정보시스템 감리의 지식체계

신동익*

Common Body of Knowledge of IS Audit

요 약

정보시스템감리의 유용성과 중요성이 날로 점증하고 있는 시점에서 정보시스템감리인이 되고자 할 때 기본적인 공통지식에 대한 세밀한 정의가 부족하여 어려움을 겪는 사례가 많이 발생되고 있다. 본 논문은 정보시스템감리 관련 국내외 체계를 분석하고 국내의 감리 실무를 참조하여, 정보시스템감리의 공통 지식체계를 도출하고자 하였다. 아직까지는 높은 수준에서 분석이 이루어졌으나 추후 좀더 세밀한 연구가 진행되면 정보시스템감리 분야의 전문성 향상에 도움이 되리라 생각된다.

1. 정보시스템감리 지식체계

1.1 개요

정보시스템감리는 정보화가 급진전되어 많은 정보화사업이 추진되는 환경에서 정보시스템의 개발, 운영 및 유지보수 사업이 성공적으로 수행되었는지를 독립적 위치에서 감시하고 평가하기 위하여 수행되게 되었다. 정보시스템감리는 단순히 감시, 평가 뿐만이 아니라 경우에 따라서 자문이나 지원의 역할도 담당하기도 한다. 우리나라의 경우 최근 공공부문을 중심으로 수많은 대규모의 정보화사업이 추진되었고 발주자나 개발자 모두 이와 같은 규모의 정보화사업을 한 경험이 부족하므로 사업을 성공적으로 추진하는 것이 매우 어려운 현실이었다. 이러한 상황에서 다양한 사업을 관찰하고 경험한 정보시스템 감리인은 한 사업에서 축적된 경험 지식을 다른 사업으로 전파하는 중요한 역할을 담당하였고, 또한 정보화사업에 대한 감리 경험을 토대로 사업의 성공적 추진을 위해 필요한 요인들을 적극 권장할 수 있게 되었다. 정보시스템감리에 대한 이러한 긍정적인 인식은 정보시스템감리의 폭발적인 수요를 창출하게 되었고, 현재는 많은 사업

* 홍익대학교 교수 (dishin@hongik.ac.kr)

에서 감리를 수감하는 것을 당연하고 또한 필수적인 것으로 인식하게 되었다.

이러한 긍정적 측면 외에 정보시스템감리는 다분히 자의적이고 주관적이라는 비판을 들어왔다. 즉 감리의견이 감리인의 개별적, 주관적 판단에 크게 좌우되고, 따라서 감리의 잣대가 일관성있게 적용되지 않는다는 점이다. 이러한 문제를 극복하기 위해 정보통신부는 감리기준을 고시하였고 이 기준은 감리 실무에서 준수해야 되는 표준으로 정립되었다(정보통신부고시제1999-104호). 그러나 이 기준은 감리절차와 감리항목 위주로 작성되어 감리인 기본적으로 갖춰야 할 지식체계에 대해서는 구체적으로 명시하지 못하고 있다. 따라서 본 장에서는 적절한 지식체계의 도출을 위하여 다양한 감리체계를 비교분석하고 이를 토대로 현재 우리나라의 감리 실무에 적절한 지식체계를 정립하고자 한다.

1.2 정보시스템감리 체계

감리기준은 정보시스템 감리인이 갖춰야 할 전문적 자질로서 다음과 같이 명시하고 있다.

1. 정보시스템 관련 분야의 특급기술자 이상의 자격을 취득한 자
2. 한국전산원의 감리인 양성 교육과정을 수료한 자
3. 통신·전자·정보처리 등의 분야의 기술자격을 취득한자 또는
   이와 동등한 학력, 경력 인정자 중 본조 제1호 또는 2호에 상응하다고 감리의뢰인이 인정하는 자

이러한 정의는 매우 포괄적이고 종합적이어서 실제로 감리인이 되기 위해서 필요한 지식체계가 무엇인지를 명확히 알기 어렵다. 감리에 대한 정의 역시 다음과 같이 매우 포괄적이어서 명확한 지식체계를 알아내기 어렵다.

