경영정보학연구
제15권 제1호
2005년 3월

중소기업 정보보호관리 모델의 개발: 실증 연구

이 정 우*, 박 준 기**, 이 준 기***

Developing Information Security Management Model for SMEs: An Empirical Study

Jungwoo Lee, Jungi Park, Zoonky Lee

This study is to develop an information security management model (ISMM) for small and medium sized enterprises (SMEs). Based on extensive literature review, a five-pillar twelve-component reference ISMM is developed. The five pillars of SME's information security are: centralized decision making, ease of management, flexibility, agility and expandability. Twelve components are: scope & organization, security policy, resource assessment, risk assessment, implementation planning, control development, awareness training, monitoring, change management, auditing, maintenance and accident management.

Subsequent survey designed and administered to expose experts' perception on the importance of these twelve components revealed that five out of tweleve components require relatively immediate attention than others, especially in SME's context. These five components are: scope and organization, resource assessment, auditing, change management, and incident management. Other seven components are policy, risk assessment, implementation planning, control development, awareness training, monitoring, and maintenance. It seems that resource limitation of SMEs directs their attention to ISMM activities that may not require a lot of resources.

On the basis of these findings, a three-phase approach is developed and proposed here as an SME ISMM. Three phases are (1) foundation and promotion, (2) management and expansion, and (3) maturity. Implications of the model are discussed and suggestions are made for further research.

Keywords : Small Businesses, Small and Medium Size Enterprises, Information Security, Information Security Management, Security Management Model

* 연세대학교 정보대학원(교신저자)
** LG이노텍
*** 연세대학교 정보대학원

Ⅰ. 서 론

중소기업은 국민경제 내에서 차지하는 비중으로 볼 때 각 산업분야의 발전에 초석이 될 뿐만 아니라 자아실현과 고객감동의 질 높은 서비스를 실현하는 데 적합한 기업형태이다. 그러나 중소기업은 그 소규모성에서 오는 장점보다는 자금·인력·기술 또는 정보 등 여러 면에서 대기업에 비하여 상대적으로 취약한 것이 현실이며, 중소기업이 영위하는 업종이 다종다양 하듯이 중소기업이 갖는 문제 또한 각양각색 이어서 이러한 문제를 중소기업이 자력으로 해결하기 어려운 경우도 많다[정보보호진흥원, 2003].

최근의 정보화 환경에서 새롭게 대두되는 정보화의 역기능은 정보의 활용이 고도화 되는 현재 환경에서 중요한 기업 경쟁력 저해요인으로 대두되고 있다. 특히, 대규모 정보화 투자를 진행하는 대기업이나 정부 공공기관에 비해 상대적으로 열약한 중소기업에게는 경쟁력의 확보를 위해서는 이러한 정보화의 역기능들 중 특히 정보보호 관리는 선결 과제가 되고 있다.

우리나라의 경우, 2003년 중소기업정보화경영원에서 1,261개의 중소기업과 66개의 대기업을 대상으로 직접 방문하여 정보화 역기능에 관한 실태 조사를 실시한 결과에 따르면, 지난 1년간 컴퓨터 해킹이나 바이러스 등의 정보보호 침해사고로 중소기업과 대기업을 불문하고 50%이상이 피해를 경험하였으며, 중소기업의 경우 정보보호 관련 대책 수립의 경우 대기업이 57.6%를 실시하고 있는 반면, 중소기업의 경우 16%만을 추진하고 있으며, 정보보호 전담조직의 구성도 대기업의 19.7%에 비해 중소기업은 9.4%만이 확보하고 있어 매우 낮은 상황임을 알 수 있다[중소기업정보화경영원, 2003]. 네트워크화가 심화되고 중소기업들이 대기업과 연계한 네트워크 경제가 발달하여 가면서 정보보호는 점차로 더 중요하여 질 것으로 보이며 특히 중소기업의 경우에는 사활이 걸린 문제로 등장할 가능성이 많다.

한편 지금까지의 정보보호에 관한 연구들은 대체적으로 다음과 같은 한계점을 지니고 있다. 첫째 기술적 접근이 중심이 되어 있고 정보보호와 관련하여 관리적 요인과 환경적 요인에 대한 연구가 매우 부족하다[김현수, 2000]. 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[김정덕, 2002]. 셋째, 기존의 정보보호 연구들이 이렇게 아직 기초적인 수준에 머물러 있는 관계로 중소기업의 특성을 적용한 정보보호의 연구가 매우 부족하다. 자본 규모가 크고 인력 활용이 비교적 자유로운 대기업의 경우와는 달리 한정된 자원과 인력으로 영위하는 중소기업의 경우 환경적 그리고 자원적 요인으로 인하여 정보보호의 특성이 다르게 인식되고 따라서 대응방안도 다르게 나타나야 할 것으로 보인다.

다시 말해서 기존의 정보보호에 대한 연구에 있어 중소기업에 관한 고려가 매우 부족하여 현재 제시되고 있는 방법론들이나 수준 평가를 중소기업에 그대로 적용하는 데에는 현실적으로 무리가 있는 것이 현실이다. 중소기업은 대기업과 다른 다양한 특징을 가지고 있기 때문에 무리한 적용은 적용하지 아니함만 못한 경우로 나타나기 십상이기 때문이다[Margi, 1999]. 따라서, 중소기업의 정보보호를 활성화하고 촉진하기 위해 전사적 관점에서 중소기업과 대기업의 정보보호 관리의 특성적 차이에 관한 연구가 필요하다.

본 연구에서는 (1) 중소기업의 경영과 정보화에 관련된 특성들을 연구하여 중소기업 특유의 필요조건들을 이론적으로 도출하였고 (2) 이어서 국내외 문헌 조사를 통하여 정보보호 관리모델을 제시하였고 (3) 실증 연구를 통하여 정보보호 관리모델의 각 구성요소들의 중요성을 비교 분석하여 중소기업 입장에서의 선결요소들을 구분해내고 (4) 이에 근거한 중소기업 특유의 정보보

호 관리 모델을 제시하였다.

Ⅱ. 이론적 고찰

2.1 정보화 역기능과 정보보호 정책

정보화가 급속히 진행되면서 정부, 기업, 개인 등과 같은 모든 경제 주체의 생활 방식과 거래 관행 등 사회의 전반적인 시스템이 급속히 변화되고 있다. 그러나 이러한 정보화의 급속한 확산 뒤에는 역기능이 존재하고 있다. 정보화 초기에는 정보화 마인드 확산을 위하여 주로 정보화의 순기능이 강조되었으나 최근 들어 정보화 추진에 걸림돌이 될 수 있는 역기능 문제에 대한 사회적 관심이 고조되고 있다. 인터넷 이용이 확산될수록 해킹, 바이러스, 감청 등 인터넷 보안 문제가 심각하게 대두되고 있다

2003년 초 우리나라의 초고속 기간망이 정지되는 사태가 발생하여 사회 전반적으로 수백억의 피해를 가져왔고, 또한 IT 선진국이라는 명예가 실추되는 사태가 발생했다. 이 처럼 정보시스템에 대한 예기치 않은 사태는 기업의 경쟁력뿐만 아니라 사회 전반적 경쟁력에 중요한 위협요인으로 작용하고 있다. 그 대표적인 사례로 정보시스템의 해킹 사례는 1999년에 572건, 2000년에 1,943건, 2001년 7월말 현재 3,074건에 달하는 등 매년 급속히 증가하고 있다[한국정보보호센터, 2002].

정보화의 진전은 기업의 중요한 의사결정 수단으로 정보시스템의 의존도가 높아져 가고 있으며, 중요한 정보와 지식의 디지털화를 촉진 하고 있으나, 빛의 속도로 정보전달이 가능해짐에 따라 정보화역기능 또한 불특정 다수에게 빠르고 폭넓은 피해를 유발하고 있다. 그러므로 정보화역기능 문제는 국가안보 및 사회전반의 건전한 윤리 확립에 중대한 도전이 되고 있는 것이며 정부와 대기업, 중소기업의 사활이 걸린 중요한 문제로 대두되고 있다.

국가적으로도 1996년 4월 정보화촉진 기본법에 의거해서 정보보호센터를 설립하였고 2001년에는 정보통신망이용촉진 및 정보보호 등에 관한 법률을 공포하면서 정보보호센터를 한국정보보호진흥원으로 격상시키면서 정보보호에 관한 인식을 높이는 데에 노력을 기울이기 시작하였다. 여기서는 인터넷 침해사고 대응지원, 주요 정보통신 기반시설 취약점 분석·평가, 스팸 메일 대응 및 개인정보보호 활동, 전자서명인증, 정보보호 산업 지원, 정보보호정책 개발 및 교육홍보 등 정보화 역기능의 방지에 중점을 둔 정책사업을 펼치고 있다.

