EDI감사를 위한 의사결정시스템의 개발

이상재
한국과학기술원 테크노경영대학원 박사과정
(sjlee@msd.kaist.ac.kr)
한인구
한국과학기술원 테크노경영대학원 부교수
(ingoohan@msd.kaist.ac.kr)

본 연구에서는 EDI감사를 위한 의사결정지원시스템을 개발하였다. EDI감사를 위한 의사결정지원시스템은 통제, 위험, 회사의 개요, 테스트 항목등의 데이타를 저장한 데이타베이스 시스템에 기반을 두고 있다. 시스템개발을 위하여 E-R(Entity-Relation) 및 DFD(Data Flow Diagram)분석을 통해서 논리적인 설계를 하였다. 시스템 개발은 데이타베이스팩키지인 FoxPro를 사용하였다. 이 시스템을 통해서 감사인이 필요한 테스트 결과를 조회하거나 저장할 수 있고 통제, 위험, 회사등의 상호조회를 통하여 필요한 통제나 위험정도를 쉽게 조회해 볼 수 있다. 회사마다 필요한 통제, 위험, 테스트 항목등의 체크리스트가 달라지는 경우에 이 시스템을 통해서 입력 저장하여 각각의 회사에 대해 다른 체크리스트를 저장하여 놓을 수 있다. 본 시스템은 EDI감사뿐만 아니라 일반 EDP감사분야에도 적용가능할 것이다.
EDI환경하에서는 전통적인 감사증적이 없음으로 인해 전통적 방식에 의한 EDI감사는 적합하지 않게 된다. EDP감사시스템분야의 국내 연구가 전무한 실정에서 EDI감사를 지원하는 시스템의 개발을 시도하였으며 앞으로 이 분야의 연구가 활성화하리기를 기대한다.
본 연구는 EDI의 보안 및 감사업무의 효율성을 높이고 EDI에 대한 위험에 효율적으로 대처하는데 기여할 수 있을 것이다. 그리고 이러한 보안 및 감사기법과 통제모형을 지식베이스로 구축해서 실제의 위험노출상황에서 보안을 위한 통제방안이 여러가지가 있는 경우에 비용/편익 분석, 효율성, 회사방침 및 법률적인 문제등을 고려해서 최적의 보안통제 및 감사기법을 선택하는 것을 지원할 수 있을 것이다.

I. 서 론

EDI(Electronic Data Interchange)는 경제적 거래 당사자들이 사업상의 문서를 공공이나 산업상의 표준형식에 따라 통신회선을 통해서 컴퓨터간에 주고 받는 것을 가능하게 하는 시스템으로서 표준형식, 변환소프트웨어, 데이타통신연결의 세가지로 구성된다.

EDI는 사업환경에서 문서전달과 처리에 드는 비용, 문서기입으로 인한 시간낭비, 자료입력의 실수로 인한 손해를 줄이고 궁극적으로 고객에 대한 서비스를 향상시킴으로써 경쟁력을 제고시킬 수 있다. 이러한 장점으로 인해 급속히 확산되고 있으며 이에 따라 EDI의 활용에 따른 위험도 증가하고 있다. EDI를 효과적으로 활용하기 위하여는 EDI의 위험을 평가하고 이에 대처할 수 있는 보안통제를 개발하고 유지하여야 하며 적절한 감사기법 및 절차를 선택하여 적용하여야 한다.

감사분야의 의사결정시스템연구는 회계감사분야의 의사결정지원시스템연구가 대부분을 차지하고 있다. EDP감사분야의 의사결정지원시스템 연구는

논문 접수일 : 95. 11 게재확정일 : 97. 11

Hansen and Meisser(1987)의 연구등 비교적 최근에 이르러서 이루어지고 있다. EDP환경하에서의 감사는 전통적인 수작업환경에서의 감사와는 기법 및 절차등에서 상당한 차이가 있다. 더구나 EDI는 조직간에 구현되는 자동화된 정보통신시스템으로서 이의 보안 및 감사에 대한 관심은 일반적인 다른 정보시스템에 비해서 상당히 높은 것으로 여러 문헌에서 제시됐다. EDI를 통하여 기업간의 법률적 계약이 이루어지는데 보안상의 문제는 기업간의 분쟁을 유발할 수도 있다. 사람의 개입이 없이 이루어지는 자동화된 시스템으로서 오류의 영향이 다른 응용시스템으로 파급되는 영향이 높게 나타날 것이다. EDI의 위험을 억제하고 보안성을 높이기 위하여 EDI에 대한 감사의 중요성이 크며 이를 지원하는 컴퓨터시스템의 개발이 필요하다고 할 수 있다.