"감리"라 함은 감리대상으로부터 독립된 감리인이 정보시스템의 효율성, 효과성 및 안전성 향상을 위하여 정보시스템의 구축·운영에 관한 사항을 종합적으로 점검·평가하고 감리의뢰인 및 피감리인에게 개선이 필요한 사항을 권고하는 것을 말한다

감리기준이 비록 감리 절차와 항목에 대한 많은 혼란을 줄이는 중요한 역할을 담당하고 있으나 지식체계를 정립하기에는 미흡한 점이 많이 있다. 따라서 감리와 유사한 국내외 체계를 비교 분석하여 공통기반 지식을 도출하기로 한다. 유사 체계로는 다음과 같은 체계를 고려한다.

- ISACA(General Standards)

- 일본 시스템감사(시스템감사 기준)
- 품질시스템 감사(ISO 9000/ISO 10011)
- 소프트웨어 감사/평가(ISO 12207, CMM, SPICE)

2. 정보시스템감리 체계의 비교분석

2.1 ISACA(Information Systems Audit and Control Association)

ISACA는 정보시스템감사와 통제에 전문화되어 있는 국제단체이며, CISA(Certificate of Information System Auditor)라는 자격증 제도를 운영하고 있다. 이 단체는 오랜 역사를 갖고 있으면 주로 회계감사를 지원하는 형태의 정보시스템 감사로부터 시작하여 현재는 정보시스템의 품질, 보안 등에도 많은 강조를 하고 있다. ISACA는 감사와 관련되어 <표 2-1>과 같은 표준을 발표하고 있다.

표 2-1 ISACA 표준

표준	제목	감사인	감사 체재	감사 절차
Independence	1.attitude and appearance	X		
	2.organizational relationship		X	
	3.code of professional ethics	X		
Technical Competence	4.skills and knowledge	X		
	5.continuing professional education	X		
Performance of Work	6.planning and supervision		X	
	7.evidence requirements			X
	8.due professional care	X		
Reporting	9.reporting of audit coverage			X
	10.reporting of findings and conclusions			X

위의 표준은 일반적 표준으로 모든 감사인이 지켜야 할 것으로 제시되었다. 위 표준 중에서 작업 성과에 관한 표준에는 좀더 자세한 지침이 필요하였다. 이러한 지침은 실제로 정보시스템 감사의 지식 체계를 구성한다는 점에서 매우 중요하다. 이러한 지식체계를 구성하는데 있어 전통적으로 ISACA는 통제(control)중심의 감사를 중요시하였다. 통제가 강조되는 것은 ISACA가 회계감사를 지원하는 형태의 정보시스템 감사에 초점을 맞추었기 때문이다. ISACA는 원래 회계감사를 수행하던 중 많은 회계자료가 전산처리 되면서 정보시스템에 의해 저장 및 처리되는 회계자료의 무결성에 대한 보증을 필요로 했고 이러한 보증활동은 전산 기술에 이해가 높은 회계감사인이 아닌 다른 전문가에 의해 수행될 필요가 생

겼으며, 이러한 목적을 위해 수립된 기구이다. 따라서 ISACA의 감사 초점은 시스템 개발 분야보다는 운영분야에 그리고 정보시스템의 향상 측면보다는 정보시스템의 통제에 더욱 무게중심을 두게 되었다.

통제는 일반적으로 사업목적의 달성과 원하지 않는 사건의 예방, 탐지 및 교정을 위한 합리적인 보증을 제공하기 위해 설계된 방침, 절차, 실무관행 및 조직구조를 말한다(COSO Report, 1992). 이러한 정의에 기초하여 정보기술 통제는 원하는 결과 또는 목표의 달성을 위해 정보기술 활동에 구현되는 통제로 정의되었다(IIARF, 1992). 이러한 정의 위에서 ISACA는 최근 정보시스템 감사를 위한 IS 보안과 통제에 대한 일반적 체계를 COBIT(Control Objectives for Information and related Technology)으로 발표하였다(ISACF, 1995). COBIT은 기존에 연구된 COSO보고서, SAC, SASs 55/78을 기초로 통합적인 체계를 만들고자 노력하였다. SAC는 주로 내부감사의 정보시스템감사를 돕기 위해 작성된 보고서이며, COSO는 관리층이 통제시스템을 어떻게 평가하고 향상할 수 있는가 하는 점에 초점을 맞추고 있으며, SASs는 조직의 재무제표를 외부감사인이 수행할 때 내부통제가 감사의 계획과 수행에 미치는 영향에 대한 지침을 제공하고 있다.

