韓國 컴퓨터情報學會 2008 제38차 하계학술발표논문집
第16卷 第1號, 2008. 06.

보안성 평가를 통한 정보시스템 위험관리 및 예산관리 연구

김 선 태*, 전 문 석*, 박 대 우**

A Study on the Security Assessment for Information System Risk Management and Budget Management

Sun-Tae Kim*, Moon-Seog Jun*, Dea-Woo Park**

요 약

정보보호를 효율적이고 효과적으로 실천하는 방법으로 정보자산을 기준으로 위험관리를 수행하는 GMITS(ISO 13335)과 정보보호 관리체계 수립을 위한 ISMS(ISO 27001), 정보보호 능력성숙도 모델을 제시하는 SSE-CMM 등의 국제 표준이 존재한다. 그러나 각 표준은 위험관리를 위한 절차를 제시하거나 관리체계 수립방안, 그리고 능력성숙 수준을 제시하는 등 관리, 기술, 운영의 종합적인 보안방안을 제시하지는 못하고 있다. 또한 현 보안문제를 최고 관리자 수준에서 판단할 수 있는 종합적인 방안을 제시하지 못하고 있다. 본 논문에서는 정보시스템 보안평가를 통해 보안 기술, 관리, 운영측면의 문제점을 종합하여 위험관리가 가능하도록 하는 방안을 제안하고, 또한 제안한 위험관리를 통해 도출된 문제점을 최고관리자 수준에서 직관적으로 판단 할 수 있는 방안을 제시하여 정보보호 예산과 연계할 수 있는 방법을 제안한다.

▸ Keyword : Risk Management, Security ROI, Security budget management, Risk Indicator, Risk Assessment

• 제1저자 : 김선태
* 숭실대학교 컴퓨터학과 ** 호서대학교 벤처전문대학원

Ⅰ. 서 론

정보기술의 발전은 사회의 패러다임을 산업사회, 지식정보사회로 발전시켜 가고 있다. 정보사회로의 발전에 따라 사회/경제활동의 편의성, 정보격차의 해소 등의 정보화의 순기능으로 인한 긍정적 효과가 있지만, 해킹과 바이러스 등로 대표되는 정보화의 역기능 또한 점차 진보하여 정보 위험사회(Risk Society)의 도래를 예측하고 있다.

정보 위험사회는 사회의 모든 비즈니스 활동이 IT환경과 기술에 대한 의존/결합도가 높아짐에 따라, 정보보안 사고가 사회적 혼란을 유발할 수 있을 정도로 피해규모가 확대될 수 있는 등 정보 침해로 인한 사회적 위험이 높아진 사회를 의미한다.[1] 정보 위험사회에서의 해킹 대상은 과거 서버, 네트워크, 개인 PC 등 단위 IT Infrastructure를 대상으로 하는 해킹에서 개인정보, 산업기술 정보, 내부 중요정보 등의 특정 정보를 해킹하는 것으로 대상이 변화하였다. 그리고 해킹 목적 또한 단순 자기 과시형의 공격에서 점차 금전적/상업적 목적을 추구하거나 이익집단의 목적을 달성하는 수단으로 활용하는 등 해킹 목적이 변화되었다[2].

이와 같은 정보 위험사회에서의 해킹 대응은 IT 인프라 중심이 아닌 IT 서비스 중심으로, 그리고 IT에 대한 기술적 보호가 아닌 관리/물리/기술/프로세스가 융합된 보호(Converged Security)가 필요하게 되었다.

최근까지도 위험평가에 대한 보안관리가 가장 효율적이고 효과적으로 정보보호를 실현하는 방법으로 받아들여지고 있다. 그러나 국제 표준으로 제시되는 ISO 13335의 위험평가 방법론은 위험평가에 대한 기본 개념과 수행절차를 제시하는 이론적 수준이기 때문에 실제 적용하기 어려운 면이 있다. 또한 정보보호 관리체계에 대한 국제 표준인 ISO 27001은 관리체계와 관리 프로세스 중심이어서 기술적 해킹사고를 예방하고 관리하기 위한 방법과 연계하기 어려운 특징이 있다. 또한 일반적으로 적용되는 정보시스템에 대한 취약점 분석/평가는 해당 시스템에 존재하여 해킹 사고에 직접적인 문제가 되는 기술적 취약점을 제거하고 관리하는 수준에 머무르고 있다.

본 논문에서는 위험관리 표준, 정보보호 관리체계 수립 표준, 정보보호 능력성숙도 평가모델 및 각종 정보보호와 관련된 보안성 평가 기준을 비교 분석한다. 그리고 정보시스템 측면에서의 보안성 평가를 통하여 정보시스템을 안전하게 보호할 수 있도록 하는 종합적인 정보시스템 위험관리 방안과 기술, 관리, 운영 측면에서 현 보안수준을 평가하여 정보보호 투자예산을 관리할 수 있는 방안을 제시하고 실험을 통해 전통적 위험관리와 비교하여 제안한 모델의 실효성을 검증한다.

