공공부문 정보시스템 감리의 현황과 개선방안

이장형

대구대학교 회계정보학과

초 록

정보화 시대를 살아가면서 더 많은 조직들이 업무에 있어서 정보의 중요성을 인식하고, 대부분의 조직들은 정보시스템을 주된 기능으로 대체하는데 기초를 둔 컴퓨터 환경으로 변화시킬 계획들을 가지고 있다. 하지만 많은 조직들은 정보시스템의 효율성과 신뢰성을 조사할 필요가 있고 심지어 불평까지 하는 경우도 있다. 오늘날 정보시스템 감리에 대한 수요는 정보시스템의 성공적인 개발을 지원하기 위해 증대하고 있다. 감리의 목표는 정보시스템의 부작용을 막고, 예산의 효율적인 사용을 확신하며 조직의 내부 감리 능력과 인식을 제공하는 것이다. 이런 목표를 성취하고 감리 품질을 높이기 위하여 정보시스템 감리를 제도화하고 공공부문의 정보시스템 감리현황을 조사하고 개선할 필요가 있다.

이 연구에서는 우선 감리와 선행연구, 우리나라 현황 등을 기술한다. 그리고 공공부문 정보시스템 감리의 개선방안을 제시하고자 한다.

Ⅰ. 서 론

정보화사회에서는 일상의 업무처리를 정보시스템에 의존한다. 정보시스템은 자료처리, 정보의 제공, 의사결정 지원 등 나날이 영역이 확대되어 가고 있다. 따라서 많은 공기업이든 사기업이든 정보시스템을 구축하고 관리를 하고 있다.

정보시스템의 구축 및 관리에는 많은 위험과 비용이 수반된다. 이에 대한 적절한 대책이 필요한 것은 말할 나위가 없다. 정보시스템 감리가 그 중 하나의 대책이다. 이는 정보시스템의 계획, 개발, 운영 등 전반적인 측면에서 효율성과 효과성을 포함하여 종합적인 성과의 평가를 하는 것이다.

미국, 일본, 유럽 같은 선진국들은 정보시스템 감리를 발전시키기 위해 활발히 활동하고 있는 반면에 우리 나라는 1980년대 초에 정보시스템 감리가 소개되었으나 국내 공공부문의 기술감리에 치중하고 있다. 선진국에서는 운영중인 정보시스템의 내부통제 검토에 역점을 둔다.

1987년 제 1 차 행정전산망 사업에 대한 감리로 본격적인 정보시스템 감리가 한국전산원에 의해 수행되어 최근에는 민간 감리 법인이 설립되어 위탁 감리를 실시하고 있다. 감리는 일종의 보험과 같은 성격을 지닌 것이어서 감리를 위한 적절한 정책과 자율적인 규제는 필요하다.

정보시스템 감리는 감리대상으로부터 독립된 감리인이 정보시스템의 안전성, 효율성 및 효과성 향상을 위하여 정보시스템의 구축, 운영에 관한 사항을 종합적으로 점검, 평가하고 감리의뢰인 및 피감리인에게 개선이 필요한 사항을 권고하는 것이다.

정보시스템 감리의 대상은 다방면에 걸쳐 있는데 그 중에서 응용업무부문은 특히 중요하며 감리의 해석에 차이가 있어서는 안 된다. 응용업무부문은 컴퓨터 시스템의 주된 요소인 동시에 대응하는 업무의 중추적 요소이기도 하다는 이면성을 가지고 있다. 응용 시스템 감리는 응용업무부문을 컴퓨터 시스템의 요소로서 위치시킬 때의 감리이다.

미국, 일본 등 외국의 경우에는 운영중인 정보시스템 내부통제 검토에 역점을 두나 우리나라는 기술감리가 중심이다. 이는 우리 나라 공공부문 정보시스템 개발과정에 위험요소가 많기 때문이다.

따라서 공공부문의 응용업무가 제각기 다르며, 아직 초보적인 단계에 있는 정보시스템 감리는 개선할 필요가 있다. 그러므로 본 연구는 감리 실제를 중심으로 공공부문감리의 현황을 살펴보고 이를 개선시키려는 것이다. 제

2 장에서는 선행연구이고, 제 3 장은 정보시스템 감리에 대한 현황이다. 제 4장은 정보시스템 감리의 개선방안이며, 제 5 장은 결론을 제시한다.