COBIT은 ISACA가 생각하는 정보시스템의 감사에 대한 전반적인 지식체계를 보여주고 있다. 이 지식분야는 다음과 같이 하나의 프로세스와 6개의 컨텐츠 영역으로 구분되어 있다.

프로세스 영역

- IS 감사 프로세스 (10%) : 조직의 정보기술과 사업시스템이 적절하게 통제되고, 모니터되고 평가되는 것을 보증하기 위하여 일반적으로 받아들여지는 IS 감사 기준 및 지침에 따라 IS 감사를 수행

컨텐츠 영역

- 정보자산의 보호 (25%): 정보자산을 비인가된 사용, 노출, 변경, 피해 및 손실로 부터 보호하기 위한 조직의 사업 요구사항을 충족함을 보증하기 위하여 논리적, 환경적 및 IT 인프라의 보안을 평가
- 사업 응용시스템 개발, 취득, 구현 및 유지 (16%): 사업 응용시스템 개발, 취득, 구현 및 유지가 조직의 사업목표를 충족함을 보장하기 위하여 이에 사용된 방법론 및 프로세스의 평가
- 사업 프로세스 평가와 위험 관리 (15%): 조직의 사업목표에 상응하여 위험이 관리됨을 보장하기 위하여 사업 시스템과 프로세스를 평가
- 기술 인프라와 운영 실무 (13%): 조직의 사업목적이 적절하게 지원됨을 보증하기 위하여 조직의 기술 및 운영 인프라의 구현과 수행중인 관리의 효과성과 효율성을 평가
- IS의 관리, 계획 및 조직 (11%): IS의 관리, 계획 및 조직을 위한 전략, 정책, 표준, 절차 및 관련된 실무를

- 재해 복구 및 사업 연속성 (10%): 재해 발생시 사업 운영 및 IS 프로세스의 지속을 위한 계획의 개발과 유지 프로세스를 평가. 이러한 계획은 문서화되고, 논의되고, 시험되어야 한다

우선 감사절차를 다루는 프로세스 영역은 감사가 일반적으로 인정된 표준이나 지침에 적합하게 진행되어야 함을 의미한다. 다음 컨텐트 영역은 감사인이 감사를 위하여 필요한 기술 지식을 포함하고 있다. 가장 중요하게 다루고 있는 것이 보안 관련 이슈로서 정보자산의 보호, 비상계획 등이 35%의 비중을 차지하고 있다. 다음으로는 정보시스템의 개발, 운영, 유지보수에 관한 공학적인 사항으로 31%의 비중을 차지하고 있고, 관리적 이슈인 업무절차 평가나 조직에 관한 사항은 26%로 가장 적은 비중을 차지하고 있다. 전반적으로 ISACA는 대단히 광범위한 분야를 포함하고 있고 따라서 감사인은 다양한 환경에서 활동할 수 있도록 정립된 것으로 파악된다. 이러한 포괄성은 감사인이 여러가지 역할을 담당할 수 있다는 측면에서는 바람직하나 실질적인 전문적 경력으로서의 경쟁력이 의문시될 수 있다. 즉 보안 같은 분야만 하더라도 보안 전문가를 양성하고 인증하는 프로그램이 따로 있으며, 공학적 분야 역시 기술분야별로(즉 데이터베이스, 네트워크 등) 다양한 전문가들을 양성하는 프로그램이 있다. 이러한 점에서 상당히 많은 분야를 포함하고 있으나 이러한 분야들의 지식들을 단순히 혼합한 것 이외에 감사라는 측면에서 새로운 기술요소가 개발되어 첨가되었는지는 여부는 확실치 않다.

2.2 일본시스템감사

일본은 시스템감사제도를 국가적 차원에서 수립하였으며 지속적으로 인력을 양성하고 산업을 육성하고 있다. 일본 시스템감사는 정보시스템의 신뢰성, 안전성, 효율성의 향상을 도모하고 정보화사회의 건전화에 이바지하기 위한 것을 목적으로 하고 있으며, 감사의 일관성을 유지하기 위해 시스템감사기준을 제정하여 고시하고 있다. 감사의 목적 중에서 신뢰성은 정보시스템의 품질과 장해의 발생, 영향범위 및 회복의 정도를 의미하고, 안전성은 정보시스템을 자연재해, 부정 접근 및 파괴행위로부터 보호하는 정도를, 효율성은 정보시스템의 자원활용 및 비용대효과의 정도를 뜻한다. 이러한 정의에서 보듯이 일본의 시스템감사도 주로 보안과 안전성에 중점을 두고 있으며, 이러한 이유는 일본의 환경적 요인 즉 잦은 지진, 홍수 등에 기인한 것으로 보인다.

