情 報 保 護 學 會 誌
第 14 券 第 4 號, 2004. 8

# 기업의 정보보호수준 및 성숙도 진단을 위한 정보보호수준 통합평가시스템 개발에 관한 연구*

정 희 조**, 김 진 영***, 임 춘 성****

요 약

조직의 정보보호 목표를 효율적이고 효과적으로 달성하기 위해서는 조직의 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 이를 위해 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가 지표나 기준이 필요하고 우리나라에서 적용 가능한 정보보호 시스템들의 평가방법론이 연구되어야한다. 따라서 본 연구에서는 정보보호와 관련된 기술적 요소와 관리적 요소, 물리적 요소를 기본으로 하는 정보보호 지표체계를 구성하고 정보보호수준을 종합적이고 체계적으로 평가하기 위한 정보보호 성숙 5단계 모형을 통해 서로 매핑될 수 있는 정보보호수준 통합평가시스템을 개발하였다. 이러한 통합평가시스템은 기존연구와의 비교 및 사례적용을 통해 그 실효성을 검증하였다.

## Ⅰ. 서 론

사회전반에 걸쳐 정보화가 급속히 진행되면서 정보보호의 중요성에 대한 인식이 증가하고 있는 것은 시대의 흐름이라 할 수 있겠다.[1] 이러한 시대의 흐름에서 정보보호는 단순히 정보시스템이나 정보기술에 국한된 문제가 아니라 조직 전반에 걸쳐 포괄적으로 검토되어야 하는 문제로 대두되고 있다.[6]

정보보호 평가의 선진국인 미국, 영국, 독일, 프랑스 및 캐나다 등은 1980년대부터 변화하는 사회와 국제환경에 적응하도록 정보보호제품을 평가하기 위한 평가제도를 운영하여 왔다. 국내에서도 1995년 10월에 제정된 정보화촉진기본법과 동법 시행령에 의거 국내 평가 및 인증제도가 구축되어 시행되고 있으며 현재는 정보통신망 침입차단시스템 평가기준과 침입탐지시스템 평가기준을 이용하여 제품에 대한 평가를 실시하고 있다.

하지만 이러한 정보보호 평가 기준은 단지 제품에 대한 기술적인 평가에만 그치고 있어 한 기업의 총괄적인 정보보호 수준을 측정하는 것은 불가능한 현실이다. 따라서 기업의 정보보호수준을 종합적으로 평가하기 위해 보다 체계적인 평가체계의 개발이 요구되게 되었고 이에 본 연구에서는 정보보호와 관련된 기술적 요소, 관리적 요소, 물리적 요소를 기본으로 하는 정보보호 지표체계를 구성하였고 정보보호수준을 종합적이고 체계적으로 평가하기 위해 정보보호 평가절차 및 정보보호 성숙모형의 개발을 통해 기업의 전반적인 정보보호 수준을 측정할 수 있는 정보보호수준 통합평가시스템을 제시하였다.

본 연구의 목적은 기업이 가속화되는 정보보호 위협에 대응하여 조직의 정보보호수준을 종합적이고 체계적으로 파악하여 조직의 정보보호수준의 위치를 인지하고 보다 발전적인 방향을 제시하기 위해 정보보호 성숙모형 및 정보보호 통합평가시스템을 개발하는데 있다.

Ⅱ장에서는 정보보호 수준평가 및 지표, 성숙모형과 관련된 연구를 분석하여 관련 연구의 한계점을 제시하며 Ⅲ장에서는 본 연구에서 개발한 정보보호 통합평가시스템을 소개하고 Ⅳ장에서는 개발된 정보보호 통합평가시스템을 기업에 실제 사례적용해 봄으로써 그 실효성을 검증해 보고자 한다.

* 본 연구는 한국정보보호 진흥원(정책연구 02-05)의 연구비 지원으로 수행되었습니다.
** 연세대학교 일반대학원 기술경영학협동과정(reggie31@yonsei.ac.kr)
*** 포스데이타 IT컨설팅팀(aiejin@empal.com)
**** 연세대학교 컴퓨터산업시스템 공학과 교수(leem@yonsei.ac.kr)

## Ⅱ. 관련 연구

정보보호수준 통합평가시스템을 개발하기 위해 정보보호 수준평가, 정보보호 지표, 정보보호 성숙모형 관련 연구를 살펴보았다.

### 1. 정보보호 수준평가

기업의 정보보호수준을 종합적이고 체계적으로 측정할 수 있는 평가체계는 아직까지 없지만 제품의 기술적 수준을 측정하기 위해서 TCSEC, ITSEC, CC, BS7799등의 평가체계가 사용되어져 왔으며 사)기업정보화지원센터에서는 기업정보화수준평가의 일부로서 정보보호수준지표가 활용되고 있다. TCSEC, ITSEC, CC[9][18]는 각국의 보안 제품 및 시스템 평가를 위한 평가체계로 기본적으로 제품이라는 기술적 부분에만 한정되어 평가를 하는 반면에 BS7799는 영국의 상무성 주관으로 '정보보안관리 실무규범'이라는 제목하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되어진 권고안의 성격을 지니고 있다.[2][11][13][15] 정보화수준평가의 일부로 측정되는 정보보호수준지표는 평가지표가 10개밖에 안되어 전반적인 정보보호 수준을 측정할 수는 없지만 개략적으로나마 기업의 정보보호 수준을 평가하고 있다. 정보보호 수준평가에 관련된 기존 연구를 정리하면 [표 1]과 같다.