Ⅱ. 보안성평가 관련 국제표준 및 사례 연구

보안성 평가와 관련된 국제표준은 정보자산(Asset)을 중심으로 위험을 평가하는 ISO/IEC 13335(GMITS)와 조직의 보안 관리체계 수립을 위한 ISO/IEC 270001(ISMS), 그리고 보안관련 능력성숙도 모델을 제시하는 ISO/IEC 21827(SSE-CMM)이 관련 국제 표준으로 등재되어 있다.

2.2 보안 위험평가(ISO 13335)

ISO/IEC 13335는 국제 표준기구인 ISO/IEC JTC1 SC27 WG1에서 작성된 표준 기술보고서로 IT 보안 관리를 위한 가이드라인(GMITS, Guidelines for the Management of IT Security)을 제시하는 표준이다. 보안 위험평가와 위험관리에 대한 프로세스와 구체적인 위험분석/평가 기법은 Part 2와 Part3에 정의되어 있으며, 기타 ISO/IEC 27001, ISO 2000(BS 15000, ITIL) 등의 표준에서는 이 기법과 프로세스를 따르는 것으로 권고되어 있다. 또한 2009년도에 정보보호 위험관리 표준인 27005로 등재될 예정이다.

보안 위험관리는 자산(Asset), 위협(Threat), 취약점(Vulnerability)간의 비례관계로 나타나며, 위험도는 " R = A*T*V " 표현한다. 위 표현식에서 정의한 비례관계는 각 조직의 위험관리 기준에 따라 상대적으로 변하는 것으로 정의하고 있다.

$$R=A*T*V$$

(R: Risk, A: Asset, T: Threat, V: Vulnerability)

위험관리 절차는 자산분석, 위협분석, 취약성 분석을 통해 도출된 위험평가 결과에 따라 잔여위험 평가를 수행 절차에 따라 위험을 관리한다.

자산분석: 자산분석은 정보시스템, 문서 등을 포함한 유형 자산과 가치가 있는 브랜드, 이미지 등의 무형자산을 포함한다. 자산분석 절차는 자산의 식별, 자산목록 작성, 중요도 평가기준 정의, 중요도 평가, 우선순위 분류의 단계를 통해 수행된다.

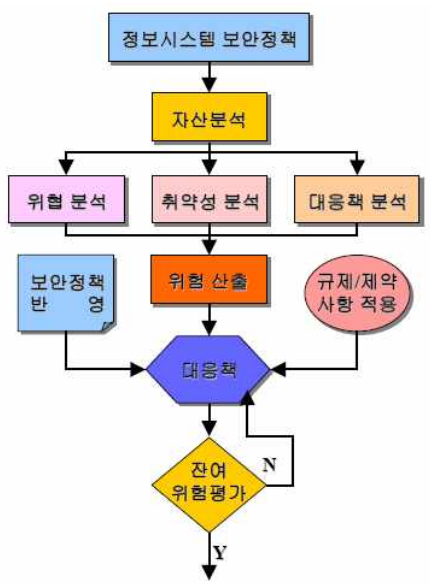
위협 분석: 위협분석은 자산에 손상이 가해질 수 있는 위

협의 빈도와 실제 위협이 발생할 경우 발생할 수 있는 피해영향의 비례에 따라 위협을 분석한다.

취약성 분석: 취약성 분석은 실제 정보자산에 해킹 등의 보안사고(Security Incident)가 발생할 수 있는 문제점을 분석하는 것으로 일반적으로 서버, 네트워크, Application에 대한 기술적 취약성을 분석한다.

위험평가: 자산, 위협, 취약성의 분석 및 평가 결과에 따라 도출된 위험지수(Risk Indicator)에 따라 위험지수를 낮추기 위한 보호대책의 적용여부를 평가한다. 위험평가를 통한 위험관리는 위험의 제거, 완화, 수용, 이전(전이)의 4가지 유형에 따라 관리한다.

잔여위험 평가: 위험평가 결과 도출된 위험을 제거, 완화, 수용, 이전한 결과 잔재한 위험이 수용 가능한 수준인지를 정의한 DoA(Degree of Assurance) 수준을 평가한다.