EDI의 보안 및 감사업무의 효율성을 높이기 위하여는 데이타나 시스템의 보안문제를 진단해 주거나 적절한 통제절차를 제시하는 의사결정지원시스템을 구축하는 것이 필요할 것이다. 컴퓨터감사분야의 전문가시스템이나 의사결정시스템에 대한 연구는 아직 초보적인 단계이다. 지능형 의사결정지원시스템(Intelligent DSS)은 지식베이스를 활용하여 반정형적(semi-structured) 또는 비정형적(unstructured)인 의사결정을 지원하는 의사결정지원시스템이라 할 수 있다. 이러한 지능형 의사결정지원시스템은 모형에 관련된 지식과 데이타가 함께 활용되는 구조를 가지고 있다. 본연구에서는 EDI의 감사나 보안문제에서 발생되는 비정형적인 감사의사결정을 내릴 때 EDI의 보안 및 감사담당자가 활용할 수 있는 의사결정지원시스템을 개념적으로 설계하고 프로토타입 시스템을 개발할 것이다. 또한 지능형 의사결정지원시스템으로 발전해 나가기 위한 개념적 틀을 제시할 것이다.

II. 문헌연구

회계감사분야의 전문가시스템 활용에 관한 연구인 William and Edward(1989)는 내부감사인이 예를 들면 현금흐름의 관리나 부서가 경영정책이나 예산을 준수하는지 등에 관한 감사를 할때 전문가시스템이 활용될 수 있다고 주장했다. 또한 내부감사에 관한 규칙생성과 관리를 중심으로 전문가시스템을 구축할 때 필요한 고려사항을 제시했다. Bailey et al.(1987)는 감사분야의 전문가시스템에 대한 연구는 제품개발을 위한 것과 기본적인 연구목적을 가지고 있는 것으로 구별하고 있고 전통적인 인간정보처리 방법론을 인공지능 연구기술과 결합해서 새로운 전문가시스템 연구접근법을 제안하여 인간정보처리모형을 연구했으며 전문가 시스템 접근법을 구현하기 위해 필요한 몇가지 방법론을 제시했다.

그리고 Messier and Hansen(1987)은 감사환경이 복잡해지면서 보다 효율적인 감사기술을 추구하게 되고 감사인간에 의견의 조정 그리고 감사인의 의사결정과정의 연구를 위해서 감사분야의 전문가시스템의 연구가 필요하다고 주장했으며 이러한 논거는 여러 연구에서도 제기되었는데 주장했으며 이러한 논거는 여러 연구에서도 제기되었는데 그중에서 Grace(1985)에 의하면 감사분야는 수치적인 데이타를 이해해고 해석을 내리며 많은 경험을 요구하고 복잡하고 대안이 많기 때문에 일관된 지식을 제공하는 전문가시스템이 적합한 분야라고 제시하였고 전문가 시스템은 내부통제를 지원하고 감사

기준을 지식베이스로 구축할수 있으며 감사인에게 훈련을 제공하는등의 이점을 가지는 것으로 보았다. Mai and Paul(1989)는 감사분야의 전문가 시스템 적용시 장점 및 단점을 보다 구체적으로 제시했다. 즉 전문가시스템을 통해서 감사분야 지식의 확장, 전문화, 노동 및 훈련비용 감소, 질적 향상, 빠른 의사결정과 반복적인 의사결정의 지원, 기술의 전파, 지식의 축적등의 효과를 이룰 수 있고 반대로 비용 및 법률적 문제나 감사지식에 관하여 전문가들간의 동의를 구하는 문제, 시스템의 기계적인 수용이나 경시하는 태도등을 단점으로 제시했다. Steinbart(1987)는 감사 계획단계에서 중요도(materiality)를 판단하는 전문가 시스템을 연구하였는데 중요도 판단과정을 중요도를 계산하기 위한 기반설정과 그러한 기반을 통해서 중요도를 계산하여 적절한 확률을 설정하는 두가지 단계로 이루어진다고 보았다. 그리고 고객의 성격, 고객의 미래계획, 재무제표에 대한 요구의 인지도에 따라서 그러한 기반과 확률설정에 영향을 미친다고 주장했다. Han and Choi(1993)은 감사분야의 전문가시스템을 개발하는데 있어서 적절한 대상감사업무를 선정하는 것이 중요하고 이를 선정하는 체계적인 방법으로서 평가특징을 사용하는 것과 가중시스템을 제안했다.

