정보시스템 감리품질향상을 위한 보안감리평가에의 정량화모델 적용 연구

김 동 수* · 김 현 수**

Applying a Quantitative Model on Information System Security Audit Evaluation for Improving Auditing Quality

Dongsoo Kim* · Hyunsoo Kim**

Abstract

Many researchers have proved that information systems auditing is a very effective tool for improving information systems quality. However, information system auditing in Korea still includes many subjective judgements. This study deals with applying a quantitative model to improve information system auditing quality on security domain. First of all, we have looked at previous researches on information systems audit, especially on security audit. Based on this survey, we have come up with solutions to improve the evaluation efficiency on security audit. We have merged the security audit guidelines of NCA and KISA, and developed a quantified evaluation scheme. We have proved the validity of this model by interviews with experts and by case studies.

Keyword : Information System Audit, Security Audit Evaluation, Quantitative Model

논문접수일 : 2003년 8월 20일 논문게재확정일 : 2004년 3월 21일

* 국민대학 BIT 박사과정
** 국민대학 BIT 대학원 교수

1. 서 론

1.1 배경

정보화 수준의 향상과 국가 정보화 사업의 추진 확대로 정보시스템에 대한 의존도는 점점 심화되고 있으며, 정보시스템감리가 이러한 정보화 사업의 버팀목으로서 1987년부터 꾸준히 양적, 질적 성장을 이루고 있다. 정보화 사업에 대한 정보시스템 감리의 역할에 대해서 어떤 영향을 끼치고 있는가는 감리의 효과성에 관한 여러 연구를 통하여 밝혀진바 있다[한국전산원 1998; 한국전산원 2002].

한편, 정보화 사업이 성공적으로 구축하였다고 하더라도 소프트웨어의 미흡한 개발이나 컴퓨터 사고 등으로 인한 정보시스템의 안전성, 효율성, 효과성이 저하되고 있으며, 기업의 연속성에도 많은 영향을 미치게 되어 정보자산을 보호하기 위한 다양한 보안 분야에 대한 시도가 행해지고 있다. 그럼에도 불구하고 정보시스템 감리에서의 보안 분야는 기존의 소프트웨어 개발감리 영역중 시스템 아키텍쳐 분야의 일부분에서 연구되거나 감리점검항목을 도출하였을 뿐이다. 정보시스템 보안 기술의 급격한 발전에 비해 보안분야의 감리에 대해서는 연구가 부족하여 관련된 지침이 정비되지 않았으며, 감리인의 보안 분야에 대한 기술수준이 미흡한 상태이다. 이에 반해 보안 분야의 감리에 대한 관리기관인 한국전산원, 정보보호진흥원, 국가정보원의 보안기술연구 등에 대한 업무이해가 상충되고 있는 실정이다. 다양한 정보보호 사업 또는 시스템 통합사업 수행시 감리인이 세부점검사항을 통하여 객관적인 판단이 될 수 있는 기초자료가 제공되어야 하나 대부분의 관련 연구는 감리중점사항 및 세부 점검표를 개발하는데 그치고 있으며 연구된 점검표도 서로 상이하여 활용이 지극히 저조한 실정이다.

본 연구에서는 관련 기관의 점검표를 소프트웨어 개발 측면에서 통합하고 감리인이 점검표에 대하여 객관적으로 판단할 수 있도록 정량화 방안을 제시하고자 하며, 이 정량화 방안이 감리품질의 향상에 도움이 되는지를 파악하고자 한다.

1.2 문제제기

국내 정보시스템감리가 1987년 이래 시작된 이래 양적 성장과 질적 성장을 거듭하여 온 현시점에서도 정보시스템 감리는 감리 전문인의 개인적인 경험과 전문성에 의존하는 바가 크다고 할 수 있다. 그러나 현재 감리현장에서 적용하고 있는 감리지침이나 평가방안 등이 서술적으로 기술되어 프로젝트에 적용하여 판단하기 어려운 경우가 많아 감리인들이 적용하기가 어려운 실정이다. 감리의 자동화를 위한 연구에서 밝힌 벡터방법론이나, GQM(Goal-Question-Metric 이하 GQM)방법 등이 제시되고 있으나 현실적으로 적용이 어려운 형편이다.

특히 보안분야는 정보자산의 보호를 위하여 더욱 세분화되고 다양한 전문기술이 필요하여 보안 분야의 감리평가는 다른 분야에 비하여 상대적으로 깊은 전문적인 지식을 요구하고 있다. 그러나 현재 감리현장에서 적용하고 있는 보안감리지침이나 평가방안 등이 다수 존재하고 있으나 서로 상이하며 해외의 평가방안인 BS7799 등을 준용하는 경우가 많아 SI 구축 현장의 보안 감리에 적용하기가 어려운 형편이다. 보안 감리평가의 경우는 감리인들의 개인적으로 보유한 경험에 크게 의존하기 때문에 감리인마다 서로 다른 평가가 존재할 수 있을 뿐만 아니라 감리 평가시 개선권고사항의 도출시 보안 정책 등 일반적인 사항의 권고사항만 도출하여 감리 품질의 심각한 저하를 낳고 있다. 기

존 감리결과를 조사하여보면 평균도출건수가 1.35건에 불과하였으며, 도출된 내역을 보면 보편적인 개선사항만 제시하였을 뿐이다. 이는 감리의뢰자인 발주자 측으로부터도 신뢰성에 영향을 끼치고 있으며, 피감리기간인 사업용역기관에서도 감리인에 대한 불신감을 초래하게 된다.

최근 연구된 많은 연구들의 대부분이 감리품질속성을 밝히는 연구는 하였으나 감리자체에 대한 품질향상에 대한 연구는 다루지 못했다. 정보시스템 감리가 정보시스템 구축에 긍정적인 효과를 보인다는 것에는 이견은 없으나 정보시스템 감리품질속성에 어떤 영향을 주는지에 대한 연구는 다루지 못했다[정승렬 1998].

본 연구에서는 감리품질속성을 준거성, 효과성, 신뢰성, 효율성, 안정성 측면으로 나누고 이 속성에 영향을 미치는 요인으로서 보안감리평가에 대한 정량화 모델도입여부가 감리품질속성에 어떤 영향을 미치는 지를 고찰하여 감리품질향상에 긍정적인 영향을 끼치는 요인을 찾아낼 필요가 있다고 본다. 따라서 본 연구에서는 보안 감리평가에 국한하여 정량화 모델 도입을 함으로써 감리품질향상에 미치는 영향을 살펴보았다.

즉, 본 연구에서 제시하는 보안감리평가 정량화 모델을 실제 감리에 적용함으로써, 그 결과로 감리품질속성인 준거성, 효과성, 신뢰성, 효율성, 안전성 등에 어떤 영향을 미칠 것인지를 분석하기로 한다.

2. 관련 문헌연구

본 연구에서는 외국의 정보시스템 보안평가 사례의 검토와 한국전산원, 한국정보시스템 감리인협회, 정보보호인증센터 등에서 연구한 기존의 연구 결과를 포함하여 고찰하였다. 또한, 감리의 효과성에 관한 국내의 연구 결과를 고찰하고 문제점에 대한 개선방안을 도출하기로 한다.

2.1 보안평가에 대한 국내외 연구

<표 1>에서는 국내외에서 개발 및 적용중인 보안부문의 평가지침이나 모형을 정량화관점에서 개략적으로 요약하였다. 국외에서 개발, 적용중인 평가지침이나 모형에서는 평가영역으로서 보안정책, 데이터베이스보안 등이 다루어지고, 평가결과는 대체로 등급으로서 정량화되어 제시되는 모형이 주류를 이루고 있다. 반면에 국내의 평가지침은 평가영역 및 항목 등은 보다 세분화되어 있는 반면에 평가결과는 정량화되어 제시되지 않고 있다.

<표 1> 국내외 보안부문 평가지침 및 모형요약

구 분	평가영역	평가결과	정량화 여부
미국 평가지침 (TCSEC)	보안요구사항 5개영역	7개 등급	△
영국 평가지침	보안통제 6개 영역 보안목표 5개 영역	6개 등급	△
공통인증 기준 (C C)	보안기능 6개 영역	10개 등급 (보안등급) 6개 정확성	△
BS7799	보안기능 10개 영역		△
전산원	5개 영역	3단계 평가	X

범례) O : 정량화, △ : 미흡, X : 정량화 안됨

1) 외국의 지침

미국의 평가기준 지침서(TCSEC)에서는 보안정책 등 5가지의 보안요구사항을 7등급으로 표시하고 있으며, 영국의 평가기준은 강제규정인 보안

통제와 비강제규정인 보안목표로 나누며 평가 등급은 6등급으로 표시하고 있다[김소연, 2001; Peltier,2001].