또한 2002년 8월에는 "중장기 정보보호 기본계획"을 수립하면서 정보보호에 관한 국가적 중요성과 시급성에 대한 정책적 기본 방향을 설정하였다. 이러한 정부차원의 정보보호 정책에서는 우리나라가 정보화 역량에 비해 상대적으로 낙후된 정보보호 현황에 맞춰 기술과 인력 등 정보보호 인프라 구축을 중점적으로 추진하고 있으며, 특히, 정보보호 산업의 저변확대를 위한 마인드 확립, 패러다임 전환등 대국민 의식수준 향상에 그 초점을 맞추고 있다. 하지만 아직 대기업에 비해 상대적으로 열악한 실제 개별 중소기업에게 지속적으로 정보보안에 대한 관심과 투자를 유도할 수 있도록 하는 정책은 부족한 것으로 보인다.

2.2 정보보호 관리 기준

정보보호는 최신의 방화벽을 구축하고 보안회사를 계약을 통해 24시간 내내 이용하는 것만으로 끝나는 상황이 아니다. 정보보호에 대한 전체적인 접근방법에 있어서, 그리고 서로 다른 정보보호 수단을 통합하는데 있어서 각각의 요소들이 가장 효과적일 수 있도록 하기 위해서는 이들이 관리되어야 할 필요가 있다. 이에, 정보보호 관리가 필요한 것이며 이를 통해 자사의 정보보호를 위한 노력이 효과성을 발휘할 수 있게 된다

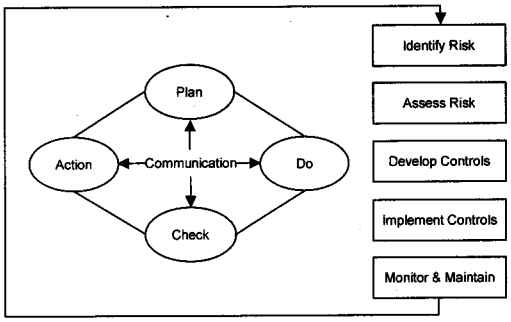
[BSI, 2001]. 이러한 전사적 정보보호를 위해 최근 정보보호 관리체계의 도입이 대기업을 중심으로 이루어지고 있다.

정보보호 관리체계(Information Security Management System, ISMS)란 조직의 자산에 대한 안정성 및 신뢰성을 향상시키기 위한 절차와 과정을 체계적으로 수립하고 문서화하여 지속적으로 관리, 운영하고 정보보호 목표인 정보의 비밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 실현하기 위한 일련의 과정 및 활동이다[BSI, 1999]. 이러한 관리체계는 기업이 민감한 정보를 안전하게 보존하도록 관리할 수 있는 체계적 경영시스템이며 이에는 인적 자원, 프로세스 및 IT 시스템 모두를 그 대상으로 포함하게 된다.

ISMS는 정보화의 역기능을 체계적으로 방지하고 대응하는 방법으로 크게 전사적 차원의 접근과 정보시스템이 기반이 되어 접근방식으로 분리할 수 있다. 우선 전사적 차원에서 접근하는 방식은 국내의 정보보호 관리지침과 영국의 표준방식인 BS7799이며, 나머지는 대부분이 정보시스템에 대한 기술적 기반으로 하여 접근하고 있다.

카네기 멜런대학이 개발한 SSE-CMM(System Security Engineering - Capability Maturity Model)은 적용 대상이 전체적인 구조를 소프트웨어 생명주기(Software Life Cycle)에 관한 국제표준인 ISO/IEC 12207에 기초하여서 조직이 구현한 IT 정보보호 프로세스를 각각의 단계와 매핑하여 정보보호의 성숙도를 측정하는 수단으로 활용할 수 있도록 개발이 되었다. 또한 IT Baseline Approach Method는 독일에서 표준으로 활용하는 방법론으로서 기술적인 정보보호를 중심으로 기업에서 정보보호를 수행할 경우 최소한으로 필요한 가이드라인을 정의하요 놓고 참조모델로 적용할 수 있도록 세부적인 절차와 방법을 제시하고 있으며, GMITS(Guidelines for the Management of IT Security)는 기본적으로 정보기술을 어떻게 보호하느냐, 다시 말해서 정보자산을 보호의 주요대상으로 삼고 있다.

일반적으로 정보보호 관리 체계의 기본적인 개념은 <그림 1>에 도식화 된 것과 같이 조직화된 보안개념으로 정보보호와 관련된 위험을 인식하고 평가하여 이를 통제할 방법들의 대안을 강구하여 실행하고 모니터하는 Plan-Do-Check-Action(PDCA) 사이클을 통한 지속적인 개선과정을 가리킨다[Ren-Wei fung, 2002].



<그림 1> 정보보호 관리체계에서의 PDCA 모델

앞에서 예시된 정보보호 관리 기준과 체계들의 정보보호 관리 프로세스는 품질 관리측면, 공학적 측면 및 정보보호 관리측면에서 다양하게 정의되고 있다. 품질 관리 측면에서는 정보보호 관리체계의 수립, 구현, 운영 및 개선의 순환적 활동으로 정의하고, 공학적 측면에서는 문제 해결의 과정 즉, 위험 식별 및 대책 그리고 시험 활동으로 정의하고, 정보보호 관리 측면에서는 정책 및 조직의 구성, 위험 평가 및 대책 구현 그리고 운영 활동으로 정의하고 있다.

품질 관리측면에서의 BS7799와 공학적 측면에서의 SSE-CMM 그리고 정보보호 관리측면에서의 GMITS와 IT Baseline Approach등의 프로세스의 정의를 비교하면 기존의 정보보호 관리 기준들이 4개의 단계인 정보보호 정책 수립, 위험 분석, 정보보호 대책의 선택 및 구현, 확인 그리고 사후 관리의 공통된 활동들을 수행하는 공통점을 확인 할 수 있다. 이와 같은 단계들을 정보시스템의 개발 유지 보수에서 적용되는 생명

주기(System Life Cycle)를 바탕으로 요구분석, 위험분석, 보안구현, 사후조치로 정의하고 있다 [김정덕 2002].

2.2 정보보호관리에 관한 연구들

최근 정보보호 관리의 중요성을 인식하기 시작하면서 이러한 정보보호관리를 어떻게 하여야 하는 지 정보보호의 여러 가지 측면에서 연구가 되고 있다.

주로 관리적인 부분인 기업의 정보보호 정책 구성, 환경조성 부분, 정보보호 조직 구성과 정보보호의 핵심적인 프로세스인 위험 분석 부분 그리고 구현 유지보수를 위한 지속적 인식 훈련, 사후조치로서의 사고처리절차와 준거성 확인에 대한 연구들을 중심으로 성공적인 정보보호 관리 요인에 대해서 기술하는 연구들이 있고[홍기향, 2001] 정보보호 관리를 위한 정책들은 기업의 비즈니스 환경뿐 만 아니라, 조직의 정보화 환경과도 밀접한 영향관계를 가지고 있음을 여러 연구에서 밝히고 있다. Karin[2002]은 정보보호 관리가 조직의 목표와 사명을 반영하고, 조직의 목표달성을 위해서 조직의 보안 목표가 설정되어야 하며, 조직 문화와 맞아야 하고, 조직 문화 내에서 개발되어야 한다고 했으며, 정보보호에 대한 경영자의 동의와 자원을 명시하고, 조직의 비전과 목표 달성을 위해서 정보보호가 수행하는 역할을 명확하게 정의되어야 정보보호 정책이 효과적으로 수립된다고 보았다. Gerald [1998]는 조직 문화의 변화에 따라 어떤 영향이 발생하는지를 인식하여 회사의 역사, 비즈니스, 경쟁 환경을 고려하고 그에 따른 사명과 비전, 품질관리 등과 같은 실제 적용관련 사항 등을 적용해서 정보보호 정책 수립에 반영해야 한다고 주장하고 있다.

또한, 정책의 내용이 일관성과 관리의 용이성 그리고 이해성이 높아야 한다는 주장을 하는 연구들이 많으며 이러한 맥락에서 Karin[2002]은 기존의 법률 준수내용과 연결되어야 하며, 정책 위반에 관련된 원칙 등이 명시되어, 실제로 사용자의 필요와 업무의 효용성이 동시에 만족되는 입장에서 이해하기 쉽고, 의미가 있으며, 실제로 실용적으로 활용할 수 있어야 한다고 보았고 Dario[2000]는 단일 관점에서 보안정책으로 구현되어 일관성을 유지하고, 중앙에서 정의 관리하여 사용이 용이하고 통제가 용이하도록 유지되도록 관리해야 한다고 주장하고 있다.

정보보호 조직의 구성에 관해서는 Gerald [1998]의 연구가 대표적인 데 조직의 권한과 한계 그리고 사용 가능한 예산을 인식하고 정보보호 인력의 효과적인 조달 방법을 결정하고 실행해야 하는 것을 전제하고 무겁고 관료적인 조직이 아니라 효과적이고 효율적으로 구성되는 것이 중요함을 강조하고 있다. 또한 사명과 비전, 그리고 품질관리와 관련된 사항들을 고려하여 조직을 구성하여야 하며 경영 계획과 정보보호 계획이 같이 수립되어서 이러한 계획을 실현할 수 있는 조직을 구성하고 이러한 구성은 경영자의 승인과 지원을 통해 추진력을 확보해야 한다고 얘기하고 있다. 또한 Forte[2000]는 보안 조직의 사명이 정의되어 있는 상황에서 임무 수행에 적합한 인원을 조직 내부에서 찾아내서 임명하고, 이러한 정보보호 조직의 책임을 적절하게 그리고 명확하게 설정하여 조적 전체에 설명이 되어야 하며 서비스의 내용을 명확히 규정하여야 한다고 주장하고 있다.