<그림 1> 위험관리 절차

2.2 보안 관리체계 수준평가(ISO 27001)

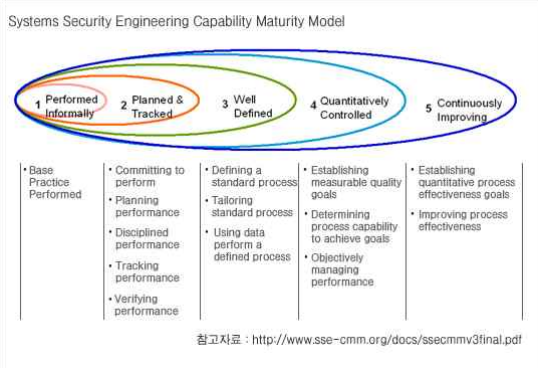
정보보호 관리체계에 대한 국제 표준은 ISO/IEC 27001로 등재된 ISMS(Information Security Management System)로, 보안 관리체계를 수립하기 위한 Code of Practice와 인증규격을 제시한다. ISO/IEC 17799는 정보보호 관리체계 수립을 위해 필요한 11가지 통제영역과 131개의 통제항목으로 구성되어 있다. 또한 정보보호 관리프로세스를 PDCA(Plan, Do, Check, Act) 사이클로 제시하여 체계적인 보안관리가 가능하도록 하는 실행 프로세스를 제시한다.

<표 1> 국가 정보보호 수준평가 지표

보안정책	정보보호에 대한 경영진의 방향성 및 지원을 제공함
보안 조직	조직 내에서 정보보호를 관리하는데 활용함
자산 관리	자산을 파악하고 이를 적절히 보호하는데 활용함
인원 보안	인적 오류, 절도, 사기, 시설의 오용에 따른 위험을 저감함
물리적 환경적 보안	사업장의 비 인가된 접근 및 방해요인을 예방함
통신 및 운영 관리	정보 처리 시설의 정확하고 안전한 운영을 보장함
접근 통제	정보에 대한 접근을 통제함
정보시스템 취득, 개발, 유지보수	정보시스템 내에 보안이 수립되어 있음을 보장함
보안 사고 관리	보안사고에 대한 대응 절차의 수립 및 이행을 보장함
사업 연속성 관리	비즈니스 활동에 대한 방해요인에 대응하며 중대한 실패 또는 재난으로부터 중요한 비즈니스프로세스를 보호하기 위함
준거성	각종 법령/규정 또는 계약 의무 및 보안 요구사항에 대한 위반을 피하기 위함

2.3 보안 능력성숙도 평가(SSE-CMM/ISO 21827)

SSE-CMM은 SE(Systems Engineering)-CMM을 기본으로 하여 시스템보안공학(Systems Security Engineering) 관점에서 보안 능력 수준 즉 성숙도를 평가하기 위한 모델이다. SSE-CMM은 보안 효과성과 보안 보증 요구사항을 충족할 수 있도록 하기 위하여 5단계의 능력수준을 단계로 제시한다. 1단계는 Performed informally로 비정형화된 프로세스의 수행단계이고, 2단계(Planed and Tracked)는 정의된 절차에 의해 보안이 수행되고 이를 보증할 수 있는 보안 프로세스가 계획되고 관리되는 수준이다. 3단계(Well Defined)는 계획 및 점검 확인의 수행이 조직 전체의 표준 프로세스에 근거하여 계획과 관리가 수행되는 수준이다. 4단계(Quantitatively Control)은 수행에 대한 세부적인 측정이 수집되고 분석됨으로써 프로세스 수행 능력에 대한 정량적 이해가 가능하고 개선 가능성에 대한 예견이 가능한 수준이다. 마지막 5단계(Continuously Improving)는 정의된 프로세스의 수행과 창의적인 아이디어와 기술의 실험이 수행에 의한 정량적인 피드백에 의해 지속적이 프로세스의 개선이 이루어지는 수준이다.



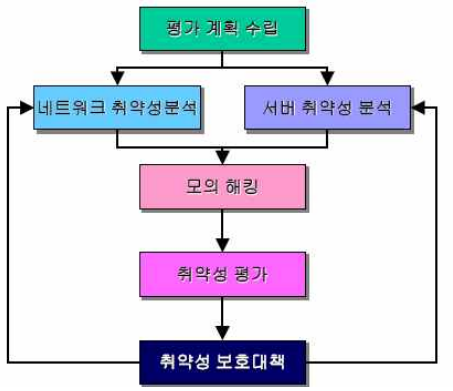
<그림 2> SSE-CMM 5단계 능력 성숙도 평가 모델

2.4 국내 취약점 분석/평가(정보통신기반보호법)

국가주요정보통신기반시설의 안전한 보호를 목적으로 국가의 중요 기반시설로 지정된 금융/통신/에너지 등의 국가 기반시설로 지정된 기관은 법령에 따라 취약점 분석/평가(법 제9조), 보호대책 수립(법 제5조), 침해사고 예방 및 대응(법 제13조, 14조)을 매년 의무적으로 매년 수행하도록 규정되어 있다

위험관리 절차 중 특히 해킹 등의 보안사고와 밀접한 관계를 갖는 취약점 분석은 산업계에 가장 일반적으로 적용되고 있다. 특히 국내의 경우 금융/통신/운성/에너지 등 국가 사회 기반시설의 안전한 보호를 목적으로 2001년 1월 제정된 정보통신기반보호법에 따라 취약점 분석평가를 수행하는 것이 일반화된 Best Practice로 자리 잡고 있다.

