Journal of Korea Multimedia Society Vol. 13, No. 1, January 2010(pp. 111-121)

중소기업 산업기술 유출방지를 위한 정보보호 관리체계 설계

장 항 배†

요 약

중소기업들은 산업기술 유출방지에 필요성을 인식하여 많은 예산을 들여 정보보호 시스템을 구축하고 있으나, 정보보호 전담조직을 구성하여 통합적인 정보보호 관리체계에 따라 일관성 있는 정보보호 시스템을 구축하지 못하고 특정시스템의 단발성 도입이 이루어지고 있다. 본 연구에서는 중소기업 산업기술 유출현황 조사결과를 바탕으로 대기업과 차별된 중소기업 산업기술 유출방지를 위한 정보보호 관리체계를 설계하고 하였다. 세부적으로 중소기업 산업기술 유출현황 및 취약점 등에 관한 사례를 분석하여 정리하고, 델파이 방법을 적용하여 중소기업 산업기술 유출방지 관리체계를 설계한 다음 이에 대한 적합성을 검증하였다. 본 연구의 결과를 활용하여 중소기업은 적정한 정보보호 투자수준을 산정하고 이에 대한 통제도구를 개발할 수 있을 것으로 기대된다.

The Design of Information Security Management System for SMEs Industry Technique Leakage Prevention

Hang Bae Chang†

ABSTRACT

Since SMEs have recognized needs for industrial technique leakage prevention, they tend to construct information security system causing huge consumption of budget, yet they cannot organize information security team to operate integrated information security management system with consistency and it is fact that there only occur instant introductions of certain system. In this study, we designed information security management system for SMEs' industrial technique leakage prevention which is differentiated from those of large enterprises based on current status of SMEs' industrial technique leakage. Specifically we analyzed current status and vulnerability of SMEs' industrial technique leakage and we designed industrial technique leakage prevention management system for SMEs. Then we applied Delphi method to validate appropriateness of study result. We strongly believe that SMEs may estimate a appropriate level of investment on information security and develop countermeasures for control by utilizing this study result.

Key words: Data Leakage(정보유출), Information Security(정보보호), Information Security Management System(정보보호 관리체계)

※ 교신저자(Corresponding Author) : 장항배, 주소 : 경기도 포천시 선단동 산11-1(487-711), 전화 : 031)539-1752, FAX : 031)539-1750, E-mail : hbchang@daejin.ac.kr
접수일 : 2009년 8월 21일, 수정일 : 2009년 9월 1일
완료일 : 2009년 9월 14일
† 종신회원, 대진대학교 경영학과 조교수
※ 본 연구는 2008년도 한국산학협동재단 학술연구지원사업에 의해 수행되었습니다.

1. 서 론

최근 벤처기업을 중심으로 한 기술기반의 중소기업이 세계수준의 기술을 보유하게 되면서 중소기업이 보유한 기술에 대한 국내외 경쟁기업들의 관심이 높아진 상황에 기인하여 중소기업이 보유하고 있는 산업기술 유출에 따른 피해건수와 금액은 대기업에 비하여 상대적으로 급격히 증가하는 추세에 있다. 이러한 산업기술 유출에 따른 피해는 기업의 보유기술 수준이 기업의 경쟁력과 직결되는 지식정보화 사회에서 기업의 발전 속도를 지연시킬 뿐만 아니라 국가경쟁력을 약화시킨다는 점에 있어서 심각한 문제가 되고 있다.

이에 대한 해결방안으로 국내 중소기업들은 산업기술 유출방지에 필요성을 인식하여 많은 예산을 들여 정보보호 시스템을 구축하고 있으나, 정보보호 전담조직을 구성하여 통합적인 정보보호 관리체계에 따라 일관성 있는 정보보호 시스템을 구축하지 못하고 특정시스템의 단발성 도입이 이루어지고 있다. 이러한 형태의 단순한 정보보호 시스템 구축은 새로운 취약점들이 발생할 때마다 이에 대한 투자가 산발적으로 발생하게 되므로, 정보보호 투자에 대한 목표를 효율적이고 효과적으로 달성하기 위해서는 기업의 정보보호 추진을 조직수준(Managerial Level)의 관점에서 바라보면서 구성원의 정보보호 인식정도, 정보보호 시스템 구축수준, 정보보호 기술적용 가능성 등을 통합적으로 관리하는 정보보호 수준 평가모형에 따라 부분별로 개선하는 과정이 진행되어야 한다.

이에 대하여 지금까지의 정보보호에 관한 연구들은 대체로 다음과 같은 한계점을 지니고 있다. 첫째 기술적 접근이 중심이 되어 있고 정보보호와 관련하여 관리적 요인과 환경적 요인에 대한 연구가 매우 부족하다. 둘째 기존의 정보보호에 관한 연구들은 정보보호의 방법론을 소개하고 적용의 필요성에 대한 소개들이 대부분이며 최근에 와서야 정보보호 수준평가에 대한 관심과 정보보호 관리체계에 관한 연구들이 진행되고 있다. 셋째 기존의 정보보호 연구들이 앞서 설명한 바와 같이 아직 기초적인 수준에 머물러 있는 관계로 중소기업의 특성을 적용한 정보보호 연구가 매우 부족하다. 자본 규모가 크고 인력활용이 비교적 자유로운 대기업의 경우와는 달리 한정된 자원과 인력으로 영위하는 중소기업의 경우 환경적 그리고 자원 적 요인으로 인하여 정보보호의 특성이 다르게 인식되어야 하며 대응방안도 대기업과는 차별되게 나타나야 한다.

본 연구에서는 중소기업 산업기술 유출현황 조사 결과를 바탕으로 대기업과 차별된 중소기업 산업기술 유출방지를 위한 정보보호 관리체계를 설계함으로써, 중소기업이 실제로 정보보호를 추진하는데 있어 적정한 정보보호 투자수준을 산정하고 이에 대한 통제도구를 제공하고자 한다.