Ⅱ. 선행연구

우리 나라 공공부문 정보시스템 감리에 대한 연구는 감리 일반, 프로젝트 관리, 생명주기 공정별, 요소기술 등에 관한 연구로 대별해 볼 수 있다.

Ⅱ.1 감리일반에 대한 선행연구

정보시스템 감리일반에 대한 연구로는 전산감리 편람이 3권으로 1993년에 전산망 감리요청 및 시행절차, 전산감리 점검표, 관련법령 및 기준이라는 주제로 연구되었다. 전산감리 기준 세칙을 1994년에 제정하면서 감리점검표에 대한 연구가 있다. 행정 전산망 외주용역 관리지침에 관한 연구가 같은해 있었다. 1996년에는 전산감리 세칙을 개정하였으며, 소프트웨어 프로세스 평가지침에 대한 연구도 있다. 1997년에는 시스템 개발 방법론의 적용기준에 관한 연구가 진행되었고, 정보시스템 감리 업무의 개정방안에 대한 연구도 있다. 1998년에는 공공 정보화 사업 계약관리에 관한 연구가 있다.

Ⅱ.2 프로젝트 관리에 대한 선행 연구

정보시스템 감리 중 프로젝트 관리에 대한 선행 연구로는 주로 감리지침에 대한 연구이다. 1997년에 정보시스템 프로젝트 감리지침, 형상관리 감리지침, 1998년에 품질관리 감리지침에 대한 연구가 있다.

Ⅱ.3 생명주기에 대한 선행연구

정보시스템 감리 중 생명주기(공정별)에 대한 선행연구로는 정보시스템 생명주기별로 연구를 한 것이다. 1997년부터 정보시스템 기획, 분석, 설계, 시험에 대한 연구가 있다. 그리고 1998년에는 정보시스템 유지보수, 운영 감리지침에 대한 연구가 있다.

Ⅱ.4 요소기술에 대한 선행연구

정보시스템 감리에 대한 선행연구로 정보시스템 요소 기술에 대한 연구가 있다. 1995년에 데이터베이스 개발, EDI시스템, 네트워크 설계/구축 감리지침에 관한 연구가 있다. 그리고 1996년에는 전산망 운영, 클라이언트/서버 시스템, 분산DB설계 및 개발에 관한 감리지침을 연구하였다. 1998년에는 정보시스템 보안/통제, 정보시스템 객체지향 개발 감리지침에 대한 연구가 있다.

Ⅲ. 정보시스템 감리현황

Ⅲ.1 한국의 정보시스템 감리 제도

한국의 정보시스템 감리제도는 정보화의 역기능을 예방, 제거하고 정보시스템의 이용을 촉진한다는 것을 기본목표로 하고 있다.

한국의 본격적인 정보시스템감리는 1986년에 제정된 「전산망 보급확장과 이용촉진에 관한 법률」에 의하여 한국전산원이 설립되면서부터 시작되었다. 한국전산원은 1987년부터 제1단계 행정전산망 사업에 대한 감리를 시행해 오고 있으며 1990년에는 국가기관 등의 정보시스템에 대한 기술적 검토 및 감리를 위하여 「국가 전산망감리지침서」를 발간하는 등 정보시스템감사의 발전에 많은 기여를 하고 있다.

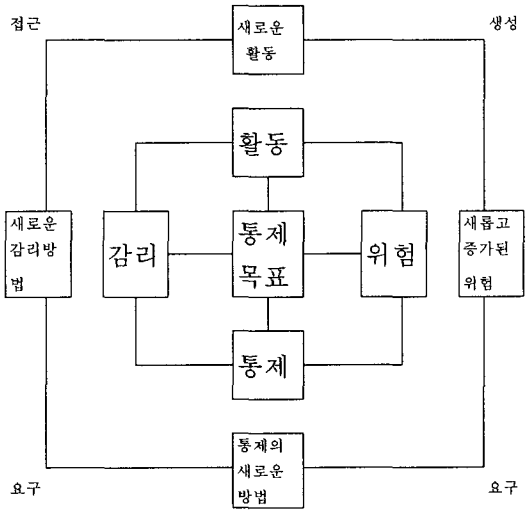
1990년대 들어서는 정보통신부, 감사원 및 한국전산원이 중심이 되어 공인정보시스템감사제도의 도입을 위한 연구가 진행되었으나 큰 진전을 보지 못하고 있는 실정이다. 1990년에는 「공인 정보시스템감사제도의 법제화 방안에 관한 연구」, 1992년에는 「전산감리제도 도입에 관한 연구」 등 많은 연구 및 세미나 활동이 전개되고 있다. 1993년에는 「전산망 확장과 이용촉진에 관한 법률」의 개정 및 관련 규정을 제정하여 정보시스템감사의 발전에 기여하고 있다.