취약점 분석은 네트워크, 서버, Application 등의 정보통신 시설 즉 IT Infrastructure를 대상으로 해킹 사고의 직접적인 원인이 되는 취약점을 찾아내 분석 및 평가를 통해 발견된 취약점을 제거하는 절차로 수행한다.



<그림 3> 취약점 분석/평가 절차(정보통신기반보호법 기반)

2.5 국가 정보보호 수준 평가

국가정보보호 수준 평가지수에 대한 연구는 범 국가적 측면에서 정보보호 수준을 계량적으로 측정/분석함으로써 적절한 정책의 수립과 효과적인 정책추진을 목적으로 개발된 연구결과이다. 이 수준평가 기준은 아직 국가적으로 또는 세계적으로 합의된 것은 아니다.

국가정보보호 수준평가 연구결과는 국가의 정보보호 수준을 평가하기 위하여 국가의 구성요소인 개인, 정부, 기업의 3가지 관점에서 정보보호 수준과 정보화 역기능 수준을 구분하여 평가하였다. 그리고 정보보호 수준은 정보보호 기반과 정보보호 환경지수를 결합하여 국가 정보보호 수준을 평가하는 방식을 사용 한다.

<표 2> 국가 정보보호 수준평가 지표

구분	분류	세부지표
정보보호 수준지수	정보보호 기반	백신 보급률
		패치 보급률
		PKI 보급률
		Firewall 보급률
		IDS 보급률
		보안서버 보급률
	정보보호 환경	정보보호 관련 예산 비율
		정보보호 전문인력 비율
		보안의식 수준 비율
정보화 역기능 수준지수	정보화 역기능	해킹/바이러스 신고비율
		개인정보 침해 신고비율
		스팸메일 수신비율

2.6 기업 정보화 수준평가

기업 정보화 수준평가는 체계적인 정보화수준 평가방법을 적용하여 국내 기업의 전반적인 정보화수준을 파악하기 위하여 한국정보사회진흥원이 주관하고 한국신용평가정보(주)에서 수행한 결과이다.

기업 정보화 수준은 “기반구축, 업무정보화, 전사정보화, 협업정보화, 지식정보화“의 5단계로 구분되며 각 단계는 평가지수에 의한 평가결과를 20점 단위로 구분하여 평가하였다. 기업정보화 수준평가는 정보화 전략, 정보화 환경 등의 5대 영역과 11대 소영역의 지표로 구성된다.

<표 3> 기업 정보화 수준평가 영역 및 지표 계

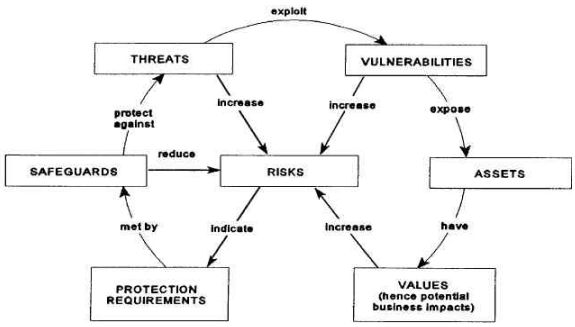
5대 영역	11대 소영역	지표번호
정보화 전략	정보화 계획	4
	정보화 투자	5,15
	경영진 마인드	11
정보화 환경	정보화 제도	6
	정보화 조직	16,17
	조직원 마인드	12
정보화 인프라	하드웨어	1,2
	네트워크	3,
정보시스템	정보시스템	7,8
정보화성과	정보시스템 활용효과	9,13
	정보화 효과	10,14

III. 관련연구 평가 모델의 성과 및 한계

3.1 보안 위험평가(ISO 13335)의 성과 및 한계

ISO 13335(GMITS)는 체계적인 위험관리를 위하여 자산(Asset)을 기반으로 위협, 취약점, 보호대책, 위험의 5개의 주요소와 보안요구사항, 자산의 가치의 2개 부요소를 포함한 총 7개의 요소로 구성하여 종합적인 관점에서 위험을 평가한 모델이다.

자산은 가치가 있는 모든 것을 의미하며 위험은 자산의 중요도에 비례한다. 즉 효과적인 위험관리 사이클은 자산 가치에 비례한 높은 위험에 대하여 요구되는 정보보안 대책을 적용함으로써 위협과 취약성을 감수할 수 있는 수준으로 낮추는 것을 말한다.