2. 중소기업 산업유출 특성

2.1 산업기술 유출 유형

최근 들어 빈번하게 발생하고 있는 불법적인 산업기술 유출유형은 크게 4가지 정도로 요약될 수 있다. 그 첫째가 인력이동에 의한 산업기술 유출이다. 고액연봉과 인센티브로 경쟁자 직원을 유인하거나, 제품시연 등을 위해 해외출장중인 국내 엔지니어를 매수하는 등 해외 경쟁업체가 국내에 지사를 설치하고 핵심인력을 스카우트하는 방법이다. 둘째로 부품 및 장비에 체화된 경험지식 이전의 방법이 있다. 국내 협력업체가 공동 개발한 핵심부품 및 장비를 경쟁업체에 수출하거나, 협력업체가 영업활동을 위해 국내 완제품, 설비업체 등의 기술정보를 수집하여 제공하는 등 협력업체의 부품 및 장비 수출에 의해 기술 및 경험지식이 유출되게 되는 경우가 해당된다. 셋째로 기술거래에 의한 산업기술 유출이 있다. 기술이전 받은 해외업체가 무단으로 다른 기업에 기술을 공여하거나 제3국 기업과 기술허가권 계약을 체결하는 경우, 또는 지분일부를 기술로 출자하여 합작회사를 설립했으나 현지 기업이 기술이전 교육만 받고 계약을 일방적으로 파기하는 등 기술이전 계약을 위반하거나 일방적으로 파기하는 사례가 증가하고 있는데 이 경우가 해당된다. 마지막으로 산업스파이에 의한 산업기술 유출이다. 국내 기업에 연구원, 기술고문 등으로 근무하는 외국인이 자국 정부기관이나 업체의 요청을 받고 기밀을 압수하는 등 내부 및 협력업체 인력, 위장취업 등 수법이 다양화되고 있는데 이러한 사례가 본 유형에 속한다 하겠다[1].

2.2 중소기업 산업기술 유출현황

중소기업은 핵심기술의 기업 내 비중이 대기업에

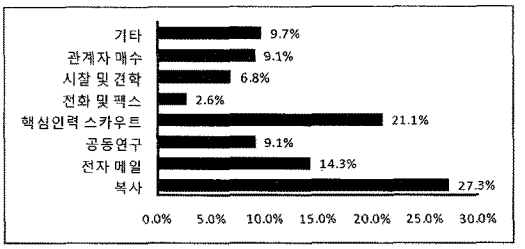

그림 1. 중소기업 산업기술 유출경로

비하여 상대적으로 많은 부분을 차지하고 있으며, 이에 따라 산업기술 유출가능성에 대한 위험정도도 높은 편이다. 중소기업청 자료에 의하면, 중소기업이 보유하고 있는 핵심 산업기술로서는 연구개발 기술 및 결과가 가장 많았으며, 산업 재산권, 생산기술, 영업비밀 또는 노하우 등으로 조사되었다. 산업기술 유출방법은 그림 1에서와 같이 복사 및 절취와 핵심인력 스카우트가 대부분을 차지했으며, 이는 퇴직자가 관련기밀을 빼돌려 스카우트 기업에 제공하는 전형적인 형태라고 할 수 있다. 그 밖에 전자메일, 합작사업 및 공동연구, 관계자 매수, 시찰 및 견학 등과 같이 다양한 경로를 통하여 산업기술이 유출되고 있다. 그러나 이에 대한 중소기업의 대응체계는 방문자 출입통제와 입사 시 비밀엄수서약을 제외한 모든 항목에서 취약한 것으로 조사되었다[2-7].

3. 정보보호 관리체계 연구

3.1 정보보호 관리체계 선행연구

정보보호 관리체계(ISMS, Information Security Management System)는 조직의 자산에 대한 안정성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리하고 운영함으로써, 정보보호 3 요소(기밀성, 무결성, 가용성)를 실현하기 위한 일련의 과정 및 활동이며 기업의 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적 경영시스템으로 인적 자원, 프로세스 및 정보시스템 모두를 그 대상으로 포함하고 있다[8].

'BS7799'는 영국 내 주요 기업들과 함께 영국의 상무성 주관으로 '정보보안관리 실무 규범'이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하여 조직의 보안 표준이 되도록 개발되었다. 'BS7799'는 기업이 직면하고 있는 상황에 필요한 통제를 식별하기 위한 단일한 참조 점을 제공하고, 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하여 공통적인 정보보안관리 문서를 참조함으로써 기업들 간의 교류에 있어서 상호신뢰가 가능하도록 설계되었다. 하지만, BS7799는 관리체계에 대한 인증으로서 정보보호 제품 및 시스템에 대한 인증과는 무관하며, 급변하는 정보보호 환경에 적응성과 유연성이 부족하고 높은 수준의 평가 기준만을 제공함으로써 중소기업에 그대로 적용하기에는 어려움이 많다.

한국정보보호진흥원에서는 'BS7799'의 내용을 기본으로 하여 정보 기술적 측면보다는 조직이나 환경적 측면에서 관리적 방식을 기초로 하여 다양한 환경에 종합적으로 적용할 수 있도록 정보보호 관리체계를 개발하였다. 이 관리체계는 크게 정보보호 관리(전략정책, 위험분석, 보안계획, 보안구현, 인식교육 및 보안감사의 업무를 수행하는 부분), 정보보호 산업(정보보호 제품과 정보보호 기반기술을 주로 담당하는 부분), 정보보호 기술(인증, 법률, 홍보, 표준화 관련하여 외부와의 접촉이 잦으며 기술의 표준이 필요한 부분), 정보보호 기반(정보보호의 최저 기반이 되는 기본 기술로서 암호화, 사고대응, 인정, 법률, 표준화, 홍보) 등 4가지 부분에 걸쳐 13개의 통제 분야를 제시하고 있다. 이 한국정보보호진흥원 관리체계는 정보보호 관리, 정보보호 산업, 정보보호 기술 등의 통제 분야를 제시하고 있으나 세부적인 적용방법론의 부재로 인하여 아직 적용사례가 부족하고 포괄적인 평가로 인하여 특정관리 분야가 과다하게 계상될 한계성을 가지고 있다[9-12].