1994년 전산망조정위원회에서 전산감리기준을 제정한 바 있으나 정보화 사업이 소프트웨어 개발 위주에서 시스템 통합(SI: System Integration)형태로 바뀌고 있고 정보기술의 급격한 발전 변화 등 현실적인 환경 및 여건을 반영하여 이를 정비할 필요가 있어, 1999년 개정된 정보화 촉진기본법 15조 2항에 따라 정보통신부 장관이 [정보시스템 감리기준]을 확대실시하고 있다.

또한 최근 급증하고 있는 공공부문 정보화 사업에 대한 감리수요의 충족과 민간부문의 감리전문인력을 양성하기 위하여 한국전산원에서는 정보시스템 감리인 양성교육을 실시하고 있다.

정보시스템 감리도 정보화와 함께 새로운 활동들이 추가됨에 따라 감리의 새로운 접근방법으로의 연구가 계속적으로 행해져야 한다.

이를 그림으로 나타내면 다음 <그림1>과 같다.



<그림1> 기업환경변화와 정보시스템감리

Ⅲ.2 한국 정보시스템 감리 현황

(1)사업비별 감리 투입 자료

우선 사업비에 따른 감리인력 및 감리시행기간과 감리회수가 다르다는 것이 발견되었다. 감리인력은 사업비가 10억 미만이면 4명, 20억미만이면 5명, 50억 미만이면 6명, 100억미만이면 7명, 100억 이상이면 8명이다. 또 사업비 20억미만은 2회, 30억미만은 3회, 50억미만은 4회, 100억미만은 5회이고 100억이상은 5회이상이다. 감리기간도 최소 8일에서 21일까지 분포되어 있음을 알 수 있다. <표 1>이 이를 종합한 것이다.

<표 1>사업비별 정보시스템 감리현황

내역 / 사업비	감리인력수 (인)	감리시행기간 (일)	감리시행회수 (회)
5억미만	4	8	2 이하
10억미만	4	10	2
20억미만	5	11	2
30억미만	6	13	3
50억미만	6	15	4
100억미만	7	18	5
100억이상	8 이상	21	5 이상

(2) 민간감리법인 현황

지금 우리 나라는 11개의 민간감리법인이 있다. 본격적인 정보시스템 감리인 양성 교육이 1997년 10월에 이루어짐에 따라 아직까지 감리법인이 그 형식 및 모습을 완벽하게 갖추고 있지는 않지만, 1998년 이후 한국전산원과 감리법인의 공동노력으로 민간감리 활성화를 위한 꾸준한 시도가 이루어지고 있다.

현재 민간감리법인이 활동을 시작하였거나 준비하고 있는 것으로 추정되며 빠른 시일내에 본격적인 민간 감리체제가 구축될 것으로 예상된다.

감리법인으로 등재되기 위해서는 자본금 1억원 이상과 1인 이상의 상근 감리인 및 2인 이상의 위촉 감리인(비상근)을 확보하고 있는 법인으로 최소한의 요건을 정하고 있다. 아래의 <표2>는 민간 감리법인의 현황이다.

<표2>민간 감리법인 현황

	자본금	종업원수	1999년 감리건수	1999년 감리매출액	1999년 총매출액	1999년 순이익
법인수	11	11	8	8	8	8
합계	1.7E+09	315	164	4.2E+09	5.5E+09	1.2E+08
평균	1.5E+08	29	21	5.2E+08	6.9E+08	2.4E+07
표준편차	8.0E+07	49	12	2.9E+08	3.4E+08	4.3E+07

<표2>에서 보는 바와 같이 자본금은 11개 법인이 자본금 합계가 1,700,000,000원이고, 평균적으로 150,000,000원이다. 또 종업원수는 전체 315명이며 평균적으로 29명인 것으로 나타났다. 3개법인은 1999년 중에 설립이 되어 이를 제외한 8개법인의 감리건수와 감리매출액은 다음과 같다.