정보시스템감사를 위한 소프트웨어에 있어서 미국이 가장 높은 수준의 기술을 보유하고 있다. 1980년대부터 많은 정보시스템감사용 소프트웨어가 개발되기 시작하였는데 소프트웨어하우스들이 개발한 범용감사소프트웨어(GAS: Generalized Audit Software)로서 ACL(Audit Command Language), Audassist, Audit Analyzer, Audit Reporter등이 있으며 Big-8(현재는 통합으로 인하여 Big-6임)으로 불리우는 초대형 회계법인이 개발한 것으로 Arthur Anderson의 Audex 100, Deloitte Haskins & Sells의 Auditape, Coopers & Librand의 Auditpak II, Ernest & Whitney의 Auditronic등이 있다. GAS외에도 금융기관의 정보시스템감사에 활용되는 CAPS등 산업별 감사소프트웨어도 다수 개발되어 있으며 GAS에서 수행하지 못하는 특수한 감사업무에 적합한 특수감사소프트웨어(SAS: Specialized Audit Software)등도 개발되어 있다. 일본에서도 다수의 감사소프트웨어가 개발되어 활용되고 있다.

Niv and Doretta(1986)는 온라인 실시간 시스템과 같은 진보된 EDP시스템을 감사하는 감 사도구와 기술을 조사했다. 여기에서 동시감사기 법이나 모의실험등의 감사기법을 제시했다. 통합 검사시설(integrated test facility), 스냅사진(sanpshot) 등의 동시감사기법(concurrent audit technique)에 대한 활용은 아직 활성화 되지 못했다(Lawrence, 1988). 감사인의 기술적 능력부족과 그러한 기술을 개발할 자금부족 그리고 이러한 기술은 시스템 개발중에 시스템속에 일부로 포함되어야 하는데 시스템 설계단계에서 이에 대한 고려가 이루어지지 않은 점등이 주요원인으로 제시됐다.

Steve(1989)는 가장 위험도가 큰 PC를 선택하고 그것의 위험을 전문가 시스템을 통해서 평가하는 PC보안문제를 사례를 통해서 소개했다. PC의 위험도를 입력되는 데이타의 중요도에 따라서 전문가 시스템이 민감도 분석을 수행할 수 있음을 보였다. William and Carver(1990)은 EDI의 통제를 EDI의 구현과 유지, 데이타와 프로그램, 파트너와의 협정등에 관한 일반 통제(general control)와 입력의 전부성(completeness)과 정확성, 거래의 인가등에 관한 응용통제(application control)

로 나누어서 통제방안을 제시했다.

감사분야의 의사결정지원시스템에 관한 연구로서는 감사인이 내부통제시스템을 모형화하기 위해서 모의실험 프로그램을 사용하는 것이 있는데(Burns and Loebbecke, 1975). SIMSCRIPT와 같은 모의실험 프로그램을 사용해서 EDI의 통제시스템을 모델링하여 메시지 전송이나 변환소프트웨어의 내부통제의 신뢰도를 모의실험할 수 있을 것이다. Dijk and Williams(1990)에 의하면 준거성 검증을 위한 전문가시스템은 EDI와 같은 전자적 데이타만이 존재하는 시스템의 감사의 경우에 효과적 감사 시스템이 될수 있다. 또한 EDI와 같은 통합시스템인 경우에 여러 응용시스템의 감사를 통합하는 통합감사가 중요하고 이것이 이루어지면 모든 감사의 병목 현상이 제거될 수 있다고 하였다. 내부통제와 관련된 전문가시스템으로서는 INTERNAL - CONTROL - ANALYZER(Gal 1985)가 있다. 이 시스템은 목표의 계층구조를 가지고 있는데 최고 상위의 목표는 회계통제의 질이고 그 다음 목표는 모집단통제, 업무분장, 정확성통제이다. 모집단통제에는 완전성통제와 승인통제가 있고 정확성통제에는 비교와 수학적 통제가 있다. 계층적 분류모형을 가지는 전문가시스템으로서는 AUDITOR (Dungan and Chandler, 1985), EDP-XPERT(Hansen and Meisser, 1986b), Internal Control Analyzer(Gal and McCarthy, 1985), ICES(Grundnitsdki, 1986), AUDIT-PLANNER (Steinbart, 1987)등이 있다.

