 산업기밀보호센터)

구 분	계	매수	무단 보관	공동 연구	위장 합작	내부 공모	기타
건수	160	89	30	9	6	17	9
비율 (%)	100	55.6	18.8	5.6	3.8	10.6	5.6

2.1.3 기술유출 동기

개인영리와 금전적 유혹의 비율이 75%를 차지하며, 조직에 대한 불만에 의한 기술유출 동기도 17%를 차지하는데, 이는 전체 유출사건의 92%를 차지하는 동기요인으로 작용.

〈표 4〉 2004~2008년 유출동기별 산업기술 해외 유출주체별 비중(국정원 산업기밀보호센터)

구 분	계	개인 영리	금전 유혹	처우 불만	인사 불만	비리 연루	기타
건수	160	68	52	16	11	4	9
비율 (%)	100	42.5	32.5	10.0	6.9	2.5	5.6

3. 문제점 및 체계 분석

3.1 국내 · 외 산업기술 유출 사례 분석

3.1.1 인력이동 유출 사례

인력 스카우트에 드는 비용은 해당 개인에게는 파격적인 액수이지만 기업에서 들인 시간과 비용에 비해서는 미미한 수준이다. 이를 이용해 국내에서 적발된 해외 스카우트 사건의 경우 국내업체가 205억 원을 투입해 개발한 최신 휴대폰기술을 얻기 위해, 홍콩 기업이 8명에게 스카우트비와 연봉을 11억 6천 만 정도만 들여 산업기밀은 얻으려는 사례가 있다. 또한 2001년부터 추진한 국내 초음파 진단기 제조회사의 인수 협상이 결렬되자 2002년 8월에 한국에 지사와 초음파 연구소를 설립하여, 국내 초음파 진단기 회사의 핵심인력 3명이 독일 기업의 한국지사로 이직하는 과정에서 3년 동안 420억 원을 투자해 개발한 3차원 동영상 초음파 진단기 기술을 유출 시킨 사례가 있다. 이와 같이 해외 경쟁업체가 국내에 지사를 설치하고 고액 연봉과 각종 인센티브 등의 조건으로 핵심인력을 스카우트 하는 형태의 핵심기술 유출을 시도한다.

3.1.2 기술거래로 인한 유출 사례

외국 기업에서 한국 기업의 무선단말기 공급 및 기술이전 계약을 체결하고 주요 기술 자료를 계속 제공받았다. 제공받은 기업은 국내 경쟁업체인 다른 기업의 소속 연구원에게 다른 업체를 설립하게 하고 국내 업체에서 입수한 자료를 토대로 제품을 개발하도록 하였다. 개발이 완료되자 기존의 계약을 맺은 한국 기업과 계약을 일방적으로 파기하고 새로 설립하게 한 제품을 상용화하려고 추진하다가 적발된 사례가 있다. 지적재산 보호가 엉성한 국가의 기업에게 기술을 이전하는 경우, 계약을 위반하거나 일방적으로 파기하는 사례가 다발하는 경우가 있다.

3.1.3 산업스파이 활동으로 인한 유출 사례

과거 국내 대기업이 개발한 60인치 PDP TV가 독일 하노버에서 개최된 첨단 전자제품 전시회에 전시된 후에 뉴델리로 이송 중 도난이 된 사례가 있다. 또한 국내 타 대기업의 63인치 PDP TV가 미국 라스베가스에서 개최되는 방송장비쇼에 전시할 목적으로 힐튼호텔로 이송 중 도난 되는 사례가 있었다. 이는 경쟁업체가 내부인력 포섭, 위장취업 등의 방법으로 불법 스파이 활동을 전개하는 형태의 산업기밀 유출 사례이다[2].

3.1.4 인수합병으로 인한 유출 사례

과거 중국 자본에 의해 국내기업 인수합병 및 시도 된 사례가 있었다. 국내 유명 자동차 기업의

자동차 생산기술은 모두 중국 자동차 기업으로 모든 기술이 넘어간 사례가 있었으며, TFT-LCD 생산기술을 가지고 있던 국내기업 또한 중국의 한 기업에 의해 인수된 사례가 있다. 첫 번째는 외국기업이 국내기업 인수를 통해 기술을 획득하는 것은 합법적인데, 국가 차원에서 보면 중대한 기술이 유출되는 경우가 있다. 두 번째로는 인수를 빙자로 인수 과정에서 인수하고자 하는 기업의 정보만 입수하고 인수를 포기하는 경우도 있다.