1999년 감리건수는 총 164건에 4,200,000,000원이었고, 평균적으로는 21건에 520,000,000원이었다. 또 이들 8개 법인의 1999년 총매출액과 순이익을 보면 총계 5,500,000,000원, 120,000,000원이었다. 평균적으로 보면 총매출액이 690,000,000원, 순이익은 24,000,000원이었다.

민간감리법인은 아직 영세하며, 주로 수입원을 감리에 의존하다보니(76.36%) 감리가 좀더 활성화가 되어야 됨을 알 수 있다. 공공기관 감리만이 아닌 미흡하지만 일반 기업체의 감리도 최근에 와서 자발적으로 행해지고 있다.

법인자체계약 감리실적을 보면, 삼성물산, 데이콤ST, 한국소프트웨어진흥원, 연구개발정보센터, LG선물, 코오롱정보통신, 한국건설기술인협회, 한국광고단체연합회, 한국체육진흥(주), 한국구제협력단, 충남테크노파크, 한국후지필름등이 있다.

(3) 공공부분 감리실시에 대한 분석

1)공공부문 정보시스템감리의 법적 근거

현재까지 공공기관에서 주관하는 정보화사업에 대하여 반드시 감리를 받아야 한다는 법적 의무사항은 없다. 그러나 공공기관에서 주관하는 정보화사업들이 다부처 연계와 정보의 공동활용 등으로 갈수록 그 중요성이 증대하고 사업 규모가 커지고 있으므로 사업의 품질보증과 안정성 및 신뢰성 등을 위하여 사업을 발주하는 주관기관들이 감리를 필요로 하고 있는 실정이다.

참고로 감리의 의무에 관한 사항은 아니지만 관련이 있는 법적인 내용들을 발췌하면 다음과 같다.

①정보화촉진기본법(제정 1995·8·4 법률 제4969호, 개정 1999·1·21 법률 제5669호) 제15조 2항을 보면 다음과 같다.

제15조2 (정보시스템에 대한 감리) ①정보통신부장관은 정보를 수집·가공·저장·검색하기 위한 기기 및 소프트웨어의 조직화된 체제(이하 "정보시스템"이라 한다)의 효율적인 구축·운영과 안전성 및 신뢰성의 확보를 위하여 정보시스템에 대한 감리의 기준을 정하여 이를 고시하고, 정보시스템을 개발·구축 또는 운영하는 자에게 이 기준의 준수를 권고할 수 있다.

② 1999년도 세출예산집행지침(1999.1 예산청) 중 정보화관련경비(56쪽)의 세부집행지침에 보면 다음과 같다.

정보시스템을 개발할 경우에는 원칙적으로 한국전산원 등의 정보시스템 감리법인의 감리를 받아야 하며, 감리대가는 『정보시스템감리비 산정기준』(구:전산망감리비 산정기준, 한국전산원)에 의한다.

2) 공공부문 정보시스템 감리 실시

정보시스템 감리는 내용에 따라 일반관리감리와 공정별 감리로 크게 나눌 수 있고, 시기에 따라 중간감리와 최종감리로 나눌 수 있다.

일반관리를 위한 공통적인 감리영역으로는 범위관리, 일정관리, 위험관리와 같은 프로젝트 관리가 있고, 형상관리, 품질관리, 프로젝트 표준 및 기타의 개발방법론 및 표준이 있다.

공정별 정보시스템 감리는 기획 공정, 개발공정, 운영공정, 유지보수 공정으로 4개로 나눈다. 이를 그림으로 나타내면 다음<그림2>와 같다.

<그림2> 내용에 따른 감리 분류

중간감리와 최종감리에 따라 감리내용이 차이가 있다. 중간감리에서는 프로젝트 관리, 표준 및 품질보증, 응용시스템, 데이터베이스, 아키텍쳐 및 보안으로 구성된다.

최종감리는 여기에 시험결과부분이 추가가 된다.