Choi(1994)는 감사의사결정과정이 선택적 주의과정(selective attention), 가설검정을 통한 전진적 추론과정(forward chaining), 복수의 지식원천등의 요소를 포함한다고 지적하였다. 이러한 논리에 따라 붉은 깃발(red-flagging)모형을 제시하였는데 이는 감사인들이 다양한 지식원천을 나타내는 블랙보드(blackboard) 구조로부터 필요한 지식을 도출하여 결론을 제시하는 모형이다. 이 모형은 전통적인 계층적 지식분류모형을 통한 추론의 계산적 복잡성이 커지는 것을 극복할 수 있다고 하였다.

Deliso et al.(1994)는 감사위험을 측정하는 전문가시스템을 개발했다. 위험요소(risk factor)와 시험목록(library of tests)를 서로 관련시켰다. 이 시스템은 위험의 정도와 오류의 유형의 중요도에 따라서 감사계획을 제시할 수 있게 되어 있다. 이러한 감사계획안을 선정하는 것은 배낭(Knapsack)알고리듬을 사용했고 프레임구조를 사용하여 위험요소, 에러유형, 테스트항목등을 저장했다. 이러한 프레임의 관계는 슬롯(slot) 값으로 저장되어 있고 점수계산등은 데몬(demon)에 의해 계산되게 했다. 이 시스템은 개발 후에 사용자에게 설문지등을 통해서 평가과정을 거쳤다.

Morris(1994)는 사례기반추론(case-based rea- soning) 방법을 사용하여 시스템통제 방안을 제시하는 시스템을 구축했다. 이것은 GOLDWORKS II라는 전문가시스템 개발도구를 사용해서 개발되어 졌다. 이 시스템은 사례를 저장해서 문제에 대한 비슷한 사례를 도출하고 새로운 사례를 계속 저장하는 시스템이다. 이 시스템은 종래의 지식기반적 시스템이 규칙을 추론하는 과정에서 문제가 복잡한 경우 추론이 길어지면서 사용자가 추론과정을 추적하기가 어렵다는 단점을 극복했다고 주장했다. 산업유형, 응용시스템유형, CPU유형에 따라 위험과 내부통제가 달라진다고 주장하고 이에 따라 사례를 구축했다. 비슷한 유형의 사례가 한개 이상인 경우는 운영체제, 보안 소프트웨어의 존재여부, 시스템 부서의 크기등의 여

러 요소의 유사성을 체크한 순위(rank)를 각 사례별로 부여해 가장 큰 유사성을 가진 사례를 찾아낸다.

관계형 의사결정지원시스템에 관한 연구로는 Lefons et al.(1989)의 연구가 있는데 사용자로 하여금 다양한 원천으로부터 들어온 데이타를 〈 데이타, 의미(semantics) 〉로 정리하여 다양한 데이타에 대한 의미통합(semantic integration)을 가능하게 하였다. 여기서 의미는 사용자의 데이타에 대한 분류이다. 이러한 관계형 데이타베이스에 기반을 둔 의사결정지원시스템은 실행모듈, 질의편집기, 데이타편집기등으로 구성되어 있으며 과학분야의 분산데이타베이스시스템으로 개발되었다. Suh (1989)는 관계형 의사결정지원시스템의 대화기능에서 하나의 베이스를 별도로 개발할 필요가 있다고 하였다. 이러한 대화베이스외에 모델베이스나 데이타베이스의 기능이 필요하다고 하고 이러한 세가지 베이스를 통합해서 관리하는 의사결정관리시스템을 제안했다. 이러한 대화베이스는 메뉴방식의 대화를 저장하고 새로운 뷰(view)를 만들수 있도록 하여 최적의 질의를 찾아주는 기능을 가지고 있다.

De and Sen(1988)은 조직의 내부통제를 데이타베이스시스템 설계시에 제약조건으로 고려하는 문제를 연구했다. 이러한 내부통제에 대한 모델링은 EDI통제에 대한 모델링으로 응용시킬 수 있겠다. 내부통제를 모델링하기 위해 세단계 구조로 된 구조를 제시했는데 논리적인 모형을 〈객체, 과업, 통제〉의 쌍으로 표현하는 방법이다. 객체를 모델링하는 것은 E-R(Entity-Relationship)모형과 비슷하게 속성을 가진 객체와 그것들의 관계를 표현하는 것이고 과업을 모델링하는 것은 어떤 프로세스를 ESD(Event State Diagram)로 표현하는 것이다. 통제를 모델링하는 것은 데이타객체간의 관계를 어떤 형태로 나타냄으로써 표현된다.