[표 1] 정보보호 수준평가 관련 연구

| | 내 용 |
|---|---|
| TCSEC [18] | · 미국에서 개발된 세계 최초의 평가기준<br>· 미국방성 컴퓨터 시스템의 보안성을 평가하기 위하여 개발<br>· 정보보호의 요소 중 기밀성만을 강조하여 민간기업에는 적용하기가 어려움 |
| ITSEC [18] | · 유럽국가들이 보안성 기준을 통합하기 위해 개발된 세계 최초의 국제 통합기준<br>· 단일 기준으로 모든 정보보호제품을 평가<br>· 보안보증 부분만으로 제품에 대한 평가를 수행 |
| CC[9] | · CTCPEC, TC, TCSEC, ITSEC의 단일 평가 기준으로 국제공통 평가기준 |
| BS7799 [2][11] [13][15] | · 정보보안을 유지하고 구현하는 관리자를 위한 보편적인 기준<br>· 기업이 선택해야 하는 지침과 권고안의 성격을 지님<br>· 평가대상이 IT 보안에 집중되어 주로 높은 수준에 정보호호 기준을 제공 |
| 정보보호 수준지표 [5] | · 사)기업정보화지원센터에서 매년 정보화수준 평가의 일환으로 정보보호 투자정도, 정보보호제도 및 운영, 정보보호시스템 구축정도를 평가 |

### 2. 정보보호 지표

정보보호 지표에 대한 연구는 크게 정보화지표와 BS7799와 관련된 연구로 나누어진다. 전산원은 매년 정보화를 구성하는 정보설비, 정보이용, 정보투자분야의 각 측면에 대해 정의에 맞는 통계 항목을 측정하여 정보화 지표를 산출하고 있으며[7][8] BS7799는 조직이 효과적인 정보보호관리 체계를 수립, 수행, 감시하기 위한 종합적인 가이드라인을 제공하고 조직 상호간의 신뢰성있는 거래를 위한 기반을 제공하기 위한 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안, 의사소통 및 운영관리, 접근통제, 시스템 개발 및 유지보수, 업무지속성관리, 준수의 10가지 분야에 대한 통제항목을 제시한다.[2][11][13][15] 정보보호 지표에 관련된 기존 연구를 정리하면 [표 2]과 같다.

[표 2] 정보보호 지표 관련 연구

| | 내 용 |
|---|---|
| 정보화 지 표 [7][8] | · 정보통신기술을 이용한 전자계 정보화를 중심으로 정보설비, 정보이용, 정보투자지표 분야로 설정하여 각 분야별 구체적인 항목을 제시 |
| BS7799 [2][11] [13] [15] | · 조직의 효과적인 보호관리 체계를 위한 종합적인 가이드라인을 제공<br>· 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안, 의사소통 및 운영관리, 접근통제, 시스템 개발 및 유지보수, 업무지속성관리, 준수의 10가지 분야에 대한 통제항목을 제시 |

### 3. 정보보호 성숙모형

정보기술 환경의 급속한 발달과 더불어 고객의 요구사항이 다양해지고, 정보화가 지원하는 영역이 점진적으로 확대되면서, 이러한 요구사항에 대응하기 위하여 정보화 수준 또한 점진적으로 성숙되어 가고 있다. 이에 따라 이러한 성숙도를 표현할 수 있는 모델이 필요하게 되었는데 본 연구에서는 미국의 NIST가 제시하는 컴퓨터시스템의 라이프 사이클의 성숙단계와 SSE-CMM이 제시하는 조직의 보안공학 프로세스의 성숙단계를 바탕으로 새로운 정보보호 성숙모형을 제시하고자 한다. 미국의 NIST는 컴퓨터 시스템의 라이프 사이클에서 보안과 계획에 관한 개략적인 절차를 제공하는데 NIST의 컴퓨터 라이프 사

〔표 3〕 정보보호 성숙모형 관련 연구

| | 내 용 |
|---|---|
| NIST 〔12〕 | · 컴퓨터시스템의 라이프 사이클에서 보안과 계획에 관한 계략적인 절차를 시작, 개발 및 도입, 구현, 운영 및 유지보수, 폐기의 총 5단계로 구분하여 제공 |
| SSE -CMM 〔14〕 〔19〕 | · 보안공학 라이프 사이클로서 비공식적으로 수행되는 수준1부터 지속적인 계획의 수준5까지 5단계로 보안성숙도 단계를 제시 |

이클은 크게 시작, 개발 및 도입, 구현, 운영 및 유지보수, 폐기의 총 5단계로 구분되어진 성숙단계를 제시하고 있다.〔12〕 SSE-CMM은 조직의 보안공학 프로세스의 핵심적인 특징을 묘사하고 있으며 비공식적으로 수행됨, 계획되고 관리됨, 잘 정의됨, 정량적으로 통제됨, 지속적인 개선의 총 5단계 보안 성숙도 모형을 제시하고 있다.〔14〕〔19〕 정보보호 성숙모형에 관련된 기존 연구를 정리하면 〔표 3〕와 같다.

