정보시스템보안감리평가의정량화모델개발

김동수*, 김현수**

*국민대 BIT대학원, **국민대학교 정보관리학부

Developing A Quantitative Evaluation Model for Information System Security Auditing

Kim, Dongsoo,
Graduate School of KMU BIT,
E-mail : dskim@kisac.co.kr,

Kim, Hyunsoo
Kookmin University
hskim@kookmin.ac.kr

요약

지금까지 국내 보안감리 평가는 정성적인 평가에 머물러 있어 평가를 담당하는 감리인마다 평가 결과가 서로 상이하여 피 평가자에게 신뢰를 심어주지 못하는 결과가 초래되고 있다. 본 연구에서는 보안감리에 대한 국내의 연구와 해외 사례를 참조하여 SI사업에서의 보안감리평가 효율성을 제고할 수 있는 방안 및 평가체계를 정량화하는 방안을 제시하였다. 이를 위해 SI사업의 소프트웨어 개발 및 개발 환경(네트워크, 서버 등)을 중심으로 한국전산원에서 제시하고 있는 보안감리 지침과 한국정보시스템감리인협회의 보안관련 세부 감리지침을 통합하고 세부 감리지침에 따른 평가를 정량화 하였다. 보안감리 평가의 정량화 방안에 대한 감리전문가의 인터뷰와 사례 프로젝트의 적용을 통하여 연구 모형에 대한 검증을 실시하였다.

1. 서론

정보화 수준의 향상과 국가 정보화 사업의 추진 확대로 정보시스템에 대한 의존도는 점점 심화되고 있으나 소프트웨어의 미흡한 개발이나 컴퓨터 사고 등으로 인한 정보시스템의 안전성, 효율성, 효과성이 저하되고 있다. 또한, 기업의 연속성에도 많은 영향을 미침에도 불구하고 정보시스템 감리에서의 보안 분야는 기존의 소프트웨어 개발감리 영역중 시스템 아키텍쳐 분야의 일부분에서 연구되거나 감리점검항목을 도출하였을 뿐이다. 정보시스템 보안 기술의 급격한 발전에 비해 보안 분야의 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 한다..

2. 보안 평가 연구

본 연구에서는 외국의 정보시스템 보안평가 사례의 검토와 한국전산원, 한국정보시스템감리인협회, 정보보호인증센터 등에서 연구한 기존의 연구 결과를 고찰한다.

2.1 외국의 관련 연구

미국의 평가기준 지침서(TCSEC)에서는 보안정책 등 5가지의 보안요구사항을 7등급으로 표시하고 있다.

[표 2-1] 미국 TCSEC 평가 지침

보안요구사항	보안정책, 표시, 식별, 기록성, 연속적보호
평가등급	D, C1, C2, B1, B2, B3, A1

영국의 평가기준은 강제규정인 보안통제와 비강제규정인 보안목표로 나누며 평가등급은 6등급으로 표시하고 있다.

[표 2-2]영국 평가 지침

보안통제	X1 ~ X6 (기록성, 인증, 허락, 객체보호, 객체 재사용, 부인 봉쇄)
보안목표	Y1 ~ Y5 (부가사항없음, 손실없음, 포함, 시간영속성, 자원거부없음)
평가등급	L1, L2, L3, L4, L5, L6

이외에도 북미, 유럽 각국이 독자의 보안평가 방법을 내놓아 상호간 인증의 문제가 크게 대두되어 다음과 같은 공통인증기준이 나오게 되었다.

[표 2-3] 공통인증기준

참여기관	미국 : NSA, NIST 캐나다 : CSE 영국 : CESG 프랑스 : SCSSI 독일 : BSI 네덜란드 : NLNCSA
보안기능	식별과 인증, 액세스 제어, 기록성, 감사, 객체재사용, 정확성, 데이터무결성
보안등급	F1 ~ F10
정확성	E0 ~ E6
효과성	기능의 적합성 및 결함성, 침투에 대한 보호 메카니즘의 강도, 편리성, 운영침투에 대한보호
종합평가	E0, (F1, E1), (F2, E2), (F3, E3), (F4, E4), (F5, E5), (F6, E6)

한편, BS7799는 BT, HSBC, Unilever 등 주요업체와 더불어 영국의 상무성 주관으로 BSI(British Standard Institude)의 DISC에서 운영하는 위원회BDD/2에서 개발한 보안관리 지침으로 조직의 정보보호관리시스템을 구현, 관리하는 데에 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 신뢰성있는 거래를 위한 기반을 제공하는 데 있으며, 다음과 같은 특성이 있다.