Everest and Weber(1977)는 "사건"중심의 회계시스템을 개발하는데 있어서 관계형 데이타베이스이론을 적용시켰다. De and Sen(1984)는 사건상태(Event State)모형을 사용해서 프로세스를 모형화시켰다. 여기서 사건은 어떤 일이 발생하는 것으로서 예를 들면 주문이 도착한다든지와 같은 것이다. Peters and Lewis(1989)는 내재위험(inherent risk)을 측정하기 위한 지식기반모형을 제시했다. 내재위험은 여러 요소에 의해서 판단할 수 있겠는데 이런 요소들에 대한 지식베이스를 구축해서 위험을 평가하는 것이다.

EDP감사용 전문가시스템으로서 Hansen and Meisser(1986b)은 EDP-XPERT를 개발했다. 이 시스템은 고급의 EDP시스템에서 통제의 신뢰성을 평가하는 것으로서 133개의 규칙이 조정의 신뢰성(reliability of supervisory), 입력, 처리, 출력통제의 네가지 목표하에서 만들어 졌다. EDP-XPERT의 규칙베이스는 온라인 시스템, 실시간 시스템, 데이타베이스 시스템의 통제부분을 포함하기 위해 확장되어 왔다. 시스템 사용자에 대한 설문조사결과 어느 정도 사용자들이 전문가시스템의 결론에 영향을 받아서 판단을 내리는 것으로 나타났다. 그리고 Hansen and Messier(1984)는 관계형 데이타베이스를 활용하여 각 위험요인에 대하여 적절한 통제방안을 제시할 수 있는 의사결정시스템을 제안하였다.

감사분야의 개발된 전문가 시스템을 요약하면 〈 표 1 〉과 같다.

〈 표 1 〉 감사분야의 전문가시스템의 현황

시스템	개발자	개발도구	년도	문제영역
AUDITOR	Dungan and Chandler	AL/X	1985	고객 대출에 대한 적정성
INTERNAL-CONTROL -ANALYZER	Gal	EMYCIN	1985	내부통제평가
TICOM	University of Minnesota	PASCAL	1985	내부통제평가
EDP-XPERT	Hansen and Meisser	AL/X	1986	진보된 EDP시스템의 통제의 신뢰성 체크
ExpertTAX	Coopers and Lybrand	QSHELL	1986	기업에 대한 세금 감사계획 지원
ARISC	Meservy, Bailey and Johnson	Galen	1986	내부통제 평가
GC-X	Biggs and Selfridge	LISP	1986	계속적 업무(going-concern) 에 관한 의사결정 지원
AOD	Dilliard and Mutcher	XINFO	1986	감사의견결정
AUDITPLANNER	Steinbart	EMYCIN	1987	중요도(materiality) 평가지원
CFILE	Peat, Marwick, Mitchell & Co.	INSIGHT2	1988	은행 대출손실 측정
PLANET	Deliso, McGrowan and Walter	JOSIE	1994	감사위험 측정과 계획
ICE1	Choi	C. M.1	1994	내부통제평가

III. 논리적인 설계

EDI와 같이 고급의 시스템은 감사에 있어서도 고급의 기술을 필요로 한다. 전통적인 감사기술은 고도의 통제를 하는데 부적절하다. EDI 감사를 지원해 줄 수 있는 관계형 데이타베이스를 이용한 의사결정지원시스템의 개발을 통해서 감사인이 EDI 통제를 평가하는데 도움을 줄 수 있을 것이다. 이러한 데이타베이스시스템의 필요성을 지지하는 관련 연구로는 Snograss(1982)와 Hansen and Meisser(1984) 등이 있다. Snograss(1982)는 분산시스템을 통제하는 관계형 데이타베이스시스템을 개발했다. 이러한 통제기능에서는 데이타수집기능이 중요하다고 지적하고 데이타 구조, 프로세스, 하드웨어 요소들이 실체이고 프로세서에서 처리되는 처리와 대기하는 메시지등을 관계로 설정했는데 이를 시간적으로 변하는 관계로 제시하였다. 이러한 관계형 데이타베이스 시스템의 질의기능(query)은 TQuel(Quel 보다 범위가 큰)로 작성되었는데 이것은 시간을 중요한 요소로 포함할 수 있는 문법과 의미가 포함된 것이다.