이외에도 북미, 유럽 각국이 독자의 보안 평가 방법을 내놓아 상호간 인증의 문제가 크게 대두되어 공통인증기준이 나오게 되었다[김소연, 2001; Tipton, 2001; Tudor 2001].

한편, BS7799는 BT, HSBC, Unilever 등 주요업체와 더불어 영국의 상무성 주관으로 BSI(British Standard Institute)에서 개발한 보안관리 지침으로 조직의 정보보호관리시스템을 구현, 관리하는데에 요구되는 사항을 제공하며, 다양한 조직의 보안 표준 및 효과적인 보안관리에 작용되는 기준을 제시한 것으로 목적은 조직이 효과적인 보안 관리 체계를 수립, 수행, 감사하기 위한 종합적인 지침을 제공하고 조직 상호간의 신뢰성 있는 거래를 위한 기반을 제공하는 데 있으며, 다음과 같은 특성이 있다[김유진, 2000; 이완석 2002].

외국의 평가 사례는 공통인증기준인 CC(Common Criteria)로 통합된바 있으나 이는 보안 운영측면에서 다루고 있다. 또한, BS7799역시 영국에서 개발되어 지금은 ISO 표준까지 되었으며 국내에도 소개되어 정보보호에 대한 인증을 수행하고 있으나 정보보호 운영측면에서 강조되고 있다[이병욱외, 2002].

2) 보안감리평가에 대한 국내의 연구결과 현황

국내 정보시스템 감리는 대부분 공공기관의 정보화를 대상으로 하고 있으며 현재의 평가 기준이 되고 있는 것은 정통부 고시기준으로 1999년 12월에 발표한 것을 근간으로 삼고 있다[한국전산원, 1999].

한국정보보호진흥원의 정보보호관리체계 인증제도에서는 보안요구사항을 5단계의 관리과정 요구사항과 문서화요구사항 및 15개 분야의 48개 통제사항을 가진 통제요구사항으로 나누고 있다<표 2>. 개발에 관한 점검사항은 13개 항목에 46개 점검항목으로 기관의 정보자산에 대한 보호측면에서 다루어져 개발측면은 다소 미흡한 상태이다[한국정보보호진흥원, 2000; 정보통신부, 1999].

<표 2> 기관별 감리분야에 대한 비교

분야	KISA	KISAA	NCA
정보보호정책	O	O	△
정보보호조직	O	O	△
외부자보안	O	O	△
정보자산분류	O		△
교육및훈련	O		
인적보안	O	O	△
물리적보안	O	O	△
시스템개발보안	O	O	△
암호통제	O		
접근통제	O		△
운영관리	O	O	
전자거래보안	O		
보안사고관리	O		
검토,모니터링및감사	O		
업무연속성관리	O		
네트워크보안		O	△
서버보안		O	△
클라이언트보안		O	△
보안 계획			O
보안 분석			O
보안 설계			O
보안 구축			O

범례 : O ==> 반영, △ ==> 부분 반영

한국정보시스템감리인협회의 보안감리지침은 11개분야로 나누어지고 점검항목은134개 항목과 세부 점검항목은 299개로 구성되었다<표 3>. 개발에 관련된 항목은 응용시스템과 데이터 보안으로 36개 항목과 67개 지침으로 이루어져 개발보다는 정보시스템 운영측면에서 도출하였다[정보시스템감리인협회, 2002].

한국전산원의 보안감리지침은 보안계획, 분석,

설계 및 구현 등 4개 분야로 나누고 점검항목은 49개 항목과 세부 점검항목은 213개로 구분하였다. 전산원의 보안감리지침은 소프트웨어 개발에 대한 점검항목위주로 도출하였다[한국전산원, 1998].

<표 3> 기관별 심사점검표와 보안감리지침

KISA인증심사점검표		
분야	통제항목	점검항목
정보보호정책	5	7
정보보호조직	4	7
외부자보안	4	8
정보자산분류	4	7
교육및훈련	4	8
인적보안	5	16
물리적보안	12	29
시스템개발보안	13	46
암호통제	3	5
접근통제	14	24
운영관리	22	61
전자거래보안	5	19
보안사고관리	7	19
검토,모니터링및감사	11	30
업무연속성관리	7	18
KISAA 보안감리지침		
분야	점검항목	세부항목
보안정책및조직	9	16
인원보안	15	29
보안운영관리	23	47
준거성	12	13
업무연속성	6	11
응용시스템보안	31	60
데이터보안	5	7
네트워크보안	10	17
서버보안	13	39
클라이언트보안	3	25
물리적환경적보안	7	35
한국전산원 보안감리지침		
분야	점검항목	세부항목
보안계획	8	20
보안분석	4	16
보안설계	19	90
보안구축	17	87

3) 평가모형에 관한 국내외 연구결과에 대한 문제점

한국정보시스템 감리인협회의 보안 감리지침은 외국 표준 (BS7799, ISO17799 등)을 원용한 것은 바람직하나 실제 활용측면에서의 현실성이 다소 미흡한 상태이다. 점검표에서 제시한 중요도를 상중하로 구분한 것은 좋으나 각 점검항목의 긴급성이나 다음 단계로의 전개시 반드시 필수적으로 해결해야 하는 등의 구분이 필요하다. 시스템 운영적인 측면에서 접근하여 소프트웨어 시스템 개발을 정보시스템 획득 차원에서 다루고 있어 국내 개발 감리 대상인 정보시스템 개발에 대한 세부적인 점검이 다소 미약하다. 또한, 세부 점검항목을 토대로 한 점검항목의 평가나 점검항목을 토대로 한 전반적인 평가 기준이 없다.

정보보호진흥원의 정보보호관리체계 인증심사 점검표도 감리인 협회와 유사하게 BS7799로부터 원용하였으며, 정보시스템 운영측면의 인증에 초점이 모아져 있다.

한국전산원 보안감리지침의 경우는 소프트웨어 개발 위주로 초점을 맞추었으나 시스템 통합의 입장에서 소프트웨어 개발외적인 요소에 대한 평가부분이 취약한 상태이다.

따라서 국내의 세개의 감리 지침을 서로 통합하여 보완하여야 시스템 통합 측면의 보안 감리를 다룰 수 있다고 판단된다.

2.2 정보시스템 감리 효과성에 관한 연구

1) 연구 현황

정보시스템의 감리 효과성에 관한 연구는 일본의 연구조사 2건과 국내의 연구조사 4건을 대상으로 살펴보았다. 처음 두건은 일본의 연구조사이고 나머지 셋은 국내 연구조사 건이다.

1992년 일본 행정정보시스템연구소의 조사로 본 연구의 특징 중 하나는 시스템 감사 관련 속성을 8가지로 구분하여 이 구분된 8가지 속성 즉, 안전성, 신뢰성, 기밀성, 준거성, 채산성, 적시성, 생산성, 대응성 등에 대해 시스템 감사의

효과를 평가하였다. 전체적으로 신뢰성(33.3%)이 가장 높았고 안전성(29%), 채산성(12.9%)이 뒤를 이었다[정승렬, 1998].

1995년 일본 정보처리 개발 협회의 연구조사로 정보 시스템 감사로 가장 효과가 올라가는 속성은 적합성, 채산성, 생산성이고, 가장 효과가 기대되는 분야로서 휴먼에러 방지대책, 사고대책, 컴퓨터범죄 방지대책 등이다. 또한 개선된 분야로는 보안대책의 향상, 규칙, 수속 등의 준수, 문서류의 정비, 정보의 보호대책의 향상, 품질관리의 향상 등을 들 수 있다[정승렬, 1998].

1992년 한국전산원이 주관한 정보시스템 감사의 효과에 관한 연구는 시중은행 30개를 바탕으로 한 실증적 연구로 정보시스템 감사의 효과에 대한 연구이다. 연구의 결과 정보시스템의 대한 감사전담조직이 설치, 운영되는 경우가 그렇지 않은 경우에 비해 정보시스템의 신뢰성, 안전성, 능률성, 효과성의 수준에 있어 모두 높은 것으로 나타났다[한국전산원, 1992].

또 다른 연구로 1998년 한국전산원이 주관한 연구로 정보시스템 감리가 본래의 목적인 시스템 개발 위험의 감소, 시스템 효율성, 안전성, 효과성 및 경제성을 향상시키는데 크게 기여하고 있는 것으로 나타났다. 또한 정보시스템 감리와 관련된 속성을 안전성, 신뢰성, 효율성, 효과성, 준거성으로 구분하여 제시하였다[한국전산원, 1998].