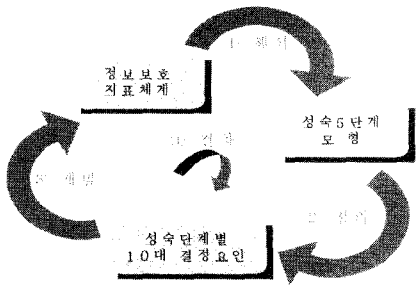
## 4. 관련 연구의 한계점 및 개선방안

정보보호 통합평가시스템 개발을 위한 관련 연구는 크게 정보보호 수준평가, 정보보호 지표, 정보보호 성숙모형에 관한 연구로 구분된다. 이러한 관련 연구는 크게 두 가지 면에서 한계점을 지니는데 첫째, 정보보호 평가 지표가 기술적인 부분에만 한정되어 있어 하나의 제품이나 시스템에 대한 평가는 가능하지만 기업이나 조직의 전반적인 정보보호 수준을 측정하기는 어렵다는 것이고 둘째, 급변하는 정보보호환경에 적응성과 유연성이 부족하여 기존 정보보호 지표들로서는 현재 정보보호 수준에 대한 체계적인 해석이 불가능하다.

따라서 이러한 한계점을 해결하기 위해서 본 연구에서는 기술적인 부분뿐만 아니라 기업의 관리적, 물리적인 부분까지 포함한 정보보호 지표체계를 제시하고 정보보호 환경에 적응성과 유연성이 뛰어난 정보보호 성숙모형의 개발을 통해 기업의 전반적이고 체계적인 정보보호 수준을 측정할 수 있는 정보보호 통합평가시스템을 통해 정보보호 수준을 측정하고자 하는 것이다.

# Ⅲ. 정보보호수준 통합평가시스템

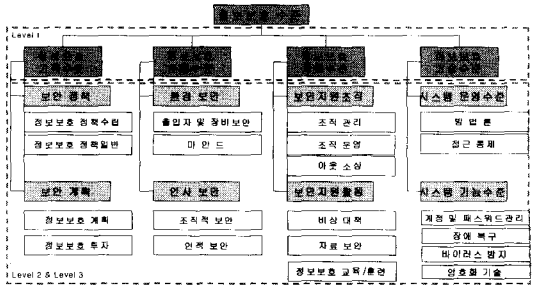
정보보호수준 통합평가시스템은 크게 4단계로 구성된다. 먼저 기획수준, 환경수준, 지원수준, 기술수준의 4대 평가영역 및 8개 지표항목으로 구성되는 정보보호 지표체계를 통해 성숙 5단계모형을 해석하는 첫 단계 그리고, 해석된 성숙 5단계모형을 바탕으로 정보보호 성숙단계별 10대 결정요인이 정의되는 두 번째 단계, 이러한 성숙단계별 10대 결정요인을 통해 정보보호 지표체계를 개발하는 세 번째 단계, 마지막으로 정보보호 수준 평가를 통해 앞에 세단계가 반복되는 절차의 네 단계로 구성된다. 본 연구에서 제시하는 정보보호수준 통합평가시스템의 흐름도는 〔그림 1〕과 같다.




〔그림 1〕 정보보호수준 통합평가시스템의 흐름도

## 1. 정보보호 지표체계

본 연구에서는 정보화지표와 BS7799를 기반으로 체계적이고 종합적인 정보보호 지표체계를 개발하였다. 기업의 보안수준을 기획수준, 환경수준, 지원수준, 기술수준의 네 가지 관점(Level 1)에서 바라보고 있으며 정보보호의 취약점을 분석하고 그에 따른 정보보호 수준을 평가할 수 있도록 하고 있다. Level 2는 보안정책, 보안계획, 환경보안, 인사보안, 보안지원조직, 보안지원활동, 시스템 운영수준, 시스템 기능수준으로 구성되며 새롭게 개발된 정보보호 지표체계는 정보보호 계획 및 정보보호 투자, 마인드 및 조직적 보안, 아웃소싱, 바이러스 방지등 BS7799에서 권고하고 있는 사항이 아닌 시대에 맞는 새로운 지표를 제시하였다. 본 연구가 제시하는 정보보호 지표체계는 〔그림 2〕와 같다.