일본의 시스템감사기준은 일반기준, 실시기준, 보고기준으로 구성되어 있으며 각 항목별 세부 내용은 다음과 같다. 일반기준은 ISACA의 표준과 같이 감사인이 지켜야 할 일반적인 기준을 제시하고 있다. 실시기준은 감사인이 실제로 감사를 수행할 때 고려해야 할 감사 항목들을 제시하고 있으며, 보고기준은 감사인이 감사 수행 후 작성해야 되는 보고서와 사후조치에 대해 설명하고 있다.

일반기준

체제

감사

시스템감사인의 책임.권한

직업윤리

비밀엄수 의무

실시기준

기획업무: 정보전략, 전체계획, 개발계획, 시스템분석.요구 정의

개발업무: 개발순서,시스템설계, 프로그램설계. 프로그래밍, 시스템시험, 이행

운영업무: 운용관리, 입력관리, 데이터관리, 출력관리, 소프트웨어관리, 하드웨어관리, 구성관리, 건물.관련 설비관리

보수업무: 보수순서, 보수계획, 보수의 실시, 보수의 확인, 이행(전환)

공통업무: 문서관리, 진척관리, 요원관리, 외부위탁, 재해대책

보고기준

보고서 작성

보고

후속조치

일본의 시스템감사기준에서 정한 분야를 분석해 보면 대체로 일반기준과 보고기준은 감사절차에 속한 내용이고, 감사내용에 관한 사항은 실시기준에 포함되어 있다. 실시기준은 크게 공학적인 사항 즉 기획, 개발, 운영, 유지보수를 포함하고 공통업무는 관리적인 사항을 축약하여 포함하고 있다. 감사내용을 ISACA와는 달리 정보시스템의 주요 프로세스(개발, 운영, 유지보수)와 관리 측면으로 국한한 것은 더욱 전문성을 갖게 할 수 있으며 따라서 감사인으로서의 독자적 경쟁력이 더욱 뛰어날 수 있을 것으로 보인다. 일본의 시스템감사는 국제표준인 ISO/IEC12207 "software life cycle"의 영향을 받아 대폭 수정한 것으로 대체로 일반적인 감사절차에 ISO/IEC12207의 내용을 접목한 것으로 보인다.

2.3 품질시스템 감사

정보시스템감리의 정의 중에는 감리가 추구해야 할 목표로 효율성, 효과성 및 안전성으로 명시하고 있으며 이러한 사항 중에서 개선이 필요한 사항을 권고한다고 되어 있다. 그러나 우리가 개선을 목표로 한다면 현재의 상태를 파악하고 정해진 개선의 목표가 있어야만 개선의 방법을 찾아내게 된다. 흔히 우리는 우리가 구축하고자 하는 시스템 목표를 "요구사항"이라는 문서로 작성하며 구축된 시스템이 얼마나 잘 요구사항을 만족하는지 여부를 기초

로 시스템의 수준을 평가하게 된다. 이러한 개념은 기본적으로 품질의 개념과 동일하다. 흔히 품질은 다음과 같이 정의된다.

- *ISO8402 Quality Vocabulary*
  The totality of features and characteristics of a product or service that bear upon its ability to satisfy stated or implied needs
- Juran, J. M
  Fitness for purpose or use
- Feigenbaum, A, V.
  The total composite product and service characteristics of marketing, engineering, manaufacture and maintenance through which the product and service in use will meet the expectation by the customer
- Crosby, P. B.
  Conformance to requirements