1998년 시행된 정보시스템 감리의 효과성에 관한 연구로서 소프트웨어 개발프로세스 관점에서 본 감리의 인지된 효과성 분석에서는 프로세스관점에서 본 감리의 효과성은 정보시스템 그 자체보다 정보시스템이 만들어지는 과정에 초점을 두고 있으며, 생명주기의 각 단계에서 실시하는 감리가 개발과정에서 수행하는 여러 활동 및 산출물 향상에 영향을 미치는 지를 분석하고 있다. 감리의 효과성을 측정하기 위하여 정보시스템 감리의 효과성을 측정하기 위한 과학적인 측정치를 개발하여 제시하였다[정승렬, 1998].

2002년도에 행한 한국전산원의 정보시스템 감리효과에 관한 연구로 정보시스템 감리가 정보화 사업에 어떤 효과가 있는지를 고찰하였으며, 정보시스템 감리를 실시할 경우에 정보화 사업의 절차나 사업관리 수준을 제고하고 정보시스템의 질을 높이는지 검증하기 위한 항목을 도출하고 실증적 연구를 수행한 결과를 제시하였다[한국전산원, 2002].

2) 감리효과성에 대한 관련 연구의 문제점

1992년의 일본연구에서는 8가지 시스템 감사 관련 속성(안전성, 신뢰성, 기밀성, 준거성, 채산성, 적시성, 생산성, 대응성)별로 조사하였고, 1995년의 일본연구에서도 적합성, 채산성, 생산성 등을 기반으로 조사하였다. 1992년이나 1995년의 한국전산원 자료에서도 정보시스템 감리의 속성에 기초한 효과를 조사하였다. 결국 감리의 효과를 감리 목적을 중심으로 살펴보게 되는 하향식 위주의 분석이 되었고 따라서 산출물 즉, 프로덕트 중심의 효과 분석만이 이루어지게 되는 결과를 낳았다. 위의 연구들은 감리를 실시한 기업이나 관공서를 대상으로 하여 감리 속성에 대한 성취도만을 파악하였으며 감리 프로젝트와 비감리 프로젝트 간의 비교를 통한 효과분석이나 감리 전 기대효과와 감리 후 실제 체감효과와의 비교 분석 등은 시도되지 못하였다[정승렬 1998].

감리의 효과성에 관한 연구에서 제시한 바와 같이 감리가 소프트웨어 개발이나 프로세스 관점에서 효과성을 검증하는 데는 연구의 관점이 모아졌으나 감리자체 품질에 대한 연구는 아주 미흡한 실정이다. 본 연구에서는 정량화 모델이 감리품질속성에 미치는 영향을 파악하였다.

2.3 감리자동화 및 평가방안에 관한 연구

1) 연구 현황

감리자동화에 관한 연구는 1986년부터 "시스템 감사사"제도를 도입한 일본의 경우 컴퓨터를 이용한 감사기법을 초기부터 적용하고 있으며, 국내에서는 정보시스템 감리가 개발감리 중심으로 도입되었고 감리도구는 일부 감리업무에 제한적으로 적용되어 왔다. 회계법인에서 외국의 감리도구를 도입하여 데이터 검사 등에 활용하고 있으나 정보시스템 개발감리에 대한 자동화도구는 통제 체크리스트에 의한 검토와 DB설계 검증 등에 부분적으로 사용하고 있는 실정이다. 정보시스템감리기준이 1999년 고시되어 감리시 검토해야 할 기본적인 감리 체크포인트가 제시되어 있으나 산출물이나 S/W, DB등을 검토하기 위한 감리 점검항목과 자동화도구 지원은 미흡한 실정이므로 자동화 도구의 시범적 개발과 적용이 필요한 시점이 도래하였다. 이를 통하여 감리의 객관성 확보, 여러 감리인의 감리 지식 공유 및 축적 등으로 감리 생산성을 증진하고 정보시스템 개발 프로젝트의 성공에 실질적으로 지원할 수 있을 것으로 기대된다[한국전산원, 2001].

정보시스템 감리 평가 체계가 가지는 단점인 주관적이며 정성적인 문제를 보완할 수 있는 방법으로 벡터 형식의 평가 기법이 제안되었다. 이러한 평가기법은 평가의 근거를 수치 즉 비율로 표시할 수 있는 장점이 있다. GQM 방법은 목표지향적 프로세스를 사용하는 평가방법으로, 측정하기 어려운 비정형적인 목표로부터 시작하여 목표를 만족하기 위해 필요한 활동을 문제로 구성하고, 각 문제들의 충족수준을 척도로 측정하는 방법이다. 이러한 GQM 개념을 좀더 확장하여 목표를 하위목표로 계속적으로 분할하여 최종적으로는 측정 가능한 수준으로 까지 전개하는 것을 목표 중심적 프로세스 방법이라고 한다. 이러한 전개에서 가장 중요한 것은 하위목표와 상위목표 간의 추적성을 유지하는 것이다[한국전산원, 2001].

2) 감리의 자동화 및 정량화 평가방안 연구에 대한 문제점

정량화 평가방안에서 제시된 벡터방식의 문제점은 감리항목이 사전에 표준화된 것이 있어 동일한 항목이 여러 감리에 적용가능 하다는 것을 가정하고 있고, 또한 감리항목의 개수가 동일하지 않은 경우 종합하기 어렵다는 점이 있다. 실제 감리의 경우 감리항목이 감리 목적이나 대상에 따라 달라지므로 표준화된 감리항목을 수립하는 것은 사실상 불가능하다. 따라서 이 방법은 계량적 평가결과를 제공하고자 하는 좋은 의도로 시작되었으나 현실적으로 사용하기에 매우 어려울 것으로 보인다[한국전산원, 2001].

GQM 방법의 단점은 확장하여 목표를 하위목표로 계속적으로 분할하여 최종적으로는 측정 가능한 수준으로 까지 전개하는 것이 상당히 어려운 작업으로 아직 현실성이 없는 작업으로 판단된다. 또한, 하위목표와 상위목표 간의 추적성을 유지하는 것이 매우 어려운 작업이다.

3. 실증연구의 설계

3.1 보안감리 평가의 정량화 모형의 개요

최근의 보안분야는 정보자산의 보호를 위하여 더욱 세분화되고 다양한 전문기술이 필요하여 보안 분야의 감리평가는 다른 분야에 비하여 상대적으로 깊은 전문적인 지식을 요구하고 있다. 그러나 현실적으로 정보시스템 보안감리평가는 보안감리를 담당하는 개인의 경험과 전문성에 의존하는 바가 크다고 할 수 있다. 현재

감리현장에서 적용하고 있는 각종 보안감리지침이나 보안감리평가방안 등이 서술적으로 기술되어 프로젝트에 적용하여 판단하기 어려운 경우가 많다. 이런 각종 지침들을 보안 감리평가를 담당하는 감리인들이 감리평가현장에서 적용하기가 어려운 실정으로 보안감리 정량화 모델의 필요성이 절실히 요청되고 있다.

또한, 감리인들이 보안감리평가시 감리인들의 개인적으로 보유한 경험에 의존하기 때문에 감리인마다 서로 다른 평가가 존재할 수 있을 뿐만 아니라 감리 평가시 개선권고사항의 도출시 일반적인 사항의 권고사항만 도출하여 감리 품질의 심각한 저하를 낳고 있다. 기존 감리결과를 조사하여보면 평균도출건수가 1.35건에 불과하였으며, 도출된 내역을 보면 보편적인 개선사항만 제시하였을 뿐이다. 이는 감리의뢰자인 발주자 측으로부터도 신뢰성에 영향을 끼치고 있으며, 피감리기관인 사업용역기관에서도 감리인에 대한 불신감을 초래하게 된다. 따라서 본 연구는 우선 보안감리평가에 대한 정량화 모델의 제시하여 감리평가의 품질향상에 기여하고자 하였다.

본 연구의 대상 범위는 시스템 통합 (SI) 에서 다루는 소프트웨어 개발 및 개발 환경(네트워크, 서버 등)에 국한하였다. 또한, 본 연구에서는 앞에서 고찰한 국내 사례의 감리점검표 또는 감리지침에 대한 연구결과를 바탕으로 시스템 통합 사업시 하나의 통합된 시각으로 접근하기 위한 통합된 감리세부지침을 제시한다. 감리평가의 일관성을 기하기 위하여 제시된 세부 감리지침에 의한 평가시 정량적인 평가모델을 도출한다.

도출된 정량화 모델이 감리 품질 속성에 어떤 영향을 끼치는지를 살펴본다.

