기업의 정보보호 수준 평가를 위한 평가지표*

나윤지** · 조영석*** · 고일석****

요 약

인터넷 및 정보기술의 발전은 정보의 생성 및 관리기술 뿐만이 아니라 정보보호의 중요성을 증대시키고 있다. 정보보호는 기술적인 측면만이 아니라 관리적인 측면을 포함한 영역이며 관리적 측면에서 정보보호 수준 평가에 대한 연구가 이루어지고 있다. 현재까지 대부분의 정보보호 평가체계는 정보보호제품에 중점을 두고 있다. 본 연구는 기업의 조직 관점에서 정보보호 수준 평가에 대한 연구를 목적으로 하고 있다. 기업의 정보보호수준을 평가하기 위해서는 기업 조직 전반에 대한 분석과 이를 기반으로 한 종합적이고 체계적인 평가 체계가 필요하다. 본 연구에서는 기업 전반에 대한 정보보호 요인을 기획, 환경, 지원, 기술, 관리의 수준으로 구분하고 이를 기반으로 지표를 개발하여, 기업조직 전체의 정보보호 수준을 측정함으로서, 기업의 정보보호수준 위치 파악과 이를 통한 발전적인 정보보호 방향을 제시하기 위한 정보보호수준 평가체계를 연구하였다.

A Study on the Evaluation Indices for Evaluation of the Information Security Level on the Enterprise Organization*

Yun Ji Na** · Young Suk Cho*** · Il Seok Ko****

ABSTRACT

Until now, most of the evaluation systems have performed evaluation with an emphasis on information security products. However, evaluating information security level for an enterprise needs analysis of the whole enterprise organization, and a synthetic and systematic evaluation system based on it. In this study we subdivided the information security elements of the whole enterprise such as planning, environment, support, technology, and management; developed indices based on them; finally, made the information security level of the whole enterprise organization possible to be measured. And we tried to grasp the information security level of the whole enterprise organization, and develop an evaluation system of information security level for suggesting a more developing direction of information security.

Key words : Evaluation Systems, Evaluation Indices

---

* 본 과제는 산업자원부 지역혁신연구센터 지원으로 연구가 이루어졌음.

** 호남대학교 인터넷소프트웨어학과

*** 교신저자, 동국대학교 컴퓨터학과

**** 동국대학교 컴퓨터학과

1. 서 론

인터넷 및 정보기술의 발전은 정보의 생성 및 관리기술 뿐만이 아니라 정보보호의 중요성을 증대시키고 있다. 정보보호는 기술적인 측면만이 아니라 관리적인 측면을 포함한 영역이며 관리적 측면에서 정보보호 수준 평가에 대한 연구가 이루어지고 있다.

정보보호는 단순히 정보시스템이나 정보기술에 국한된 문제가 아니라 조직 전반에 걸쳐 포괄적으로 검토되어야 하는 문제로 대두되고 있다. 또한 기업의 정보처리 의존도가 점점 증가함에 따라 정보시스템의 보호대책 미비로 인한 손실 또한 증가하고 있다[1-3].

조직의 정보보호 목표를 효과적으로 달성하기 위해서는 조직 전반의 정보보호 수준을 정확히 평가하고 이를 개선시킬 방향을 제시하는 기준이나 평가모델이 필요하다. 또한 이를 위해 부문별 정보보호 수준을 평가하고 개선할 수 있는 평가 지표가 요구된다[4-6].

대표적인 정보보호 평가 기준으로는 ITSEC, TCSEC, BS7799 등이 있다. 정보보호 시스템 평가의 경우 ITSEC, TCSEC, CC 등과 같은 평가기준이 있으나 이는 정보보호 제품의 보안기능에 대한 기술적 평가를 위해 개발되어 졌으며, 그에 따른 한계를 가지고 있다. 또한 BS7799의 경우는 관리체계의 인증이며, 제품의 인증이 아니다. 따라서 시스템 기능에 대한 평가와 기업의 전반에 대한 평가 곤란하다는 단점이 있다[9, 10].