Hansen and Meisser(1984)은 EDP감사를 지원하는 관계형 데이타베이스시스템을 제안했는데 많은 감사인들이 소형컴퓨터를 사용하여 감사를 하므로 소형컴퓨터용 DBMS인 dBASE II로 구현하여 보였다. 이러한 시스템을 통해 시스템에 대한 통제간의 복잡한 관계와 이러한 통제가 취약할 경우에 발생할 위험을 파악할 수 있다. 테스트테이블에서 나온 결과로부터 발생가능한 위험이 어느 것인지 또는 어떤 통제와 관련이 있는 것인지를 통제, 위험, 테스트테이블들에 대한 조인과 프로젝션 과정을 통해 알 수 있게 된다. 반대로 특정 통제 부재시 어떤 위험이 초래되는지도 알 수 있게 된다. 또한 관계형 데이타베이스는 감사인이 이해하기 쉬우며 미리 어떤 식의 모델베이스를 구축할 필요가 없고 단지 질의(query)와 뷰(view)를 정해주면 된다고 하였다. 이점은 감사분석에 상당한 유용성을 제공하는데 이러한 유용성을 관계형 연산이 지원한다. 이러한 시스템에 있어서 문제점으로는 데이타를 수집하는 메커니즘의 설정 문제와 이러한 시스템의 효과가 비용보다 클 수 있다는 것을 지적했다. 후자의 문제는 단지 이 시스템에만 국한된 문제가 아니라 모든 의사결정지원시스템의 개발시 고려되는 문제이기도 하다.

EDI감사용 의사결정 지원시스템은 통제, 위험, 테스트항목, 회사 등과 이들에 대한 관련 데이타를 데이타베이스에 저장하여 감사인이 효과적으로 감사업무를 수행하도록 지원해 주는 시스템이라 할 수 있다. 이러한 관계형 데이타베이스시스템을 통해 관계형 연산(relational algebra)과 질의를 써서 통제, 위험 그리고 테스트에 관한 결과를 알 수 있고 이러한 질의를 하나의 뷰로 정의하여 감사인에게 필요한 모형에 대한 해를 제공할 수 있을 것이다. 즉 위험분석이나 통제방안을 뷰를 통해 그 결과를 제공하는 것이다. 이러한 데이타베이스시스템을 기반으로 간단한 관계연산을 통해 복잡한 통제, 위험항목 및 테스트항목에 대한 자료를 인출함으로써 보다 일관된 감사의사결정을 지원하게 될것이다. Date(1990) 는 뷰가 제공할 수 있는 잇점을 크게 네가지로 제시했다. 첫째, 데이타베이스의 필드나 테이블의 재구성시 논리적 데이타독립성을 제공하고 둘째, 같은 데이타를 다양한 사용자에게 다른 시각으로 볼 수 있게 해 주고 셋째, 사용자는 필요한 데이타만 간편하게 조회하고 네째, 뷰기능만으로 데이타를 접근하도록 사용자를 통제한다면 뷰는 데이타보안의 도구가 된다는 것 등이다. 여기서 뷰의 두번째 장점은 같은 데이타가 관심사항이 다른 사용자이거나 같은 사용자라도 문제상황이 달라지는 경우에 뷰는 이러한 요구사항을 지원하는 도구가 된다는 것이고 관계형 데이타베이스시스템이 의사결정시스템의 기능을 하도록 지원하는 부분이 있음을 뜻한다. 즉 뷰는 Suh and Hirohide (1990)의 세가지 베이스중에 모델베이스의 역활을 할 수 있을 것이라고 기대된다.

EDP감사인들에게는 EDP통제 체크리스트를 제공하는 진보된 수단이 필요하다(Weber, 1980). 관계형 데이타베이스시스템의 설계를 위해서 오스트레일리아 EDI협회(EDICA)와 EDP감사인협회(EDPAA)가 공동으로 편집한 EDI통제 지침서(EDI Control Guide)에서 제시된 통제와 위험의 체크리스트를 기초자료로 했다. 이 책자는 통제와 위험의 체크리스트를 6가지로 분류했다(EDICA and EDPAA, 1991a). 정규화가 되지 않은 예비적 테이블을 설계하면 다음과 같다.

통제(통제#, 통제이름, 통제분류, 통제_설명)
위험(위험#, 위험이름, 위험_설명)

통제_위험(통제#, 위험#, 중요도)
회사(회사코드, 회사이름, 업종, EDI투자액)
통제_회사(통제#, 회사코드, 통제정도, 비용, 통제중요도)
위험_회사(위험#, 회사코드, 위험정도, 손실)
테스트_결과(테스트#, 회사코드, 테스트코드, 날짜, 결과, 결과_설명)
테스트(테스트#, 테스트이름, 테스트설명)
테스트_통제_관리(테스트#, 테스트#1, 테스트분류1)
테스트_통제_응용(테스트#, 테스트#2, 테스트분류2)
테스트_통제_인증(테스트#, 테스트#3, 테스트분류3)
테스트_통제_컴퓨터(테스트#, 테스트#4, 테스트분류4)
테스트_통제_통신(테스트#, 테스트#5, 테스트분류5)
테스트_통제_제3자(테스트#, 테스트#6, 테스트분류6)

정규화를 위해서 일차적으로 속성간의 어떤 의존관계가 있는지를 알아보기 위해서 속성간의 함수종속성을 표시하면 다음과 같다.