3.1.5 해킹, 바이러스 인한 유출 사례

기술유출은 사람에 의해서만 이뤄지는 것이 아니다. 과거 해커를 고용하여 자료를 빼낸 후 타사에 제공하려다 적발된 사례가 있다. 기업의 기밀뿐 만아니라 개인정보 피해 사례가 날이 갈수록 빈번히 일어나고 있다. 해킹에 의한 기밀유출은 당하고도 모를 수 있는 점이 특징이며, 고도의 프로그램 운영능력 보유자들이 기업-공공기관의 전산망 등에 침투하여 정보를 빼내거나 삭제하는 행위.

3.2 국내·외 산업기술 유출 대응 방안

3.2.1 기술거래 유출 대응 방안

기술 거래는 정상적인 일대일 계약 체결이 아닌 제 3국 기업과의 이중 계약과 같은 불법적 거래를 통해서 이루어진다. 또는, 기술 이전을 받는 회사가 교육 이후 일방적인 계약 파기를 통해서 핵심기술이 유출되는 경우가 있다. 이는 회사 간의 확실한 계약 문서화 및 검토를 통해서 해결할 수 있는 문제이다. 하지만 인원 매수를 통해 노트북, 외장 하드디스크 또는 E-mail 등을 이용한 기술 거래 유출의 경우는 정보보안, 인원보안으로 해결하는 방법으로는 한계가 있다. 융합보안관제를 통해서 예방 통제할 수 있다. 실시간으로 보고되는 관제 시스템과 정보시스템의 융합 기술을 통해서 사전 예방 혹은 원천 봉쇄가 가능하다. 이는 산업 기밀 유출의 가장 전형적인 형태로 융합보안관제의 필요성을 강조시킨 형태중 하나이다.

- ○ 기술 거래社간의 긴밀한 계약 및 문서화를 통한 법적 규제 및 통제
- ○ 융합보안관제를 통한 기밀 유출 사전 예방 및 원천 봉쇄

3.2.2 산업스파이 유출 대응 방안

산업스파이는 더 이상 한 기업의 문제가 아닌 국가의 경쟁력이 달린 국가적 차원의 문제로 이에 대한 현재의 실태를 분석하고 대응방안을 모색해야 할 중요한 문제가 되고 있다. 산업스파이로 인하여 산업기밀이 유출되고 나면 범인을 체포하더라도 이미 유출된 산업기밀로 인하여 기업의 피해는 막대할 수밖에 없다. 산업스파이는 사후대응보다 사전에 예방하는 것이 가장 효과적인 방법이다. 사전에 예방하기 위해서는 보안 관리 감독체계가 구축되어야 한다. 기업 내 담당부서를 설치하여 보안담당자를 지정하고, 정기적으로 보안점검 및 감사를 실시하는 등 사전에 산업스파이를 예방할 수 있는 보안관리 감독시스템을 구축하여야한다. 대기업의 경우는 자체적인 보안관리 시스템 구축의 예산이 뒷받침 되지만 중소기업이나 벤처기업의 경우에는 규모의 영세성으로 인하여 정부차원에서 핵심기술의 보안관리를 위한 예산을 지원하는 방안도 대응방안 중 하나이다. 또한 민·관 협력체계의 구축을 도모하여 효과적인 협력체계를 구축하여야 한다. 기술 인력에 대한 관리체계의 구축도 이루어져야 한다. 산업스파이는 대부분 전·현직 직원이 개인영리를 위하여 발생하는 만큼 기업은 핵심인력에 대하여 기술 개발에 전념을 다할 수 있도록 충분한 보상과 대우를 해주어야 한다. 이제 차별화된 보상시스템을 구축해야 한다.

3.2.3 인수합병 유출 대응 방안

적대적 M&A에 대한 사전 및 사후 방어 전략으로 나누어서 대응해야 한다. 사전 방어 전략으로

는 유사시 기존 주주에게 신주 매입할인인권 부여하는 독약조항과 M&A 관련 결의는 평상시보다 더 많은 찬성표를 요구할 수 있는 특별다수권, 모든 이사를 일괄적으로 바꾸지 못하도록 금지하는 이사 선임권 및 이러한 방식은 사전방어 전략이며, 사후방어 전략을 살펴보면 우호적인 제 3자에게 지분을 넘기는 전략인 백기사 전략, 유통 주식수 감소를 통해 공격자의 주식확보를 방해하는 자사주취득과 주요 자산을 매각해 공격 유인 요소를 제거하는 주요자산매각을 적용 시켜 사후 방어 전략을 갖춰 놓으면 적대적 인수합병에 대응할 수 있다.