기업의 보안은 기업 조직 전체 대한 분석을 기반으로 하여야한다. 기업 조직에 대한 전반적인 보안은 개별 보안 제품의 조합으로만 달성될 수 없으며, 보안 기능을 제공하는 제품/시스템과 관리적인 보안대책이 적절히 융합되어 전반적인 보안관리체계가 제대로 운영되고 있을 때 한 조직의 정보보안이 효과적으로 유지될 수 있다[7, 8]. 또한 한 조직의 전체적인 보안 수준은 조직 고유의 운영 환경과 보안 요구사항에서 도출되는 보안 정책이 적절하게 구현되고 운영되는지를 통하여 평가하여야 한다.

현재까지 대부분의 정보보호 평가체계는 정보보호제품에 중점을 두고 있다. 본 연구는 기업의 조직 관점에서 정보보호 수준 평가에 대한 연구를 목적으로 하고 있다. 기업의 정보보호수준을 평가하기 위해서는 기업 조직 전반에 대한 분석과 이를 기반으로 한 종합적이고 체계적인 평가 체계가 필요하다. 본 연구에서는 기업 전반에 대한 정보보호 요인을 기획, 환경, 지원, 기술, 관리의 수준으로 구분하고 이를 기반으로 지표를 개발하여, 기업조직 전체의 정보보호 수준을 측정함으로서, 기업의 정보보호수준 위치 파악과 이를 통한 발전적인 정보보호 방향을 제시하기 위한 정보보호수준 평가체계를 연구하였다.

본 연구에서는 기업조직의 전체의 정보보호 수준을 측정할 수 있도록 하기 위하여 기업 전반에 대한 정보보호 요인을 기획, 환경, 지원, 기술, 관리 수준으로 세분화하고 이를 기반으로한 지표체계를 연구하였다. 따라서 본 연구의 결과는 기업의 조직 관점에서 정보보호수준을 종합적이고 체계적으로 평가하는 것이 가능하다.

〈표 1〉 정보보호산업 기술 분류

기술 분야	관련 기술	활용 분야
암호화 기술	비밀키 암호 알고리듬	데이터 보호, 전자우편 보호, 디지털 서명
	공개키 암호 알고리듬	전자상거래, CALS 등의 정보보호, 사용자 인증
	암호화 프로토콜	전자상거래, CALS, 전자투표 등
인증 기술	전자지불	전자상거래, 전자화폐
	디지털 서명 및 인증	전자상거래, EDI 등 전자문서의 내용 인증
응용 기술	정보보호시스템 평가기술	정보보호시스템 기능 및 신뢰성 평가
	침해사고 대응기술	해킹 예방 및 대응

2. 관련연구

정보산업은 정보인프라 구축, 정보제공, 정보가공, 정보응용 산업에 걸쳐 다양하게 적용되는 산업이며 이런 관점에서 총체적인 시각이 요구된다. 또한 정보보안산업은 그 특성상, 기술적 분류가 중요하다. 정보보호산업의 기술은 <표 1>과 같이 크게 암호화 기술, 인증 기술, 응용 기술로 분류되어질 수 있다.

정보화의 빠른 진행은 정보시스템의 안전·신뢰성 확보 등 정보보호의 중요성이 부각시켰고 이와 관련된 정보보호제품에 대한 수요도 점차적으로 증가하고 있다.

정보보호산업의 성장구도는 보안인프라(infrastructure security), 위협관리(threat management), 취약성관리(vulnerability management), 그리고 정보위험관리(information risk management)의 단계를 거쳐 발전하고 있다.

- 보안인프라

접근제어 기능을 갖춘 방화벽, 사용자의 신분을 확인하는 인증, 통신상의 데이터 보호를 위한 VPN 제품, 바이러스 치료를 목적으로 하는 백신 프로그램 등이 초기 정보보안시장 육성에서 중요한 역할을 수행했다.

- 위협관리

보안 인프라가 구축된 후 정보보호산업은 시스템의 내/외부 침입을 확인하기 위한 침입탐지, 실시간 경보, 데이터 및 시스템의 복구를 위한 재난복구 기능을 탑재한 제품군이 주도하였다.

- 취약성관리

취약성 분석 단계에서는 위협분석은 물론, 위협요인에 대한 대안분석, 정책 수립 등의 다소 상위관점의 작업이 진행되었으며 이때 부터 보안시장이 급격하게 증가하였다.