통제# ---〉 통제이름, 통제분류, 통제설명
위험# ---〉 위험이름, 위험설명
통제#, 위험# ---〉 중요도
회사코드 ----〉 회사이름, 업종, EDI투자액
통제#, 회사코드 ---〉 통제정도, 비용, 통제중요도
위험#, 회사코드 ---〉 위험정도, 손실
테스트#, 회사코드 ---〉 테스트코드, 날짜, 결과, 결과설명
테스트# ---〉 날짜, 결과, 결과_설명, 통제#
테스트# ---〉 테스트이름, 테스트설명, 테스트#1, 테스트분류1, 테스트#2 테스트분류2, 테스트#3, 테스트분류3, 테스트#4, 테스트분류4, 테스트#5, 테스트분류5, 테스트#6, 테스트분류6
테스트#1 ---〉 테스트분류1
테스트#2 ---〉 테스트분류2
테스트#3 ---〉 테스트분류3
테스트#4 ---〉 테스트분류4
테스트#5 ---〉 테스트분류5
테스트#6 ---〉 테스트분류6

이러한 속성간의 의존성을 제거해서 만들어진 제3차 정규화된 형태(Third Normalized Form)의 테이블을 도시하면 다음과 같다.

통제(통제#, 통제이름, 통제분류, 통제_설명)
위험(위험#, 위험이름, 위험_설명)
통제_위험(통제#, 위험#, 중요도)
회사(회사코드, 회사이름, 업종, EDI투자액)
통제_회사(통제#, 회사코드, 통제정도, 비용, 통제중요도)
위험_회사(위험#, 회사코드, 위험정도, 손실)
테스트(테스트#, 테스트이름, 테스트_설명)
테스트_결과(테스트#, 테스트코드, 날짜, 결과, 결과_설명, 회사코드)
테스트_통제_관리(테스트#, 테스트#1)
테스트_통제_응용(테스트#, 테스트#2)
테스트_통제_인증(테스트#, 테스트#3)
테스트_통제_컴퓨터(테스트#, 테스트#4)
테스트_통제_통신(테스트#, 테스트#5)

테스트_통제_제3자(테스트#, 테스트#6)
테스트_테스트분류1(테스트#1, 테스트분류1)
테스트_테스트분류2(테스트#2, 테스트분류2)
테스트_테스트분류3(테스트#3, 테스트분류3)
테스트_테스트분류4(테스트#4, 테스트분류4)
테스트_테스트분류5(테스트#5, 테스트분류5)
테스트_테스트분류6(테스트#6, 테스트분류6)

최종 정규화된 테이블을 가진 데이타베이스 시스템의 실체관계 모형 및 의미론적 객체모형은 〈 그림 1 〉과 〈 그림 2 〉와 같다.

데이타흐름도를 도시하면 다음과 같다. 크게 회사, 통제, 위험, 테스트등의 객체를 가지고 있다. 먼저 〈 그림 3 〉의 기본다이어그램(context diagram)은 데이타 흐름도를 작성하는데 필요한 기본적인 감사시스템의 기능을 나타낸다.

〈 그림 4 〉는 피감사회사에 대한 체크리스트 작성 및 수정 그리고 점수부여등의 과정을 도시한 데이타 흐름 다이어그램이다.

〈 그림 5 〉는 테스트 결과에 대한 통제, 위험, 그리고 통제-위험 상관관계를 조회하는 과정을 도시한 데이타흐름 다이어그램이다.

다음은 데이타베이스시스템의 뷰의 예이다. EDI 감사를 위해 필요한 정보를 제공하기 위한 뷰에는 테스트 결과와 관련된 통제사항을 알아내는 뷰, 테스트 결과와 관련된 위험사항을 알아내는 뷰, 테스트결과와 관련된 통제-위험상호성을 알아내는 뷰, 테스트 세부번호와 관련된 통제사항을 알아내는 뷰, 테스트 세부분류와 관련된 위험사항을 알아내는 뷰등이 있다. 이러한 뷰를 통해서 통제, 위험, 테스트결과등의 관계를 조회할수 있다.