[표 2-4] BS7799 평가 지침

보안정책	정보보호정책
보안조직	정보보호기반구조, 제3자 접근 보안, 아웃소싱
자산분류 및 통제	자산의 책임성, 정보 분류
인원보안	직무정의와 고용보안, 사용자교육, 보안사고대응
물리적및환경적보안	보호구역, 장비보안, 일반통제
통신및운영관리	운영절차 및 책임, 시스템 계획 및 승인, 소프트웨어에 대한 보호, 하우스키핑, 네트워크 관리, 미디어취급 및 보안, 정보 및 소프트웨어 교환
접근통제	업무요구사항, 사용자접근관리, 사용자 책임, 네트워크접근통제, 운영시스템접근통제, 응용통제, 시스템접근 및 사용모니터링, 이동통신 및

	텔레워킹
시스템개발 및유지보수	시스템보안요구사항, 응용시스템보안, 암호통제, 시스템파일보안, 개발 및 지원공정보안
업무연속성	업무연속성관리측면
준거성	법적준거성, 보안정책의 검토 및 기술적 준거성, 시스템 감사고려사항

외국의 평가 사례는 공통인증기준인 CC로 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.

2.2 국내의 연구결과 현황 및 문제점

1) 국내의 연구 결과

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

[표 2-5] 정보통신부 감리기준

중점검토항목	요구사항도출, 분석, 설계, 구현, 관리방안 등 5항목
전체평가방법	적정, 보통, 부적정
항목별평가방법	긴급개선, 통상개선, 권고사항

한국정보보호 인증센터의 정보보호체계인증제도에서는 보안요구사항을 5단계의 관리과정 요구사항과 문서화요구사항 및 15개분야의 48개 통제사항을 가진 통제요구사항으로 나누고 있다[표 2-6]. 개발에 관한 점검사항은 13개 항목에 46개 점검항목으로 기관의 정보자산에 대한 보호측면에서 다루어져 개발측면은 다소 미흡한 상태이다.

[표 2-6] KISA 인증심사점검표

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

한국정보시스템감리인협회의 보안감리지침은 11개분야로 나누어지고 점검항목은134개 항목과 세부 점검항목은 299개로 구성되었다[표 2-7]. 개발에 관련된 항목은 응용시스템과 데이터 보안으로 36개 항목과 67개 지침으로 이루어져 개발보다는 정보시스템 운영측면에서 도출하였다.

[표 2-7] 감리인협회 보안감리지침

분야	점검항목	세부 점검 항목
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

한국전산원의 보안감리지침은 보안계획, 분석, 설계 및 구현 등 4개 분야로 나누고 점검항목은 49개 항목과 세부 점검항목은 213개로 구분하였다[표 2-8]. 전산원의 보안감리지침은 소프트웨어 개발에 대한 점검항목 위주로 도출하였다.

[표 2-8] 한국전산원 보안감리지침

분야	점검항목	세부 점검 항목
보안계획	8	20
보안분석	4	16
보안설계	19	90
보안구축	17	87

2) 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.

3. 보안감리평가의 모형

3.1 모형의 개요

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.

3.2 모형의 설정

보안감리의 평가항목은 정보통신부에서 1999년 12월에 고시된 감리기준에 의거하여 1998년 발표된 전산원 보안 감리지침을 근간으로 감리인협회의 연구자료[표2-6]와 정보보호진흥원의 인증심사점검표[표2-7]를 참조하여 감리점검표를 보완하였다. 따라서, 전산원 감리지침[표 2-8]에서 제시된 보안계획, 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 230개로서 소프트웨어 개발위주로 도출하였다.

[표 3-1] 제안된 감리지침

분야	점검항목	세부항목
보안계획	8	20
보안분석	4	16
보안설계	19	90
보안구축	22	104

한국정보시스템감리인협회의 감리지침은 운영위주의 지침으로 개발에 대한 세부지침

이 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 [표3-1]과 같이 점검항목과 세부 점검항목이 다소 증가하였다.

2) 보안계획의 주요점검항목은 보안조직, 보안요구사항, 정보자산의 파악, 정보보호대상업무선정, 정보보호계획 등이며, 보안분석단계의 주요점검항목은 관리적보안사항분석, 물리적보안사항분석, 정보보호대상업무에 대한 분석, 자산분류도 작성 등이다. 보안설계단계는 보안대응책, 정보보호모델도, 정책의 설계단계반영, 보안조직구성, 비상사태복구대책, 교육, 감사, 출입통제, 환경보안, 서버접근통제대책, 클라이언트보안, 네트워크보안, 시스템사용에 대한 추적성 등이다. 마지막으로 보안구축단계는 접근통제구현, 정보보호체계통합설계 작성 및 구현, 감사, 보안사고발생시복구대책, 물리적대응책구현, 서버의 보안반영, 네트워크의 보안반영, 응용시스템구축시 보안반영, 보안기능의 시험 등이다.