- 정보위험관리

정보위험 관리 단계는 정보보호산업의 다음 발전 모델이라 할 수 있으며 단순한 제품군, 혹은 그 결합이 아니라 하나의 산업으로서의 형태를 모두 갖추게 되는 단계라 할 수 있다. 이 단계에서는 보안 컨설팅, 보안 정보전략 수립, 보안 정책 수립, 보안 강화를 위한 업무 프로세스 개선 등의 작업이 이루어지게 된다.

또한 정보보호 평가 측면에서 기존 연구의 내용들은 크게 두 가지 접근방법에 의해 구분된다[7-9]. 첫 번째는 TCSEC, ITSEC, CC 등과 같이 제품이나 시스템의 보안 기능과 성능 측면을 중심으로 하는 평가 체계이다. 이러한 기존의 평가기준이 주로 제품별 평가기준을 사용함으로 인하여 민간분야에서 요구하는 다양한 제품을 평가할 수 없어 융통성 면에서 제약을 받고 있다. 두 번째는 BS7799과 같이 관리적 측면을 중심으로 한 평가 체계이다.

본 연구는 이 두 가지 측면의 연구와 모두 관련이 되어 있어 각 방법의 특징과 장단점에 대해 살펴본다.

2.1 TCSEC(Trusted Computer System Evaluation Criteria)

1983년 미국은 안전한 컴퓨터 시스템을 위한 평가 기준인 일명 "Orange Book"이라 불리는 TCSEC의 초안을 NCSC(National Computer Security Center)에서 제작하였고, 2년 뒤인 1985년에 미국방성 표준(DoD STD 5200.28)으로 채택되었다. TCSEC은 컴퓨터 시스템의 보안성을 효과적으로 평가하고 안정성 및 신뢰성이 입증된 컴퓨터 시스템을 각 기관에 보급을 목적으로 운영체계를 6등급(C1, C2, B1, B2, B3, A1)으로 분류하고 있다. TCSEC은 특히 보안요소 중 비밀성을 강조하고 있다. TCSEC의 특징을 살펴보면, 세계최초의 평가기준으로 여러 가지 자료가 많이 존재하고 여러 사례에 적용시킬 수 있는 해설서가 존재한다. 또한 시행착오를 거치면서 관련된 경험이 축적되어 있다. 그러나 기능성과 보증성의 구분이 없이 고정되어

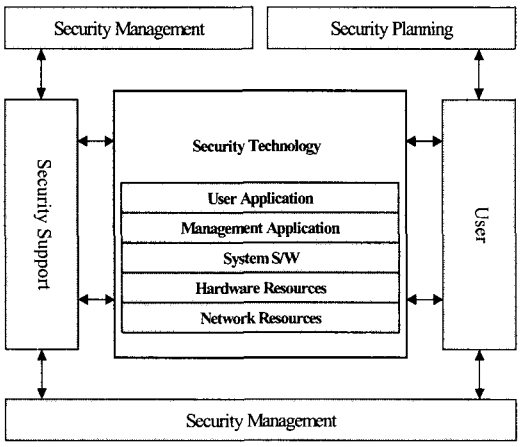
진 기준만을 사용하고 보안의 요소 중 기밀성만을 위주로 개정되어 가용성과 무결성을 중시하는 민간 기업에 적용하기 어려운 한계점을 가지고 있다.

2.2 ITSEC(Information Technology Security Criteria)

1991년 5월 프랑스, 독일, 영국, 네덜란드의 유럽 국가들은 각국의 보안성 표준을 조화롭게 통합 조정하여 IT시스템에 대한 공동 보안평가 기준인 ITSEC 초안을 발표하였다. 이들 국가들은 유럽국가 간 무역장벽을 피하고 기본적인 표준안과 시험에 관한 지침서로 활용하기 위해 ITSEC을 작성하였다. 그리고 다국적 개발과 이질적인 시스템인 경우 평가과정에서의 중복된 노력을 최소화하기 위해서 이기도 했다. ITSEC에서는 기본적으로 보안 기능에 의한 기준과 보증 요구사항에 의한 기준에 의해 구분되어진다. ITSEC은 세계최초의 국제 통합기준으로써 기능성과 보증성을 분리하고 있으며 기준을 일반적으로 정의하여 유동성을 유지하며 TCSEC의 내용을 대체로 포함하고 있다. 그러나 기준이 일반적으로 기술되어서 이해하기가 어렵고 보안수준에 의해서 세분화되어 있지 않아 평가 시 주관적인 견해가 포함될 수 있다는 한계점을 가지고 있다.

