정보시스템 감리품질 향상을 위한 자동화된 위험평가 기법

안상임° 이우진 정기원
숭실대학교 대학원 컴퓨터학과
siahn69@ssu.ac.kr°, bluewj@dreamwiz.com, chong@computing.ssu.ac.kr

Automatic Risk Assessment Method for Improvement of Information System Audit Quality

Sangim Ahn°, Woojin Lee, Kiwon Chong
Department of Computing, Graduated School, Soongsil University

요 약

감리는 정보시스템의 품질을 향상시키기 위한 일련의 활동들 중 하나로 독립된 제3자가 정보시스템 구축 및 운영에 관련된 각종 위험 및 통제 상태를 점검하고 평가하여 개선이 필요한 사항을 권고하는 것이다. 그러나, 대부분의 평가가 감리인의 전문적 경험 및 주관적 판단에 의존한 정성적 방법으로 수행되고 있어 중요한 위험을 간과할 문제점을 내포하고 있다. 이에 따라, 본 논문에서는 다양한 비정형 산출물을 DTD와 스키마를 포함한 XML 메타 모델인 표준포맷을 생성 후 단계별 및 통합적 방법으로 의미분석을 실시하여 자동으로 위험요소를 식별하고 평가할 수 있는 위험평가 프레임워크, 위험평가 모델, 위험평가 기준을 제안한다. 이와 같은 시스템화된 감리품질 개선기법을 통하여 추출된 결과는 감리인에게 사전에 전달됨으로써 감리노력과 일정을 절약할 수 있어 효율적인 감리수행 및 효과적인 감리결과가 보장된다.

1. 서 론

비즈니스 환경이 다양해지고 제품 및 서비스의 부가가치를 높여 마켓플레이스에서 경쟁적 우위를 선점하기 위한 IT의 의존도가 지속적으로 심화됨에 따라 국내외 많은 기업들은 IT에 대한 투자를 대폭 늘리고 정보자원들을 효과적으로 관리하고자 많은 노력을 기울이고 있다. 감리는 이러한 정보자원의 품질을 향상시키기 위한 일련의 활동들 중 하나로 독립된 제3자가 정보시스템 구축 및 운영에 있어서 효율성, 효과성, 안정성을 증진시키기 위하여 각종 위험 및 통제 상태를 점검·평가하고 개선이 필요한 사항을 권고하는 것이다.

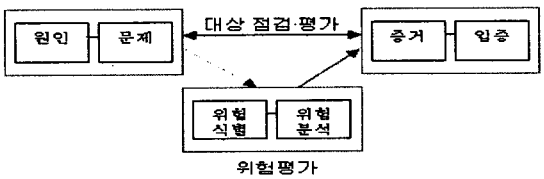
그러나, 대부분의 감리가 관련 지침을 근거로 하여 산출물 및 행위에 대한 평가를 감리인의 전문적 경험 및 주관적 판단에 의존한 정성적 방법으로 수행되고 있어 대형 프로젝트 및 운영 감리를 수행 시 점검범위를 잘못 추정하거나 점검항목을 누락하여 중요한 위험을 간과할 문제점을 내포하고 있다. 이를 개선하기 위하여 본 논문에서는 주요한 위험을 식별하는 방법을 시스템화하여 사전에 감리인에게 전달함으로써 효율적인 감리수행 및 효과적인 감리결과를 추출할 수 있는 방안을 제안한다.

2. 관련 연구

2.1 감리 프로세스

감리 프로세스는 ISO/IEC 12207 및 IEEE Std. 1028-1997에 정의된 정보시스템 감리를 수행하기 위한 절차이다. 본 논문에서는 감리대상에 대한 위험을 사전에 평가하여 해당부분을 중점적으로 점검함으로써 감리품질을 향상시키기 위하여 기존 감리 프로세스에 위험기반 접근방법을 추가하여 적용한다[1][2].

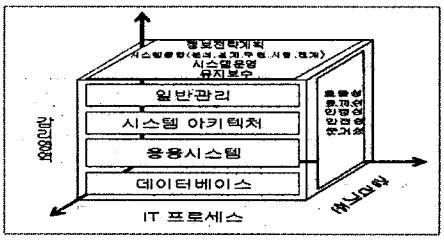
- 감리영역 이해
- **감리대상 위험 평가**
- 감리계획 수립
- **감리대상 점검·평가**
- 감리결과 보고
- 사후보고



[그림 1] 위험기반 평가 프로세스

2.2 감리 프레임워크

정보시스템 평가를 위한 감리 수행관점은 감리영역, 프로세스, 평가기준으로 구분할 수 있다. 감리영역은 시스템 아키텍처, 응용시스템, 데이터베이스 등의 정보기술부문과 범위관리, 일정관리, 형상관리, 품질관리 등의 일반관리부문이 해당되며, 프로세스는 정보시스템 구축·운영에 관련된 모든 절차로 전략계획(ISP), 시스템통합(SI), 시스템운영(SM), 유지보수(MA)로 나눌 수 있다. 평가기준은 감리영역 및 프로세스를 대상으로 표준기준, 지침, 절차 등에 따른 수행여부를 효율성, 효과성, 안정성, 안전성, 준거성 등에 근거하여 점검하는 부문이다[3].