정보보호의 위험을 분석하는 과정은 일반적으로 정보보호 자산에 대한 식별을 바탕으로 자산의 가치를 측정하고, 자산의 위협요소와 취약성 요인들을 정리한 후 자산에 실제 영향을 주는 정도를 계산하여 가치의 손해 혹은 손실 정도를 위험으로 평가하고 있다. 이러한 위험 평가에 있어서 Bill[1997]은 중요한 자산들을 중심으로 파악하고 자산에 대한 위협 요소들을 파악하여 실제 고용인에 의해서 발생되는 손해나 다양한 영향에서 발생될 수 있는 손해와 손실을 예측하고

측정할 것을 강조하고 있다. 또한 이러한 영향이 실제 발생되거나 발생될 확률을 계산하기 위한 전쟁게임과 같은 시나리오 훈련이 필요하다고 보았으며 위협요인의 목록을 지속적으로 갱신하여야 한다고 얘기하고 있다. Zbigniew[1997]는 수용 가능한 위험의 수준이 정의된 상태에서 전체 업무 프로세스와 연관된 위험을 평가하고 서로 다른 시스템 및 응용시스템 간의 의존관계가 고려되어야 한다고 기술하고 있다. Broderick [2001]은 위험 분석 작업에 적절한 조직 자원이 동원되어야 업무의 변경이 있을 때 효과적인 위험 관리가 수행되어야 하며, 새로운 위협요인이나 취약성이 나타나는 경우에 대비하여 정기적으로 위험분석이 수행되어야 한다고 보고 있다.

정보보호에 대한 조직 전체의 인식 교육 훈련에 대한 연구들도 있는 데 Charles[1997]에 따르면, 이러한 연구 훈련들의 지속적이고 정기적인 실행이 중요하고 예외사항이 발생하는 경우에 어떻게 처리할 것인지 명확한 절차가 필요하고 가시적인 경영자의 지원과 명확한 목표의 설정과 달성에 대한 피드백이 필수적이며, 이러한 구현에 필요한 자원이 확실히 배분될 수 있도록 지원되는 체계가 마련되어야 한다고 보고 있다. 전사적인 직원 인식 강화 프로그램과 같은 변화 관리 프로그램이 동시에 운영되어야 함을 중시하고 있다.

또한 정보보호의 사후조치와 관련하여서는 Cohen[1998]의 연구에서 준거성 확인을 위해서는 업무를 적절하게 이해하는 것이 중요하고 이러한 이해를 바탕으로 관련된 위협의 인식이 선행되어야 함을 보여주고 있고, 사고 처리단계와 관련하여 Rob[2001]의 연구에서는 사고를 정의하고 그에 따른 탐지, 고지, 대응절차와 조직을 어떻게 설계하는 지를 설명하면서 사고의 원천적인 봉쇄를 위한 사고원인의 제거 작업 과정과 사고 발생시에는 사고 이전의 상태로 신속하게 복구할 수 있도록 유지하는 방법에 관해서 논하고 있다. 특히 보안 대책의 변경 후, 혹은 검토가 수행된 이후의 사후 조치작업에 중점을 두고 분석하고 있다.

2.3 중소기업 특성과 정보보호

중소기업은 대기업에 비해 매출액, 자본, 인적자원이 작다는 피상적인 측면들뿐만이 아니라 이러한 근본적인 차이에서 비롯되어 여러 측면에서 다른 특성들이 나타난다. 경영의 측면에서 중소기업은 소유자와 경영자가 대개 동일인 인 경우가 대부분이며 모든 의사 결정에 있어서 경영자의 역할이 절대적이다. 또한 최고 경영자가 기업의 여건에 대한 상당한 지식을 가지고 있으며 보통 개인 사업으로 구성된 경우가 많아 개척정신을 갖고 사업을 운영하며, 분권화된 대기업의 의사결정과는 달리 최고경영자 한 사람이 절대적인 의사결정권을 가지고 있어 의사결정 속도가 매우 신속하다[박경렬, 2001; 유세준, 임동환, 2001].

업무 조직적 측면에서는 사업규모가 작아 업무조직이 간단하고 한 조직이 여러 업무를 동시에 수행하는 경우가 많고 표준화된 업무의 절차나 규범이 없어 세부 업무에 대한 정의가 상세하지 않은 경우가 많다. 조직이 체계적으로 구성되지 못해 직급에 대한 정의와 권한이 불분명하여, 모든 조직이 작고 경영자와 밀접한 관계에 있기 때문에 관료주의적인 성격이 적다. 경영환경 측면에서는 일반적으로 자금, 인력, 기술 등에 한계를 가지고 있으며, 주로 노동 집약적인 산업에 속해 있다. 정보수집이 주로 경영자에 의해 수행되고 기업 내 정보 공유가 잘 이루어지지 않아 형화된 기업경영 계획과 전략이 정의 되어 있지 않다. 중소기업의 일반적인 특성을 <표 1>와 같이 정리하였다[Margi, 1998; Gupta, M., 1996; Georgios, 1996; Georgios, 1996; 조희영,2001].

이러한 측면에서 중소기업의 정보화와 정보보호에 있어서 나타나는 특성들은 대기업의 경우와 다르게 나타날 것으로 보이며 박경렬[2001], Margi[1988]등 기존의 중소기업의 특성에 관한

<표 1> 중소기업의 일반적 특성

항 목		특 성
경영방식	관리방법 경영자 의사결정권 의사결정	직관적 전근대적 소유자 집중적 직접적, 신속적, 충동적
업무조직	업무 조직 권한과 책임	업무기능 분화부족, 비 정형화 비체계적 불분명함
경영환경	환경적응 시장규모 일반적 여건	탄력적 신축적 협소함, 지역시장 취약함
생산기술	생산형태 제품형태 생산기술의 성격 산업의 중심	다품종소량생산 부품 및 반제품 노동집약적 경공업

연구들을 바탕으로 하여 중소기업 정보화의 중점적인 특성들을 정보화 환경, 정보화 조직, 정보화 기능, 그리고 정보 시스템적 측면의 네 가지 큰 관점보면 <표 2>과 같이 정리할 수 있을 것으로 보인다.

정보화 관점에서 중소기업의 특성은 아래와 같이 제 가지 정도로 요약할 수 있다. 첫째, 중소기업이 스스로 정보를 생산하기보다는 외부의 정보수집과 해석이 주를 이루고 있다는 점이다 둘째, 상대적으로 열악한 자금 사정에 따른 솔루션 도입의 제약이다. 현재 공급되고 있는 대부분의 정보화 시스템의 하드웨어, 소프트웨어, 컨설팅 등을 막론하고 대부분 높은 가격대를 형성하고 있어 중소기업이 도입하기에 부담이 되고 있다. 셋째, 중소기업은 정보화 추진 주체에 따라 결과가 상이하게 나타나게 된다. 중소기업은 대기업과 같은 정보경영 관리자나 스텝에 의한 장기적 안목의 과학적인 정보화 마스터플랜을 수립할 수 없지만 오히려 작은 조직과 유연성 때문에 최고 경영자의 정보화 의지여부에 따라 대기업 보다 훨씬 더 짧은 시간에 적은 노력으로 더 많은 성과를 기대할 수 있다. 마지막으로, 중소기업 정보시스템은 대외 의존도가 높다. 개발과 유지보수를 담당할 전문 인력이 절대 부족하고, 이를 위한 인력 확보도 어려운 실정이다[유세준, 2001].

이와 같은 맥락에서 중소기업이 정보보호 수행을 위한 정책과 시스템을 도입하는데 다양한 애로사항이 존재한다. 정보보호진흥원에서 실시한 2003년도 정보보호 실태조사를 보면, 중소기업은 거의 모든 분야에서 기본적인 정보보호시스템을 갖추지 못한 경우로 들어났다. 첫째, 정보

<표 2> 정보화 관점의 중소기업의 특성

항 목		특 성
정보화 환경	경영자 전 략 정보생산 자 원 Infrastructure	정보화 마인드 부족 효율적인 측면 강조 외부 환경에 의존 지속적인 정보화 투자 부족 주로 단순 PC 환경
정보화 조직	업 무 조 직 권 한 인 력	다른 업무와 겸임 정보화 담당 조직의 부재 최고 경영자에게 집중 기술 전문 인력 부족
정보화 기능	고유성 업무 프로세스	표준화 되지 못하는 프로세스 존재 대기업에 의존적임
정보 시스템	계 획 분 석 도 입 활 용	세부 실행 계획의 부족 정보수요분석 및 정보관리체제 부재 시스템 선택의 제약 개인 업무에만 치중

보호 전반에 걸친 기준과 지침 그리고 수행할 노하우가 전적으로 부족하다. 조사에 따르면 중소기업의 지침 준수율은 전체평균인 50.2%이하인 43.6%로 나타나 전반적으로 지침에 대한 인식이 부족하고, 체계적인 보안관리 수행이 미흡한 것으로 나타났다.