3.2.4 산업기술 유출 대응 방안

대응방안의 선행요건으로 관련 법률을 정비할 필요성이 있다. 부정경쟁방지 법과 산업기술유출방지법이 이원화되어 있어서 이를 적절하게 보완해야 할 것이다. 현행 부정경쟁방지법과 기술유출방지법의 이원적 체제로 나아가되, 부정 경쟁방지법은 본래 목적상의 취지에 맞게 영업비밀 침해행위에 대한 민사적 규제에 관한 사항만을 규정토록 하고, 기술유출방지법은 그 동안 국내 법제에서 미흡했던 사전보안의식 및 사전보안체제 확립에 대한 근거 법률적 역할과 함께 기술유출에 대한 강력한 형사적 규제를 담당하도록 양 법률의 역할을 이원화 시키는 방안이 바람직할 것이다. 양 법률의 중복적인 부분을 방지하고 각 법률의 목적에 따라 그 기능을 강화함으로써 보다 나은 산업보호 법제를 완성해야 할 것이다[3].

4. 산업기밀 융합 보안 체계 개발

4.1 융합보안 체계 분석

4.1.1 보안관리 체계 현황

현재 대다수의 조직 혹은 기관에 적용 되어있는 보안체계를 살펴보면, 크게 세 가지 영역으로 분리되어있다. 각 물리적 보안 영역, 관리적 보안 영역, 기술적 보안 영역으로 분리되어 운영되고 있는 상황이다.

4.1.2 보안관리 체계 분석

기존의 보안관리 체계는 독립적으로 영역을 구성하여 운영되고 있는 보안체계의 지배구조 하에 있지만 관리자 및 관리 대상이 상이하여 서로간의 상호연계성에 큰 어려움이 있다. 즉 각각의 보안체계가 잘 수립되어있더라고 하나의 영역에 취약점이 발생 하였다면, 전사적인 차원의 보안사건/사고를 예방 혹은 대처가 어려운 현실이다.

4.2 산업기밀 융합 보안 체계 개발

4.2.1 기존 보안관리 체계 주요 보완 측면

기업의 에코시스템은 급속도로 확장하고 있으며, 이는 새로운 기술 적용 및 사업 수행 방식의 변화로 조직 구조를 보다 복잡하게 만드는 요인으로 작용하고 있다. 이는 대다수의 기업과 기관들은 비용절감을 통한 경쟁력 확보에 중점을 두고 있으며, 이를 위하여 외부의 제 3자로부터 일부 IT 기술을 아웃소싱하고 있으며, 이러한 제 3자는 전 세계적으로 확장되고 있다. 이런 경우 제 3자로부터의 보안이 중요점으로 대두되고 있다[4].

(1) 위험 관리 프로세스

위험 관리 프로세스는 사람과 프로세스와 기술을 포함하여 관리하여야 한다. 위험 관리의 목적을 달성하기 위해 적절한 권한과 충분한 역량을 갖춘 관리자에 의해 수행되어야 하며, 대부분의 경우에 프로세스를 수정해야하고 리스크 관리 활동의 결과에 따라 재배열, 새로운 위험이 나타나지 않도록 해야 합니다. 기술은 리스크 관리를 지원하는 역할을 해야 하며, 그것을 효과적으로 활용하

여야 한다. 이에 각 요소간의 원활한 커뮤니케이션과 위험 카탈로그 보다 일관성 있는 모니터링을 조성할 수 있는 전용 리스크 관리 소프트웨어의 사용을 통해 품질과 일관성을 향상 시켜야한다. 정부 또한 위험 관리 프로세스를 만들어 전체 기업에 미치는 영향을 보안 위험으로 간주하고 다른 기업의 위험 및 비즈니스 목적과 목표의 큰 컨텍스트 내에서의 해결을 보장해야 한다.

(2) 융합 보안 체계 분석 및 개발

기존의 서로 다른 영역에서 수행된 보안 활동을 연계하여 하나의 영역에서 관리되어짐이 필요하다는 것 알 수 있다. 하지만 현재 국내에서 연구되고 있는 융합보안은 두 가지 차원에서 혼용되고 있으며, 그 의미가 상이한 만큼 적용 영역이나 기술체계도 다르다고 할 수 있다. 이는 향후 연구 및 적용에 혼란을 가져올 우려가 있기에 확실한 체계 정립이 필요하다.