3.2 산업기술 유출방지를 위한 관리적 보안 선행연구

산업기술 유출방지를 위하여 어떤 정책을 사용할 것인지, 관리방법은 어떻게 할 것인지 등을 결정하는 관리적 보안은 내부 인원에 대한 보안관리, 외부 인원에 대한 보안관리, 중요 자료에 대한 보안 관리로 분류할 수 있다. 내부 인원에 대한 보안 관리는 기업 내에서 근무하게 되는 인원에 대한 관리를 말한다. 직원의 채용, 재직, 퇴직 등의 단계별로 관리하며 채용 시 정보사용에 대한 기업에 맞는 보안 서약서를 작성하는 것이 좋다. 또한 정기적인 보안교육이 필요하며 퇴직 시 재직 중에 관리하였던 연구 · 개발 및

영업비밀과 관련된 일체를 반납하고 이를 확인하여야 한다. 외부 인원에 대한 보안 관리는 기업 내부에서 일하는 직원을 제외한 업무상 정기적으로 출입하는 협력업체 직원 등에 관한 관리이다. 외부에서 출입하는 직원에 대해서는 최소한으로 제한하고 출입지역도 일정한 한계를 두어 핵심시설에는 일체 접근하지 못하도록 엄격하게 통제해야 한다. 다른 업체·단체에 제공한 자료는 반드시 회수하고 별도의 보안대책을 수립하여 시행하여야 하며, 하청 및 부품업체와 제품 판매업체 직원 등에 대해서도 중요정보에 접근하지 못하도록 사안별로 적절한 보안대책을 강구해야한다. 중요 자료에 대한 보안 관리는 기업의 핵심이 되는 정보·자료의 관리에 관한 것이다. 제품의 설계도·소스코드 등 핵심기술 자료는 영업비밀로 분류하고 비인가자는 접근하지 못하도록 물리적·기술적 보안대책을 강구해야한다.

중요자료를 외부에 제공하거나 열람시키는 것은 엄격히 제한하되 부득이하게 제공해야 할 경우에는 관련인원을 최소한으로 제한하고 보안서약서를 받는 등 적절한 보안대책을 강구해 두어야 한다. 또한 기술이전이나 하청계약 체결 시 자료를 제공할 때에는 반드시 비밀 유지 의무조항을 포함시키고 이를 위반하였을 경우 책임소재를 명시하는 등의 관리가 필요하다. 표 1은 내부정보 유출방지를 위한 관리적 보안을 위한 세부지침을 정리한 내용이다.

표 1. 내부정보 유출방지를 위한 관리적 보안 지침(예시)

항목	지 침
1	전사적 위험평가를 주기적으로 수행
2	전 직원 대상 주기적인 인식제고 훈련 수행
3	직무분리 및 최소권한부여 원칙 준수
4	강력한 사용자인증 및 계정관리 정책과 절차 준수
5	직원들의 시스템 사용에 대한 로그·모니터링 및 감사
6	시스템 관리자 및 특수권한 소유자에 대해 각별한 주의 수행
7	유해코드로부터의 적극적이고 능동적인 방어 활동
8	원격접근 공격에 대비한 단계별 방어 전략
9	의심스럽고 파괴적인 행위에 대한 모니터링 및 대응
10	퇴사 시 해당 시스템 접근권한 차단
11	향후 조사에 대비한 자료의 수집과 보관
12	안전한 백업과 복구절차 실행
13	내부자 위협 대응책에 대한 명확한 문서화

3.3 산업기술 유출방지를 위한 물리적 보안 선행연구

물리적 보안은 실제 정보에 대해 정보를 관리하는 구역, 장소, 방법 등에 대해서 관리하게 된다. 물리적 보안은 중요시설 보호 관리와 출입자 통제로 나눌 수 있다. 중요시설은 기업의 핵심 기술이나 정보가 있는 곳으로 이것을 물리적으로 보호하는 것은 최후이자 가장 확실한 방법이라 할 수 있다. 중요 시설, 생산 공장, 사무실, 연구실 등 중요 시설의 위치·특성 등을 면밀히 검토하여 시설 자체보다는 그 시설이 가지고 있는 기능을 보호할 수 있는 대책을 강구해야 한다. 그리고 출입 통제를 위하여 중요시설에 접근하는 모든 출입자의 통제를 통해 중요시설을 보호하며 사용하는 내·외부를 감시할 수 있다. 핵심시설에 대해서는 출입 인가 자를 지정하고, 인가된 자 이외에는 출입하지 못하도록 통제하며 협력업체 시설 또는 장비 보수 등을 목적으로 출입하는 인원은 사전에 신원확인에 필요한 서류를 확보하여 비치하고 보안서약서를 받는 것이 좋다. 또한 임시출입자는 먼저 신분을 확인한 후 출입대장에 인적사항, 방문목적, 연락처 등을 기재하고 입사출입증을 소지하게 하여 반드시 직원 안내를 받아 출입하도록 조치하는 것이 필요하다.

3.4 산업기술 유출방지를 위한 기술적 보안 선행연구

기술적 보안은 위험분석 과정 속에서 도출된 취약점 분석결과에 따라 취약점 문제를 해결하기 위한 기술을 설계하는 위험분석 기반 산업보안 기술 설계 방법론에 따라 정리할 수 있다. 보안 취약점은 개인용 컴퓨터 정보자산에 대한 보안 취약점, 전자문서에 대한 보안 취약점(그림 2), 데이터베이스 보안 취약점, 네트워크 보안 취약점(그림 3)으로 나뉠 수 있으며, 이러한 보안 취약점들을 보호하기 위한 기술보안 방법은 일반적으로 다음과 같이 유형을 정리될 수 있다. 산업정보의 유출을 방지할 수 있는 기술적인 보안방법으로는 정보에 대한 접근을 제한하거나 차단하는 방법, 데이터나 파일을 암호화하여 권한이 없는 사용자는 파일의 내용을 열어볼 수 없도록 하여 정보의 노출을 방지하는 방법, 데이터나 파일이 유출되는 경우에 로그를 남기어 유출되는 내용을 모니터링 하는 방법이 있으며, 유출경로에 대해 복사를 제