3) 전산원 지침에서 제시된 레벨 1,2,3에 대한 구성체계를 그대로 수용하되 이를 긴급도의 순위로 바꾸고 점수화하였다. 즉 레벨 1의 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 긴급도(3, 2 또는1) * 적용(1 또는 0) * 적정평가(2) => 표준 점수로 부여하고, 각 세부항목에 대한 평가 점수는 긴급도(3, 2, 또는 1) * 적용(1 또는 0) * 평가치 (2, 1, 또는 0) => 평가점수로 부여 한다.

7) 중규모 단위의 세부점검항목별로 평가점수를 합산하여 표준점수대비 평가점수 획득율을 계산하였다([표 3-2]참조).

8) 획득율에 따라 50% 이하의 경우 긴급개선을 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 3-2] 감리지침의 평가표 예시

점검항목	세부항목	긴급구분	적용	표준평가	표준점수	감리평가	평가점수	획득율
응용시스템보안반영	사용자별 접근통제 구현	3	1	2	6	2	6	100
정보보호체계 설계	통합보안 설계서 작성	2	1	2	4	1	3	75
합 계					10		8	80

4. 연구결과

제시된 모형에 대한 타당성 검토를 위하여 관련 전문가인 보안감리인의 인터뷰를 실시하여 모델이 적용가능한지를 검토하였다. 또한, 본 평가모델의 개발목적이 감리현장에서 보안감리평가에 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 감리인중 보안 감리를 1회이상 경험한자 10인을 대상으로 하였으며, 기술사, 한국전산원 인정 감리인, 한국정보시스템감리인협회 인정 감리인 들로서 감리전문가라고 할 수 있다. 인터뷰는 2003년 3월 3일부터 3월 22일까지 사이에 실시하였으며, 인터뷰시 질문은 아래의 [표4-1]과 같은 내용으로 인터뷰를 실시하였다.

[표 4-1] 인터뷰시 질문내용

질문내용
1. 객관성 유지가 가능한가?
2. 감리 품질 즉, 평가의 일관성을 유지할 수 있는가?
3. 보안감리평가에 대한 정량화가 가능한가?
4. 보안감리평가의 정량화는 타당성이 있는가?
5. 보안감리평가의 정량화를 통해 발주자에게 신뢰감을 줄 수 있는가?
6. 본 평가를 통하여 개발자에게 신뢰감을 줄 수 있는가?
7. 본 평가의 개선할 점은 무엇인가?

질문전개방법은 보안감리평가표를 사전에 메일로 보낸 후 감리인 개개인별로 인터뷰를 실시하였다.

4.1.2 인터뷰 결과

보안감리전문가 대상으로 구조적 면담을 실시한 결과는 다음과 같다.

첫째, 객관성유지에 대하여서는 감리인이 바뀌더라도 감리평가결과가 거의 유사하게 도출할 수 있을 것으로 판단되었다. 그 이유로는 53개 점검항목과 230개의 세분화된 감리지침을 제공함으로써 감리인의 주관적인 판단을 할 수 있는 부분을 최소화하였다. 또한, 각 세부지침마다 적정, 미흡, 부적정의 3단계 평가를 하게되어 감리인이 평가시 애매모호한 판단을 할 수 있는 여지가 줄어들었다.

둘째, 감리인이 가진 경험에 따라 감리개선사항 도출이 차이가 나는데([표 4-3]참조), 본 모형에서 제시된 평가표에 따르면 구체적인 개선사항이 도출되며, 감리인에 따른 평가의 편차를 최소화시켜 평가결과에 대한 일관성을 제공할 수 있을 것으로 판단된다.

셋째, 정량화 가능성에 대하여는 항목별 긴급도 구분에 따른 점수부여, 세부지침에 대한 프로젝트에의 적용, 미적용여부, 감리인의 세부지침에 대한 3단계 평가를 통하여 표준점수와 평가점수 및 평가 획득율 계산 등으로 인하여 보안감리평가에 대한 정량화가 가능하다는 판단을 할 수 있었다.

넷째, 정량화의 타당성에 대하여는 감리인의 주관적인 판단에 의한 것보다는 세분화된 지침과 적용여부, 3단계 평가, 긴급도 구분 등은 대부분 명료한 평가로 판단되어 평가의 정량화가 어느 정도는 타당성을 부여한다는 의미가 있었으나 일부 개선의 여지가 있을 수 있다는 의견이 제시되었다.

다섯째, 평가의 정량화를 통한 발주자의 신뢰감 부여는 애매모호한 지적사항 위주로부터 점검항목의 어느부분이 개선여지가 있는지 제시 되었으며, 특히, 각 항목에 대한 정량화로 획득율이 계산되어 평가에 대한 신뢰도를 높였다.