3.2 보안감리평가의 정량화 모형의 설정

보안감리의 평가항목은 정보통신부에서 1999년 12월에 고시된 감리기준에 의거하여 1998년 발표된 전산원 보안 감리지침을 근간으로 감리인협회의 연구자료와 정보보호진흥원의 인증심사점검표[표2-4]를 참조하여 감리점검표를 보완하였다. 따라서 전산원 감리지침[표 2-4]에서 제시된 보안 계획, 보안 분석, 보안설계, 보안 구축의 분야를 그대로 수용하였으며, 전산원의 연구과제에서 제시된 소프트웨어 개발위주의 점검항목과 더불어 감리인협회에서 제시된 점검표를 병합하였다.

정보시스템감리인협회에서 제안된 테스트 데이터보호, 외주개발 등 전산원 지침에서 배제된 분야를 보안구축분야에 추가 시켰다. 또한, 각 점검항목에 대하여 보안의 기본적 요구사항인 신뢰성, 보안성, 가용성을 구분하여 본 감리점검표가 보안기본 요구사항에 충실함을 보여주도록 하였다.

보안 감리 평가시 감리인의 경험에 의해 평가결과가 상이하게 도출되는 것을 막고 평가에 대한 일관성을 기하기 위해서는 평가모형을 다음과 같이 제시하고자 한다.

1) 제안된 보안감리 지침은 통상적인 정보시스템 개발주기(System Development Life Cycle)를 고려하여 보안계획, 분석, 설계, 구현 등 4개 점검분야를 설정하고 점검항목 53개 항목과 세부 점검항목 235개로서 소프트웨어 개발위주로 도출하였다.

<표 4> 제안된 감리지침

분 야	점검항목	세부항목
보 안 계 획	8	20
보 안 분 석	4	16
보 안 설 계	20	101
보 안 구 축	21	98
합 계	53	235

한국정보시스템감리인협회의 감리지침은 운영위주의 지침으로 개발에 대한 세부지침이 다소 미약한 반면, 한국전산원의 세부지침은 적용하기에 타당한 것으로 판단되었다. 다만 보안 시스템을 구축하고 실제 사용자에게 인수될 때까지의 구현위주의 단계에서는 감리인협회의 점검사항이 비교적 우수하여 채용하였으며 그 결과 <표 4>와 같이 점검항목과 세부 점검항목이 다소 증가 하였다.

<표 5> 각 단계별 주요 점검항목

분야	주요점검항목
보안계획	프로젝트설명서 확인 보안조직 보안요구사항 정보자산의 파악 정보보호수준진단 정보보호대상업무선정 정보보호계획서 작성 프로젝트수행과정에 대한 보안대책
보안분석	관리적보안사항분석 물리적보안사항분석 정보보호대상업무에 대한 분석 자산분류도 작성
보안설계	보안대응책 및 정보보호모델도 정보보호모델도 평가 정보보호정책의 설계단계반영 보안조직구성 비상사태복구대책 교육 감사 출입통제 환경보안 장비에 대한 물리적보안 대응책확인 서버접근통제대책 서버 사용 및 운영에 대한 추적성 제거된 위험요소에 대한 대응방안 추가보안도구서버보안깅화설계 네트워크보안 운영방안 설계 외부망 보안 대책 민감한 정보 네트워크전송보호방안 클라이언트보호방안 응용시스템 접근시 사용자별/시스템별 접근통제적용 설계 암호화정책 데이터베이스인증 및 접근통제
보안구축	접근통제구현 정보보호체계통합설계 작성 및 구현 계획단계의 이행계획 재정립 확인 정보보호정책, 절차/지침 수정보완 보안사고 예방대책과 복구대책 물리적 보안 대응책의 구현 서버 보안구축시 고려할 보안사항 보안도구의 설치 확인 서버 보안 운영 방안 마련 네트워크보안 기능들의 반영 네트워크 보안 도구의 설치 네트워크 보안구현 및 보안장비통제 응용시스템 보안기능 반영 응용시스템의 운영 보안대책 위험분석도구의 위험분석결과 요소별 보안기능 검증 및 평가 사용자 점검서 작성 및 승인 데이터베이스로그관리 테스트데이터의 보호 소프트웨어 외주개발

<표 6> 기관별과 제안모델간 감리분야 비교

분 야	KISA	KISAA	NCA	제안
정보보호정책	O	O	△	△
정보보호조직	O	O	△	△
외부자보안	O	O	△	△
정보자산분류	O		△	△
교육및훈련	O		△	△
인적보안	O	O	△	△
물리적보안	O	O	△	△
시스템개발보안	O	O		O
암호통제	O			O
접근통제	O		△	O
운영관리	O	O		
전자거래보안	O			
보안사고관리	O			
검토,모니터링및 감사	O			
업무연속성관리	O			
네트워크보안		O	△	△
서버보안		O	△	△
클라이언트보안		O	△	△
보안 계획			O	O
보안 분석			O	O
보안 설계			O	O
보안 구축			O	O

범례 : O ==> 반영, △ ==> 부분 반영

2) 보안계획, 보안분석, 보안 설계, 보안 구현 단계의 주요점검항목은 <표 5>와 같이 정리할 수

있다. 더불어 기관별과 제안모델간 감리분야에 대하여 비교한 결과를 <표 6>에 나타내었다.

3) 전산원 지침에서 제시된 레벨 1,2,3에 대한 구성체계를 그대로 수용하되 이를 긴급도의 순위로 바꾸고 점수화하였다. 즉 레벨1의 경우 3점, 레벨 2의 경우 2점, 레벨 3의 경우 1점으로 가중치를 주었다.

4) 각 세부항목이 경우에 따라서는 적용 할 필요가 없는 경우도 있으므로 적용할 경우 1이라는 가중치를 부여하여 표준점수에 반영하였고, 적용하지 않을 경우 0이라는 가중치를 부여하여 표준점수에서 배제토록 하였다.

5) 감리인이 각 세부항목에 대하여 평가할 때 만족스럽거나 적정하다고 판단될 경우는 2점을, 실행은 하였지만 다소 미흡한 경우는 1점을, 아주 미흡하거나 실행하지 않은 경우는 0점을 부여토록 하였다.

6) 표준점수산정은 각 세부항목에 대하여 <표 7>과 같이 표준점수로 부여하고, 각 세부항목에 대한 평가 점수도 <표 7>과 같이 계산하여 부여한다.

<표 7> 점수 부여 방법

구 분	계산 방법
표준점수	긴급도(3, 2 또는1) * 적용(1 또는 0) * 적정평가(2)
평가점수	긴급도(3, 2, 또는 1) * 적용(1 또는 0) * 평가치 (2, 1, 또는 0)

7) 중규모 단위의 세부점검항목별로 평가점수를 합산하여 표준점수대비 평가점수 획득률을 계산하였다(<표 8>참조).

8) 획득률에 따라 50% 이하의 경우 긴급 개선을 70% 이하의 경우 통상 개선으로 판단토록 하였다.

9) 각 세부항목 평가를 한 후 중점 검토항목별로 병합 검토하여 긴급개선, 통상개선, 권고사항 등을 판단한다.

10) 전체항목에 대한 평가를 획득율과 개선항목의 긴급도에 따라 적정, 보통, 부적정으로 평가하였다.

<표 8> 감리지침의 평가표 예시

점검항목	세부항목	긴급구분	적용	표준평가	표준점수	감리평가	평가점수	획득률
응용시스템 접근을 위하여 사용자 별 과 시스템별 접근통제 적용 설계	패스워드 노출방지대비 시스템지원 방안	3	1	2	6	2	6	100
	동일ID로 한명이 상로그인시 보안대응	3	1	2	6	2	6	100
	일정시간 사용이 없을 경우, 일시 중지	3	1	2	6	1	3	50
	화일읽기, 쓰기, 삭제, 복사, 실행 등의 접근권한	3	1	2	6	0	0	0
	접근기록, 유지관리방안 설계	3	1	2	6	1	3	75
합 계					30		18	60

이를 실제 적용한 것을 <표 8>에 예시하였다. 표에서 보는 보와 같이 점검항목은 응용시스템 보안 반영이라는 중간항목에 대하여 5개의 세부항목으로 나누어지는 것을 알 수 있으며, 각 세부항목별로 긴급구분, 적용여부, 표준평가, 표준점수, 감리시 평가 수준, 평가점수, 그리고 획득률을 나타내고 있다. 본 예시자료에 따르면 5개 세부항목에 대하여 표준점수로는 30점을 나타내고 있으며, 획득점수는 18점으로 획득률은 60%를 나타내고 있다.