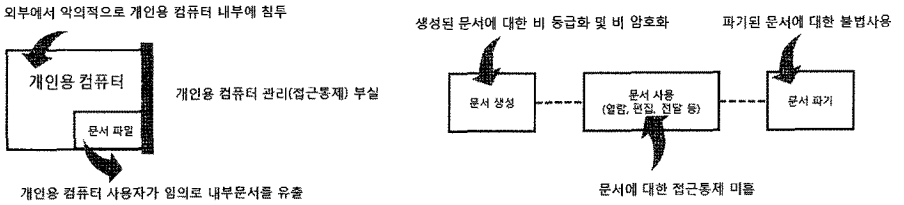

그림 2. 개인용 컴퓨터 및 전자문서 취약점 유형(예시)

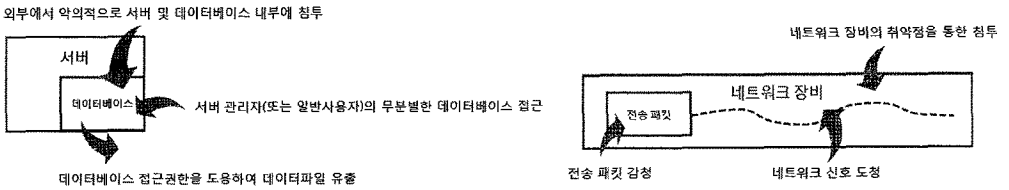

그림 3. 데이터베이스 및 네트워크 보안 취약점 유형(예시)

한하거나 파일의 전송을 차단하는 방법, 데이터나 파일이 저장된 장치를 파괴하는 방법 등이 있다.

3.5 산업기술 유출방지를 위한 중소기업 정보보호 관리체계 설계 요구사항

산업기술 유출방지를 위한 중소기업 정보보호 관리체계를 개발하기 위하여 선행연구들의 한계성을 고려하여 다음과 같이 개발 요구사항을 정리하였다. 먼저 '중소기업의 정보보호 현실을 고려하여 복잡한 구조보다는 단순한 구조를 가져야 한다.'는 특성을 고려하여 많은 수의 관리체계 영역을 설정하기보다는 객관적으로 측정이 가능한 관리체계 영역에 중점을 두고 주관적 관리체계 영역을 최소화하는 방안을 수립하고자 한다. 중소기업은 내외부적인 변화에 의하여 영향을 많이 받기 때문에 생략 및 간소화가 용이하고, 지속적인 수정과 보완이 가능하도록 하기 위하여 어느 기업에게나 적용할 수 있는 보편타당한 정보보호 관리체계를 개발하고자 한다.

또한 중소기업은 경영자원의 부족으로 인하여 중소기업에서 정보보호를 수행하고자 할 때에는 매출활동 중단이나 지연이 발생할 수 있으며, 이것이 중소기업에 미치는 영향이 매우 크기 때문에 시간과 비용이 많이 소요되는 프로세스 모형보다는 통제모형으로 설계하고자 한다. 마지막으로 대기업에 비하여 국제규격을 취득하거나 이를 유지하기 위한 경영자원이 불충분하다는 점을 참고로 하여 다양한 기준으로 확장이 가능하고 대외 경쟁력을 확보할 수 있는 국제 표준규격 기반의 정보보호 관리체계를 구성하고자 한다.

4. 정보보호 관리체계 설계

4.1 정보보호 관리체계 설계를 위한 개념적 이해

정보보호는 기업의 정보화 수준에 부합되도록 수준 및 전략을 설계하여야 하기 때문에 기업의 일반적인 정보화 계층구조(Application Architecture, Technical Architecture)를 기반으로 설계되어야 한다. 이를 위하여 본 연구에서는 정보화에 대한 수준평가 연구와 함께 정보보호 관리체계에 대한 선행연구를 동시에 진행했다. 그 다음 분석된 선행연구에 따라 정보화 자산식별과 정보화 구성요소에 대한 정리하여 이들을 보호하기 위한 정보보호 범위와 함께 중소기업 정보보호 관리체계 영역을 정의했다(표 2). 정보보호 관리체계 세부항목은 정의된 정보보호 관리체계 영역에 따라 정보보호 관리체계에 관한 선행연구들을 참고로 하여 세부항목들을 배치하고 정보보호 전문가에 대한 설문과정을 반복 실시한 다음, 중소기업의 정보보호 특성에 적합하지 않은 부분은 삭제함으로써 중소기업 정보보호 관리체계 세부항목을 구성하였다[13-15].

4.2 중소기업 정보보호 특성연구

사전에 진행된 중소기업 정보보호 현황조사를 바

표 2. 중소기업 정보보호 관리체계 영역 설계

정보화 구성요소		정보 자산	정보보호 관리체계 영역	
정보화 지원환경	정보화 의지	→	정보보호 의지	정보보호 지원환경
	정보화 지원 조직		정보보호 조직	
	정보화 인식 확산		정보보호 인식	
	정보화 정책		정보보호 정책	
	정보화 투자		정보보호 투자	
정보화 기반구조	기술적 요소	시설물	물리적 보안	정보보호 기반구조
		네트워크	기술적 보안	
		서버		
		개인용 컴퓨터		
	지식 및 경험적 요소	공유된 전자문서	관리적 보안	
	공유 정보 서비스 요소			
정보화 감사	규정 준수	→	준수확인	정보보호 운영관리
	사고 대응		보안사고 대응	

탕으로 본 연구에서는 대기업과 차별화된 중소기업 특유의 정보보호 특성을 추출하기 위하여 중소기업(312개 기업) 및 대기업(158개 기업)을 대상으로 2008년 10월~12월까지 3개월 동안 설문조사를 진행하였다. 설문내용에 따른 세부적인 조사결과 및 시사점을 표 3과 같이 정리하였다.

먼저 기업 규모별 정보보호에 대한 필요성 인식여부에 관한 문항에서는 중소기업(90%)과 대기업(98%) 모두 정보보호에 대한 필요성을 어느 정도 인식하고 있었다. 기업 규모별 보호하여야 할 정보자산의 종류로는 중앙의 정보시스템에 정보자산을 설치하고 이를 공유하는 대기업과는 달리, 중소기업의 경우, 선행연구 결과와 마찬가지로 개인용 컴퓨터에 저장된 정보자산이 상대적으로 많았다.