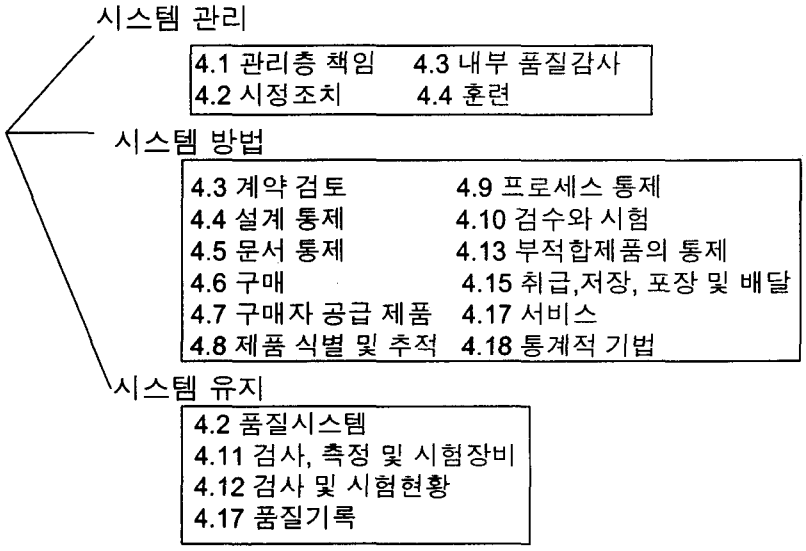
위의 정의에서 보듯이 품질은 사용자의 요구를 만족시키는 것이며, 서비스나 프로덕트 모두에 해당되고 또한 사용자의 요구를 문서화하여 문서화된 요구사항을 준수하는 것 등이 주요한 개념으로 정의되고 있다. 이러한 품질의 개념은 다양한 산업 분야에 적용이 되어 왔으며 특히 프로세스 중심의 품질은 ISO9000의 광범위한 적용으로 크게 보급되었다. 프로세스 품질의 기본적인 입장은 제품이나 서비스를 생산하는 과정이 우수하면 그 과정에서 나오는 최종 결과물인 제품/서비스 역시 우수할 것이다라는 것이다. 또한 프로세스의 품질을 단계적으로 향상하여 점차적으로 좋은 품질의 제품이나 서비스를 제공할 수 있게 된다는 측면도 강조되고 있다.

품질은 기본적으로 기업의 발전을 위해 필수적인 요소이며, 기업의 모든 분야가 품질에 영향을 받으므로 관리기능(기획, 조직, 동기화, 통제)는 품질은 추구하는 방향에서 수행되어야 한다는 입장을 취하고 있다. 따라서 조직은 최고경영자가 공식적으로 선언하는 품질과 관련된 활동의 방향과 전반적으로 품질에 대한 의향을 품질방침으로 작성하여 대내외적으로 알리게 된다. 품질관리는 품질방침을 결정하고 구현하는 전반적인 관리기능을 말하며 ISO9000은 다음과 같은 기능들을 제시하고 있다.

- 마아케팅과 시장조사
- 설계/명세 공학과 제품 개발
- 구매
- 프로세스 기획과 개발
- 생산
- 검사 및 시험

- 포장과 보관
- 판매와 배포
- 설치와 운영
- 기술적 지원과 유지
- 사용후 폐기

품질관리는 품질시스템을 구현하여 수행되게 된다. 품질시스템이란 조직의 활동 전반에 걸쳐 품질이 보호되고 향상되고 있는지를 보증하기 위해 관리층에 의해서 수립된 조직 구조, 절차 등을 말한다. 품질시스템은 시스템관리, 시스템방법, 시스템유지 요소로 구성되어 있다.



품질의 개념은 소프트웨어 분야에서도 적용되어 많은 연구가 수행되었다. 그러나 제조업 중심으로 수립된 ISO9000표준은 소프트웨어 분야에 직접 적용하기에 어려운 점이 있었다. 우선 제조업 중심의 제품과 정보화시대의 꽃인 소프트웨어 제품과는 특성에서 큰 차이가 있다. 즉 제조 제품의 경우 품질의 흔히 1000개를 생산할 때 불량률이 어떤가 하는 것에 초점을 맞추나 소프트웨어 제품은 설계와 구현이 어렵지 동일한 제품을 다량 생산하는 것 즉 복사하는 것은 어렵지 않다는 것이다. 이러한 차이점이 소프트웨어 제품의 경우 품질의 의미에 소프트웨어 공학적인 측면이 반영되어야 한다는 주장을 설득력 있게 하였다. ISO는 이러한 문제점을 인식하고 ISO9000-3을 발표하였다. 그러나 이 표준 역시 소프트웨어 공학적인 이슈가 충분히 반영되지 못했다는 지적을 받고 있다.