이 예시에서는 3번째 세부항목이 다소 미흡하여 1점으로 평가하였으며, 4번째 항목은 미비하여 0점 처리를 하였다.

결과적으로 개선 도출항목은 중간점검항목인 응용시스템 접근을 위하여 사용자별과 시스템별

접근통제적용 설계의 보완이 필요라는 것이 도출되고, 세부항목으로는 두개가 도출되어 한개는 다소 미흡으로, 한개는 미흡한 것으로 표시할 수 있겠다(<표 9> 참조).

기존 문헌조사에 의하면 평균도출건수가 1.35에 불과하였으며, 대부분 보안 정책이나, 대책 수립 및 사용자 접근 권한에 대한 부분에 치우침을 볼 수 있다(<표 10> 참조).

<표 9> 개선권고사항 도출 예시

개선권고사항	응용시스템 접근을 위하여 사용자별과 시스템별 접근통제적용 설계의 보완이 필요
문제점의 세부 내용	1) 응용시스템에 로그온 이후 일정 시간 동안 시스템의 사용이 없을 경우, 일시적으로 사용 중지 되며, 재 사용시 재 인증을 요구하는 기능이 응용시스템 설계에 반영하게 되어있으나 다소 미흡함.
	2) 사용자별로 응용시스템에서의 화일에 대한 읽기, 쓰기, 삭제, 복사, 실행 등의 접근권한에 대해서 기능별로 제한하는 방안이 설계에 반영하게 되어 있으나 되어 있지 않음.

<표 10> 기존문헌의 개선권고사항 도출 유형

개선권고사항 유형	건수
보안정책의 보완	42
사용자접근권한의 보완	12
침입탐지시스템의 보완	2
보안요구사항도출, 분석, 설계, 구현	6
시스템연동시 보안대책	3
전자상거래보안안전성, 신뢰성대책	1
개발자, 출입자보안대책	7
합 계	73

이상에서와 같이 본 연구에서 제시된 모형의 특징을 정리하면 다음과 같다.

첫째, 평가영역 및 평가항목 등을 3단계의 계층모형으로 한 평가체계를 구성하고 있다.

둘째, 평가영역은 시스템통합(SI) 프로젝트에서의 단계별 보안업무 프로세스를 수용하여 계획, 분석 설계, 구축 등을 고려함으로써 실무적인 적용성을 높였다.

셋째, 평가항목은 한국전산원의 보안감리 지침연구가 소프트웨어 측면의 계획, 분석, 설계, 구축에 초점을 맞추었기 때문에 시스템통합(SI) 사업의 보안 감리 평가에 비교적 적합하다고 판단되나 소프트웨어가 구동되는 환경이 배제되어 한국정보시스템 감리인협회의 보안 감리 지침과 한국정보보호 인증센터의 정보자산 평가 지침에서 환경에 해당되는 시스템 부문을 발췌하여 통합시켰다.

넷째, 감리보고서의 핵심이 문제점의 도출 및 개선 권고사항의 제시라고 볼 때 본 연구에서는 제시된 지침에 대하여 정량화 방안을 통하여 미흡한 세부 내역에 대하여 정량화를 제시함으로써 같은 업무에 대하여 평가하는 감리인서로 상이 하더라도 유사한 평가를 도출할 수 있는 방안을 제시하였다.

다섯째, 감리인이 정량화 모델을 적용을 통하여 구체화된 개선사항을 도출하여 신뢰성을 향상시켰다.

여섯째, 다른 연구들의 많은 좋은 제안들을 이론적으로 제시하였지만, 현실적으로 적용하는 데는 무리가 따르는데 비하여 본 모델은 적용이 매우 용이하다는 장점을 가지고 있다.

4. 연구결과

제시된 모형에 대한 타당성 검토를 위하여 관련 전문가인 보안감리인의 인터뷰를 실시하여 모델이 적용가능한지를 검토하였다. 또한, 본 평가모델의 개발목적이 감리현장에서 보안감리 평가에 대한 정량화를 통하여 감리의 객관성, 일관성 등 감리 품질제고에 있어 실제 프로젝트에서의 적용은 매우 중요하다고 할 수 있다.

사례 프로젝트의 적용을 통하여 본 모델의 타당성을 검증하였다.

4.1 전문가 인터뷰

4.1.1 전문가 인터뷰 개요

전문가 인터뷰 대상자는 정보시스템 감리 인증 보안 감리를 1회 이상 경험한자 15인을 대상으로 하였으며, 기술사, 한국전산원 인정 감리인, 한국정보시스템감리인협회 인정감리인 들로서 감리전문가라고 할 수 있다.

1차 인터뷰는 2003년 3월 3일부터 3월 22일까지 사이에 10명을 대상으로 실시하였으며, 2차 인터뷰는 6월 9일부터 6월 30일까지 5명을 추가하여 실시하였다. 인터뷰시 질문은 아래의 <표 12>와 같은 내용으로 인터뷰를 실시하였다. 인터뷰시 각 항목에 대하여서 많은 도움이 된다, 약간 도움이 된다, 도움이 안된다라는 답변을 유도 하였다.

질문전개방법은 보안감리평가표를 사전에 메일로 보낸 후 감리인 개개인별로 인터뷰를 실시하였다.

4.1.2 인터뷰 결과

보안감리전문가를 대상으로 구조적 면담을 실시한 결과는 다음과 같다.

첫째, 감리의 준거성에 대하여서는 감리인이 바뀌더라도 감리평가결과가 거의 유사하게 도출할 수 있을 것으로 판단되었다. 그 이유로는 53개 점검항목과 235개의 세분화된 감리지침을 제공함으로써 감리인의 주관적인 판단을 할 수 있는 부분을 최소화하였다. 또한, 각 세부지침마다 적정, 미흡, 부적정의 3단계 평가를 하게 되어 감리인이 평가시 애매모호한 판단을 할 수 있는 여지가 줄어들었다. 15인의 감리인중 준거성에 긍정적인 영향을 줄 것이라고 전원이 답변하였으며, 66.7%인 10명이 매우 긍정적인 도움을 줄 것으로 답변하였다. 나머지 33.3%인 5명도 약간의 도움을 줄 것으로 답변하여 본 정량화 모델을 통하여 준거성을 확보할 것이라는데 는 이견이 없었다. 감리경력별로 보면 3년 미만의 경우 2인 모두가 많은 도움을 줄 것으로 기대하고 있으며, 3년 이상 5년 미만의 경우도 5명중 4명이 매우 긍정적이라고 답변하였다. 다만, 감리인중 고경력자에 해당하는 5년 이상의 감리인들은 8명중 4명이 매우 긍정적이고 나머지 4명은 긍정적인 답변을 하였다.

<표 11> 감리경력별 감리품질 영향조사

	구 분	경력별			
		3년 미만	3년 이상	5년 이상	합계
준거성	많은 도움을 준다.	2	4	4	10
	약간 도움이 된다.	0	1	4	5
	도움이 안된다.	0	0	0	0
효과성	많은 도움을 준다.	0	0	0	0
	약간 도움이 된다.	2	5	5	12
	도움이 안 된다.	0	0	3	3
신뢰성	많은 도움을 준다.	2	5	4	11
	약간 도움이 된다.	0	0	4	4
	도움이 안 된다.	0	0	0	0
안전성	많은 도움을 준다.	2	5	5	12
	약간 도움이 된다.	0	0	3	3
	도움이 안 된다.	0	0	0	0
효율성	많은 도움을 준다.	2	4	3	9
	약간 도움이 된다.	0	1	5	6
	도움이 안 된다.	0	0	0	0

둘째, 감리의 효과성측면은 소프트웨어 개발과정중에서 기획업무의 타당성검토, 개발공정의 적합성검토 및 개발된 소프트웨어의 품질보

증 등에 대한 검토를 통하여 정보시스템의 효과를 증진시킬 수 있는 것이다. 이와 같은 측면에서 볼 때 감리의 효과성 향상은 정량화 모델을 통하여 획기적인 향상보다는 다소 향상된 것으로 나타났다. 즉, 정량화 모델이 아니더라도 감리를 통하여 어느 정도의 정보시스템의 효과를 얻을 수 있는 것으로 나타났으며, 정량화 모델을 도입함으로써 얻어질 수 있는 것은 간접적인 향상을 기대할 수 있겠다. 전문가들의 의견을 살펴보면 효과성측면은 매우 긍정적일 것이라는 답변을 한 사람은 없었으며, 약간 도움을 줄 것이다 라는 답변에는 3년 미만의 경력자의 경우는 약간 2명 모두가, 3년 이상 5년 미만의 경우는 5명 전원이 5년 이상의 경우는 8명중 5명이 약간 도움을 줄 것이라고 의견을 주어, 이 정량화모델을 도입하여도 약간의 도움은 받을 수 있지만 큰 도움은 기대할 수 없는 것으로 나타났다.