기업규모별 정보자산을 보호하기 위한 활동 중 어려운 점으로는 대기업 및 중소기업 모두 정보보호 투자(정보보호 투자금액이 미비함) 및 개인용 컴퓨터 보안(정보보호 관련 업무를 모두 직원 개인에게 일임함으로써, 개인의 정보보호 인식 및 도덕성에 의존도가 높음)분야에 상대적으로 어려운 점을 가지고 있으며, 중소기업의 경우 정보보호 인식부분 어려운 점을 가지고 있었다.

표 3. 기업 규모별 보호하여야 할 정보자산 현황

	공유 전자문서	개인용 컴퓨터	네트워크	서비스 서버
중소기업	29%	39%	21%	11%
대기업	27%	26%	24%	23%

구체적인 정보보호 활동으로서 기업규모별 정보보호 정책수립 현황의 경우, 선행연구 결과와 유사하게 조사대상 중소기업의 대부분(86%)이 정보보호 정책수립이 없는 상태이며, 대기업의 경우에는 정책이 수립되어 수행과 함께 지속적인 개선까지 진행되고 있다. 또한 기업규모별 정보보호 교육 프로그램 운영현황은 선행연구 결과와 유사하게 조사대상 중소기업의 대부분(97%)이 별도의 정보보호 교육 프로그램이 미비한 상태이며, 대기업의 경우에는 정보보호 교육 설계와 실행이 진행되고 있었다.

기업규모별 정보자산 보호를 위한 제한구역 운영현황은 중소기업의 대부분은 자원부족을 인하여 정보자산 보호를 위한 별도의 제한구역 운영을 못하고 있으나, 대기업의 경우 제한구역 설정뿐만 아니라, 제한구역을 출입하는 사용자에 대한 기록을 별도로 보관하고 있다. 또한 기업규모별 정보화 장비를 보호하기 위한 활동현황(표 4)의 경우 중소기업의 대부분은 장비관리에 대한 목록이 없거나, 장비관리 목록은 존재하고 있으나 보안 등급은 설정되지 않은 상태(이상 83%)이다. 이와 반면에 대기업은 장비관리 목록과 함께 보안등급에 따른 차별화된 관리가 진행되고 있다(이상 86%).

기업규모별 조직운영을 위한 정보보호 정책현황으로 중소기업의 대부분은 조직운영에 관리를 위한

표 4. 기업규모별 정보화 장비를 보호하기 위한 활동현황

	장비관리 목록 없음	장비관리 목록은 존재하나, 보안등급이 없음	장비관리목록과 보안등급 설정	장비관리 목록, 보안등급에 따라 실제로 관리	장비관리 규정이 지속적으로 변경
중소기업	48%	35%	9%	5%	3%
대기업	14%	32%	14%	26%	14%

표 5. 기업규모별 정보보호 시스템 구축현황

	시설물 및 장비보안	네트워크 보안	서비스 서버 보안	개인용 컴퓨터 보안
중소기업	50%	41%	35%	78%
대기업	81%	90%	84%	96%

세부적인 활동이 부족한 상태(입사 시 보안 서약서만 받고 있는 상태)이며, 대기업의 경우 조직인원의 생애주기에 따라 세부적인 보안활동을 진행하고 있다. 또한 기업규모별 문서보안 관리현황은 중소기업의 문서보안 관리현황은 정보화 장비관리 현황과 유사하게, 문서관리 목록이 없거나, 목록이 있어도 보안등급이 부여되어 차별화된 관리가 되지 않고 있다.

기업규모별 정보보호 시스템 구축현황(표 5)을 살펴보면, 선행연구 결과와 유사하게, 중소기업은 개인용 컴퓨터 보안에 시스템 구축이 중점적으로 진행되었으나, 다른 정보자산에 대한 정보보호 시스템 구축은 부족한 상태이다. 참고적으로 정보보호 시스템은 문헌 및 조사결과를 고려해 볼 때, 개인용 컴퓨터 보안, 시설물 및 장비보안, 네트워크 보안, 서비스 서버 보안 순으로 진행되는 경향을 보이고 있다.

기업규모별 보안사고 발생 시 보안사고 처리절차의 경우에도 대기업 수립 비율이 상대적으로 높으며, 보안사고 정책개선에 대한 절차 수립 율은 낮은 상태이다. 특히 중소기업은 대기업에 비하여 보안사고 체계 및 보안사고 정책 개선 절차가 매우 미흡한 상태이다.

전체적인 중소기업의 정보보호 수준은 대기업의 절반 수준에도 못 미치는 상태이며(표 6), 중소기업 기업규모에 따라 중소기업의 정보보호 수준도 함께 증가하고 있으며, 특히 직원 수 50명, 100명 지점에서 정보보호 수준차이가 급격히 발생하고 있다(표 7).

또한 중소기업 정보보호 측정항목을 계량화한 다음, 중소기업들을 대상으로 정보보호 수준을 기준으로 3계층으로 군집분석(clustering)하여, 중소기업 정보보호 수준별 집단 간 정보보호 결정요인을 도출한 결과 중소기업 정보보호 수준 1~2 단계 사이에 정보보호 수준 결정요인은 정보화 자산 제한구역 운영 및 보안사고 발생 시 처리절차 여부로 도출되었으며, 중소기업 정보보호 수준 2~3단계 사이에서는 보안사고 발생 시 처리절차 여부, 문서보안, 정보보안 시스템 구축 등으로 도출되었다(그림 4).