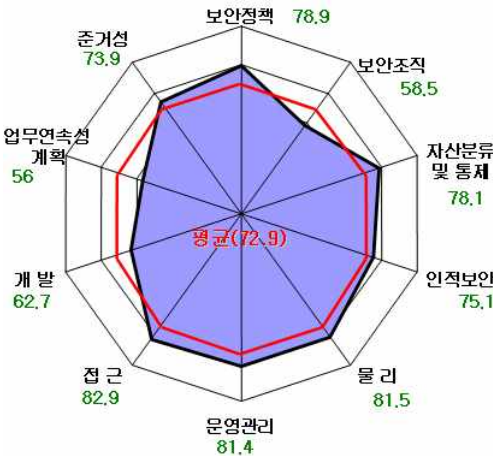


<그림 4> 위험관리 요소의 Life Cycle

ISO 13335의 가치는 위험관리를 위한 개념과 절차를 체계적으로 정립하였으며, 보안 위험관리에 대한 국제표준의 표준으로 적용될 만큼 위험관리의 기본으로 자리 잡았다. 그러나 위험관리에 대한 이론적 성숙에 비교하여 실제 업무에서 사용하기 어려운 한계를 가지고 있다.

3.2 보안 관리체계 수준평가(ISO 27001)의 성과 및 한

ISO 27001은 정보보호 관리와 관리체계 수립을 위한 11개 통제영역과 131개의 세부적인 통제항목을 제공함으로써 정보보호 관리에 대한 포괄적인 접근방법을 제공한다. 그러나 관리체계의 수립이 보안사고를 방지할 수 있는 수준으로 연계할 수 있는 기술적 보호대책이 부족하다. 아래 평가결과의 사례분석을 통해 운영관리, 접근, 개발 부분이 기술 분야에 관련된다. 하지만 실제 해킹, 웜/바이러스 등을 방어하기 위한 기술적 통제대책의 적용과 사고예방을 위한 대책 등과 관련된 부분은 제시되어 있지 않다.



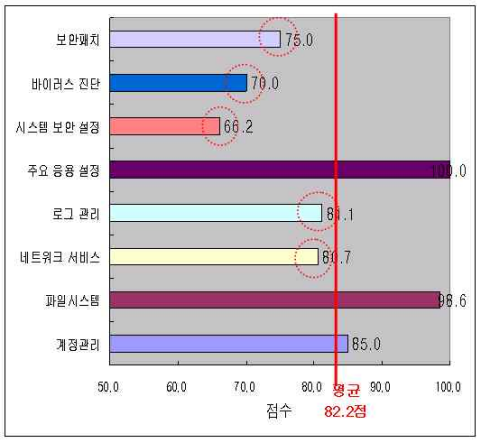
<그림 5> 보안 관리체계 수준평가 결과(사례)

3.3 보안 능력성숙도 평가(SSE-CMM/ISO 21827)

SSE-CMM은 시스템보안공학(Systems Security Engineering) 관점에서 보안 능력 수준 즉 성숙도를 평가하기 위한 모델로 그 의미가 있다. 그러나 프로세스 중심의 성숙도 평가모델은 해킹 등의 보안 사고에 대한 대응능력 수준과 이를 예방하기 위한 해킹공격에 대한 대응 수준을 평가하기에는 한계가 있다.

3.4 국내 취약점 분석/평가(정보통신기반보호법)

정보통신기반보호법 기반의 정보시스템 취약점 분석/평가 방법은 해킹, 웜/바이러스 등의 보안사고 발생의 직접적인 원인이 되는 취약점에 대한 보안수준을 평가하는 효율적인 지표이다. 그러나 보안 사고를 유발하는 취약점에 대한 평가를 통해 그에 대한 보호조치를 위한 방법에는 한계가 있다. 즉 문제점이 되는 취약점을 시스템 상에서 제거하는 방법을 제시하지만, 그것을 지속적으로 유지 관리할 수 있는 방안을 제시하지 못한다. 또한 그 정보시스템의 서비스 영향으로 취약점을 제거할 수 없는 경우 취약점의 인지 이외의 대처 방안을 제시하기 어려운 한계를 가지고 있다.



<그림 6> 정보시스템 취약점 분석/평가 결과

Ⅳ. 정보시스템 위험관리 및 예산관리 모델

정보시스템 위험관리 및 예산관리 모델을 수립하기 위하여 보안성 평가와 관련한 국제표준 및 선진사례에 대한 연구를 통해 각 각 모델의 성격와 한계를 분석하였다. 그 결과 ISO 13335(GMITS)는 잘 정의된 개념적 절차를 제시하지만 현실적인 보호대책과 연계할 수 있는 방안이 부족한 것을 발견하였다. 보안 관리체계와 관련한 ISO 27001(ISMS)는 보안관리를 위한 전체 프레임워크와 프로세스는 잘 정의되어 있지만 기술대책과의 연관성이 부족한 특징이 있다. 그리고 국내 정보통신기반보호법에 의한 정보시스템 취약성 분석/평가는 정보시스템의 운영과 관리부분을 포괄적으로 포함하지 못한 특징이 있는 것을 분석하였다.