셋째로, 감리의 신뢰성 향상 측면에서는 넷째항인 안전성과도 연관있으며, 발주자와 개발자가 감리평가 결과에 대한 신뢰성도 살펴볼 수 있겠다.

보안감리평가의 정량화를 통한 발주자의 신뢰감 부여는 애매모호한 지적사항 위주로부터 점검항목의 어느 부분이 개선여지가 있는지 제시 되었으며, 특히, 각 항목에 대한 정량화로 획득률이 계산되어 평가에 대한 신뢰도를 높일 수 있음을 예상할 수 있고, 개발자에 대하여서는 세부 지침으로부터 개선권고사항의 정확한 도출과 정량화를 통한 평가의 수준을 가시화하여 감리결과에 대한 정확한 판단근거를 제시할 수 있음으로서 신뢰감을 높일 수 있을 것이라는 의견을 주었다.

전문가들의 의견은 신뢰성 향상에 큰 도움을 줄 수 있을 것이라는 의견에 3년 미만의 경력자의 경우 2명 전원이, 3년 이상 5년 미만의 경력자의 경우 5명 전원이, 5년 이상의 경우 8명중 4명이 답변을 하여 신뢰성 향상에 매우 높은 향상을 기대할 수 있음을 보여주고 있다. 약간 도움을 줄 것이라는 의견은 5년 이상의 경력자 8명중 4명이 약간 도움을 줄 것이라는 의견을 주었다.

넷째로, 감리의 안전성은 데이터의 무결성, 기밀성 및 가용성을 그 하부 속성으로 포함하고 있으며 특히 데이터 무결성은 정보시스템의 효과를 보장하는 가장 중요한 속성인 동시에 정보시스템감리가 보장하는 특성이라 하겠다. 이러한 데이터 무결성을 보장하기 위해서는 정보시스템의 분석, 설계도 중요하지만 운영상의 결함을 방지함으로써 데이터의 무결성을 확보할 수 있는 각종 통제의 시행이 필요하다. 이 부분에 대해서는 기존 감리의 관점에서 볼 때 중요한 요이나 감리인의 경력이나 전문성에 크게 의존하는 바가 커서 정보시스템 감리를 통해서 안전성을 확보한다는 것은 확정적이지 않다고 볼 수 있다. 본 연구에서 제시하는 정량화 모델을 통하여 점검상의 누락의 방지와 함께 구체적인 무결성확보를 위한 사항을 평가하게 함으로써 안전성 향상에 영향을 끼칠 수 있다는 것을 전문가들의 의견은 안전성 향상에 큰 도움을 줄 수 있을 것이라는 의견에 3년 미만의 경력자의 경우 2명 전원이, 3년 이상 5년 미만의 경력자의 경우 5명 전원이, 5년 이상의 경우 8명중 5명이 답변을 하여 정량화 모델이 안전성 향상에 매우 높은 향상을 기대할 수 있음을 보여주고 있다. 약간 도움을 줄 것이라는 의견은 5년 이상의 경력자 8명중 3명이 약간 도움을 줄 것이라는 의견을 주었다.

다섯째로, 감리의 효율성은 정보시스템의 개발 및 운영조직 가운데 문제점은 어디 있으며, 그리고 무엇을 우선적으로 개선해야 하는지를 제안, 권고함으로써 정보시스템의 효율성을 높

이는데 목적이 있는 것으로, 일반적인 정보시스템 감리가 지향하는 바가 효율성의 제고에 있다고 하겠다. 그러나 본 연구를 통하여 보다 정확한 개선 권고안을 명확히 제시함으로써 감리의 효율성을 높일 수 있다는 것에 인터뷰자 모두가 만장일치로 공감하였다.

전문가들의 의견은 효율성 향상에 큰 도움을 줄 수 있을 것이라는 의견에 3년 미만의 경력자의 경우 2명 전원이, 3년 이상 5년 미만의 경력자의 경우 4명 전원이, 5년 이상의 경우 8명중 3명이 답변을 하여 신뢰성 향상에 매우 높은 향상을 기대할 수 있음을 보여주고 있다. 약간 도움을 줄 것이라는 의견은 3년 이상 5년 미만의 경우 5명중 1명이 5년 이상의 경력자 8명중 5명이 약간 도움을 줄 것이라는 의견을 주었다.

4.1.3 전문가 인터뷰 시사점

전문가 인터뷰시 본 연구모형에 대하여 긍정적인 답변을 하였으나 다음과 같은 개선점이 도출되었다.

1) 평가 점수에 대한 가중치의 차별화 적용에 대한 검토가 필요하다. 또한, 중규모 단위의 점검항목간에도 가중치의 별도부여검토가 필요하다.

2) 대부분의 항목은 충분히 상세화 되었으나 일부 항목은 상세화가 필요하다.

3) 감리지침의 세부항목에 대한 평가 적용 여부를 사이트의 경. 중에 따라 융통성있게 적용하는 것이 필요하다.

4.2 사례 프로젝트 적용 결과

4.2.1 사례 개요

본 보안감리 정량화모델이 감리품질에 실제 감리프로젝트에서 어떤 영향을 나타내는가를 조사하였다. 사례 적용한 프로젝트는 다섯 개로서 2003년 3월부터 7월까지 사이에 감리를 시행한 프로젝트이다. 첫째 적용된 사례프로젝트의 개요는 서울의 A구청에서 기 운영중인 정보시스템들을 정보공동활용 및 시스템 활용성 제고 측면에서 연계 및 접근 창구를 단일화하여 구정 전반의 흐름행정을 구현하고, 인터넷 등의 다양한 대민 접촉 채널과 내부 행정 시스템을 유기적으로 연계한 서비스 제공으로 주민참여적 정보사회구현에 일조하며, MIS/GIS 통합기반의 서비스 체계 구축을 성공적으로 구현 정착시키기 위한 것이다.

둘째 프로젝트는 중앙정부의 지방 단위 정보화 프로젝트로 개요는 전국의 마을 중에서 시범 마을을 선정하여 정보화 마을을 구현하는 프로젝트로 중앙기관에서 중앙에서 포탈시스템을 운영하고 마을장터 등과 같은 전자상거래는 중앙에서 공동으로 처리하고 마을단위는 마을 고유의 홈페이지 등을 성공적으로 구현 정착시키기 위한 것이다.

셋째 적용된 사례프로젝트의 개요는 은행프로젝트로서 기존의 정보시스템을 통합하기위하여 정보공동활용 및 시스템 활용성 제고하여 통합기반의 정보화 체계 구축을 성공적으로 구현 정착시키기 위한 것이다.

넷째 적용된 사례프로젝트의 개요는 공사의 통합정보시스템 프로젝트로 역시 기존에서 운영중 정보시스템들을 정보공동활용 및 시스템 활용성을 높이고, 내부 업무 시스템을 유기적으로 연계한 서비스 제공으로 통합기반의 정보제공 체계 구축을 성공적으로 구현 정착시키기 위한 것이다.

다섯째 적용된 사례프로젝트의 개요는 지방광역시의 웹사이트 보강 프로젝트로 동북아시대의 관문역할을 하는 기관으로써 다양한 검색

및 컨텐츠관리, 뉴스클리핑, 전자우편을 통합홍보시스템, 전자우편응답시스템 등 정보의 공동활용 및 시스템 활용성 제고 측면에서 연계 및 접근 창구를 단일화하여 시정 전반의 흐름행정을 구현하고, 인터넷 등의 다양한 대민 접촉 채널과 내부 행정 시스템을 유기적으로 연계한 서비스 체계 구축을 성공적으로 구현 정착시키기 위한 것이다.

본 사례프로젝트들에 공동 적용하기위한 목표로는 전문가 인터뷰시 사용하였던 질문항목과 동일한 내용으로 정하였으며, <표 16>과 같이 정리할 수 있다. 사례 프로젝트 적용시 참여감리인이 일부는 중복되었으나 새로운 감리인들이 투입되어 한 감리인은 정량화모델도입을 통한 감리와 기존 방법을 병행한 감리의 진행을 동시에 진행하였고, 다른 감리인인 정량화 모델 도입을 적용한 감리만 수행하여 비교하였다.