표 6. 중소기업 정보보호 수준별 정보보호 항목 측정결과

정보보호 항목	1 단계	2 단계	3 단계
정보보안정책	1.18	3.00	4.31
정보보안교육	0.96	2.74	4.59
자산보호제한구역	1.00	4.00	5.00
장비보호정책	1.42	3.38	5.00
조직운영정책	0.83	1.85	3.58
문서보안	0.00	1.55	3.68
정보보안시스템구축	1.00	2.48	4.57
보안사고발생시처리절차	0.76	2.71	4.91

표 7. 중소기업 기업규모별 보안사고 발생에 따른 처리절차 현황

기업 규모별 그룹	100점 기준	격차
1(5~9명)	25.80 점	
2(10~19명)	27.39 점	1.59점
3(20~49명)	27.59 점	0.2점
4(50~99명)	32.07 점	4.48점
5(100~299명)	36.53 점	4.46점
6(300명 이상)	36.08 점	-0.45점
평균	30.91 점	

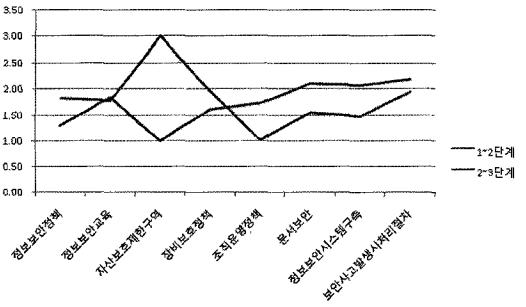

그림 4. 중소기업 정보보호 수준별 정보보호 결정요인 추출

4.3 산업기술 유출방지를 위한 정보보호 속성 연구

산업기술 유출방지를 위한 정보보호 활동은 일반적인 정보보호 활동과는 차별적으로 크게 4가지의 속성 관점에서 차이가 있다. 본 연구에서는 이러한 특성을 고려하여 중소기업 산업기술 유출방지를 위한 관리체계 영향요인으로 정의하였다. 산업기술 유출 위험은 접근성, 중요성, 복제성에 비례하고, 탐지성에 반비례한다(그림 5). 다시 말하면, 정보에 대한 접근빈도가 증가하는 행위, 정보의 중요성이 높은 경우, 정보의 복제가 쉬울수록 위험이 높아지며, 정보

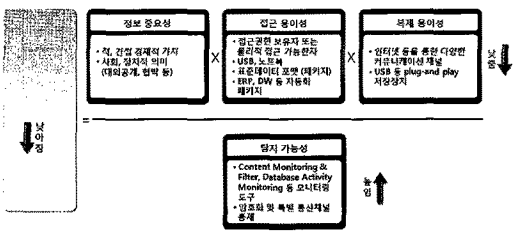

그림 5. 산업기술 유출방지를 위한 정보보호 속성

사용의 탐지가 강력해 질수록 위험이 줄어든다. 따라서 산업기술 유출방지를 위한 정보보호 관리체계는 접근성, 중요성, 복제성을 낮추며 탐지성을 개선시킬 수 있는 활동으로 구성되어야 한다[16-19].

4.4 산업기술 유출방지를 위한 중소기업 정보보호 관리체계 설계

중소기업 산업기술 유출방지를 위한 관리체계를 설계하기 먼저 일반적인 정보보호와는 차별화 된 선행연구 분석결과에 따라 취약점을 도출하고 이에 대한 해결방안을 전문가 회의(학계 3명, 산업계 3명)를 통하여 델파이 방법을 진행하였다(표 8). 델파이 방법은 전문가 집단으로부터 설문을 통하여 의견을 듣고 통계분석 결과를 다시 설문하여 의견을 수렴 집계하는 반복과정을 말한다. 이 방법은 각자의 전문가 의견을 수정할 기회가 주어지고, 다른 전문가의 의견을 활용할 수 있다는 점에서 매우 긍정적이며, 현재 기술 예측연구 분야에서는 90% 이상이 델파이방법을 사용할 정도로 보편적인 방법으로 자리 잡고 있다. 또한 전문가 집단의 참여를 통하여 신뢰성 있는 평가 결과를 얻을 수 있으며, 비교적 광범위하고 분석적인 견해를 제시하여 줄 수 있다.

도출된 산업기술 유출방지를 위한 해결방안들은 속성에 따라 산업기술 보호를 위한 관리체계 항목으로 정의되고, 문헌적 방법을 통하여 세부적인 산업기술 관리체계를 구성하는 세부 관리항목을 설계하였다(표 9). 그리고 설계된 관리항목들에 대하여 앞서 설명한 산업기술 유출방지를 위한 정보보호 속성과 연결하여 검증하고, 중소기업 정보보호 특

표 8. 산업기술 유출 취약점 및 대응방안

산업기술 유출 취약점	산업기술 유출방지 방안
산업기술 유출 방지 정책 및 절차 등이 미흡	산업기술 보호정책
산업기술 유출 사고 방지는 불가능하다는 인식	산업기술 보호 인식제고
산업기술 유출방지 역량 부족	산업기술 보호 교육 및 훈련
무방비한 산업기술 정보 접근	산업기술 처리절차
산업기술에 대한 조사 및 등급 분류 미흡	산업기술 정보 체계화
내부자의 불만의식(승진, 연봉, 발령 등)	산업기술 업무 담당자 관리
다양한 정보유통 경로 상의 정보유출 통제 미흡	산업기술 보호 시스템
산업기술 접근권한 공유 및 변경관리 미흡	산업기술 규정 준수
응용프로그램 상의 책임 추적 성 확보 미흡	산업기술 유출 보안사고 대응

표 9. 중소기업 산업기술 유출방지 관리체계

산업기술 유출방지 방안	관리체계 항목	관리체계 세부항목		관리체계 영역
산업기술 보호 인식제고	산업기술 교육 및 훈련	· 산업기술 보호 홍보(인식제고) · 산업기술 보호 전문교육		산업기술보호 지원역량
산업기술 보호 교육 및 훈련				
산업기술 보호정책	산업기술 관리적 보안	· 산업기술 보호 정책 · 산업기술 보유현황 관리 · 산업기술 정보 등급 및 분류 · 산업기술 업무처리절차 · 산업기술 활동 보안감사 · 산업기술 사고처리 절차		산업기술보호 지원환경
산업기술 처리절차				
산업기술 정보 체계화				
산업기술 규정 준수				
산업기술 업무 담당자 관리	산업기술 인적보안	· 산업기술 보호 담당조직 · 산업기술 인력변동 관리 · 산업기술 인력보상 체계		
산업기술 보호 시스템	산업기술 물리적 보안	접근통제	· 산업기술 제한구역 관리 · 산업기술 처리장비 관리 · Access Control System · Alarm Monitoring System	산업기술보호 기반구조
		책임추적	· CCTV System	
	산업기술 기술적 보안	접근통제	· Mail&Messenger Security · Document Security · DB Security · Network Access Control	
		책임추적	· Content Monitoring and Filtering · Digital Forensic	