둘째, 정보보호를 추진하는데 있어, 비용적인 부담을 가지고 있다. 주요 데이터에 대한 보안대책으로 '기타(6.5%)'를 선택한 기관 중 중소기업(11.8%)이 가장 높은 수치를 나타내어, '백업', '접근통제', '암호화' 의 방법 외에 '직접통제' 등 비용부담을 최소화하는 방법을 모색하는 걸로 판단되었다.

셋째, 비상복구 계획 수립 수립현황과 마인드가 총체적으로 미비하다. '재해 및 침해사고에 대한 비상복구계획 없음(59.1%)' 중 중소기업은 72.4%를 차지하면서, 가장 비상복구 계획 수립 의식이 부족한 것을 알 수 있다[정보보호진흥원, 2003].

현재, 국내에서는 기업의 실정에 적합한 정보보안 관리 지침 작성에 대한 노력이 있으나 가시적인 결과를 맺지 못하고 있으며, BS7799등의 국제 표준등과 호환성을 고려한 정보보호 관리 프로세스 기반의 연구도 미흡한 실정이다[김정덕, 2000]. 특히, 중소기업의 경우 대기업 비해 정보보호를 추진할 수 있도록 정부의 관심이 더욱 요구되나, 정보보호 관리에 있어 대기업에 비해 상대적으로 필요한 지원 영역과 지원 범위에 관한 연구가 부족하여 실제 정부 정책과 기업 자원이 효율적으로 이루지지 않고 있다.

2.4 중소기업 정보보호 관리의 요구사항

중소기업의 정보보호의 경우, 중견 기업 및 대기업과는 다른 접근 방식을 필요로 한다. 우선 정보보호의 대상이 매우 다양하여 정보보호 관리모델이 신축성있게 반영되고, 신속하며, 효율적으로 구현되도록 해야 한다. 이를 위해서는 PDCA 모델 전체를 통해서 여러 활동들이 유기적으로 연결되고, 향후 확장이나 통합되어 적용될 수 있도록 되어야 하며, 급변하는 기업 환경에 유연하게 대응할 수 있도록 해야 한다. 이러한 중소기업 특유의 정보보호 관리 요구사항을 정리하여 보면 다음과 같다.

첫째 집중화된 의사결정을 지원해야 한다. 중소기업은 앞에서 살펴본 것과 같이 정보화 추진에 있어 조직의 구성이 최고경영자에게 집중된 의사결정의 특징을 보이고 있다. 이러한 의사결정은 의사결정 단계가 짧고 다양한 정보를 최고경영자가 파악하기 쉬운 조직의 특성으로 정보보호 관리는 최고경영자의 의지와 추진방안에 따라 강력하게 수행될 수 있도록 지원되어야 한다.

둘째, 지속적 관리가 용이해야 한다. 일반적으로 기업 자원이 부족한 중소기업의 경우 정보의 획득 비용보다는 정보의 유지관리 비용이 상대적으로 높은 비용을 차지한다. 또한 정보의 획득도 외부환경에 의존하고, 전문적인 인력을 확보해서 정보보호와 정보화를 수행하기는 것이 매우 어렵다. 그러므로 정보보호 관리는 표준화된 프로세스와 체계를 갖고 지속적인 관리가 용이하고 쉽게 유지 될 수 있도록 지원되어야 한다.

셋째, 환경 변화에 대한 유연성을 가져야 한다. 중소기업은 대기업에 비해 경제 환경의 변화에 영향을 크게 받으며, 거래 기업과의 관계 변화 역시 큰 영향을 끼친다. 또한 경쟁 환경과 내부적 변화에 의한 기업의 전략적 위치 변화의 폭이 대기업에 비해 크다. 중소기업의 정보화 전략 계획을 세우는데 있어서 고려해야 할 또 하나의 사항은 기업의 프로세스가 비정형화 되어 있고, 기업마다 고유의 특성을 갖게 된다는 것이다[Margi, 1998]. 이러한 특성을 반영하기 위해서 중소기업의 정보보호 관리는 환경에 대한 유연성을 갖추고 있어야 한다. 이러한 유연성을 갖추기 위해서는 모델의 각 단계의 생략 및 간소화가 가능하고 다른 모델과의 적용이 쉽게 이루어지도록 해야 하며, 지속적인 수정과 보완이 가능한

피드백 단계가 제시되어야한다.

넷째, 신속한 구현과 도입이 가능한 모델이어야 한다. 중소기업이 고유 업무인 제품의 생산과 같은 매출 활동이외의 프로젝트(정보화 전략수립, 정보화경영체계, 기타 컨설팅) 사업을 쉽게 실시하지 못하는 이유는 매출 활동의 중단이 기업에 미치는 영향이 막대하기 때문이다. 이러한 중소기업의 특성은 중소기업을 위한 프로젝트가 신속하게 이루어 질수 있도록 지원하는 것은 매우 핵심적인 요소이다. 그러므로 짧은 단계와 짧은 시간에 내실 있게 정보보호 모델을 적용할 수 있는 특성을 갖춰야 한다.

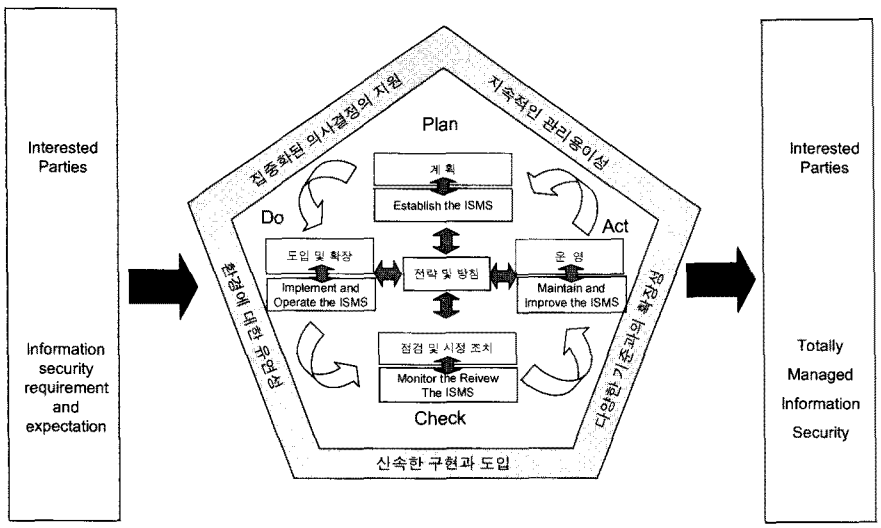
마지막으로 다양한 기준으로의 확장성을 갖춰야 한다. 기업의 프로세스 개선을 가져오는 다양한 표준체계의 도입은 대내외적으로 효과적인 경영활동을 유지하는 방식으로 평가받을 수 있다. 그러한 점에서 대기업들의 정보보호국제 규격인 BS7799의 도입이 확산되는 것은 정보보호 시스템 규격을 통한 효과적인 통제수단을 확보하는 것 이외에 적극적인 정보보호 정책을 도입하는 방법으로 볼 수 있다. 중소기업의 경우는 대기업에 비해 국제 규격을 취득하거나 유지하기 위한 자원이 충분치 않기 때문에 중소기업의 실정에 적합한 모델을 도입해야 하지만, 향후 기업의 성장과 환경의 변화에 맞춰 대외 경쟁력을 제고 할 수 있는 국제 표준 규격으로 확장이 쉽도록 지원해야한다.

Ⅲ. 연구 모델과 실증 분석

본 연구에서는 (1) 위에서 논의된 중소기업 특유의 요구사항을 반영한 중소기업 정보보호관리의 일반적인 프로세스를 정리하고 (2) 이러한 정보보호관리 프로세스의 각개 요소들에 관한 대기업과 중소기업의 인식의 차이를 측정하여 중소기업 정보보호관리의 특성들을 실증적으로 규명하고 (3)이러한 실증적 차이에 근거하여 중소기업 특유의 단계별 접근 모델(Phased Approach Model)을 제안하였다.

3.1 중소기업 정보보호 관리 모델의 개발

중소기업의 정보보호 관리모델은 정보보호 관리를 위해서 필요한 방침과 목표를 달성하기 위



<그림 2> 중소기업 정보보호 관리모델

해 관리프로세스를 적용하여 정보보호 관리수준을 향상하는 목적을 지닌 모델로 정의할 수 있는데 본 연구에서의 정보보호 관리 모델은 BS7799에서 제시하는 PDCA 사이클로 구성되면서 동시에 중소기업의 특유의 정보보호 요구사항인 집중성, 관리용이성, 유연성, 신속성 그리고 확장성을 다섯 가지의 환경요인으로 보아서 <그림 2>과 같이 구성하였다.