2.3 BS7799

BS7799[9, 10]는 BT, HSBC, Marks and Spencer, Shell International, Unilever 등 주요 업체와 더불어 영국의 상무성 주관으로 '정보보안관리 실무 규범(A Code of Practice for Information security management)'이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용되도록 개발되었으며, 조직의 보안 표준의 기반이 되도록 고안되었다. BS7799는 1995년에 처음 제정되어 1999년에 개정되었으며, 영국 이외에 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이, 핀란드, 인도 등에서 사용되고 있고, 1999년 10월에 ISO 표준으로 제안되어 ISO/IEC 17799-1이 되었다. 영국 정부에서는 전자정부를 향한 노력을 뒷받침하기 위하여 2001년 3월까지 대부분의 정보시스템에 대하여 BS7799 인증을 받도록 하여 국가 핵심 정보 기반구조를 보호하기 위한 수단으로 활용하고 있다. BS7799는 기업이 고객정보의 비밀성, 무결성 및 가용성을 보장한다는 것을 공개적으로 확인하는데 초점을 둔다. 또한 개발 배경은 기업들이 직면하고 있는 대부분의 상황에 필요한 통제를 식별하기 위한 단일한 참조점을 제공하고, 중소기업은 물론 대기업까지 광범위한 범위에 적용될 수 있도록 하여 공통적인 정보보안관리 문서를 참조함으로써 기업들 간의 네트워킹에 있어서 상호 신뢰가 가능하도록 한다. 물론 이 표준에서 제시하고 있는 통제들 모두가 모든 상황에 적용될 수 있는 것은 아니며, 개별적인 환경적 또는 기술적 제약조건을 고려하여 선택하여야 할 것이다. 따라서 BS7799 표준은 지침과 권고안의 성격을 갖는다. BS7799는 관리적 측면을 중심으로 한 평가 체계여서, 제품과 기능에 대한 정보보호에 대한 평가가 어렵다는 한계점을 가지고 있다.



(Figure 1) Information Security System on the organization viewpoint

3. 지표체계의 구성

2장에서 살펴본 바와 같이 기존의 평가 체계는 기업 전반에 대한 정보보호 수준을 종합적이고 효과적으로 파악하기에 어려움이 있다. 본 연구에서는 기업 전반의 정보보호 수준을 기업 조직의 전반적인 관점을 통해 평가할 수 있는 체계를 개발하였다.

(그림 1)은 조직의 전반적인 관점에서 나타낸 정보보호 지표체계이다. 이는 기업조직의 보안을 기획, 환경, 지원, 기술, 관리 수준의 다섯 가지 관점에서 정보보호의 전반적인 취약점을 분석하고 그에 따른 정보보호 수준을 평가한다. 각 지표 체계는 정보보호 기획수준 필수성공요인(CSFs)과 BS7799에서 사용되는 지표를 토대로 구성된다.

3.1 정보보호 기획 수준

정보보호 기획수준의 지표항목은 <표 2>와 같이 보안정책과 보안계획으로 구성된다. 보안 정책은 정보보호 정책과 관련된 일반사항들을 평가하게 된다. 정보보호 정책의 지표 항목은 정보보호 정책수립 여부와 정책의 검토 및 평가 그리고 정보보호 정책의 문서화 부분에 대해서 평가한다. 또한 CSFs의 정보보호 환경수준 필수성공요인 평가를 위한 항목을 포함하여 행동지침의 수립, 사고처리 절차의 수립, 예외규정명시여부, 정보 및 자산관리 여부와 정보보호 관련 인력의 서약서 작성여부, 정보보호정책의 준수 여부를 평가한다. 보안계획 지표 항목의 지표 또한 CSFs의 정보보호환경수준 필수성공요인 평가를 위한 항목을 포함하여 정보보호 계획과 정보보호 투자를 평가한다.