표 10. 중소기업 산업기술 유출방지 관리체계 검증

관리체계 영역	관리체계 항목	유출방지 속성	가중치
산업기술보호 지원역량	산업기술 교육 및 훈련	정보 중요성	0.22
산업기술보호 지원환경	산업기술 관리적 보안	정보 중요성 및 접근 용이성	0.11
	산업기술 인적보안	정보 중요성	0.27
산업기술 보호 기반구조	산업기술 물리적 보안	접근 용이성 및 탐지 가능성	0.20
	산업기술 기술적 보안	접근 용이성 및 복제 용이성	0.20

성연구 결과에 따라 가중치를 산출하였다(표 10). 중소기업의 산업기술 유출을 최소화하기 위하여 설계된 관리체계는 크게 산업기술보호 지원역량, 산업보호 지원환경, 산업기술보호 기반구조 등과 같이 3가지 영역으로 구성된다. 산업기술보호 지원역량은 산업기술 보호활동을 추진하기 위하여 보유하고 있는 전문지식 수준을 의미하며, 산업기술 지원환경이란 조직의 산업기술보호 활동을 효율적으로 수행하기 위하여 필요한 무형적, 유형적 자원을 제공하는 환경을 의미하며, 산업기술보호 기반구조는 산업기술을 보호하기 위하여 필요한 접근통제 및 책임추적 목적의 기술적 시스템 구축 및 운영을 말한다.

참고로 본 연구를 통하여 설계된 중소기업 산업기술 유출방지체계는 기존의 일반적인 정보보호 관리체계와 비교해 볼 때 외부로부터의 공격을 방어하기 위한 보호시스템은 포함하고 있지 않은 반면, 조직 내 안전한 정보유통 및 외부로의 정보유출 차단 시스템이 강조되고 있다. 또한 관리체계를 구성하고 있는 세부적인 항목들의 내용을 살펴보면 일반적인 정보보호 활동보다는 차별적으로 정보유출 방지활동에 특화된 내용을 포함하고 있으며, 이러한 활동들에게는 일반적인 정보보호 항목들보다 상대적으로 높은 가중치가 부여되고 있다.

5. 결 론

국내 중소기업들은 산업기술 유출방지에 필요성을 인식하여 많은 예산을 들여 정보보호 시스템을 구축하고 있으나, 정보보호 전담조직을 구성하여 통합적인 정보보호 관리체계에 따라 일관성 있는 정보보호 시스템을 구축하지 못하고 특정시스템의 단발성 도입이 이루어지고 있다. 이러한 형태의 단순한 정보보호 시스템 구축은 새로운 취약점들이 발생할 때마다 이에 대한 투자가 산발적으로 발생하게 되므로, 정보보호 투자에 대한 목표를 효율적이고 효과적으로 달성하기 위해서는 기업의 정보보호 추진을 조직수준(Managerial Level)의 관점에서 바라보면서 구성원의 정보보호 인식정도, 정보보호 시스템 구축 수준, 정보보호 기술적용 가능성 등을 통합적으로 관리하는 정보보호 수준 평가모형에 따라 부분별로 개선하는 과정이 진행되어야 한다.

이에 대하여 지금까지의 정보보호에 관한 연구들은 대체로 다음과 같은 한계점을 지니고 있다. 첫째 기술적 접근이 중심이 되어 있고 정보보호와 관련하여 관리적 요인과 환경적 요인에 대한 연구가 매우 부족하다. 둘째 기존의 정보보호에 관한 연구들은 정보보호의 방법론을 소개하고 적용의 필요성에 대한 소개들이 대부분이며 최근에 와서야 정보보호 수준평가에 대한 관심과 정보보호 관리체계에 관한 연구들이 진행되고 있다. 셋째 기존의 정보보호 연구들이 앞서 설명한 바와 같이 아직 기초적인 수준에 머물러 있는 관계로 중소기업의 특성을 적용한 정보보호 연구가 매우 부족하다. 자본 규모가 크고 인력활용이 비교적 자유로운 대기업의 경우와는 달리 한정된 자원과 인력으로 영위하는 중소기업의 경우 환경적 그리고 자원 적 요인으로 인하여 정보보호의 특성이 다르게 인식되어야 하며 대응방안도 대기업과는 차별되게 나타나야 할 것으로 보인다. 다시 말해서 기존의 정보보호에 대한 연구에 있어 중소기업에 관한 고려가 매우 부족하여 현재 제시되고 있는 방법론들이나 수준평가를 중소기업에 그대로 적용하는 데에는 현실적으로 무리가 있는 것이 사실이다. 따라서 중소기업의 정보보호를 활성화하고 촉진하기 위해서는 조직 수준의 중소기업과 대기업의 정보보호 관리체제에 관한 특성적 차이에 관한 연구가 필요하다.

따라서 본 연구에서는 중소기업 산업기술 유출현황 조사결과를 바탕으로 대기업과 차별된 중소기업 산업기술 유출방지를 위한 정보보호 관리체계를 설계하고 하였다. 세부적으로 중소기업 산업기술 유출현황 및 취약점 등에 관한 사례를 분석하여 정리하고, 이에 대한 내용을 델파이 방법을 적용하여 중소기업 산업기술 유출방지 관리체계를 설계하였다. 설계된 내용은 산업기술 유출방지를 최소화하기 위한 문헌연구 내용을 적용하여 적합성을 검증하였다. 그 결과 3개의 관리체계 영역(지원역량, 지원환경, 기반구조)이 개발되고, 5개의 관리체계 항목(교육 및 훈련, 관리적 보안, 인적보안, 물리적 보안, 기술적 보안)과 22개의 관리체계 세부항목(산업기술 보호 홍보, 산업기술 보호 전문교육, 산업기술 보호 정책, 산업기술 보유현황 관리, 산업기술 정보 등급 및 분류, 산업기술 업무처리절차, 산업기술 활동 보안감사, 산업기술 사고처리 절차, 산업기술 보호 담당조직, 산업기술 인력변동 관리, 산업기술 인력보상 체계, 산업기술 제한구역 관리, 산업기술 처리장비 관리, Access Control System, Alarm Monitoring System, CCTV System, Mail & Messenger Security, Document Security, DB Security, Network Access Control, Content Monitoring, and Filtering, Digital Forensic)이 설계되었다.