<표 12> 사례적용시 적용목표

적용 목표
1. 정량화 모델이 감리의 준거성향상에 도움을 주는가?
2. 정량화 모델이 감리의 효과성향상에 도움을 주는가?
3. 정량화 모델이 감리의 신뢰성향상에 도움을 주는가?
4. 정량화 모델이 감리의 안전성향상에 도움을 주는가?
5. 정량화 모델이 감리의 효율성 향상에 도움을 주는가?
6. 본 평가의 개선할 점은 무엇인가?

4.2.2 사례 적용 결과

첫째, 감리의 준거성에 대하여서는 정량화 모델을 이용하여 동시에 2인이 보안 감리에 적용하여 도출된 개선항목을 비교하여보니 거의 동일한 관점으로 평가가 되었다.

그 이유로는 53개 점검항목과 235개의 세분화된 감리지침을 통하여 감리인의 주관적인 판단을 할 수 있는 부분을 최소화하였고, 그에 따른 구체적인 개선항목도출이 가능하여 감리의 준거성 향상에 도움을 줄 수 있었다. 다섯 개의 프로젝트 공히 세부항목별점검을 통하여 개선권고사항 도출을 위한 명확한 근거제시가 되었다.

이는 <표 13>에서 보는 바와 같이 정량화 모형이 적용되지 않은 감리에서는 평균 1.70 건(표준편차 0.48)이 도출되었으며, 새로이 제시된 정량화 모형에 의해 실시된 감리에서는 평균 5.3건(표준편차 0.95)이 도출되었다. 이는 정량화 적용시 개선사항 도출건수가 비적용 시보다 많게 나타났으며, 적용 시나 비적용시 모두 두 감리인간의 도출 건수의 차이가 적게 나타났다.

둘째, 감리의 효과성측면은 정량화 모델을 통하여 획기적인 향상보다는 다소 향상된 것으로 나타났다. 즉, 정량화 모델이 아니더라도 감리를 통하여 어느 정도의 정보시스템의 효과를 얻을 수 있는 것으로 나타났으며, 정량화 모델을 도입함으로써 얻어질 수 있는 것은 간접적인 향상을 기대할 수 있겠다. 이는 다섯 개의 프로젝트 사례에서 공통된 현상이다.

셋째로, 감리의 효율성은 본 연구를 통하여 보다 정확한 개선 권고안을 명확히 제시함으로써 감리의 효율성을 높일 수 있다는 것을 프로젝트 적용결과 확인할 수 있었다. 즉, <표 14>를 참조하면 통상적으로 1.35개에 그치던 개선권고사항 도출건수가 5.3건으로 늘었을 뿐만 아니라 구체적으로 제시할 수 있어 감리의 효율성을 얻을 수 있었다. 이는 정량화 모델을 적용하는 A, C, D, E, F감리인의 경우 기존 방법대로 도출할 경우 대부분 2건 이하에 그치던 것이 정량화 모델 도입을 통하여 개선사항 도출건수의 향상이 늘었다. 이는 상세한 개선 사항

도출과도 직결된다고 본다.

<표 13> 정량화 모델 적용전후의 프로젝트별 감리인별 도출건수 현황 비교

구 분		도출 건수	
		미적용시	적용시
첫째 프로젝트	A감리인	1	5
	B감리인	2	5
둘째 프로젝트	C감리인	2	4
	B감리인	2	4
셋째 프로젝트	D감리인	1	6
	B감리인	2	7
넷째 프로젝트	E감리인	2	5
	B감리인	2	5
다섯째 프로젝트	F감리인	1	6
	B감리인	2	6
평균도출건수(mean)		1.70	5.3
최소도출건수(min)		1	4
최대도출건수(max)		2	7
표준편차(S. D)		0.48	0.95

<표 14> 기존 감리보고서 문헌조사와 정량화 모델적용여부에 따른 도출건수 현황 비교

구분	문헌 조사	미적용	적용
평균도출건수	1.35	1.70	5.3
최소도출건수	0	1	4
최대도출건수	4	2	7
표준편차	0.8	0.48	0.95

넷째로, 감리의 안전성은 데이터의 무결성, 기밀성 및 가용성을 그 하부 속성으로 포함하고 있으며 특히 데이터 무결성은 정보시스템의 효과를 보장하는 가장 중요한 속성인 동시에 정보시스템감리가 보장하는 특성이라 하겠다. 이러한 데이터 무결성을 보장하기 위해서는 정보시스템의 분석, 설계도 중요하지만 운영상의 결함을 방지함으로써 데이터의 무결성을 확보할 수 있는 각종 통제의 시행이 필요하다. 이 부분에 대해서는 기존 감리의 관점에서 볼 때 중요한 요인이나 감리인의 경력이나 전문성에 크게 의존하는 바가 커서 정보시스템 감리를 통해서 안전성을 확보한다는 것은 확정적이지 않다고 볼 수 있다. 본 연구에서 제시하는 정량화 모델을 통하여 점검상의 누락의 방지와 함께 구체적인 무결성확보를 위한 사항을 평가하게 함으로써 안전성 향상에 영향을 끼칠 수 있다는 것을 확인할 수 있었다.

다섯째, 발주자와 개발자가 감리평가에 대한 신뢰성도 살펴볼 수 있겠다. 보안감리평가의 정량화를 통한 발주자의 신뢰감 부여는 애매모호한 지적사항 위주로부터 점검항목의 어느 부분이 개선여지가 있는지 제시 되었으며, 특히, 각 항목에 대한 정량화로 획득률이 계산되어 평가에 대한 신뢰도를 높였다. 즉, 사업자의 PM과 Project Leader 들, 그리고 발주자인 공공기관의 담당자들과 인터뷰하여 감리평가 결과에 대한 신뢰감을 조사하였다. 조사결과 피평가자들에게 신뢰감을 줄 수 있음을 확인하였다.

<표 15> 보안 계획단계 개선권고사항 도출 현황

사례연구의 보안계획단계	보안조직 혹은 전담 담당자의 선임이 되어 있지 않음
	주관기관의 보안요구사항 도출이 되어 있지 않음
	정보화 대상 자산의 파악이 미흡함
	주관기관의 현 정보보호 수준의 진단이 미흡함
	정보보호 프로젝트 계획서의 내용이 미흡함
	프로젝트 기간 중의 정보보호 대책의 방안 마련이 미흡함
기존문헌	정보보호 정책이 미흡함.

보안계획 단계에서는 <표 15>를 보면 사례연구에서 도출된 감리 개선 사항을 열거하여 보면 건수의 차이는 다소 있으나 기존 감리결과에서

는 전반적인 표현의 지적사항을 도출하고 있으나 정량화 모델 적용시는 구체화된 지적 사항을 도출할 수 있었다.

<표 16> 보안 분석단계 개선권고사항 도출 현황

사례연구의 보안분석단계	주관기관의 관리적 보안 요구사항의 상세분석이 미흡함
	물리적 보안 사항에 대한 환경분석이 미흡함
	계획단계의 보호대상업무에 대한 상세분석이 미흡함.
	보호대상자원에 대한 자산분류도 작성이 미흡함.
기존문헌	일부 문서에서 보안분석 자료가 미흡함. 정도의 도출이 되었으며, 대부분 도출이 안되었음.

<표 17> 보안 설계단계 개선권고사항 도출 현황

사례연구의 보안설계단계	정보보호 모델도에 대한 작성과 종합적인 평가가 미흡함.
	정보보호정책이 설계 과정에서 준비되지 않았음.
	정보보호를 위한 향후 보안조직 구성 방안이 미흡함
	정보시스템의 비상사태, 자연재해에 대비한 사고예방대책이 미흡함.
	사용자 및 운영자들을 위한 보안 교육 방안이 마련이 미흡함.
	출입통제를 위한 보안 대응책이 미흡함.
	예상되는 위협환경에 대한 문서화 작업이 미흡함.
	서버 시스템 사용 및 운영에 대한 감사 추적성 확보가 미흡함.
	제거된 위협 요소에 대한 대응방안이 설계에 반영이 미흡함.
	네트워크 보안 운영에 대한 설계서 반영이 미흡함.
	사용자별과 시스템별로 접근통제를 위한 설계서 반영이 미흡함.
기존감리결과	사용자 접근권한에 대한 설정이 미흡함.

이와 유사하게 보안분석 단계나 보안설계 단계 및 보안구축단계에서도 <표 16> <표 17> <표 18>을 보면 사례연구에서 도출된 감리 개선 사항을 열거하여 보면 기존 감리결과에서는 제한적이거나 전반적인 표현의 지적사항이 도출되었으며 건수도 비교적 1 ~ 2 건에 불과하였으나 정량화 모델 적용시 구체화된 지적 사항을 도출할 수 있었으며 건수도 4 ~ 7건으로 비정량화 모델에 비하여 많았다.