이에 본 논문에서 제시하고자 하는 정보시스템 위험관리 및 예산관리 모델은 각 표준 및 선진사례들이 갖는 장점을 중심으로 단점을 보완하는 모델을 제시한다.

정보시스템 위험관리는 정보시스템에 대한 종합적인 평가를 통하여 정보시스템을 보호할 수 있는 기술적, 관리적, 운영적 대책을 포함한 종합적인 대책을 제시할 수 있도록 모델을 설계하였다. 또한 정보시스템의 보호를 위한 예산의 투자관리를 위한 방안과 연계할 수 있도록 기술적 보안솔루션과 연계할 수 있는 연계 지표를 포함하여 제시하였다. 그리고 이와 같은 단위 정보시스템의 위험관리를 총합하여 전체 정보시스템의 보안수준을 제고하고 관리할 수 있는 방안까지 확장할 수 있도록 통계적 관리방안을 제시한다.

4.1 정보시스템 위험관리 모델

제안하는 정보시스템 위험관리 모델은 ISO 13335(GMITS)의 개념과 절차를 바탕으로, 실제 단위 정보시스템의 취약점 분석/평가 방법을 보완하는 모델이다. 이는 단위 정보시스템의 자산의 가치와 위협 가능성 및 피해의 정도를 포함하여 정보시스템의 보안 수준을 종합적으로 평가할 수 있는 모델이다. 또한 정보자산의 중요도에 따라 개별 시스템별로 위험지표(Risk Indicator)를 적용함으로써 해당 시스템을 보호하기 위한 노력과 투자 수준을 고려할 수 있도록 모델을 수립하였다.

본 정보시스템 위험평가 및 예산관리 모델에서 자산은 가치가 있는 모든 것을 의미하고, 위협은 자산에 위해가 될 수 있는 원천 즉 가능성 있는 모든 것을 의미한다. 취약성은 가능성 있는 위협이 현실화 되어 직접적인 피해를 유발할 수 있는 문제점을 의미한다. 위험은 어떤 위협이 취약성을 이용하여 자산을 공격하는 경우 손실을 초래할 수 있는 가능성을 의미한다. 위험은 손실의 발생 확률과 피해의 영향이 결합으로 나타낸다.

<표 4> 정보시스템 위험관리 모델

분류	기준	평가요소
Asset	수행업무의 중요도	수행업무의 중요도
		정보시스템 및 정보 중요도
	정보시스템 및 정보 중요도	정보 중요도
		정보시스템 의존도
		대외업무 연계 정도
Threat	위협가능성 및 피해정도	위협발생 가능성
		피해영향 정도
Vulnerability	IT Infrastructure	서버
		네트워크
		보안장비
		Application
		PC

4.2 정보시스템 위험관리 확장

정보시스템의 위험관리 모델은 단위 정보시스템에 대한 자산, 위협, 취약점을 평가하여 개별 시스템의 위험도에 따른 대책수립 방안을 제시한 모델이다. 이는 정보시스템의 운영적인 측면, 기술적인 측면 그리고 관리적인 측면에서의 문제점을 고려하지 않았기 때문에 종합적인 보안수준 관리에는 부족함이 있다. 따라서 정보시스템 위험관리 확장을 통해 운영, 기술, 관리적 요소를 보완한 확장 모델을 수립하였다.

이와 같이 확장된 모델을 통한 보안성 평가를 통하여 정보시스템의 보안 위험을 종합적으로 평가하여 관리할 수 있으며, 또한 정보시스템의 보호를 위하여 기술적인 측면을 포함하여, 운영과 관리적 측면을 고려한 종합적인 보안투자를 고려할 수 있도록 모델을 설계하였다. 즉 정보시스템의 보안 취약성을 제거하기 위한 기술적 대책과 관리, 운영상에서 발생할 수 있는 문제점을 보완하기 위한 보호대책을 같이 고려하여 종합적인 보안관련 투자를 결정할 수 있도록 하였다.

<표 5> 정보시스템 위험관리 모델의 확장

분류	기준	평가요소
Operation Risk	Operation	계정관리
		보안설정 관리(취약점)
	Operation Risk	보안성검토
		모니터링 및 로그분석
		백업 및 복구
Technical Risk	Confidential	식별/인증/허가
	Integrity	무결성/책임추적성
	Availability	가용성
	Access Control	접근통제
Management Risk	ISO/IEC 17799의 11개 도메인 또는 KISA ISMS 인증의 15개 도메인	보안정책
		보안조직
		위험관리
		사고관리
		준거성

4.3 정보시스템 위험평가 방식 및 예산관리 방안

정보시스템 위험평가 방식은 전통적인 위험관리 기법에 의한 자산, 위협, 취약점에 비례한 위험평가 방법을 사용하였다.