본 연구결과를 바탕으로 중소기업은 산업기술 유출방지를 위하여 기존 경영전략 및 정보화전략 등과 연계한 정보보호 정책에 따라 정보보호 관리체계를 수립함으로써, 기존에 가지고 있었던 정보관리상의 문제점을 개선함과 동시에 효율적인 정보보호 시스템을 구축하고, 운영할 수 있을 것으로 기대된다.

먼저 학문적 측면에서는 중소기업과 대기업의 특성적 차이를 규명하는 연구들은 이제까지 많이 있었지만, 정보보호 분야에서 이러한 특성을 반영하여 실제로 산업기술 유출방지 분야에 특화된 정보보호 전략이나 모델을 중소기업에 차별적으로 적용 특화된는 아직 없었던 것으로 보이며, 이러한 측면에서 본 연구는 중소기업에 적합한 산업기술 유출방지를 위한 정보보호 관리체계를 실증적인 방법을 활용하여 도출하는데 의의가 있다. 또한 중소기업의 특성들과 중소기업 정보보호 관리체계 요소들을 실증적으로 연관 지어서 정보보호 관리체계 설계를 진행하는 접근방법은 실무에 직접적으로 적용할 가치가 있을 것이며, 정책적으로 활용할 기회가 있을 것으로 기대된다. 실무적 측면에서는 정보 유출방법의 다양화(전자메일, 인스턴트 메신저, 파일 전송, 채팅 등), 기업 내부정보 관리

체계의 부실(회사 내부의 중요 정보에 대한 중요도와 기밀 정도에 따른 보안 등급 설정 및 분류에 대한 관리 체계가 부실) 등으로 인한 중소기업의 산업기술 유출 위험을 조직관점에서 최소화 할 수 있다. 또한 산업기술 유출방지를 위한 중소기업의 정보보호 구축현황에 대하여 정확한 이해를 돕고, 아울러 기업 스스로 정보보호를 추진할 수 있도록 동기를 부여할 수 있다(성공사례를 참조하여 자발적인 정보보호 추진).

마지막으로 이러한 주제의 연구는 횡단적인(cross sectional) 접근방법으로는 한계가 있기 때문에, 정보보호 관리체계의 유효성과 효율성을 위해서는 장기적인(longitudinal) 연구를 통해 정보보호 관리체계의 적용 가능성을 향상 시킬 필요가 있다.

참 고 문 헌

[1] 중소기업기술정보진흥원, "중소기업 핵심기술 유출실태," 2007.

[2] 한국산업기술진흥협회, "기업연구소 산업기밀 관리실태 및 개선방안," 2007.

[3] 형준호, 김문선, 황순환, "중소기업 정보보호 실태분석," 2005년 경영학 관련 학회 하계통합학술대회 논문집, 2005.

[4] 김종기, 전진환, "대기업과 중소기업 간의 정보보안 요소에 대한 사용자의 인지 비교: 컴퓨터 바이러스를 중심으로," 정보보호학회논문지, 제16권, 5호, 2006.

[5] 문현정, "우리나라 중소기업의 정보 보호 역량 강화를 위한 교육 훈련 현황과 문제점," 정보보호학회지, 제19권, 1호, 2009.

[6] 여상수, 황수철, "중소기업 정보시스템의 안정적 운영 전략," 한국컴퓨터정보학회논문지, 제14권, 7호, 2009.

[7] 국가정보원, "첨단 산업기술 보호동향," 제9호, 2008.

[8] M. M. Eloff and S. H. von Solms, "Information Security Management: An Approach to Combine Process Certification And Product Evaluation," *Computers & Security*, Vol.19, 2000.

[9] NIST Technology Administration, "An Introduction to Computer Security: The NIST Handbook," NIST USA, 1998.

[10] BSI, "BS 7799 Part1: Information Security Management - Code of Practice for Information Security Management," 1999.

[11] ISACA, "Information Security Governance, Guidance for Boards of Directors and Executive Management," IT Governance Institute, 2001.

[12] 김정덕, 최홍식, 홍기향, "조직의 정보보호관리 성숙도측정을 위한 프레임웍 연구," 한국경영정보학회, 2002년 춘계학술대회, 2002.

[13] Margi Levy and Philip Powell, "SME Flexibility and the Role of Information Systems," *Small Business Economics*, Vol.2, 1998.

[14] Georgios I. Doukidis, Panagiotis Lybereas and Robert D. Galliers, "Information Systems Planning in Small Business: a Stages of Growth Analysis," *Journal of Systems and Software Archive*, Vol.33, 1996.

[15] Weill, P. and M. Vitale MIS Quarterly Executive, "What IT Infrastructure Capabilities are Needed to Implement e-Business Models?," pp. 17-34, 2002.

[16] Dodson Rob, "Information Incident Management," Information Security Technical Report, pp. 45-53, 2001.

[17] Forte, Dario, "Information Security Assessment: Procedures and Methodology," *Computer Fraud & Security*, pp. 9-12, 2000.

[18] Jay Heiser, "Understanding Data Leakage," *Gartner*, 2007.

[19] Andrew P. Moore, Dawn M. Cappelli, Thomas C. Caron, Eric Shaw and Randall F. Trzeciak, "Insider Theft of Intellectual Property in Organizations: A Preliminary Model," MIST 2009 Conference Proceeding, 2009.

장 항 배

2001년 3월~2006년 2월 연세대학교 정보시스템 박사

2007년 3월~현재 대진대학교 경영학과 조교수

관심분야 : 산업보안, u 비즈니스 전략, 정보화(정보보호) 수준 및 성과평가