[그림 2] 감리 프레임워크

2.3 감리품질 활동

감리활동의 효과성을 향상시키기 위한 감리품질 연구가 다양한 관점에서 시도되었다. [4]는 평가항목 선별을 위하여 전문가를 대상으로 설문조사를 실시하고 가중치에 따라 항목을 정비 및 정량화하였으며 감사결과를 관리할 수 있는 시스템을 구현하였으나 평가방법은 여전히 정성적 방법에 의해 실시되었으며 사후관리 중심의 한계를 가지고 있다. [5]는 감리 프로세스와 프레임워크에 대하여 체계화를 시도하였으나 ASP(Application Service Provider)산업에 국한된 제약사항을 보유하고 있다. [6]은 감리제도 및 문제점을 품질측면으로 검토하였으나 구체적인 해결방안을 제시하지 못했다. [7]은 정보통신부에서 주관한 연구로 감리결과의 신뢰성을 높이기 위해 평가요소를 세부적으로 도출하였으나 측정방법이 정성적이라는 한계를 벗어나지 못했다.

[표 1] 감리품질 연구활동 비교 평가

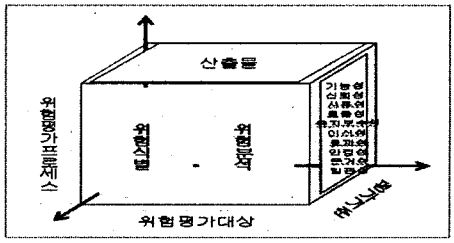
감리연구 활동 구분 / 비교항목	본 논문 활동	기존 연구 활동[4][6][7]
위험요소 평가시점	감리시작 前	감리시작 後
측정항목 선정	표준준수, 중점항목 선정	설문실시, 주관적 판단
감리수행 방법	정량적 방법에 정성요소 추가	정성적 방법에 정량요소 추가
기타	위험기반 평가방법 적용	특정업무에 적용[5]

3. 자동화된 위험평가 방안

기존연구가 평가기준 선별 및 사후관리에 제한된 점을 해결하기 위하여 본 논문에서는 위험평가 프레임워크, 모델 및 기준을 만들어 감리수행 전에 내재된 위험을 자동으로 식별 및 분석할 수 있는 시스템화된 감리품질 개선방안을 제안한다[8][9].

3.1 위험평가 프레임워크

위험평가 프레임워크는 기존 감리 프레임워크를 기반으로 위험평가 요소를 반영하여 위험평가 프로세스, 위험평가 대상, 위험평가 기준으로 구성한다. 위험평가 대상은 IT 프로세스 동안 생성된 모든 산출물을 대상으로 하며 평가기준은 ISO/IEC 9126에 정의된 품질평가 항목에 안전성, 준거성, 일관성 항목을 세분화하여 적용한다. 프로세스는 평가대상에 대하여 위험을 식별하는 부문과 분석하는 부문으로 구분한다.



[그림 3] 위험평가 프레임워크

3.2 위험평가 모델

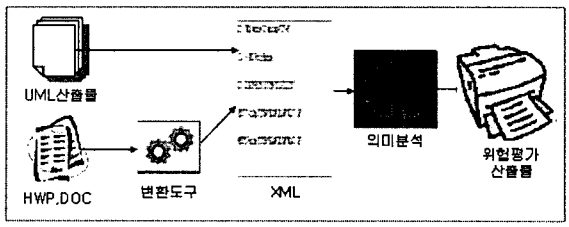
최근 정보시스템의 많은 산출물이 비정형 전자문서로 제공되는 바, 이를 DTD와 스키마를 포함한 XML 메타 모델로 변환하여 표준포맷을 생성 후 단계별 및 통합적 방법으로 의미분석이 가능하도록 위험평가 모델을 형성한다.

(1) 표준포맷 생성방법

대량의 비정형 텍스트 문서를 구조화된 전자문서로 표현하고 처리하기 위한 표준으로 사용되는 XML을 이용한다.

■ UML 산출물 : 요구사항 분석, 설계 단계 등에서 UML로 작성된 산출물은 모델링 도구를 이용하여 XML 파일로 변환한다.

■ 기타 산출물 : 기타 산출물은 텍스트 도구로 DTD 템플리트 문서를 생성 후 XML 변환 도구를 이용하여 XML 파일을 생성한다.



[그림 4] 위험평가 모델

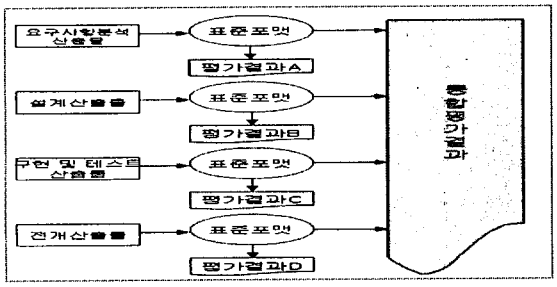
(2) 의미분석 방법

의미분석은 XML 파일들에 포함된 내용의 논리적 상관관계(Logical relatedness), 복잡도(Complexity), 응집도(Cohesion)를 감안하여 평가기준 측정치를 이용해서 적정여부를 평가한다.