〈Table 2〉 Index System of Information Planning Level

Information security planning level	
Information security policy	Security plan
Establishing information security policy or not	Applied-technology development investment amount
Verifying information security policy	
Evaluating information security policy	
Reflecting the importance of information security	Basic-technology development investment amount
Stating information security	
Verifying, and evaluating information security policy documents	
Checking technological observance	Information security investment expense
Observing security policy	
Establishing action guide	
Establishing accident-settling procedure	Information security plan investment amount
Stating exceptions	
Managing information and assets	Drawing up a security plan
Drawing up the written oath of related manpower	
Observing information security policy	
Security policy documents	

〈Table 3〉 A Information Security Environment Level Index System

<table>
<tr><td colspan="3">Information security environment level</td></tr>
<tr><td rowspan="2">Equipment security</td><td colspan="2">Personnel security</td></tr>
<tr><td>Organizational security</td><td>Human security</td></tr>
<tr><td>Admission-ticket management</td><td>Operating an information security committee</td><td>Duty definition and resource allocation security</td></tr>
<tr><td>Automatic locking device</td><td rowspan="2">The existence of business alternation policy</td><td rowspan="2">Coping with security accidents and errors</td></tr>
<tr><td>Facilities security</td></tr>
<tr><td>Network management</td><td>Organization management</td><td rowspan="2">Personnel management</td></tr>
<tr><td>Equipment security</td><td rowspan="2">Oranizational security</td></tr>
<tr><td>Tangible assets</td><td rowspan="2">Human security</td></tr>
<tr><td>Intangible assets</td><td rowspan="2">Security organization</td></tr>
<tr><td>Material availability security</td><td rowspan="2">Licensor management</td></tr>
<tr><td>Equipment security</td><td>Selecting those in charge of equipment, and assigning responsibility</td></tr>
</table>

3.2 정보보호 환경 수준

정보보호 환경수준의 지표항목은 <표 3>과 같이 장비보안과 인사보안으로 구성된다. 장비보안은 장비통제, 시설물 보안과 같이 정보보호 시설물 및 기반 장비환경에 대한 사항을 평가하게 된다. 출입증 관리 자동잠금장치, 시설물보안, 네트워크 관리, 인터넷 접속사양, 정보보호시스템 등에 기반 환경 현황에 대해 평가한다.

인사보안은 조직적 보안과 인적보안으로 구성되며 조직적 보안에서는 조직 내에 장비담당자 선정 및 책임할당 등과 같이 세부적인 정보보호 절차의 준수여부를 평가하게 되고 인적보안에서는 보안사건 대응절차 및 취약성 리포트, 인가자 관리 등과 같은 개인위주의 정보보호 사항에 대해서 평가한다.

3.3 정보보호 지원수준

정보보호 지원수준의 지표항목은 <표 4>와 같이 지원조직과 지원활동으로 구성된다.

- 조직관리

조직관리에서는 개발 및 지원프로세스보안, 정보보호 담당자의 임명 및 역할, 보안관련 자격증 수준 등을 평가하게 되며 조직운영에서는 정보보호 활동의 통합/조정 등의 조직운영에 전반적 사항을 평가하며 아웃소싱에서는 아웃소싱의 비율 및 영역에 대해 평가하게 된다.

- 보안지원활동

보안지원활동은 비상대책, 정보보호교육/훈련으로 구성되며 비상대책에서는 비상대책의 유무와 비상시의 기업의 대처능력에 대하여 평가하게 된다.

- 정보보호 교육/훈련

정보보호 교육/훈련에서는 교육대상자의 선발방식과 정보보호 교육/훈련이 어떠한 범위 내에서 이루어지고 있는지를 평가하게 된다.

3.4 정보보호 기술수준

정보보호 기술수준의 지표항목은 <표 5>와 같이 접근제어 운영과 시스템 기능으로 나누어진다.