3)감리의견의 표명 방법

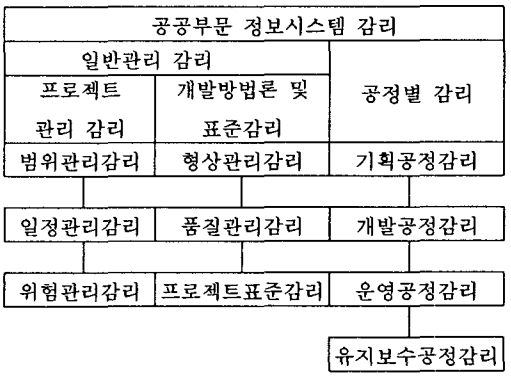
우선 세부적으로 개선해야 할 사항에 대한 개선 유형이 3가지 있다. 이를 표로 나타내면 다음 <표3>과 같다.

<표3>개선권고사항의 유형

개선 유형	내용
긴급개선	프로젝트 진행에 중요한 사항으로 긴급하게 개선해야 할 사항
통상개선	프로젝트 진행에 중요한 사항이나 타기관과의 업무협의가 필요하거나 시간을 갖고 개선할 사항
권고사항	프로젝트 진행에 도움이 되는 사항으로 상방간의 협의에 의해 추진할 사항

이 개선유형에 따라 중간감리 및 최종감리 보고서에 감리인은 감리의견을 표명한다. 그 의견은 5가지로 나누는데 <표4>와 같다.

<표4>감리의견 판단기준표



감리의견	의미
우수	개선이 필요한 중대한 요소가 없으며, 사전에 정의된 주요요구사항이 충족되었다고 판단되는 수준
양호	긴급개선이 필요한 요소는 없으나 통상개선사항이 존재하는 수준
보통	긴급개선이 필요한 일부요소가 존재하며, 계획된 자원으로 수행가능하다고 판단되는 수준
미흡	긴급개선이 필요한 중대한 요소가 존재하며 계획된 자원으로 수행가능하다고 판단되는 요소
부적정	긴급개선이 필요한 중대한 요소가 존재하며 계획된 자원으로 수행이 불가능하다고 판단되는 수준

Ⅳ. 정보시스템 감리의 개선방안

현재 공공부문에 대한 정보시스템의 개선방안은 크게 4가지 부분으로 나누어 제시할 수 있다.

Ⅳ.1 감리법인의 문제 개선방안

현재 감리법인들은 인적, 자본적으로 열세한 위치에 있다. 감리법인들을 정부에서 육성할 수 있는 법적인 제도적인 장치가 마련되어야 할 것이다. 벤처기업처럼 지원을 할 수 있는 것도 한 방법에 속할 것이다. 또 감리인 양성도 민간 감리법인에서 자율적으로 양성할 수 있도록 배려가 있어야 한다. 현재의 한국전산원의 독점적 교육보다는 민간기관의 자율적, 민주적교육이 필요하다고 본다.

Ⅳ.2 감리실시내용에 대한 개선방안

미국과 일본의 경우는 회계감사의 개념에서부터 출발하여 부정적발을 위한 통제와 개선권고의 양대 기능을 포함하는 조직내부의 전산감사를 지향하여 그 목표를 달성함으로써 정보시스템 개발의 요소기술로써 인식하고 있다.

반면 국내의 경우는 공공기관이 외부에 위탁하여 추진하는 정보화사업에 대한 개선권고 위주의 정보시스템 감리로 시행되는 실정이다. 이는 감리에 대한 사회적, 문화적인 환경 차이와 선진국에 비하여 낙후된 상황에서 기인한 적용 수준과 적용 방법의 차이로 볼 수 있다.

따라서 감리를 회계감사의 내부통제 부분에 대한 부분에 중점을 더 두는 제도적인 개선이 있어야 할 것이다.

Ⅳ.3 감리의견표명에 대한 개선방안

현재 공공부문의 정보시스템 감리는 종합의견을 표명하는 기준이 명확하지 않다. 각 부문에 대한 전체적인 의견을 표명하기 위해서는 다음과 <표5>와 같은 가중평균을 가미한 모형을 개발하여 여기에 준수하도록 하는 것이 바람직할 것이다.