정보보호관리 프로세스는 Plan-Do-Check-Act의 사이클로 규정하였고 가운데에 PDCA의 각 요소들과 상호 연계하는 전략 및 방침을 두어서 지속적인 수준향상을 꾀하는 데에 전략과 방침이 항상 연계되는 것을 나타내었다. 정보보호 관리 프로세스의 세부 항목들은 BS7799의 PDCA 모델을 근간으로 하고 여기에 중소기업의 특성을 반영하여 12가지 세부 항목으로 새롭게 정의하였으며 12가지의 세부 내용은 <표 3>에 상세하게 나타나 있다.

<표 3> 정보보호 관리 프로세스 정의

단 계		프로세스	프로세스의 정의
계획 (Plan)	요구 분석 (Requirements Analysis)	보안 환경 및 조직 (Scope & Org)	정보보호를 추진하는 기업의 구성원들의 의식과 마인드, 투자 규모, 법, 제도, 조직을 확인하고 구성한다.
		보안 정책 (Policy)	보안 환경을 분석하여 조직의 보안 목적, 전략, 정책을 수립하여 보안조직에 승인을 받는다.
	위험 관리 (Risk Management)	자산파악 (Resource Assessment)	유, 무형의 자산을 식별하고 이에 대한 가치 평가를 수행한다,
		위험평가 (Risk Assessment)	위협, 취약성 평가를 통해서 자산가치/위협/취약성의 시나리오를 정의하고, 각 시나리오 별 위험을 평가한 후 이의 우선 순위를 정한다. 위험 평가의 결과를 승인 받는다
실행 (Do)	보안 구현 (Implementation)	보안구현계획 수립 (Implementation Plan)	보안 대책 및 제약사항을 식별하고, 이에 따른 보안 구현 계획을 수립하고 승인을 받는다.
		도입 및 개발 (Development)	수립된 보안구현 계획에 따라 보안 대책을 구현하고 승인을 받는다.
		인식, 교육, 훈련 (Awareness & Training)	교육의 필요분석과 실시, 결과 모니터링을 수행하고 승인을 받는다.
확인 (Check)	사후 조치 (Corrective Action)	모니터링 (Monitoring)	보안 계획에 따라 시스템과 사용자가 적정한 보안 수준을 유지하고 있는가를 확인하는, 지속적인 활동을 수행한다.
		준거성 확인 (Audit)	보안대책이 올바르게 구현되고 사용되며, 적정하고 시험되었는가를 확인한다.
개선 (Act)		유지보수 (Maintenance)	로그 파일의 확인, 매개변수의 수정 및 버전 갱신 등을 수행하고, 보고한다.
		변경관리 (Change Management)	변경요청을 접수, 영향 분석, 승인, 공표 및 보고한다.
		사고처리 (Incident Management)	사고 발생을 탐지, 보고, 복구한 후 사후 분석을 통해 차후 보안계획에 반영한다.

정보보호 관리 프로세스는 PDCA 모델인 계획-실행-확인-개선의 각 프로세스로 구성된다. 조직의 정보보호에 대한 역량과 환경을 파악하고 정보보호 전략과 정책을 수립하는 계획 단계는 요구분석의 보안 환경 분석 및 조직과 보안 정책 프로세스와 위험분석의 자산 파악과 위험 평가 프로세스를 포함하고 있다. 계획단계는 정보보호 관리가 조직의 목표와 사명을 반영하고, 조직의 목표달성을 위해서 조직의 보안 목표가 설정되어야 하며, 정보보호가 수행하는 역할을 명확하게 정의되어야 정보보호 정책이 효과적으로 수립되어야한다[Karin, 2002].

조직의 보안 구현에 대한 계획을 수립하고 보안 통제를 구현하는 실행단계는 보안 구현의 보안 구현 계획 수립, 도입 및 개발, 인식 교육과 훈련의 3개의 프로세스를 포함하고 있다. 특히, 보안 환경의 구현이 앞에서 제시된 보안 정책에 따라 위험분석이 기업의 자원이 허락되는 범위에서 수행 되어야 하며, 실제 구현에서는 효과적이고 전사적으로 구현 결과를 극대화하기 위해서 인식 교육과 훈련을 정기적으로 실시해야 한다[Charles, 1997].

앞에서 구현된 보안통제가 운영되고 유지되는지 확인하는 단계는 사후조치의 모니터링, 준거성 확인으로 구현된다. 모니터링은 보안 수준이 적정하게 유지되고 관리되는지를 확인하는 것으로 구현 계획에 따른 수립되어 지속적인 수준이 설정되어 있어야 하며, 특히 기존에 존재하는 보안 운영 절차와 방법이 실제로 운영되는지의 여부를 확인하는 준거성 확인도 중요하게 고려되어야 한다[Cohen, 1998].

마지막으로 지속적인 개선 및 향상은 위한 개선단계는 사후조치의 유지보수 및 변경관리와 사고처리 프로세스로 구성되어 있다. 지속적인 개선은 PDCA모델에서 중요한 부분으로 선행된 절차에서 발생된 문제점이 적절하게 반영되고, 변경 절차에 따라 변경되어야 하며, 발생될 수 있는 갑작스러운 사고에 효과적으로 대처하여 비즈니스 영속성을 유지하도록 구성되어야 한다.

3.2 정보보호관리 모델의 실증 연구

이어서 정보보호 관리 모델의 12개 세부 요소들의 중요성에 관하여 설문을 구성하고 중소기업과 대기업간의 차이를 탐색할 목적으로 설문을 구성하였다. 12개의 세부 요소들을 규정하는 변수들은 BS7799의 정보보호 관리 항목과 김정덕[1998], 김현수[1999]등의 정보보호 평가항목을 바탕으로 구성하였으며 측정을 리커드 5점 척도를 근거로 하였다. <표 4>는 설문을 구성한 설문 항목들을 자세히 나타내고 있다.

설문 조사 대상은 객관적으로 선별될 수 있도록 관련 기업 및 정보보호 협회의 회원을 대상으로 E-mail 과 직접 설문조사를 통해서 이루어 졌다. 조사 대상인 총 1600명 중 167부가 수거되어 실제 수거율은 10.4%이었으며 이중 불완전한 설문지 8부를 제외하고 총 159부를 대상으로 최종적인 분석을 수행하였다.

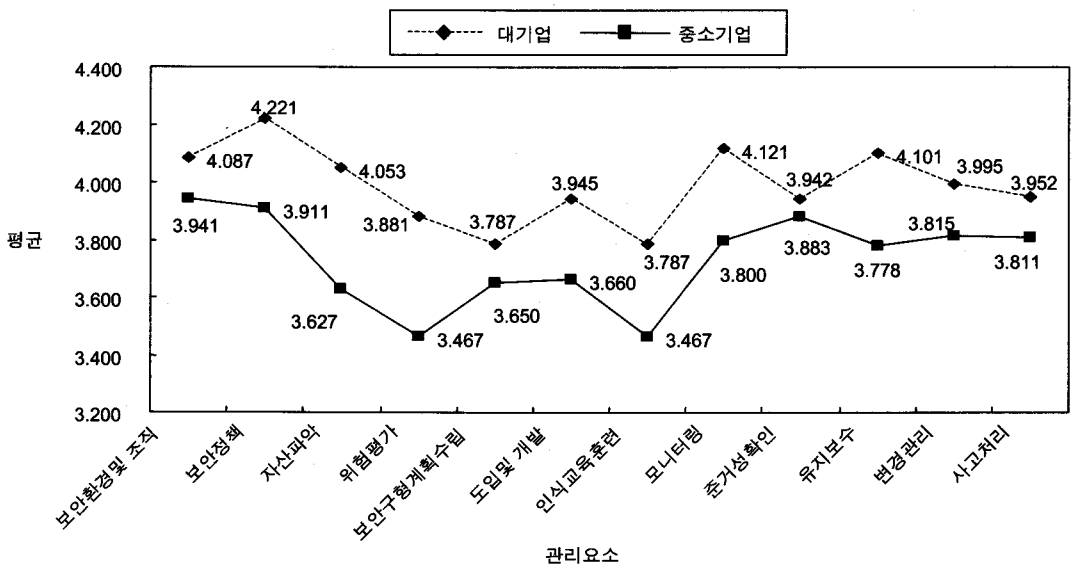
조사 대상중에서 대기업과 중소기업은 대략 4 : 6 정도의 비율로 구성되어 있었다. 최근의 보안에 대한 관심과 조사 대상자의 특성상 60% 정도가 정보보호 관리체계에 대한 교육 혹은 컨설팅 경험이 있는 것으로 조사되었으며, 3년 이상의 고급 경험자들이 전체 70%를 차지하고, 정보시스템에 관한 경험도 전체의 85%가 보유하고 있다. 다만, 정보보안과 관련된 프로젝트 경험의 경우는 기업이 정보보호에 관한 프로젝트를 활발하게 수행하지 않는 점을 보아 프로젝트 경험을 가진 인력이 전체의 50%정도를 상회하는 수준이었다. 설문 항목들의 신뢰도계수는 0.7이상으로 매우 높게 나와 항목간의 신뢰성이 존재하고 있음을 나타내고 있다.