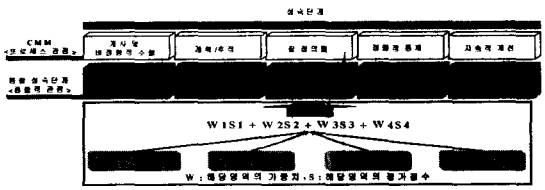



〔그림 2〕 정보보호 지표체계

## 2. 정보보호 성숙모형

정보보호수준 향상을 위한 성숙체계는 크게 정보보호 수준을 단계화 하는 '성숙단계', 성숙단계를 달성하기 위한 '성숙과정' 그리고 성숙과정을 업종별 구분에 의해 '비교하는 과정'의 세 가지 큰 흐름으로 나뉘어진다. 본 연구에서는 정보보호 성숙체계를 기반으로 기획수준, 환경수준, 지원수준, 기술수준의 4가지 평가영역을 포괄할수 있는 정보보호 성숙모형을 제시하고자 하며 이러한 정보보호 성숙모형은 5단계의 성숙도로 구성되어진다.

정보보호 성숙모형은 보안공학 프로세스의 성장단계를 제시하는 SSE-CMM과는 확연하게 구분되는데 SSE-CMM이 프로세스상에서 단순한 성숙단계만을 제시하는 반면 정보보호 성숙모형은 기업의 전반적인 정보보호 관점을 포괄할 수 있는 성숙단계를 제시한다. 본 연구가 제시하는 정보보호 성숙단계는 [그림 3]과 같이 5단계로 구성되며 각 단계가 제시하는 영역별 수준에 대한 정의는 [표 4]와 같다.




[그림 3]정보보호 성숙단계

[표 4] 정보보호 성숙 단계별 정의

| 성숙 단계 | | 정 의 |
|---|---|---|
| 전 략 적 정보보호 | | 축적된 정보보호 기술을 이용하여 새로운 비즈니스를 창출하고 기업의 가치를 증대하는 전사적인 차원의 정보보호 수준 |
| 관리적 정보보호 | 능 동 적 정보보호 | 정보보호 우수상이 도입되고 선진사례를 도입하여 기업의 정보보호에 적극 반영하며, 최신 정보보호 기술을 획득하여 기업의 총체적인 정보보호를 실시하는 수준 |
| | 수 동 적 정보보호 | 정보보호 위험에 대한 모든 것을 관리하는 단계로 정보보호 전문부서를 설치하고 정보보호 관리자를 임명하여, 정보보호 전략계획이 수립되는 수준 |
| 기 술 적 정보보호 | | 기업의 전산부서 중심의 인트라넷 정보보호가 실시되고 방화벽을 설치하며 중요문서에 대해서는 백업이 실시된다. 정보보호 전략계획이 수립되어 있지 않으며 정보보호 관련 지침이 없는 수준 |
| 기 능 적 정보보호 | | 개인차원의 정보보호가 실시되는 단계로 백신, 화면보호기등의 소극적 정보보호가 실시되는 단계 |

## 3. 정보보호 성숙 결정요인

정보보호 성숙모형에서 정의된 영역별 수준단계는 단순히 단계별 정보보호수준을 정의하고 있는데 불과하다. 이러한 단계별 정보보호 수준을 보다 세부적으로 정의하고 측정가능 하도록 하기 위해서는 각 단계별 특징을 나타낼 수 있는 성숙 결정요인이 필요하다. 본 연구에서 제시하는 정보보호 성숙 결정 요인의 각 단계별 특징에 매핑하면 [표 5]와 같이 정의할 수 있다.

[표 5] 정보보호 성숙단계별 결정요인

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | 수립되어 있지않음 | 수립시작 | 수립완료 | 주기적으로 관리 | 경 영 정책과 동시개발, 표준화 달성 |
| | 고려되고 있지않음 | 관심을 가지고 진행 | 계획의 수립과 실행 | 지속적 증 가 | 투자 효과의 검증 |
| | | | | | |
| | 기본규정 존 재 | 세부규정 존 재 | 세부규정의 이행 | 주기적 통 제 | 규정제도의 정착 및 표준화 구축 |
| | 규정존재 | 집단업무 지 원 | 통 합 데이타 베이스 활 용 | 협력업체 고객간 네트워 구 축 | 통합데이타베이스에 대한 활용성 검증 |
| | 개인적 수 준 | 시스템 고 려 | 내부망 보 호 | 외부망 보 호 | 전문화된 정보보호 조 직 |
| | | | | | |
| | 기본적 지 원 | 관리자 편성 및 사용자 서비스 강 화 | 경영자의 의사결정 지 원 | 자동화 도구의 활 용 | 지 식 베이스를 이용한 능동적 시스템 |
| | 규정이 존재하지 않 음 | 규정존재 | 규정에 따 른 이 행 | 중대성의 인식과 빠른대응 능력보유 | 전문화된 대책능력 보 유 |
| | 기본적 교 육 | 필요애 따른 교육/훈련 실 시 | 교육/훈련에 대한 확산 | 마인드 증대와 주기적인 교육/훈련 | 수준별 교육/훈련 프로그램 존 재 |
| | | | | | |
| | 기본적 수준으로 운 영 | 기능적 전문성 보 유 | 시스템적 대 응 | 활용에 의한 효과성 추 구 | 경 영 전략과 병행하여 체계적으로 실 행 |
| | 개인적 업무활동 | 기본적 정보통신 서비스 이용 | 체계적 인증 절차의 활 용 | 지속적인 갱신과 활 용 | 지 식 베이스에 의한 지속적 활용 |