<표 1> 전략적 예산관리를 위한 위험평가 모델

구분	내역	평가 방식	적용방안
Traditional Risk Assessment	Asset	Questionnaire	Information System Risk Indicator (Narrow)
	Threat	Delpi	
	Vulnerability	V=∑(E,W)	
Strategic Risk Assessment for Budget Management	Operation Risk	OR=∑(A,T,V)	Budget Management (Broad)
	Technical Risk	TR=∑(A,T,V)	
	Management Risk	MR=∑(A,T,V)	

자산의 중요도 평가는 자산 가치 산정을 위해 작성한 설문을 바탕으로 해당 자산의 소유자들이 설문에 응답하는 방식을 사용하였다. 위협평가는 위협의 발생 가능성과 해당 위협이 발생할 경우 예상되는 피해의 규모 즉 영향을 Delpi 기법을 적용하여 평가하였다. 취약점은 취약 항목별 위험도를 가중치를 적용하여 취약점을 평가하였다.

위험지수는 위험평가를 위한 각 통제 준수 값(Gov)과 통제현황지수(CCI) 평가를 통해 수준을 평가하였다. 먼저 통제준수 값(Gov)은 각 통제항목에 대한 Yes, NO, N/A의 합을 구하고 전체 설문 응답인원수에서 해당사항 없음으로 답한 수를 제외한 값(NR(i))을 구한다.

① NR = 전체설문문항 - "N/A"
② Gov = YS(i) / NR(i)

통제현황지수(CCI)는 YS("Yes" Score) 즉 통제항목별 가중치를 모든 Yes 항목에 곱한 다음 그 결과를 더한 후 FW(Weighted Fraction of Relevancy) 즉 적합성지수 가중치별 검사항목(N(i)) 중 NA로 응답한 수를 뺀 나머지 항목(NR(i))과의 비율에 가중치를 곱한 값을 구한다. 그리고 AI(Adjusted Index) : 조정지수는 'AI = 1 / FW'로 구한 후 이를 조정지수 값(AS, Adjusted Score)로 환상한다. 이를 통해서 최대 가능 값이 MPS(Maximum Possible Score)를 구한 후 통제현황지수 CCI(Control Comprehensiveness Indicator)를 평가하는 방법으로 위험지수를 평가한다.

1) "Yes" Score를 계산: 검사항목의 중요도에 따라 가중치(VH : 0.9, H:0.7, M:0.5, L:0.3, VL:0.1)를 모든 "Yes" 항목에 곱한 다음 그 결과를 더한다.

2) 적합성 지수(Weighted Fraction of Relevancy : FW)계산: 가중치별 검사항목(N(i)) 중 검사 대상 시스템에 적합하지 않다고 응답 한 질문(Not Applicable : N/A)의 수를 뺀 나머지 항목(NR(i))과의 비율에 가중치를 곱한 값인 적합성 지수(FW)를 계산한다.

$$FW = \frac{\frac{NR(VH)}{N(VH)} \times 0.9 + \frac{NR(H)}{N(H)} \times 0.7 + \frac{NR(M)}{N(M)} \times 0.5 + \frac{NR(L)}{N(L)} \times 0.3 + \frac{NR(VL)}{N(VL)} \times 0.1}{0.9 + 0.7 + 0.5 + 0.3 + 0.1}$$

3) 조정 지수(Adjusting Index : AI)를 계산: FW 값의 역수를 계산함으로써 AI를 계산한다.

$$AI = 1 / FW)$$

4) 조정된 "Yes" 값(Adjusted Score : AS) 계산

$$AS = YS * AI$$

5) 최대 가능값(Maximum Possible Score : MPS)를 계산: 모든 질문에 "Yes"를 하였을 경우 얻어지는 값인 최대 가능값(MPS)을 계산한다.

$$MPS = N(VH)*0.9 + N(H)*0.7 + N(M)*0.5 + N(L)*0.3 + (VL)*0.1$$

6) 통제 현황 지수(CCI)를 계산한다.

$$CCI = AS / MPS$$

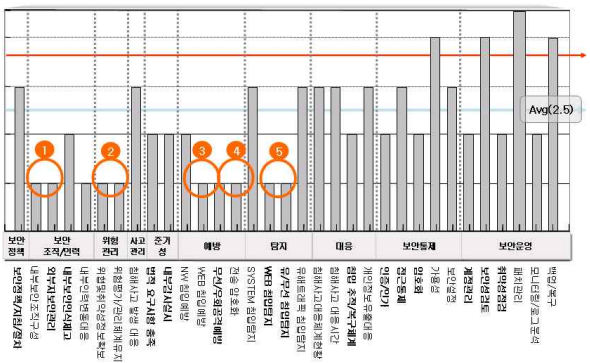
위의 CCI 계산 절차를 각 부문별로 계산하여 부문별 취약점을 평가하거나 전체 조직의 CCI 결과를 계산하여 조직의 기본 통제에 대한 보안성을 평가한다.