<그림 3>는 정보보호 관리의 각 12개의 요소별로 중소기업과 대기업 응답자들의 평균값을 나타내고 있다. 전체적으로 정보보호 관리에 대

<표 4> 정보보호 관리 설문 항목 구성 및 신뢰도계수[a]

프로세스	항목 구성	항목수	신뢰도계수
보안 조직 및 환경	CEO의 의지 및 마인드, CEO의 보안 인식 정도, 직원의 의지 및 마인드, 직원의 보안인식 정도, 정보보안 인력 수준, 외부 전문가의 정보보호 조언	6	0.746
보안 정책 확인 수립	보안정책의 문서화 체계, 정보보안 정책수립, 사용자 업무 분장구조체계, 보안 시설등에 대한 권한 부여 절차	4	0.729
자산파악	자산의 업무목적과의 연관성, 정보자산의 분류지침, 정보자산 목록체계	3	0.865
위험평가	정보자산에 대한 위험분석체계, 위험 우선순위에 따른 관리전략, 위험 분석에 결과에 따른 보안 조치, 위협식별 및 평가, 취약성 식별 및 평가	5	0.907
보안구현계획 수립	비상사태 대비계획, 위험 시나리오에 따른 통제, 시스템 운영상황의 감시체계, 업무연속성 평가, 보안 통제의 승인 및 유지관리, 비상계획 수립 정도, 정보보안 계획 수립, 인위적 위협에 대한 대책, 업무연속성 계획수립	9	0.942
도입 및 개발	보안 체계의 감사추적, 인사보안통제, 물리적 보안통제, 시스템 접근통제	4	0.851
인식, 교육, 훈련	정보보호 교육 계획, 조직의 보안교육 및 테스트, 교육성과 평가 및 반영	3	0.804
모니터링	모니터링 운영 절차, 운영을 위한 자원 확보, 보안 상태 점검'	3	0.852
변경관리	변경 후속조치, 변경 통제절차, 변경에 따른 위험평가'	3	0.837
준거성 확인	보안정책 의 준거성 검투, 기술적 준거성 검토	2	0.928
유지보수	유지보수 계획수립, 유지 보수 시 보안대책	2	0.833
사고처리	보안 사고후속처리, 보안사고 처리절차, 보안사고 대응조직'	3	0.838

주) a : Cronbach's α 계수



<그림 3> 정보보호 관리 프로세스 중요도에 대한 평균값 비교

한 인식은 대기업에서 상대적으로 높게 나타남을 알 수 있다. 특히 보안정책, 보안환경 및 조직, 모니터링, 유지보수, 자산 파악과 같은 항목들이 대기업에서 상대적으로 높은 수치를 나타내고 있으며, 중소기업의 경우는 보안환경 및 조직, 자산파악, 준거성확인, 보안정책, 변경관리, 사고처리 부분에서 상대적으로 높은 수치를 나타내고 있다. 이러한 결과를 통해 유추해 보면, 중소기업과 대기업은 관리적 측면의 요소인 보안환경 및 조직, 보안 정책과 구현된 보안 통제 환경의 모니터링, 유지보수, 변경관리를 공통적으로 중요하게 보고 있는 것으로 해석할 수 있으며 중소기업의 상황에서 중요도가 낮게 나타난 요소들은 자원 제약상 선결과제를 우선 제시하는 관점에서 중요도를 평가한 것으로 보인다.

이어서 이렇게 전반적으로 차이가 나타나는 인식이 통계적으로 얼마나 유의한 차이를 보이는 지를 심층 분석하였다. <표 5>은 각각 12개의 요소들에 관한 중요성에 대한 대기업 그룹과 중소기업 그룹의 인식의 차이가 얼마나 나는 지를 두 그룹 평균비교 t 감정을 실시한 결과이다. t 검정은 분산에 근거하여 두 그룹 평균값의 차이가 통계적으로 다른 모집단에 근거한 것인지 아닌지를 판별하는 방법으로서 통계상의 중요도(significance)는 평균의 차이가 통계적으로 유의하게 다르게 나타남을 의미한다.

<표 5> 정보보호 관리 프로세스에 대한 t검정

변 수	규 모	N	Mean	t	Sig.	평균차
보안조직 및 환경	대기업	69	4.087	1.720	0.087	0.146
	중소기업	90	3.941			
보안 정책	대기업	69	4.221	3.269	0.001**	0.310
	중소기업	90	3.911			
자산파악	대기업	69	4.053	1.419	0.158	0.164
	중소기업	90	3.889			
위험평가	대기업	69	3.881	2.062	0.041*	0.254
	중소기업	90	3.627			
보안구현계획 수립	대기업	69	3.787	2.570	0.011*	0.321
	중소기업	90	3.467			
도입 및 개발	대기업	69	3.945	2.360	0.020*	0.285
	중소기업	90	3.660			
인식, 교육, 훈련	대기업	69	3.787	2.570	0.011*	0.321
	중소기업	90	3.467			
모니터링	대기업	69	4.121	2.573	0.011*	0.321
	중소기업	90	3.800			
준거성 확인	대기업	69	3.942	0.411	0.681	0.059
	중소기업	90	3.883			
유지보수	대기업	69	4.101	2.530	0.012*	0.324
	중소기업	90	3.778			
변경관리	대기업	69	3.995	1.493	0.137	0.180
	중소기업	90	3.815			
사고처리	대기업	69	3.952	1.072	0.285	0.141
	중소기업	90	3.811			

주) * : $p < 0.05$, ** : $p < 0.01$

대기업과 중소기업을 비교한 결과 $p < 0.05$ 수준에서 유의한 차이를 보이는 프로세스는 위험평가, 보안구현계획 수립, 도입 및 개발, 인식, 교육 훈련, 모니터링, 유지보수 프로세스로 나타났으며 보안 정책에 관해서는 $p < 0.01$ 수준에서 유의한 차이가 나타났다.

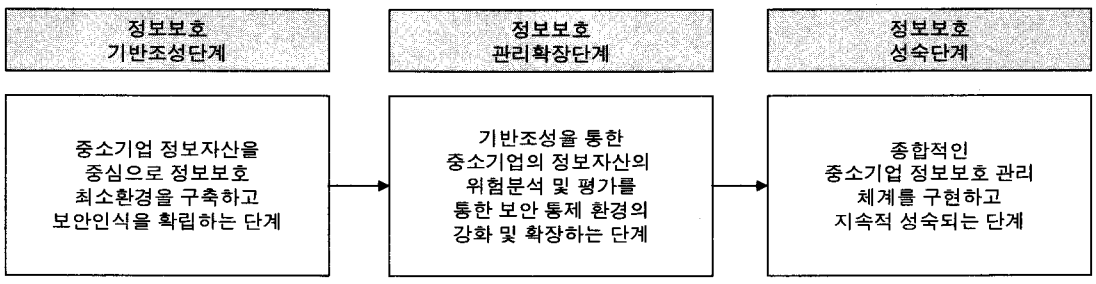
프로세스에 대한 인식적 차이가 유의하다고 밝혀진 보안정책, 위험평가, 보안구현계획 수립, 도입 및 개발, 인식교육훈련, 모니터링, 유지보수의 경우는 중소기업과 대기업간에 앞에서 예시한 특성적 차이를 반영하는 부분으로 새로운 인력 구성과 자원이 투입되는 보안 조직 구성, 보안 구현 계획 수립 그리고 모니터링 부분과 적절한 자산파악이 선행되어야 수행 될 수 있는 위험평가, 하드웨어와 소프트웨어를 도입하기 위한 예산이 확보되어야 하는 도입 및 개발 부문, 유지보수 부문들로 주로 기업의 자원이 투자되고 집중될 부분들로 구성되어 있다.

중소기업과 대기업의 인식적 차이가 크게 나타난 항목들은 중소기업에서 상대적으로 중요하지 않다고 대답한 항목으로서 위에서 설명한 현실적 원인들로 인하여 중요성 인식이 낮은 것으로 보인다. 따라서 중소기업의 정보보호에 관해서 접근할 때에는 중소기업과 대기업의 인식적 차이가 적고 기업의 자원 소모를 많이 요구하지 않으며 실제 중소기업이 중요하다고 보고 있는 요소들을 중심으로 일차 접근하여 필요한 부분들을 처리하고 이러한 처리들이 제대로 된다면 나머지 요소들에 대한 인식들도 자연적으로 높아질 것으로 보인다. 이를 위해서는 단계별 접근이 필요하며 여기서의 단계별 접근은 PDCA의 사이클에서 가리키고 있는 단계가 아니라 이러한 PDCA의 요소들 중에서 선별적으로 해결해야 할 중첩된 사이클이 있음을 의미하며 이러한 맥락에서 중소기업 정보보호 방법론으로는 PDCA를 포괄하여 정보보호의 단계들을 선별적으로 그리고 순차적으로 적용하는 단계별 접근법(phased approach)이 필요한 것으로 보인다.