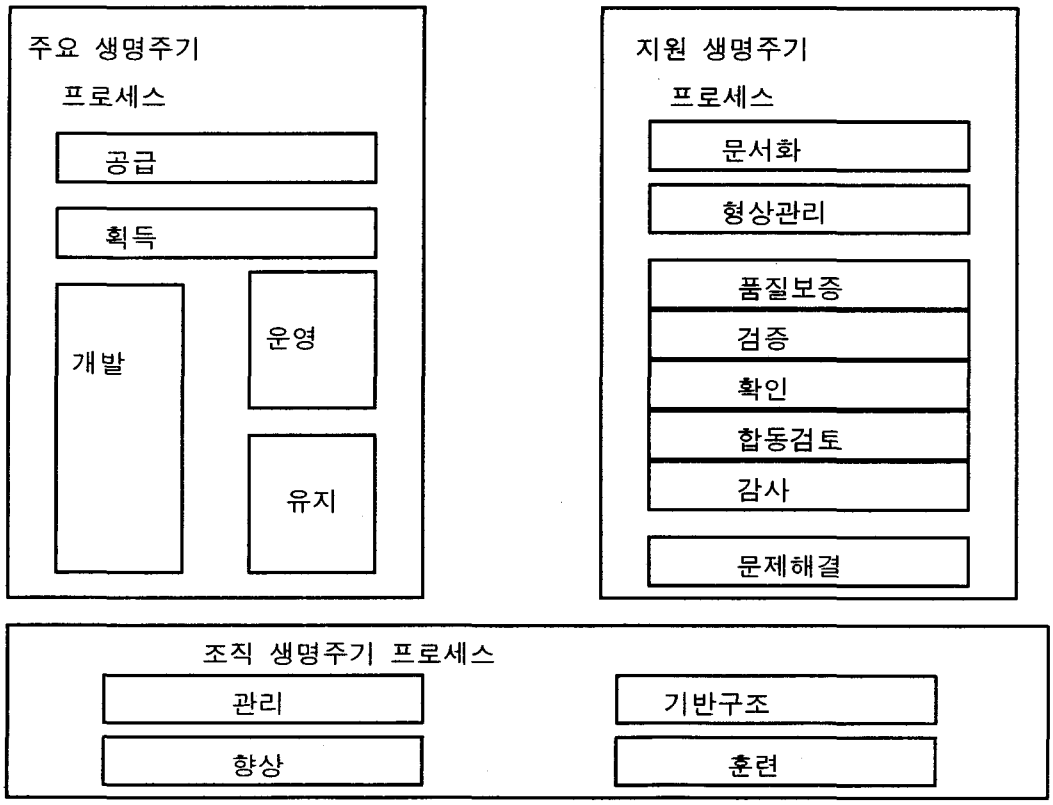
또 다른 측면은 소프트웨어는 일반 제조업이 기초하고 있는 학문인 물리, 화학 등과 같은 기초과학과는 달리 최근에 발달된 학문분야이며 따라서 아직까지도 소프트웨어에 대해 모르는 것이 많이 있으며 품질시스템이 요구하는 많은 사항은 제대로 수행하기 어려운 점이 있다는 것이다. 소프트웨어 공학 분야는 지금도 많은 변화를 겪으며 진화하고 있으며 기초과학과 같이 체계적인 이론이 구성되지 못하였다. 이러한 미성숙성은 품질시스템을 정

확하게 소프트웨어 분야에 적용하기에 어려운 걸림돌로 작용하고 있다.

실제로 소프트웨어 분야에서 ISO9000 인증은 그 효과성이 적지 않음에도 불구하고 감사인이 구현방법에 혼란을 겪고 있는 것으로 알려지고 있고, 또한 이러한 틈을 타서 인증기관이 적은 비용으로 인증을 남발하는 사태까지 발생하고 있다. 이러한 문제는 피감사기관에 많은 혼란을 초래하면서 유용성 문제까지 제기되고 있는 것이 현실이다.