〈Table 4〉 Information Security Support Level Index System

Information security support level		
Support organization	Support activity	
Support activity	Emergency countermeasure	Education training
Development and support process security	Establishing a emergency-settling plan or not	Education operation
Plant/support equipment	Agreements against emergency	Education organization
Development and support process security	Obstacle restoration	Education content
Appointing those in charge of information security	Settling preservation accidents and errors	The selection Method of educatees
Stating the roles of those in charge of information security	Backup and restoration	The yearly mean number of education days
Unification/adjustment of information security activity	Settling preservation accidents and function obstacles	User education training
Security-related license level		Education/training
		User education/training

〈Table 5〉 Information Security Technology Index System

Information security technology level	
Access control operation	System function
Access authority control	Account and password management
Access control function	Applied-system security
N/W access control	Software security
Outsider access security	Authentication technique
Operation system access control	Obstacle restoration
User access management	Virus prevention
Application access control	Encryption function
Network access control	Key management
Physical access security	The backup management of important files
User approach management	
User responsibility	
Network access control	
Operation system access control	
Applied-system access control	
System access and use supervision	

〈Table 6〉 Information Security Management Level Index System

Index items	Indices	Indes items	Indices
Information security policies	Approval and announcement of policy	Access control	Cipher policy
			Cipher use
	The system of policy		Key management
	Maintenance and management of policy		Access control policy
	an organizational system		User access management
	Responsibility and roles		Access control scope
Outsider security	Contract and service level agreement security management	Operation management	Operation procedure and responsibility
	Outsider security practice management		System operation
			Network operation
			Media and document management
Human security	Establishing a education and training program		Virulent software control
			Establishing a business continuity management system
			Establishing and embodying a business continuity plan
			Planning, testing, maintaining and managing business continuity
	Enforcement and evaluation		Mobile computing and remote working
			Information-asset investigation and responsibility assignation
			Information-asset classification and treatment
	Responsibility assignation and stipulation	Transaction security	A written exchange agreement
	Managing a qualification test and those in charge of major duties		Electronic-transaction security management
	Secret-keeping		Electronic mail
Physical security	Physical security measures		The security management of open server
	Data-center security		User official announcement
	Equipment security	Security-accident management	Countermeasure plan and system
	Office security		Countermeasure and restoration
	Analysis and design security management		Post management
	Embodiment and performance security management		
	Change management		
verification monitoring, and inspection	Observing and verifying legal requirements		
	Observing and verifying information security policy		
	Monitoring		
	Security Inspection		

• 접근제어 운영 지표항목

접근제어 운영 지표항목은 전반적인 정보보호 기술수준의 전반적인 면을 평가하는 지표로 구성된다.

• 시스템기능수준 지표항목

시스템기능수준 지표항목은 전반적인 계정 관리 및 패스워드에 관한 일반사항들과 접근제어에 필요한 기능적인 측면을 평가하는 지표로 구성된다.

3.5 정보보호 관리 수준

정보보호 관리 수준의 지표 체계는 <표 6>과 같이 관리과정 요구사항 및 문서화 요구사항, 그리고 관리적 측면의 정보보호 관리통제의 지표 항목에 대해 BS7799를 바탕으로 재구성되어져 있다.

3.6 기존 방법론과 비교

<표 7>은 기존의 방법론과 본 연구를 통해 제안한 방법을 비교한 것이다. TCSEC는 정보보호 요소 중 기밀성 강조하고 있으며, 기업 조직에 적용하기가 곤란하다는 특성이 있다. ITSEC의 경우 단일 기준으로 모든 정보보호제품을 평가하고 있으며, 제품에 대한 평가는 보안 보증 부분으로 수행한다는 특성이 있다.

또한 이 두 가지는 평가 대상이 제품 및 시스템에 한정되어 있고 각 국가별 특성과 기능적 요인 강조하고 있다는 공통의 특성이 있다. BS7799의 경우는 관리체계의 인증이다. 따라서 시스템 기능에 대한 평가와 기업의 전반에 대한 평가 곤란하다는 특징이 있다. 이 세 가지 기존의 평가 체계는 각각 보완적인 활용이 가능하다.

본 연구를 통해 제안한 체계는 기존의 이러한 체계들의 보완 확장을 통해 평가의 각 요소를 5가지 영역으로 세분화하여 기업 조직 전반에 대한 정보보호 수준 평가가 가능하도록 하고 있다. 따라서 제안 체계는 기존 체계들을 통해 평가할 수 없었던 기업에 대한 정보보호 수준 평가가 가능하다.