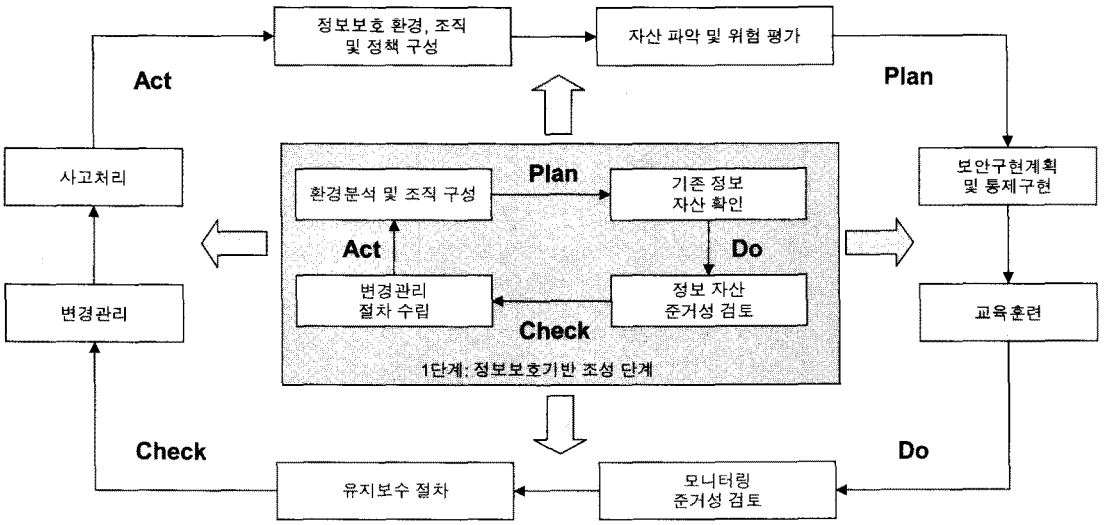
3.3 중소기업 정보보호 관리 단계별 접근 모델(ISM Phased Approach Model)

본 연구의 결과에 의하면 중소기업의 입장에서의 선결사항들은 보안조직 및 환경, 자산파악, 준거성 확인, 변경관리, 사고처리로 나타났다. <그림 4>의 단계별 접근 모델에서 보이는 바와 같이 중소기업의 선결사항들을 제일차적인 과제로 보고 이들을 확보하기 위한 '정보보호 기반조성단계'를 제1단계로 하고 나머지 요소들을 해결하는 단계를 '정보보호관리확장단계'로 명명하고 제2단계로 설정하였다. 최종적으로 이러한 PDCA의 사이클이 계속적으로 유지 활용되는 성숙단계를 제3단계로 설정하였다.

<그림 5>는 중소기업의 정보보호 단계별 접근 모델의 앞의 2단계를 좀 더 상세히 나타낸 것으로 내부의 사각형은 제1단계의 정보보호 기반 구축 단계를 나타내며 기업의 정보보호 환경을 파악하고 조직을 구성해서 조직의



<그림 4> 정보보호 단계별 접근 모델



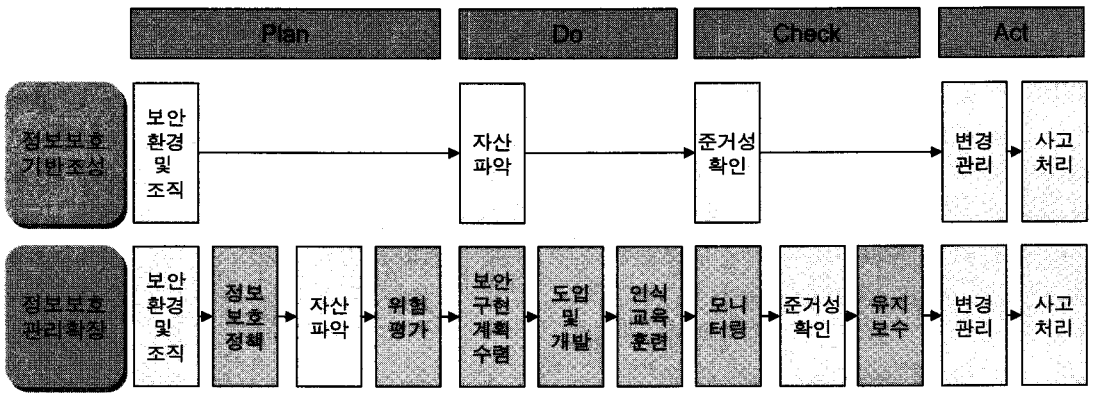
<그림 5> 정보보호 관리 단계별 접근 모델

정보화 자산을 파악하고 최소한의 통제 절차를 구현 확인하는 단계로서 기존의 중소기업이 가진 낮은 정보보호 인식을 효과적으로 끌어올리고, 최소한의 정보보호 요건을 갖출 수 있도록 정보보호에 필요하다고 중소기업들이 당면과제로 인식하고 있는 프로세스를 내부에 그려 넣은 것이다. PDCA의 항목별로 명시를 하였으며 외곽의 프로세스들은 제2단계의 확장으로 진행할 때 부가되어야 할 프로세스의 요소들로서 역시 PDCA의 사이클에 의해서 분류하였다. 제2단계는 내부와 외부의 프로세스 요소들을 전부 포함하는 확장단계로서 1단계의 PDCA요소들이 외부 사각형의 상세 항목들로 확장됨을 나타낸다.

이러한 중소기업의 접근 모델을 구성하는 각 단계를 설명하면 제1단계에서는 기존의 조직이 보유하고 있는 정보화 환경과 기업 환경에 적합한 정보보호 조직을 구성하고 신속한 정보보호 관리체계를 도입하기 위해서 정보보호 환경구현과 함께 기존의 정보 자산을 중심으로 자산 파악을 중점적으로 수행한다. 이렇게 파악된 자산이 실제로 조직에서 원래 수행할 목적과 역할을 적절하게 수행하고 있는지와 최소한의 보안통제 환경을 가지고 있는지에 대한 정보자산의 준거성 검토를 실시하고 잘못되거나 문제가 발생하는 분야에 대해서는 변경관리 및 사후 조치 절차 등을 수립하게 된다.

이어서 정보보호 관리 확장 단계인 제2단계에서는 정보보호의 기반 구축이 어느 정도 수행되어 조직의 정보보호 수준이 적정한 수준으로 향상되었음을 확인하고 이를 확대하는 경우로서 정보보호 정책을 수립하고 정보보호 관리를 위험평가 및 분석을 통한 보안 통제 구현으로 확대해서 적용하는 단계이다. 또한, 기존의 정보 자산과 새롭게 구현되는 보안통제에 대한 모니터링, 준거성 검토를 수행하고 지속적인 유지보수 변경절차를 통해서 PDCA 모델로 강화된다.

주의할 것은 제2단계는 제1단계를 포함한다는 점이다. 즉, 정보보호 정책의 수립 및 조직구성이 확대되고 기존의 정보자산에 위험분석 평가를 통한 보안 통제 내용을 포괄적으로 적용해서 준거성 검토와 변경관리, 유지보수의 사후조치 과정을 수행해서 정보보호 관리체계를 완성하는 것이다. <그림 6>는 이렇게 포함



<그림 6> 정보보호 관리 단계별 접근 프로세스

된다는 점을 강조하기 위한 그림으로서 단계별 액티비티를 상세하게 명시하고 있다. 제3단계 그림에 별도로 명시하지는 않았는데 전체 과정들을 지속적으로 수행하면서 정보보호를 계속 관리하는 성숙된 단계를 가리킨다.

여기서 제시하는 phased approach는 중소기업의 한정된 자원에 대한 분산이 없이 기존의 자원을 최대한 그대로 활용하면서 집중성을 높이고 최소의 프로세스를 기반으로 하기 때문에 관리가 매우 용이하고 단계별 접근이라는 장점으로 유연하게 적용이 가능하다. 또한, 각 단계별로 쉽고 명확한 정보보호 목표를 달성하기에 쉽도록 신속하게 적용하도록 구성했고, 향후 프로세스 중심으로 확장이 용이하도록 구성되어 중소기업의 정보보호 관리의 요구사항을 적절하게 반영하고 있다.

Ⅳ. 결 론

본 연구는 중소기업 특유의 정보보호관리 모델을 개발하기 위한 연구로서 중소기업 특유의 요구사항을 반영한 중소기업 정보보호관리의 일반적인 프로세스를 정리하고 이러한 정보보호관리 프로세스의 각개 요소들에 관한 대기업과 중소기업의 인식의 차이를 측정하여 중소기업과 대기업의 정보보호관리의 특성상의 차이를 실증적으로 규명하고 이러한 실증적 차이에 근거하여 중소기업 특유의 단계별 접근 모델(Phased Approach Model)을 도출하여 제시하였다.