## 4. 정보보호수준 통합평가절차

정보보호수준 통합평가절차는 크게 평가가 이루어지는 절차를 나타내는 평가절차와 평가의 대상이 되는 정보보호 환경을 세분화하여 나타내는 평가영역으로 나누어진다. 평가절차는 조직의 정보보호수준을 측정하고, 분석 및 해석하며, 해석결과를 정보보호수준 성숙과정으로 환류 시키는 과정을 말하며, 이러한 활동을 효율적이며, 목적 지향적으로 수행하기 위한 일련의 연속적 행위계열이다. 평가절차는 평가와 관련된 요인들의 자료를 수집하여 측정하는 측정절차와 측정된 결과를 바탕으로 조직의 정보보호수준과 문제점 및 개선사항을 도출하는 분석 및 해석절차로 구분되며 정보보호수준을 측정하기 위한 평가절차에 관한 학문적 연구는 전무한 상태이다. 따라서 본 연구에서는 평가절차에 대한 연구인 미국의 GAO(United States General Accounting Office)[10] 및 GSA (General Services Administration) 등 일부 기관에서 실무 적용을 위한 몇몇 연구를 기초하여 정보보호수준 평가를 위한 평가절차를 유도하였다. 본 연구에서 제시하는 정보보호수준 통합평가절차는 〔표 6〕과 같다.

평가영역은 정보보호의 정적인 측정요인과 각 주체간 연관관계에 의해 발생하는 효과영역인 영향요인으로 세분화된다. 측정요인은 평가절차의 측정절차에 의해 현재의 수준이 측정되고, 영향요인은 평가절차의 분석 및 해석절차에 의해 수준 및 지표로 도출된다. 또한, 평가결과가 정보보호수준 제고에 기여하기 위해서는 평가결과가 추적되고 학습되며, 환류(feedback)되어야 하므로, 학습 및 환류절차가 수립되어야 한다.

〔표 6〕 정보보호수준 통합평가절차

| | |
|---|---|
| 임무 및 요구정보 정의<br>- Stakeholder 포함<br>- 환경접속<br>- 환동, 핵심프로세스 및 자원 정렬 | - 평가목적/범위 설정 (요구결과 식별)<br>- 정보보호 성숙단계결정<br>- 평가영역/분야/요인 결정<br>- 평가절차, 자원 정열 |
| 성능 측정<br>- 조직수준별 척도 도출<br>- 자료 수집 | - 자료 수집<br>- 항목별 상태 계량화 |
| 성능 정보 활용<br>- 성능 차이 식별<br>- 정보 보고 및 활용 | - 요구결과별 평가결과 해석 및 분석<br>- 각종 결과보고서 도출 |
| 전문지식 형성 및 관리 혁신 통합 | - 성숙단계와 평가결과 간의 수준차이 분석<br>- 자료축적 및 지식 형성 |
| | - 평가결과를 성숙과정으로 환류 |

## 5. 관련 연구와의 비교

본 연구에서는 정보보호 관련 이론과 방법론을 바탕으로 정보보호 지표체계, 정보보호 성숙모형, 평가영역별 결정요인을 제시하였고 이를 바탕으로 정보보호통합평가시스템을 개발하였다. 개발된 정보보호통합평가시스템을 관련 연구와 비교해보면 첫째, 제품 및 시스템에 대한 평가만 가능하였던 BS7799, CC등과는 달리 기업의 전반적인 정보보호 수준을 체계적으로 측정할 수 있도록 정보보호 기획수준, 환경수준, 지원수준, 기술수준으로 세분화되어 측정이 가능해졌으며 둘째, SSE-CMM이나 NIST가 제시하는 프로세스상에 치우친 성숙모형과는 달리 기업의 전반적인 영역을 평가할 수 있는 5단계 정보보호 성숙모형을 통해 기업에 대한 단계별 수준 진단이 가능하게 되었으며 이러한 수준 진단을 바탕으로 기업이 추진해야할 정보보호의 향후 방향도 제시할 수 있게 되었다. 〔표 7〕은 BS7799과 본 연구에서 개발된 정보보호 지표와의 차이점을 설명하고 있다.

〔표 7〕 BS7799와 정보보호 지표체계와의 차이점

| 구 분 | 내 용 |
|---|---|
| BS7799 | 보안정책, 보안조직, 자산분류 및 통제, 인적보안, 물리적 및 환경적 보안, 의사소통 및 운영관리, 접근통제, 시스템 개발 및 유지보수, 업무지속성관리, 준수의 10가지 주요 섹션하에 127가지의 보안 통제항목을 지표로 제시 |
| 정보보호 지표체계 | BS7799의 10가지 주요 섹션의 정보보호 지표를 기반으로 BS7799가 제시하지 않고 있는 정보보호 계획 및 정보보호 투자, 마인드 및 조직적 보안, 아웃소싱, 바이러스 방지등의 6개 항목 총 32개의 새로운 지표를 포함한 총 133가지의 정보보호 지표를 제시 |

## Ⅳ. 사례 적용

본 연구에서 개발된 정보보호수준 통합평가시스템을 바탕으로 국내 굴지의 제조업체인 A사의 정보보호 역량을 평가하고 성숙도 진단을 통해 정보보호수준을 진단하였다.