4. 결론 및 향후 과제

본 연구에서는 기업 전반에 대한 정보보호 요인을 기획, 환경, 지원, 기술, 관리의 수준으로 구분하고 이를 기반으로 지표를 개발하여, 기업조직 전체의 정보보호 수준을 측정함으로서, 기업의 정보보호수준 위치 파악과 이를 통한 발전적인 정보보호방향을 제시하기 위한 정보보호수준 평가체계를 연구하였다.

본 연구에서는 기업조직의 전체의 정보보호 수준을 측정할 수 있도록 하기 위하여 기업 전반에

〈Table 7〉 Comparison of evaluation systems

	TCSEC	ITSEC	BS7799	The proposed method
Features	- Emphasizing secrecy, of information security elements. - Hard to apply to an enterprise organization - Limiting the object of evaluation to products and a system - Emphasizing each country's traits and functional elements	- Evaluating all information security products with a single criterion based - Performing evaluation of a product as a security guarantee part - Limiting the object of evaluation to products and a system - Emphasizing each country's traits and functional elements	- Authentication of a management system - No authentication of a product - Not enough to evaluate system function - Hard to evaluate the whole information security of an enterprise	- Possible to evaluate the information security level of the whole enterprise organization - Possible to evaluate a management system - Possible to evaluate products and a system - Subdividing each evaluation element into 5 levels

대한 정보보호 요인을 기획, 환경, 지원, 기술, 관리 수준으로 세분화하고 이를 기반으로 한 지표체계를 연구하였다. 따라서 본 연구의 결과는 기업의 조직 관점에서 정보보호수준을 종합적이고 체계적으로 평가하는 것이 가능하다.

참 고 문 헌

[1] PWC, secure, defend and transform : the complete e-business legal strategy, PWC, 1999.

[2] PWC, security basics : a whitepaper, PWC, 1999.

[3] Roseann Day, John Daly and Christian A. Christiansen eSecurity the essential eBusiness enabler, IDC, 1999.

[4] B. B Jenkins, security risk analysis and mand management strategies, European convention on security and detection, conference publication No. 408, 1998.

[5] Common Criteria Project, common criteria for information technology security evaluation, common criteria, 1998.

[6] B. Guptill, C. Price, a security framework for enterprise using the internet, Gartner Group, 1996.

[7] NIST, an introduction to computer security : the NIST handbook, NIST(national institute of standards and technology), 1995.

[8] Robin Moses, corporate risk analysis, 1995.

[9] Lynette Barnard et al., The evaluation and certification of information security against BS7799, Information Management & Computer Security 6/2, pp. 72-77, 1998.

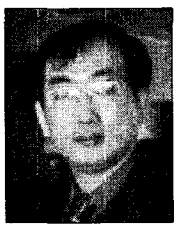
[10] Rossouw von solms, Information Security Management (3) : the code of practice for Information Security Management(BS7799), Information Management and Computer Security 6/5, management, countermeasures, Inc, pp. 224-225, 1998.

나 윤 지

경북대 생명공학과(공학사)
충북대 컴퓨터공학과(공학석사)
충북대 컴퓨터공학부(공학박사)
미) NYIT Communicaton Art 전공 석사과정 수료
현재 호남대학교 인터넷소프트웨어학과 전임강사

조 영 석

1978년 서강대학교 철학과 (문학사)
1988년 Louisiana State University(정보학 석사)
1994년 Louisiana State University(컴퓨터학 박사)
1980년~1984년 한국 후지쯔㈜ Systems Analyst
1989년~1994년 Louisiana State University, Computer Analyst
1999년~현재 동국대학교 컴퓨터·멀티미디어 학과 부교수
관심분야 : 소프트웨어 재사용, 소프트웨어개발 방법론, 실계패턴, 객체지향 방법론, information retrieval



고 일 석

경북대 컴퓨터공학 학사
경북대 컴퓨터공학 석사
USID(San Diego, USA) 경영학 석사(MBA)
연세대 컴퓨터산업시스템공학 박사
광주과학기술원(GIST) Post Doc.
현재 동국대학교 컴퓨터멀티미디어학과 조교수
현재 IBC(International Biographical Center) 부의장, Cambridge, UK.