(3) 부문별 평가방법

■ 단계별 평가방법 : IT 프로세스 단계마다 생성된 산출물에 대하여 표준포맷을 생성 후 평가기준의 적정성을 분석한다.

■ 통합적 평가방법 : 단계별로 생성된 표준포맷에 대하여 상호관계에 대한 의미분석을 실시한다.



[그림 5] 부문별 위험평가 모델

3.3 위험평가 기준

위험평가 항목은 ISO/IEC 9126 평가기준에 내부지침의 준수여부, 최근 강조되는 보안부문, 통합적 관점에서 산출물 변경 및 반영을 점검하기 위한 일관성 부문을 추가하여 적용한다.

■ **기능성**은 정보시스템이 필요로 하는 모든 기능을 갖추고 있는가를 평가하는 것으로 소프트웨어 개발 시 사용자의 요구사항과 분석 및 개발단계 등의 산출물을 비교하여 평가한다.

■ **신뢰성**은 정보시스템의 기능들이 안정적이며 의도한 대로 작동하며 문제발생시 해결대책이 정의되었는가를 산출물을 통하여 점검하고 시스템에 적용여부를 평가한다.

■ **효율성**은 정보시스템이 구동될 때 자원사용량 대비 적절한 성능을 제공하도록 방안이 제시되었는가를 산출물을 통하여 점검하고 통합테스트 실시여부 및 결과를 평가한다.

■ **사용성**은 정보시스템이 사용될 때 사용자가 이해하고 학습하고 사용하는데 용이한가를 평가하는 것으로 화면구조, 도움말 기능을 산출물을 통하여 점검하고 시스템에 적용여부를 평가한다.

■ **유지보수성**은 소프트웨어 변경에 따른 유연성을 보유하였는가를 재사용 기능의 반영여부로 평가한다.

■ **이식성**은 하드웨어, 소프트웨어, 네트워크 등의 환경이 변경되었을 경우를 감안하여 설계 및 개발되었는가를 산출물을 통하여 점검하고 시스템에 적용여부를 평가한다.

■ **안전성**은 정보시스템이 내·외부의 인가 받지 못한 침입으로부터 보호되는가를 점검하는 것으로 파일 업로드시 바이러스 점검 및 중요 자료의 암호화 등의 반영여부를 평가한다.

■ **준거성**은 표준기준 및 지침들과 내부규정, 법적 규제 등의 등의 반영여부를 평가한다.

■ **일관성**은 정보시스템 구축·운영과 관련된 전체 프로세스에 대해 승인되지 않은 변경은 없었으며 변경부분이 산출물 및 시스템에 적절히 반영되었는가를 평가한다.

[표 2] 위험 평가기준별 계량화된 측정요소 예제

평가기준	측정요소
기능성	# of adequate function
신뢰성	# of system crash, Recovery Time
사용성	# of request for help, Learning Time
효율성	Quantity of Memory, CPU and Disk
유지보수성	# of component reuse
이식성	# of constraint during implementation
안정성	# of data exposure during intrusion test
일관성	# of mismatch before and after

4. 결론 및 향후 연구

본 논문에서는 기존 감리가 감리인의 경험 및 주관적 판단에 의존한 정성적 방법으로 수행되어 중요한 위험을 간과할 문제점을 내포하고 있는 바, 이를 해결하기 위하여 위험평가 프레임워크, 모델, 기준을 만들어 감리수행 전에 내재된 위험을 자동으로 식별 및 분석할 수 있는 시스템화된 감리품질 개선방안을 제안하였다. 따라서, 본 논문에서 추출된 결과를 활용하면 감리노력과 일정을 절약하므로 효율적인 감리수행 및 효과적인 감리결과를 기대할 수 있다. 향후 연구에서는 제안된 위험평가 모델에 적용할 측정요소를 세분화하고 구현과 관련된 연구가 진행될 것이다.

참고문헌

[1] IEEE," Standard for Software Reviews," pp.25~30,1997

[2] ISACA, " COBIT Audit Guidelines," 1996

[3] 한국전산원 " 정보시스템감리기본점검표 개선," 2003

[4] 권대권 외, " 감리정보시스템의 설계 및 구현," 2000

[5] 문영준 외, " ASP모델을 위한 감리 프로세스," 2002

[6] 나종원, " 정보시스템 감리 품질향상에 관한 연구," 2002

[7] 선우종성, " 정보시스템 감리결과의 평가방안," 2004

[8] Amrit Tiwana, Mark Keil, " The One-Minute Risk Assessment Tool," Communication on ACM, pp73~77,2004

[9] Issa Traore, " Enhancing Structured Review with Mode-Based Verification," IEEE Transactions on SE, 2004