<표5> 종합의견 표명을 위한 개선모형

감리의견(i)		부문별 감리영역(j)	
우수	5	프로젝트관리	A %
양호	4	표준 및 품질보증	B %
보통	3	응용시스템	C %
미흡	2	데이터베이스	D %
부적정	1	시스템 아키텍처	E %

종합의견은 다음 수식에 의해 내리는 것이 타당할 것이다.

$$Y = \sum_{i,j=1}^{N} ij$$

여기에서 i= 감리의견 j = 부분별감리영역 가중치

이 종합 점수에 의해 총평(종합의견)을 내려야 합리적인 감리가 실시될 것이다.

Ⅳ.4 감리대상의 확대

현재 공공부문에서만 정보시스템 감리가 실시되는 것을 민간기업에서도 실시할 수 있도록 법적인 장치를 마련하여야 한다. 이는 정보시스템의 취약성을 보완하는 계기가 될 것이다.

Ⅴ. 결 론

정보시스템의 구축과 운영에는 많은 위험이 존재한다. 정보시스템 자산을 보호하기 위해 위험을 평가하고 통제대책을 세우고 적용여부를 검토하는 감리가 필요하다.

아직 우리 나라는 정보시스템 감리가 초보단계에 머무르고 있다. 정보기술의 한 요소기술로 정보시스템 감리를 보고 보다 양질의 정보를 생성하기 위한 정보시스템 감리는 공공기관만이 아니라, 일반 기업들도 행할 필요가 있다.

이는 고객인 정보이용자들에게 보다 양질의 정보를 제공하여야 E-business에서 살아남을 수 있는 것은 당연한 이치일 것이다. 공공부문이든 사부문이든지 보다 발전적이고 개선된 정보시스템 감리제도가 정착되어 양질의 정보를 제공하여야 할 것이다.

참고문헌

1. Accounting and auditing Report,"New Guidelines for Auditing On-Line Computer Systems", The Practical Accountant, February, 1984, pp.61-63.

2. AICPA, "Statements on Auditing Standards, No. 47." Audit Risk *and Materality in Conducting an Audit*, New York, AICPA, 1983.

3. An American National Standard: *IEEE Standard for Software Verification and Validation Plans*, 1992

4. An American National Standard: *IEEE standard for Software Test Documentation* 1991

5. An American National Standard: *IEEE Standard for Software Unit Testing*, 1993

6. Bailey, Jr. and Duke, Gerlach, "TICOM and the Analysis of Internal Controls", *Accounting Review*, April, 1985.

7. Canning, R. G., "Information Security and Privacy", *EDP Analyzer*, February, 1986, pp.4-16.

8. Carroll, John M., *Computer Security (2nd ed.)*, Butterworths, 1987.

9. Computer Law and Security report (CLSR), Vol. 8. No. 1-6, *Elsevier Advanced Technology*, 1992.

10. Cooper, James A., *Computer & Communication Security*, 1990.

11. EDPAF, "Control Objectives, Controls in a Computer Environment : Objectives, Guidelines and Audit Procedures", *EDP Auditors Foundation,* Carol Stream, Illinoise, 1990.

12. Farrow, Rik, *UNIX System Security,* 1991.

13. ISO/IEC, *International Standard: Information Technology Software Life Cycle Processes, Department of the Army Pamphlet 73-7: Software Test and Evaluation Guidelines* July 1996

14. Kuong, Javier F., *Computer Auditing, Security & Internal Control Manual,* Prentice Hall Inc., 1987.

15. Lane, V. P., *Security of Computer Based Information Systems*, 1985.

16. Menkus, Belden (et al), "Control Objectives", *EDP Auditors Foundation Inc.*, 1990.

17. NCC Consultancy, "IT Security Breaches Survey", *National Computers Centre*, 1992.

18. Parker, Donn B., "Restating the Foundation of Information Security", *proceedings on 14th NCSC,* 1991.

19. Porter, W. Thomas & William E. Perry, *EDP : Controls and Auditing,* Kent Publishing Company, 1984.

20. Srinivasan, C. A. and P. E. Dascher, "Access Control Assures Network Security", *Internal Auditor*, August, 1986, pp. 40-45.

21. Turney, Watne, Auditing EDP Systems, 1990.

22. Watne, D. A. and Turney, P. B. B., *Auditing EDP Systems(2nd ed.)*, Prentice-Hall International Inc., 1990.