### 1. 가중치 산정

정보보호 기획수준, 환경수준, 지원수준, 기술수준의 1

〔표 8〕 평가항목별 가중치

| 가중치 | 0.28 | | 0.1 | | 0.18 | | 0.44 | |
|---|---|---|---|---|---|---|---|---|
| 2 level | 보안정책 | 보안계획 | 환경보안 | 인사보안 | 보안지원조직 | 보안지원활동 | 시스템운영수준 | 시스템기능수준 |
| 가중치 | 0.31 | 0.69 | 0.44 | 0.56 | 0.53 | 0.47 | 0.59 | 0.41 |

level과 보안정책, 보안계획등의 2 level에 대한 가중치를 적용하기 위해 정보보호 관련 전문가 집단을 대상으로 설문조사를 통한 각 기준들 간의 가중치를 측정하였다.

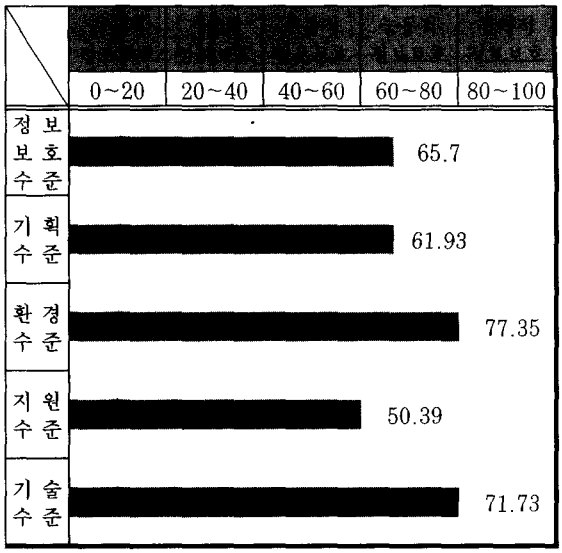
정보보호수준 평가를 위한 최상위 수준인 1 level의 가중치는 AHP기법에 의한 쌍대 비교를 통해 일관성을 어느 정도 유지하면서 산정되어졌으며 평가영역(1 level)을 구성하는 지표항목(2 level)에 대한 가중치는 10개의 설문을 통한 전문가 집단의 응답을 평균하여 산정하였다. 〔표 8〕은 평가항목별 가중치를 보여주고 있다.

## 2. 'A'사 정보보호수준 평가결과

정보보호수준 통합평가시스템을 활용하여 국내 굴지의 제조업체인 'A'사의 정보보호 수준을 평가해본 결과 65.7점으로 정보보호 수준이 정보보호 성숙모형의 3번째 단계인 능동적인 정보보호수준에 다다른 것으로 나타났다.

'A'사에 사례적용을 위한 정보보호 수준평가는 정보보호 지표체계로부터 개발된 정보보호 수준평가 설문지를 바탕으로 측정된 결과에 가중치를 적용하여 평가시스템 및 성숙모형을 통해 정보보호 수준을 해석함으로서 기업의 전반적인 정보보호 수준 및 현상황을 한눈에 파악할 수 있었다.

평가결과 A사는 2001년말에 측정했던 50점대 수동적 정보보호수준에 머물렀던 평가 결과와는 달리 2002년말에는 전반적으로 정보보호에 대한 관리가 잘 이루어지며 65.7점으로 능동적 정보보호 수준으로 향상된 것으로 나타났으며 특히 기획수준에서 두드러진 향상이 나타나 정보보호에 대한 경영진의 관심증대에 따라 투자, 정책등에 많은 영향을 미치면서 이와 같은 결과가 나타난 것으로 분석되었다. 특히 2001년에는 단순히 기술적 수준에서만 평가가 가능했던 기존 평가시스템과는 달리 관리적, 물리적 기준들이 보강된 새로운 평가시스템을 활용함으로서 투자, 정책, 마인드등 기존에 측정할 수 없었던 정보보호에서 가장 민감한 사용자와 관련된 새로운 정보보호 지표들의 보강을 통해 측정이 가능해졌으며 또한, 정보보호




〔그림 4〕 'A'사의 정보보호 수준평가 결과

성숙모형을 통해 더욱더 정확하고 가시화된 정보보호 성숙단계를 제시할 수 있게되면서 전반적인 기업의 정보보호 수준을 평가할 수 있게 되었다. 정보보호수준 통합평가시스템을 활용하여 'A'사의 정보보호수준을 평가한 결과는 〔그림 4〕와 같다.