<표 18> 보안 구축단계 개선권고사항 도출 현황

사례연구의 보안구축단계	접근통제 구현과정의 프로토타이핑 실시가 미흡함.
	정보보호 체계에 대한 통합 설계서 작성이 미흡함.
	계획단계에서 작성된 이행 계획이 미흡함.
	정보보호정책, 절차 및 지침이 수정 보완이 미흡함.
	보안사고 예방 대책과 사고 발생시 복구 대책이 미흡함.
	정보보호모델에 따른 요소별 보안기능의 검증 및 평가가 미흡함.
	보안도구의 설치가 미흡함.
	서버 보안 운영 방안이 미흡함.
	네트워크보안 기능 반영이 미흡함.
	네트워크 보안구축시 보안도구의 설치가 미흡함.
	응용시스템 보안구축시 보안기능 반영이 미흡함.
기존감리결과	네트워크 보안반영이 미흡함
	서보보안도구가 미흡함.

4.2.3 사례연구시 도출된 시사점

사례 프로젝트 적용시 도출된 개선점은 다음과 같다.

첫째, 감리인들에 대한 활용교육이 우선되어야 활용도가 높을 수 있다.

둘째, 보안요구사항이 미미할 경우 해당시스템의 기능적인 부분만 적용이 될 수 있고, 감리인이 적용여부와 평가를 판단하기 곤란한 경우가 있을 수 있어, 규모별 혹은 프로젝트 특성별 적용범위를 구분하여 점검할 수 있도록 일부 점검항목의 세부화가 필요하다.

셋째, 보안정책이나 지침이 마련되지 않은 기업의 경우는 시스템의 보안부분 점검보다 보안체계가 우선 구축되어야 하는 문제도 있다.

4.3 시사점에 대한 토의

전문가의 인터뷰와 사례 프로젝트 적용의 결과로서 도출된 시사점을 토대로 연구 모형을 다음과 같이 개선하여 추후 연구를 수행할 필요가 있다.

첫째, 세부지침의 상세화 검토로서, 현재 53개 항목, 230개 세부항목으로 도출되어 상세화 수준이 비교적 높다고 할 수 있으나 일부 항목에 대하여 추가적인 세부화를 함으로써 애매모호한 부분을 최소화할 필요가 있다.

둘째, 사례프로젝트의 규모에 따라 적용, 미적용의 항목을 중점검토항목에도 별도로 두어 판단을 하도록 함으로써 소규모의 프로젝트에는 중간 점검항목에서 적용여부를 판단하도록 할 필요가 있다.

5. 요약 및 결론

전문가 인터뷰와 사례프로젝트에 적용한 결과 다소 시행착오가 있었으나 평가 결과를 정량적으로 나타낼 수 있어 감리평가결과에 대한 발주자측이나 수주자측에 신뢰감을 주었다고 판단되며, 정량화된 모델을 통해 감리품질을 제고할 수 있었다.

첫째, 감리의 준거성에 대하여서는 감리인이 바뀌더라도 감리평가결과가 거의 유사하게 도출할 수 있을 것으로 판단되었다. 감리인이 평가시 애매모호한 판단을 할 수 있는 여지가 줄어들었다.

둘째, 감리의 효과성측면은 정량화 모델을 통하여 획기적인 향상보다는 다소 향상된 것으로 나타났다. 즉, 정량화 모델이 아니더라도 감리를 통하여 어느 정도의 정보시스템의 효과를 얻을 수 있는 것으로 나타났으며, 정량화 모델을 도입함으로써 얻어질 수 있는 것은 간접적인 향상을 기대할 수 있겠다.

셋째, 감리의 신뢰성 향상 측면에서는 보안감리평가의 정량화를 통한 발주자의 신뢰감 부여는 애매모호한 지적사항 위주로부터 점검항목의 어느 부분이 개선여지가 있는지 제시 되었으며, 특히, 각 항목에 대한 정량화로 획득률이 계산되어 평가에 대한 신뢰성을 향상할 수 있음이 예상되었다. 또한, 개발자에 대하여서는 세부 지침으로부터 개선권고사항의 정확한 도출과 정량화를 통한 평가의 수준을 가시화하여 감리결과에 대한 정확한 판단근거를 제시할 수 있음으로서 신뢰성 향상을 기대할 수 있었다.

넷째로, 감리의 안전성은 본 연구에서 제시하는 정량화 모델을 통하여 점검상의 누락의 방지와 함께 구체적인 무결성확보를 위한 사항을 평가하게 함으로써 안전성 향상에 영향을 끼칠 수 있다는 것을 80%이상의 많은 전문가들이 공감하였다.

다섯째로, 감리의 효율성은 본 연구를 통하여 보다 정확한 개선 권고안을 명확히 제시함으로써 감리의 효율성을 높일 수 있다는 것에 전문가 모두가 만장일치로 공감하였다.

향후, 모델로 제시한 정량화 평가방안에 대하여 중규모 점검항목에 대한 가중치의 별도부여 검토를 모색할 수 있을 것이다. 더 나아가서 전반

적인 감리평가 효율화를 위하여 응용시스템, 데이터베이스, 시스템 구조 및 일반관리 등 타분야에 대한 정량화 모델이 제시되어야 할 것이다.

참 고 문 헌

[1] 김명희, 정보시스템 보안의 효과성 증진방안, 고려대 석사학위 논문, 1997

[2] 김소연, 정보보호시스템의 평가 워크플로우 관리를 위한 워크플로우넷, 한남대 박사학위 논문, 2001

[3] 김유진, 정보보호프로세스평가모델개발에 관한 연구, 중앙대 석사학위 논문, 2000

[4] 이병욱외, 정보시스템보안감리지침 정보시스템감리인협회 2002.

[5] 이완석, 정보보호시스템 평가·인증제도 발전방향에 관한 연구, 동국대 석사학위논문, 2001

[6] 정보통신부, 정보보호시스템 평가.인증 지침, 1999

[7] 정승열외, 정보시스템감리효과성에 관한 연구, 한국전산원, 1998

[8] 최창훈, 컴퓨터 保安 評價等級 基準 및 檢證方法에 관한 연구, 한국외국어대 석사학위논문, 1992. 02

[9] 한국전산원, 정보시스템 보안 감리 지침 연구, 한국전산원 1998. 10

[10] 한국전산원, 정보시스템감리기준, 1999

[11] 한국전산원, 행정전산망 사업에 대한 감리효과 연구, 1992

[12] 한국전산원, 정보시스템감사 효과에 관한 연구, 1995

[13] 한국전산원, 정보시스템감리 자동화방안연구, 2001

[14] 한국전산원, 정보시스템감리효과에 관한 연구, 2002

[15] 한국정보보호인증센터, 정보보호인증심사점검지침, 2002. 12

[16] Peltier, T. R. Information Security Analysis, Auerbach, 2001, pp. 158-194

[17] Sennewald, C.A., Effective Security Management 3rd Edition, 1998, pp 235-276

[18] Tipton, H. F., and Micki Krause, Information Security Management Hand Book 4th Edition, Auerbach, 2001, pp 251-355

[19] Tudor, J. K., Information Security Architecture, Auerbach, 2001, pp101-136.

■ 저자소개

김 동 수

광운대학교에서 이학사, 서울산업대학원에서 공학석사를 취득하였으며, 현재 국민대학교 박사과정에 재학중이다. (주)효성의 전산실과 효성데이터시스템의 근무 경력이 있다. 최근에는 정보시스템 감리, 프로젝트 관리 등을 연구하고 있다. 현재, 신흥대학교에서 겸임교수로 활동하고 있으며, 감리전문법인인 (주)키삭의 대표이사이다.

김 현 수

서울대학교에서 공학사, 한국과학기술원에서 경영과학 석사, 미국 University of Florida에서 경영학 박사를 취득한 후, 현재 국민대학교 비즈니스IT학부 교수로 재직하고 있다. University of California, Berkeley에서 연구교수, University of Florida의 객원교수, (주)데이콤 근무 경력 등이 있으며, 최근에는 정보시스템 평가, 지식경영, 정보시스템 감리, 프로젝트 관리 등을 연구하고 있다. 주요 연구 결과는 Omega, European Journal of Operational Research, Intelligent Systems in Accounting, Finance and Management 등의 국제 학술지와 경영정보학연구, 경영과학, 정보처리학회논문지, 한국경영과학회지, Information Systems Review, Information Technology Applications and Management 등의 국내 학술지에 발표하였다.

◈ 이 논문은 2003년 8월 20일 접수하여 2차 수정을 거쳐 2004년 3월 21일 게재확정되었습니다.