2.4 소프트웨어 감사

품질에 대한 표준화와 병행하여 소프트웨어 공학 전문가 그룹(ISO/IEC JTC1 SC7)은 소프트웨어 공학 개념에 기초한 표준화를 추진하였고 그 중에서 특히 주목할만한 연구는 ISO/IEC12207 "Software Life Cycle Processes" 표준이다. ISO12207 은 소프트웨어 생명주기 프로세스에 대한 공통 체계이며, 소프트웨어를 포함하는 시스템의 구매, 공급, 개발, 운영, 유지보수에 적용되는 프로세스, 활동, 타스크를 정의하고 있다. 또한 소프트웨어 생명주기 프로세스의 아키텍처를 기술하고 있으며, 다만 활동/타스크의 구현방법은 기술하지 않고 있다. ISO12207의 사용은 양자간 계약(또는 비공식적 협약) 상황시 사용될 수 있도록 작성되었으며. 특정 생명주기 모델이나 개발방법을 규정하지는 않고 있다. 그러나 본 표준의 사용자는 특정 생명주기 모델을 선택하고, 이를 본 표준에서 정하는 프로세스/활동/타스크와 비교하여 준수성을 검증하도록 권고하고 있다. ISO12207은 소프트웨어 대한 프로세스를 아래 그림과 같이 정의하고 있다.



주요 생명주기 프로세스는 소프트웨어 생명주기의 근간을 이루는 프로세스로 소프트웨어를 필요로 하는 획득자와 이를 공급하는 공급자의 프로세스가 있다. 이 두 가지 프로세스는 계약관점을 나타내고 있다. 개발, 운영, 유지보수는 소프트웨어의 실제적인 생명주기 단계를 나타내며 개발과 유지보수는 공학적 관점을, 운영은 운영자의 관점을 나타낸다. 지원 프로세스는 주요 프로세스를 지원하는 프로세스로 각 주요 프로세스에서 필요한 지원 프로세스를 선택하여 적용하게 된다. 마지막으로 조직 프로세스는 조직 자체의 향상을 위해 필요한 프로세스들을 식별하고 있다.

ISO12207의 중요성은 정보시스템에서 가장 중요한 요소인 소프트웨어에 대해서 일반적으로 중요하게 인식되는 프로세스를 식별하고 적용 가능한 수준으로 정리하였다는 점이고, 또한 감사를 중요한 하나의 프로세스로 명시하고 있다는 점이다. ISO12207은 감사를 다음과 같이 정의하고 있다.

> " Conducted by an authorized person for the purpose of providing an independent assessment of software products and processes in order to assess compliance with requirements"

위 정의에 따르면 감사는 독립적인 심사활동이며, 요구사항의 만족여부를 심사하기 위해 프로덕트와 프로세스를 모두 심사하는 것으로 되어 있다. 프로세스 측면의 심사는 ISO12207을 기본으로 하여 수행할 수 있다. 즉 특정 프로젝트에서 사용하는 프로세스가 ISO12207을 만족하는지를 검토하고, 적용된 프로젝트 프로세스가 실제로 운용되고 있는지 또한 문제점은 없는지를 검토하고 개선을 권고할 수 있게 된다.

프로세스의 성숙도는 품질과 밀접한 관계를 가질 수 있으며, 따라서 단계별로 높은 수준의 프로세스를 구현하는 것이 바람직 할 경우도 있다. 이와 같이 프로세스의 향상 측면을 고려할 경우에는 SEI에서 개발한 CMM이나 ISO의 표준인 SPICE를 기본 모델로 사용할 수 있을 것이다(SEI. 1998). 그러나 어떤 프로세스 모델을 기반으로 하든 상황과 환경에 따라 창의성을 방해하지 않으면서 동시에 효율적인 프로세스를 적용하도록 하는 것이 바람직하다. 따라서 감리인은 다양한 프로세스 모델에 대한 지식과 경험이 있어야 할 것이다.

프로덕트의 평가는 프로세스와는 달리 아직 많은 연구가 더 필요한 분야이다. 기본적으로 사용되는 국제문서는 ISO/IEC9126과 같은 문서이나 아직 적극적인 활용은 미진한 편이다. 감리의 입장에서 프로덕트 평가는 최종적으로 시스템 자체에 대한 평가를 통해 요구사항의 만족 여부를 가린다는 측면에서 매우 중요하다. 또한 프로덕트 평가를 통해 기술성과를 측정하게 되고 이는 바로 기성관리와 연결되게 되므로 정확한 프로덕트 평가는 전반적인 프로젝트 관리에서 중요한 역할을 담당한다. 프로덕트의 올바른 평가를 위해서는 소프트웨어 척도와 시험에 대한 지식이 필요하다.