4.2.2 통합보안 측면

Converged CSO는 조직의 시스템이 복잡하고, 통합보안의 구현을 위한 자원이 부족할 경우, 기존의 물리적/기술적 보안 프로세스를 통합하지 않고, 각각의 보고체계를 구성하여, 개별적인 물리적/기술적 보안 프로세스를 통합적으로 관리 할 수 있다. 한편 기존의 물리적/기술적 보안 프로세스를 통합하였을 경우, 통합보안 전담 부서를 구성하여 정보보호 프로세스 및 통제를 효율적으로 평가, 모니터링 할 수 있다. 이러한 통합 보안 전담 부서는 조직의 물리적/기술적 위험을 통합적인 시각으로 식별하고, 평가하며, 위험을 허용수준 이내에서 관리할 수 있도록 한다. 또한 통합보안 적용 시 조직의 비즈니스 프로세스를 고려하는 것 또한 중요하다고 할 수 있다. 통합보안을 단순히 물리적 보안과 기술적 보안을 통합하는 개념으로 인식하는 것에는 한계점이 존재한다[5, 6].

4.2.3 복합보안 측면

복합보안은 제품 및 서비스의 안전성과 신뢰성 향상을 위해 보안이 산업에 융합되어 산업의 부가가치를 높이는 것이라고 할 수 있다. 하지만, 단순히 제품 및 서비스에 보안기능을 추가하는 것은 여전히 한계점을 내포한다. 즉, 복합보안은 산업에서 창출된 최종 결과물인 제품 및 서비스뿐 아니라, 산업의 원천기술 및 지식, 인적자원 역시 보호해야 한다는 의미이다. 그러므로 복합보안 측면에서 본다면 가장 많은 부가가치를 창출하는 요소를 식별하고, 이를 우선순위에 따라 보호해야 한다. 산업의 본원적인 활동을 생산, 운송, 마케팅, 판매, 물류, 서비스 등과 같은 현장업무라 한다면, 이러한 본원적 활동을 지원하는 구매, 기술개발, 인사, 재무, 기획 등의 제반업무가 필요하다. 이런 현장업무와 제반업무를 가치 활동이라 하였을 때, 원재료, 부품, 서비스 등을 제공하는 공급자의 가치사슬과 최종 산출물인 제품 및 서비스를 구매하는 구매자의 가치사슬에는 보안 취약점이 존재한다. 이러한 취약점으로 인해 산업 기술 및 지식이 유출될 위험이 존재할 수 있다.

5. 결 론

융합보안의 두 가지 측면과 기존 보안 체계를 고려하여 융합 보안 체계를 제시 하였다. 기존의 보안체계는 물리적, 기술적, 관리적 보안의 영역이 나뉘어져 운영되고 있었다. 이러한 단점을 보완하기 위해 융합 보안 체계기 필요하기에 위험 관리 프로세스를 기본으로 사람과 기술, 프로세스 모든 단계에서 유기적인 위험 관리가 이루어져야 하며 나뉘어져서 개발 및 운영되었던 보안 영역의 경계를 허물어야한다. 이에 다음 융합 보안 체계를 제시한다. 물리적, 기술적, 관리적 요소가 나뉘어져 있지 않고 한 가지 영역에서 유기적인 연동이 되어야 하며, 모든 과정에 있어서 보안을 고려해야

한다. 통합적 측면의 장점인 정보보호 프로세스 및 통제의 효율적인 평가, 모니터링과, 복합보안 측면의 장점인 가치사슬의 경로의 취약점을 식별하고, 비용 효과를 고려하여 우선순위에 따라 적절한 통제를 구현하고 운영한다면 산업기밀의 부가가치를 향상시키고 신뢰성과 안정성을 높일 수 있다.

참 고 문 헌

[1] 산업기밀보호센터, “첨단 산업기술 보호동향 제9호”, pp. 65-99, 2008.

[2] 이호균, 이승민, 남택용, 장종수, “기밀정보 유출방지 기술 동향”, 정보통신산업진흥원, 2006.

[3] Brian E. Bruke and Rose Ryan, “Worldwide Secure Content Management 2005~2009 Forecast Up-date and 2004 Vendor Shares : Spyware, Spam, and Malicious Code Continue to Wreak Havoc”, IDC, 2005.

[4] 김정덕, 김건우, 이용덕, “융합보안의 개념 정립과 접근 방법”, 정보보호학회, 제19권, 제6호, pp. 68-74, 2009.

[5] Brian T. Contos, “The Convergence of Logical and Physical Security Solutions”, Networks insider, IT DEFENSE, 2006.

[6] Joel M. Snyder, “Unified Threat Management”, searchsecurity.com, Opus One.

이 창 훈

2010년 경기대학교 정보보호기술공학과(석사과정)

하 옥 현

1978년 성균관대학교 정치 외교학과(정치학사)

1980년 서울대학교 행정 대학원(행정학석사)

1998년 프랑스 사회과학 대학원(EHESS) 박사과정(DEA 취득)

2005년 고려대학교 정보보호대학원(공학박사)

2008년~현재 호남대학교 경찰법행정학부 교수