## V. 결 론

본 연구에서는 정보보호수준을 종합적이고 체계적으로 평가하기 위해 정보보호와 관련된 기술적 요소와 관리적 요소, 물리적 요소를 기본으로 하는 정보보호 지표체계를 개발했다. 개발된 정보보호 지표체계를 통해 설문지를 구성하고 가중치를 적용해 측정된 결과를 정보보호 성숙모형을 통해 해석함으로써 정확하고 가시화된 기업의 정보보호수준에 대한 객관적인 평가가 가능하게 되었다. 향후 이러한 정보보호수준 통합평가시스템을 활용하여 기업 및 국가의 정보보호수준을 객관적으로 측정할 수 있으며 평가 결과를 바탕으로 민간부문의 정보보호수준 제고를 위한 정보보호정책 수립에 합리적인 의사결정의 도구로 사용될 수 있다.

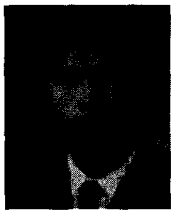
## 참 고 문 헌

〔1〕 강병준, "*인터넷 혁명과 정보보호*", 삼각형프레스, 2001

〔2〕 김기윤, 나관식, "취약성 평가에 의한 정보보호 지표의 계량화 : 정보자산가치가중치법", *한국정보보*

*호학회지*, 10(1), pp. 51-62. 2000
[3] 김인주, "정보화수준 성숙모델 기반의 통합평가시스템 개발", *연세대학교 박사학위 논문*, 2000
[4] 김정덕, 김기윤, "정보보호지표 항목개발 및 계량화 연구", *한국정보보호진흥원*, 1998
[5] 기업정보화지원센터, "2002 기업정보화수준평가결과보고서", *기업정보화지원센터*, 2003
[6] 신동진, "*인터넷 정보보안*", 동일출판사, 2001
[7] 한국전산원, "국가정보화수준 측정 및 지표개발", *한국전산원*, 2001
[8] 한국전산원, "국가정보화지표 및 OECD 국가의 인터넷수준측정", *한국전산원*, 2001
[9] Common Criteria Project, "common criteria for information technology security evaluation", *common criteria*, 1998
[10] GAO, Executive Guide, "Measuring performance and demonstrating results of information technology investments", *GAO/AMID-98-89*, 1998
[11] Lynette Barnard, "The evaluation and certification of information security against BS7799", *Information Management & Computer Security*, 6/2, pp. 72-77. 1998
[12] NIST, "An introduction to computer security : the NIST handbook", *NIST (national institute of standards and technology)*, 1995
[13] Rossouw von solms, "Information Security Management (3) : the code of practice for Information Security Management (BS7799)", *Information Management & Computer Security*, 6/5, pp. 224-225. 1998
[14] SSE-CMM project team, "Systems security engineering capability maturity model", *SSE-CMM*, 1999
[15] BSI, "BS7799", *BSI*, 1999
[16] IDC, "The 1996 IDC/World Times information Imperative Index : Toward the Third Revolution", 1996
[17] NIST, "Security Assessment Guide Information Technology Systems", *NIST Special Publication 800-26*, 2001
[18] http://www.kisa.or.kr/
[19] http://www.sse-cmm.org

## 〈著 者 紹 介〉

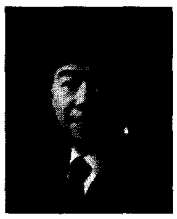


**정 희 조 (Heejo Chung)**
**정회원**

2002년 2월 : 수원대학교 고분자공학과 졸업
2002년 3월~현재 : 연세대학교 기술경영학협동과정 석사과정
〈관심분야〉 정보보호, 전자상거래 보안, 정보보호시스템

**김 진 영 (JinYoung Kim)**

2000년 2월 : 아주대학교 산업공학과 졸업
2003년 2월 : 연세대학교 컴퓨터산업시스템공학과 석사
2003년 2월~현재 포스데이타 IT컨설팅팀
〈관심분야〉 시스템/네트워크 보안, EA



**임 춘 성 (ChoonSeong Leem)**
**정회원**

1985년 2월 : 서울대학교 산업공학과 졸업
1987년 2월 : 서울대학교 산업공학과 석사
1992년 2월 : University of California at Berkeley 산업공학과 박사
1995년~현재 : 연세대학교 컴퓨터산업시스템공학과 교수
1997년~현재 : 정보통신부 산하 사단법인 기업정보화지원센터장
〈관심분야〉 정보화평가, 전자상거래, 정보보호