3. 정보시스템감리 지식분야

정보시스템감리는 일종의 프로젝트로 볼 수 있으며, 따라서 정보시스템감리에 대한 관리 방법은 프로젝트관리의 방법을 따르는 것이 타당하다. 즉 정보시스템감리는 매우 단순한 작업을 반복적으로 수행하는 것이기 보다는 매번 생소한 내용이 포함되며 또한 최종 결과물에 대한 불확실성이 높은 전형적인 프로젝트관리의 대상인 것이다. 따라서 정보시스템감리의 관리에 대한 지식체계는 일반적으로 사실상의 표준으로 인정되고 있는 PMI의 PMBOK(Project Management Body of Knowledge)를 기초로 하는 것이 바람직하다.

그러나 감리를 실제로 수행할 때에는 프로젝트 대상에 대한 지식이 필요하다. 정보시스템 프로젝트는 정보시스템 관련 기술을 잘 조합하여 사용자가 요구하는 사항에 적합하도록 개발, 운영 또는 유지보수하는 것으로 정보시스템 공학에 관한 기술과 더불어 정보시스템 관리에 관한 지식이 필요하다. 따라서 정보시스템감리는 매우 넓은 분야를 망라하고 이를 통합하여 정보시스템 프로젝트의 조기경보시스템으로서 또한 적정성을 평가하는 역할을 담당하게 되는 것이다.

정보시스템감리의 공통지식체계를 크게는 프로젝트의 관리적 측면과 공학적 측면으로 구분할 수 있으며, 여기에 더하여 감리 프로세스에 대한 지식을 첨가할 수 있다. 각 분야별로 세부 지식분야를 구분하면 아래와 같이 보여질 수 있다.

<관리>
- 프로젝트관리
- 품질관리
- 형상관리

<공학>
- 업무분석
- 소프트웨어 기술
- 데이터 기술
- 기반기술(플랫폼 + 정보통신)
- 보안 기술

<감리>
- 감리절차 및 표준

관리 분야는 프로젝트의 관리 관점에 대한 지식체계를 말하며 일반적인 프로젝트관리를 포함한다. 흔히 프로젝트관리에는 품질관리와 형상관리가 포함되나, 경우에 따라서는 중요성을 강조하기 위해 품질과 형상관리를 따로 독립적으로 구분할 수도 있다. 관리분야에서 가장 기본이 되는 문서는 PMI의 PMBOK를 들 수 있으며, 이 외에도 다양한 프로세스

모델(CMM, SPICE 등)들을 적용하여 프로젝트 관리 능력을 판단 할 수 있다. 프로젝트관리에서 특히 강조되어야 할 측면은 기성관리이다. 기성관리는 비용, 일정 및 기술성과를 통합관리하는 시스템으로 관리적 측면에서 정확한 기성을 찾아내고 계획과 비교하는 것은 매우 중요한 활동이다. 감리는 기성관리시스템의 적정성과 정확성을 판단할 수 있어야 할 것이다.

공학분야에서는 정보시스템의 구성요소별로 지식분야가 구분되어 있다. 업무분석은 정보시스템 개발이나 유지보수시에 가장 기본이 되는 활동으로 enterprise architecture 수립의 초석이 된다. 업무분석을 기초로 필요한 기반구조를 구축하고 소프트웨어와 데이터를 구현하게 된다. 또한 보안 측면의 적절성을 판단하는 것도 포함되어야 한다. 감리인은 정보기술의 각 구성요소를 분석하고 평가할 수 있는 지식을 갖춰야 할 것이다. 특히 프로덕트에 대한 시험 및 평가 기술은 필수적이라 할 수 있다.

마지막으로 감리인은 감리절차 및 표준을 숙지하고 있어야 한다. 감리는 일반적으로 인정된 절차를 준수해야 하며 또한 권위있는 기관에서 발표한 표준들을 준용해야 한다.

참고문헌

정보통신부고시제1999-104호 정보시스템감리 기준

Committee of Sponsoring Organizations of the Treadway Commission (CSOTC). 1992. *Internal Control - Integrated Framework (COSO Report).*

Institute of Internal Auditors Research Foundation (IIARF). 1991, revised 1994. *Systems Auditability and Control*

Information Systems Audit and Control Foundation (ISACF). 1995. *COBIT: Control Objectives for Information and related Technology.*

SEI, *SW-CMM,* http://www.sei.cmu.edu, 1998.