여섯째, 개발자에 대하여서는 세부 지침으로부터 개선권고사항의 정확한 도출과 정량화를 통한 평가의 수준을 가시화하여 감리결과에 대한 정확한 판단근거를 제시할 수 있음으로서 신뢰감을 높일 수 있었다.

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 단

위의 점검항목간에도 가중치의 별도부여검토가 필요하다.
2) 대부분의 항목은 충분히 상세화 되었으나 일부 항목은 상세화가 필요하다.
3) 감리지침의 세부항목에 대한 평가 적용여부를 사이트의 경.중에 따라 융통성있게 적용하는 것이 필요하다.

4.2 사례 프로젝트 적용 결과

4.2.1 사례 개요

적용한 사례 프로젝트의 개요는 서울의 A 구청에서 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 구현정착시키기 위한 것이다.
본 프로젝트에 적용하기위한 목표로는 [표 4-2]와 같이 정리할 수 있다.

[표 4-2] 사례적용시 적용목표

질문내용
1. 감리 개선항목의 도출이 용이한가?
2. 감리결과 평가가 용이한가?
3. 적용항목의 판단이 용이한가?
4. 감리평가의 정량화는 가능한가?
5. 발주자 등 피평가자들에게 신뢰감을 줄 수 있는가?

4.2.2 사례 적용 결과

첫째, 보안감리의 개선항목도출은 1998년부터 수행한 감리보고서 36건을 대상으로 분석하여본 결과 평균개선건수가 1.75에 불과하였으나 사례 프로젝트에 적용한 결과 5개로 구체화되었다([표4-3]참조).

[표 4-3] 감리개선항목도출건수

	구 분	건수
문헌연구	대상감리보고서	36
	평균개선건수	1.75
	표준편차	1.25
	최대개선건수	7
	최소개선건수	0
사례연구	사례적용시 도출건수	5

둘째, 감리결과 평가는 지침의 세부화로 애매모호한 항목이 대폭줄어 대부분 용이하게 판단을 내릴 수 있었다. 또한, 적용항목 여부도 적용, 미적용 등으로 용이하였으며, 긴급도 순위는 사전에 정의되어 있어 적용이 용이하다고 판단되었다.
셋째, 적용항목의 판단은 사례 프로젝트 규모가 비교적 소규모인 까닭에 보안계획단계부터 적용이 안된 경우로 일부 분석, 설계단계의 지침은 계획단계에서 정의 되지 않으면 지침의 적용이 어려운 경우가 있었다.
넷째, 감리평가의 정량화는 지침의 세부화와 더불어 긴급도, 적용여부, 3단계평가 등으로 비교적 용이하게 적용 가능하였다.
다섯째, 사업자의 PM과 Project Leader 들, 그리고 발주자인 구청 담당직원과 계장을 인터뷰하여 감리평가 결과에 대한 신뢰감을 조사하였다. 조사결과 피평가자들에게 신뢰감을 줄 수 있음을 확인하였다.

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 검토

현재 53개항목, 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. 또한, 감리평가결과의 일관성을 기할 수 있어 감리인간의 평가결과에 대한 이견을 없앨 수 있었다. 감리 개선항목도 통상 1.75개항목 도출로부터 5개 이상 도출되어 정확한 개선권고사항이 제시되었다.

향후, 모델로 제시한 정량화 평가방안에 대하여 중규모 점검항목에 대한 가중치의 별도부여 검토를 모색할 수 있을 것이다. 더 나아가서 전반적인 감리평가 효율화를 위하여 응용시스템, 데이터베이스, 시스템 구조 및 일반관리 등 타분야에 대한 정량화 모형이 제시되어야 할 것이다.

참고문헌

[1] 김명회, 정보시스템 보안의 효과성 증진 방안, 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 발전 방향에 관한 연구, 동국대 석사학위논문, 2001

[6] 정보통신부, 정보보호시스템 평가.인증지침, 1999

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

[8] 최형진외, 정보시스템 보안 감리 지침 연구, 한국전산원 98. 10

[9] 한국전산원, 정보시스템감리기준, 1999

[10] 한국정보보호인증센터, 정보보호인증심사점검지침, 2002. 12

[11] DoD, "Department of Defense Trusted Computer System Evaluation Criteria", Dept. of Defense Standard, 1985

[12] European Community, "ITSEC Manual', 1991

[13] Peltier, T. R. Information Secutity Analysis, Auerbach, 2001, pp. 158-194

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

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

[16] Tudor, J. K., Informaion Security Architecture, Auerbach, 2001, pp101-136