## 부록) 정보보호 지표체계

| 평가영역 | 평가항목 | 지표항목 | 세부 지표 |
|---|---|---|---|
| 정보보호 기획수준 | 보 안 정 책 | 정보보호 정책수립 | 정보보호 정책수립여부, 정책의 검토 및 평가, 정보보호 정책의 문서화 |
| | | 정보보호 정책일반 | 정보보호 정책 내용, 서약서 작성, 정보보호 정책의 준수 |
| | 보 안 계 획 | 정보보호 계획 | 정보보호 master plan 수립여부, 정보보호 master plan 갱신주기 |
| | | 정보보호 투자 | 매출액 대비 정보보호투자비용, 매출액 대비 정보보호투자증가율, 1인당 정보보호 예산, 정보보호 전담인력 비율, 정보보호 표준화 건수 |
| 정보보호 환경수준 | 환 경 보 안 | 출입자 및 장비보안 | 출입증 관리 및 인가자 확인, 출입용 카드 발급 절차, 출입증 분실에 따른 대비 절차, 자동잠금장치 및 시건장치, 장비 유지보수를 위한 절차 및 지침, 장비 유지보수, 장비담당자 선정, 장비담당자 책임할당, 가방, 꾸러미 등의 조사, 외부자, 비인가 내부직원의 출입제한, 장비관리 대장 |
| | | 환경보안 일반 | 시설물 보안, 정보통신시스템 종류, 인터넷 접속 속도, 운영중인 정보보호 시스템, 정보보호를 위한 시설물, UPS 및 자가발전설비, 사용중인 보안제품 현황, 정보보호기술현황 |
| | | 마인드 | 경영자 마인드, 정보보호 수상경력, 년평균 교육일수/정보보호 추진인력, 정보보호 수준평가 경험, 정보보호 마인드 확산 활동 |
| | 인 사 보 안 | 조직적 보안 | 책상의 청결한 유지, 화면보호기의 사용, 개인 휴지통관리, 징계 절차 수립, 소프트웨어 오류보고 절차, 이전 직무자의 접근 통제 |
| | | 인적 보안 | 보안사건 대응절차, 정보보호 제보자의 포상, 보안 사건 보고서, 취약성 리포트 |
| 정보보호 지원수준 | 보 안 지원조직 | 조직 관리 | 정보보호 담당자, 정보보호 담당자의 직급, 정보보호 관리위원회, IT관련 보안 인력의 인력확보율, 보안관련 공인된 자격증 보유수준, 정보보호 조직의 독립성, 정보보호 역할에 따른 직무 할당 |
| | | 조직 운영 | 업무순환정책의 유무, 관리자 정보 보호 인식, 전문가 자문 경험, Help Desk의 운영, 정보보호 활동의 통합/조정, 경영층으로의 직접보고 |
| | | 아웃 소싱 | 아웃 소싱 비율, 아웃 소싱 영역, 아웃 소싱 관리 |
| | 보 안 지원활동 | 비상 대책 | 비상시의 대응계획 수립, 비상시 대응 방법의 게시/홍보, 우선순위에 따른 복구순서, 정보보호 사고 일지 기록 문서 작성, 정보보호 산업체 및 관련 정부기관의 상호협약, 모의훈련 실시 |
| | | 자료 보안 | 출력장치 현황, 자료 출력물 보안, 디지털 서명, 소프트웨어 불법복제 방지 |
| | | 정보보호 교육/훈련 | 정보보호 교육/ 훈련 계획 및 실시, 정보보호 교육/훈련 일반, 관리층의 정기적 브리핑 참여, 정보보호관련 정기간행물의 비치, 정보보호 표준, 지침등의 기술서 배포, 교육 대상자 선발방식 |
| 정보보호 기술수준 | 시스템 운영수준 | 시스템 운영수준 일반 | 응용시스템의 불법변경 통제, 프로그램의 유지보수, 중요도 및 긴급성을 위한 우선순위 부여, 네트워크 운영통제 일반, 외부망 정보보호, 방화벽 |
| | | 방법론 | 방법론 사용 여부와 문서화, 유지/보수시의 엄격한 통제, 매뉴얼의 사용, 위협분석 및 절차의 평가, 방법론 일반, 보안 컨설팅 경험 |
| | | 접근통제 | 프로그램 접근전의 신원확인, 각 서버의 계정 사용 제한, 정보시스템에 대한 접근 통제, N/W센터의 접근통제, N/W센터의 상주직원수, 통제센타와 처리부서와의 분리, N/W의 변경시의 변경통제, N/W모니터링 프로그램의 설치, 루트의 특정 IP, 콘솔로의 제한 설정 |
| | 시스템 기능수준 | 계정 및 패스워드 관리 | 사용자 계정 및 패스워드 관리, 일정기간 미사용 계정의 정지, UID, GID설정 표준화, 동일한 로그인명이나 UID 허용, 정책상의 패스워드 변경 및 통지, 패스워드 자릿수제한, 패스워드 선택제한, 패스워드의 변경주기, 패스워드, ID신청서의 보관, 정지된 계정의 재사용시 최초 로그인때 패스워드 변경, 패스워드 연속 실패시 penalty 적용, 접근 수준 및 권한 확인, 접근 제어 일반, 개인 정보 접근제어, 정보보호 인증, 정보보호 로깅 |
| | | 장애복구 | 백업과 복구계획의 정기적 검사, 데이터 처리활동의 분산화, 백업설비들의 정기적 테스트, 데이터 처리장비에 대한 부품준비, 비상시 데이터처리센타의 접근통제, 중요 파일, DB의 백업, 해킹사고 경험, 해킹사고 대응 현황 |
| | | 바이러스 방지 | 바이러스 관련 백신의 사용, 바이러스 피해 경험 및 정도, 바이러스 방지를 위한 대책 수립, 바이러스 검사 주기 |
| | | 암호화기술 | 메시지의 무결성 검사, 자동 키관리 시스템, 정보보호 침해 의심시 키의 변경, 메시지 인증코드의 사용, 정보보호 매개변수의 암호화 |