V. 실험결과 및 예산관리 방안

본 위험관리 모델에서는 기존 전통적인 방법의 위험관리에서 전략적 사고를 통하여 단위 시스템에 대한 종합적인 위험관리를 가능하도록 하기 위한 모델이다. 또한 개별 정보시스템의 위험관리 결과를 위험지표(Risk Indicator)로 확장하여 정보보호를 위한 전략적인 보안 투자를 가능하게 함으로써 종합적인 정보보호를 가능할 수 있도록 한다.

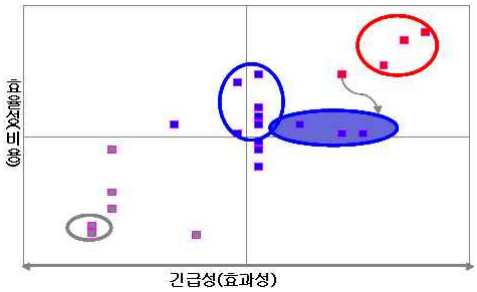
전략적인 위험관리는 기존 방법론에서 적용한 위험평가를 통계적으로 분석하여 직관적인 수준을 파악하고, 문제점을 식별함으로써 전략적인 투자의 필요성을 인지할 수 있도록 위험평가 결과를 그래프로 표현하는 방법으로 실험결과를 도출하였다.

위험평가 결과 단위 시스템의 취약점 외에 관리적인 영역, 침해사고 대응과 관련된 예방/탐지/대응의 영역, 기술적 보호대책을 표현하는 보안통제 영역, 그리고 보안 운영측면에서 필요한 보안활동을 프로세스화하여 구성한 보안운영 영역에 대한 수준을 평가하였다.



<그림 7> 위험평가 결과

보안 투자시기와 관련한 긴급성(효과성) 측면과 비용을 포함한 효율성 측면에서 네 가지 범주로 분류한다. 상위 관리자난 경영자는 이 전략 그리드(grid) 도표에 의해 효과성과 효율성 측면에서 보안개선을 위한 투자과제에 대한 개략적인 가이드 라인을 얻을 수 있다.



이와 같은 재무관리에 대한 접근 개념은 재무관리에 대한 선진사례(Best Practice)로 ITIL의 Service Delivery 영역의 IT 재무관리(Financial Management)를 참조하였다. IT 재무관리는 IT 서비스를 제공하기 위해 필요한 각종 자원이 비용 대비 효과적으로 관리될 수 있도록 하기 위해, IT 서비스에 소요되는 원가의 분석을 통하여 투자 의사결정을 지원하는 것을 목적으로 한다. IT 재무관리의 서브 프로세스는 조직의 예산 사용에 대한 계획수립과 실행의 통제를 담당하는 Budgeting 프로세스와 IT 서비스 부문에 사용된 모든 비용을 집계하는 IT Accounting 프로세스, 그리고 IT 서비스를 공급 받은 고객에게 그 대가를 청구하는 Charging 프로세스로 구성된다. 또한 정보화 투자시의 기대할 수 있는 효과는 비용절감, 생산성 향상, 매출증대, 간접인력 절감, 직원 만족도 향상, 기업 이미지 제고, 고객만족 및 대응력 향상, 신규사업영역 창출, 기업 투명성 제고, 외부기업과의 협업 강화, 업무 효율화의 12가지 측면에서 분류하고 있으며, 투자시 의사결정 요인 투자시기의 적절성, 투자비용, 투자효과, 타기업의 정보화 성패사례, 중복투자 여부, 비정보화를 포함한 종합적인 투자 우선순위로 분석되었다.

참고문헌

[1] MR.C. Gonzalez, R.E. Woods, “Digital Image Processing”, Addison Wesley, pp.433-455, (1992)

[2] 박대우, 서정만. “Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구”.한국컴퓨터정보학회 논문지, 제12권 제2호, pp175-184, 2007. 5.

[3] D.H.Ballard, Computer Vision, Prentice-Hall, Inc., pp.76-79, 1991.

[4] 국가정보보호백서, 국가정보원/정보통신부, 2006.

[5] 정태명, 침해사고대응팀의 기능과 역할, 침해사고대응팀(CERT) 구축·운영 과정 교육(KISA), 2002.

[6] 윤승노, CERT 구축요소 및 제공서비스, 한국정보보호진흥원 대응협력팀, 2004.

[7] NIST, Computer Security Incident Handling Guide(NIST Special Publication 800-61), 2004.

[8] Moira J. West-Brown, Handbook for Computer Security Incident Response Teams(CSIRTs), CMU/ SEI, SEI-2003-HB-002, 2003