이러한 단계별 접근 모델은 정보보호 기반 구축 단계, 확장 단계, 그리고 성숙단계의 삼단계로 구성되어 있으며 각 단계별로 수행되어야 할 프로세스의 요소들을 각기 달리 구성하고 있다. 중소기업 정보보호 기반 구축을 위한 제1단계는 보안환경 및 조직, 관련 자산 파악, 준거성 확인, 변경관리, 사고 처리의 다섯 가지 프로세스들로 구성되어 있으며 이는 중소기업의 특성과도 연관이 되어 자원이 부족한 상황에서 반드시 필요한 직접적인 요소들로 구성이 되어 있다. 두 번째의 확장단계는 나머지 정보보호의 요소들 - 정책수립, 위험평가, 구현, 모니터링, 유지보수 등 실제적으로 시간과 자원이 많이 투여되어야 하는 요소들로 구성이 되어 있다.

중소기업과 대기업의 특성적 차이를 규명하는 연구들은 많이 있었지만 정보보호 분야에서 이러한 특성을 반영하여 실제로 정보보호 전략이나 모델을 중소기업에 달리 적용한 연구는 아직 없었던 것으로 보이며 이러한 면에서 본 연구는 중소기업에 적합한 단계별 접근법을 실증적인 방법을 활용하여 도출한 데에 그 의의가 있다. 정보보호 전문가들이 생각하는 중요도를 근거로 하여 중소기업들의 특성과 정보보호 프로세스들

의 요소들을 실증적으로 연관 지어서 선결과제들은 앞단에 모아 놓고 나머지 요소들을 두 번째 프로세스로 모아놓은 본 연구의 단계별 접근 방법은 실무에 직접적으로 적용할 가치가 있을 것이며 정책적으로 활용할 여지가 있으리라 사료된다.

본 연구의 한계로는 정보보호 전문가들의 인식을 측정한 실증적인 연구로서 횡단적(cross-sectional) 설문에 근거하여 시급성과 중요성에 다른 분류를 하고 이에 따라 프로세스 모델을 개발하였기 때문에 정보보호 모델의 유효성과 효율성에 관해서는 장기적인(longitudinal) 관찰이 필요할 것이며 이러한 모델의 적용성을 실제 적용 과정에서 피드백에 따라 수정을 해나가야 할 필요성이 있을 수도 있다.

최근에 단순한 재난방지계획뿐만이 아니라 비즈니스의 연속성을 계획하여야 한다는 의미에서 BCP(Business Continuity Planning)가 부각되고 있는 데 본 연구에서 제시한 모델은 이러한 BCP의 한 요소로서 포함하여 활용할 필요가 있을 것으로 보이며 BCP의 관점에서 실제적인 적용을 하면서 지속적으로 결과를 관찰하고 피드백을 받아서 모델을 정화시켜나가는 것이 추후의 연구과제일 것으로 보인다.

〈참 고 문 헌〉

[1] 김정덕, 최홍식, 홍기향, "조직의 정보보호 관리 성숙도측정을 위한 프레임웍 연구," *한국경영정보학회*, 2002.

[2] 김정덕, 김기윤, "정보보호 지표항목 개발 및 계량화 연구," *한국정보보호센터 연구보고서*, 1998.

[3] 김정덕, "정보기술 보안관리 지침 표준화 동향," *통신정보보안학회*, 2000.

[4] 김현수, "정보보안 계량화 연구," *경영정보학 연구*, 1999.

[5] 박경렬, *중소기업론*, 형설 출판사, 2001.

[6] 유세준, 임동환, *중소기업의 이해*, 법문사, 2001.

[7] 임춘성, *임춘성교수의 e-Business File*, ch 11, 영진출판사, 2000.

[8] 이강산, 김학범, 이홍섭, "국내, 외 정보보호관리 모델에 관한 고찰," *정보보호학회지*, 2001.

[9] 조희영, 박상범, *중소기업경영론*, 삼영사, 2001.

[10] 정보통신부, "중장기 정보보호 기본계획," *정보통신부*, 2002.

[11] 정보보호진흥원, "2003년도 주요민간부문 정보보호 실태조사," *정보보호진흥원*, 2003.

[12] 정보보호진흥원, "정보보호영향평가제도 도입방안 연구," *정보보호진흥원*, 2003.

[13] 중소기업정보화경영원, "중소기업 정보화 역기능에 관한 실태조사," *중소기업정보화경영원*, 2003.

[14] 한국정보보호센터, "정보보호 정책수립 및 관리지침 개발," *한국정보보호센터*, 2002.

[15] 홍기향, 김정덕, "정보보호 관리체계의 핵심성공요인 및 촉진 요인에 대한 연구," *경영정보학회*, 2001.

[16] Andrew Ren-Wei Fung, Cow-Jean Farm, Abs C. Lin, "A Study on the certification of the information Security Management Systems," *Computer Standards & Interfaces*, 2003.

[17] Bernard, L. and Solms, R., "A formalized to the Effective Selection and Evaluation of Information Security Controls," *Computer & Security*, Vol. 19, No. 2, 2000.

[18] Broderick, J.S., "Information security management When should it be managed?," *Information Security Technical Report*, Vol. 6,

No. 3, 2001.

[19] Bill Hancock, "Threat assessment: Steps to successful creation of corporate threat management plan," *Computer Fraud & Security*, May 1997, pp. 15-17.

[20] BSI, "BS7799: Code of Practices for Information Security Management," *United Kingdom*, 1999.

[21] BSI, "BS7799-2: Information Security Management System - Specification with guidance for use," *United Kingdom*, 2002.

[22] Chechanowicz, Zibgniew, "Risk Analysis: Requirements, Conflicts and Problems," Computer & Security, Vol. 16, 1997.

[23] Cohen, Fred, "Managing Network Security: How does a typical IT audit work?," *Network Security*, 1998.

[24] Dodson Rob, "Information Incident Management," *Information Security Technical Report*, 2001.

[25] Detmar W. Straub, "Organizational structuring of computer security function," *Computer & Security*, Vol. 7, Issue 2, Apr. 1988.

[26] Forte, Dario, "Information Security Assessment: Procedures and Methodology," *Computer Fraud & Security*, 2000.

[27] Gerald Kovacich, "Establishing an information systems security organization," *Computer & Security*, 17, 1998.

[28] Gupta, M. and Cawthorn, G., "Managerial Implications of Flexible Manufacturing for SMEs," *Elsevier Advanced Technology, Technovation*, Vol. 16, No. 20, 1996, pp. 77-83.

[29] 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*, 33, 1996, pp. 189-201.

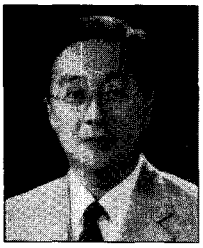
[30] Hone, Karin and Eloff, J.H.P., "What makes an effective information security policy?," *Network Security*, 2002.

[31] Margi Levy, Philip Powell, "SME Flexibility and the Role of Information Systems," *Small Business Economics*, 11, 1998, pp. 183-196.

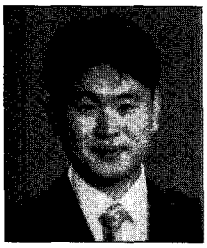
[32] Solm, "Organizational Structuring of computer security function," *Computer & Security*, 1988.

[33] Wood, C.C., "Polices alone do not constitute a sufficient awareness effort," *Computer Fraud & Security*, 1997.

◆ 저자소개 ◆



이정우 (Lee, Jungwoo)
현재 연세대학교 정보대학원에 조교수로 재직 중이며 조지아 주립대학에서 컴퓨터정보시스템에 관한 박사학위를 취득하였다. 산업체에서의 실무경력이 있고 보험 연구소의 연구원으로 근무한 적이 있으며 정보대학원 부임 전에는 미국의 네바다 주립대학교 경영대학에서 교편을 잡은 경력이 있다. 다양한 경험을 배경으로 정보시스템의 개발, 관리 및 활용의 다양한 연구 분야를 가지고 있으며 현재 데이터품질관리 포럼을 운영하고 있다.



박준기 (Park, Jungi)
현재 LG이노텍의 PI그룹 IT전략/기획Part에 재직 중이다. 서울시립대에서 공학사, 연세대에서 정보시스템 관리 석사(2004)학위를 취득하였다. 전자상거래, 시스템감리 분야의 프로젝트 경험을 가지고 있고, 직접 회사를 경영한 경험도 보유하고 있다. 청강문화산업대 전자상거래 강사를 역임했으며, 주된 관심사는 정보시스템의 투자효과 분석과 EA/ITA 분야, 정보시스템과 조직관리에 대한 영향관계이다.

이준기 (Lee, Zoonky)
서울대를 졸업하고 미시간 대학교에서 통계학 석사, 카네기멜론 대학교에서 의사결정과 정보시스템 석사, 남가주대학에서 경영정보학 박사를 취득하였다. Coopers & Lybrand에서 컨설턴트로 근무 하였으며, 미국 네브라스카 주립대(University of Nebraska-Lincoln) 경영대에서 조교수를 거쳐, 현재 연세대학교 정보대학원 부교수로 재직 중이다. 주요 관심 분야는 e 전환(transformation), 다이나믹 프라이싱, 인터넷과 채널, B2B와 e 조달 전략, 정보시스템을 통한 기업의 지식시스템구성에 관한 연구 등이다.

◈ 이 논문은 2004년 7월 26일 접수하여 1차 수정을 거쳐 2004년 11월 11일 게재확정되었습니다.