1) 테스트 결과와 관련된 통제사항을 알아내는 뷰

```
CREATE VIEW CONTROL_TEST
    AS SELECT CONT#, CONTSTATE,
       CONTCOST, CONTIMP, TEST#,
       TESTCODE, RESULT, RESULT_
       DESCR, DATE
    FROM CONTROL_COMPANY, TEST
       _RESULT WHERE TEST_RESULT.
       COMPCODE = CONTROL_
       COMPANY. COMPCODE

SELECT CONT#, CONTSTATE, TEST#,
       TESTCODE, RESULT_DESCR
FROM CONTROL_TEST
WHERE CONT# 〉= 100
AND CONT# 〈= 200 ;
```

2) 테스트 결과와 관련된 위험사항을 알아내는 뷰

```
CREATE VIEW RISK_TEST
     AS SELECT RISK#, RISKSTATE,
        RISKCOST, TEST#, TESTCODE,
        RESULT, RESULT_DESCR, DATE
        FROM RISK_COMPANY, TEST_
        RESULT WHERE TEST_RE-
        SULT.COMPCODE = RISK_
        COMPANY.COMPCODE

SELECT RISK#, RISKSTATE, TEST#,
       TESTCODE, RESULT_DESCR
FROM RISK_TEST
WHERE RISK# 〈 = 200
```

```
AND RISK# ) = 100 ;
```

3) 테스트결과와 관련된 통제-위험상호성을 알아내는 뷰

```
CREATE VIEW CONTRISK_IMP
      AS SELECT CONT#, CONTSTATE,
         CONTCOST, CONTIMP, IMPOR-
         TANCE, TEST#, TESTCODE,
         RESULT, RESULT_DESCR, DATE
      FROM CONTROL_COMPANY, TEST
         _RESULT,CONTROL_RISK
      WHERE TEST_RESULT. COMPCODE
         = CONTROL_COMPANY. COMP-
         CODE
       AND CONTROL_RISK.CONT# =
         CONTROL_COMPANY.CONT# ;

SELECT CONT#, CONTSTATE, IMPOR-
      TANCE, TEST#, TESTCODE, RE-
      SULT_DESCR
FROM CONTRISK_IMP
WHERE IMPORTANCE = 'VERY HIGH';
```

4) 테스트 세부번호와 관련된 통제사항을 알아내는 뷰

```
CREATE VIEW TEST_DETAIL#_CONTROL
      AS SELECT CONT#, CONTSTATE,
         CONTCOST, CONTIMP, TEST#,
         TEST#1, TESTCODE, RESULT,
         RESULT_DESCR, DATE
      FROM CONTROL_COMPANY, TEST_
         RESULT, TEST_CONTROL_
         MGT
      WHERE TEST_RESULT. COMP-
         CODE = CONTROL_COMPANY.
         COMPCODE
       AND TEST_RESULT.TEST# =
         TEST_CONTROL_MGT.TEST#

SELECT CONT#, CONTSTATE, TEST#,
      TEST#1, TESTCODE, RESULT_
      DESCR
FROM TEST_DETAIL#_CONTROL
WHERE CONT# )= 100
AND CONT# (= 200 ;
```

5) 테스트 세부분류와 관련된 위험사항을 알아내는 뷰

```
CREATE VIEW TESTCLASS_RISK
    AS SELECT RISK#, RISKSTATE,
       RISKCOST, TEST#, TEST#1,
       TESTCLASS, TESTCODE, RESULT,
       RESULT_DESCR, DATE
     FROM RISK_COMPANY, TEST_
       RESULT, TEST_CONTROL_MGT,
       TEST_TESTCLASS1
     WHERE TEST_RESULT.COMPCODE
       = RISK_COMPANY.COMPCODE
        AND TEST_RESULT.TEST# =
       TEST_CONTROL_MGT.TEST# ;
    AND TEST_CONTROL_MGT.TEST#1
       = TEST_TESTCLASS1.TEST#1
```

```
SELECT RISK#, RISKSTATE, TEST#,
       TEST#1, TESTCLASS, TESTCODE,
          RESULT_DESCR
FROM TESTCLASS_RISK
WHERE RISK# < = 200
AND RISK# > =100 ;
```

IV. 시스템 개발

데이타베이스 시스템은 개인용 데이타베이스시스템 개발소프트웨어인 FoxPro 2.5에 의해서 개발되었다. 기본적인 기능은 통제, 위험, 회사, 테스트 테이블의 입력, 수정기능, 이들 테이블의 상호조인(join)을 통한 상호조회기능, 보고서 작성 및 출력기능이다. 보다 다양한 기능 및 사용자 인터페이스 등이 추가되어야 할것이다.

〈 그림 6 〉은 초기화면과 기본적인 메뉴화면을 제시하고 있다.

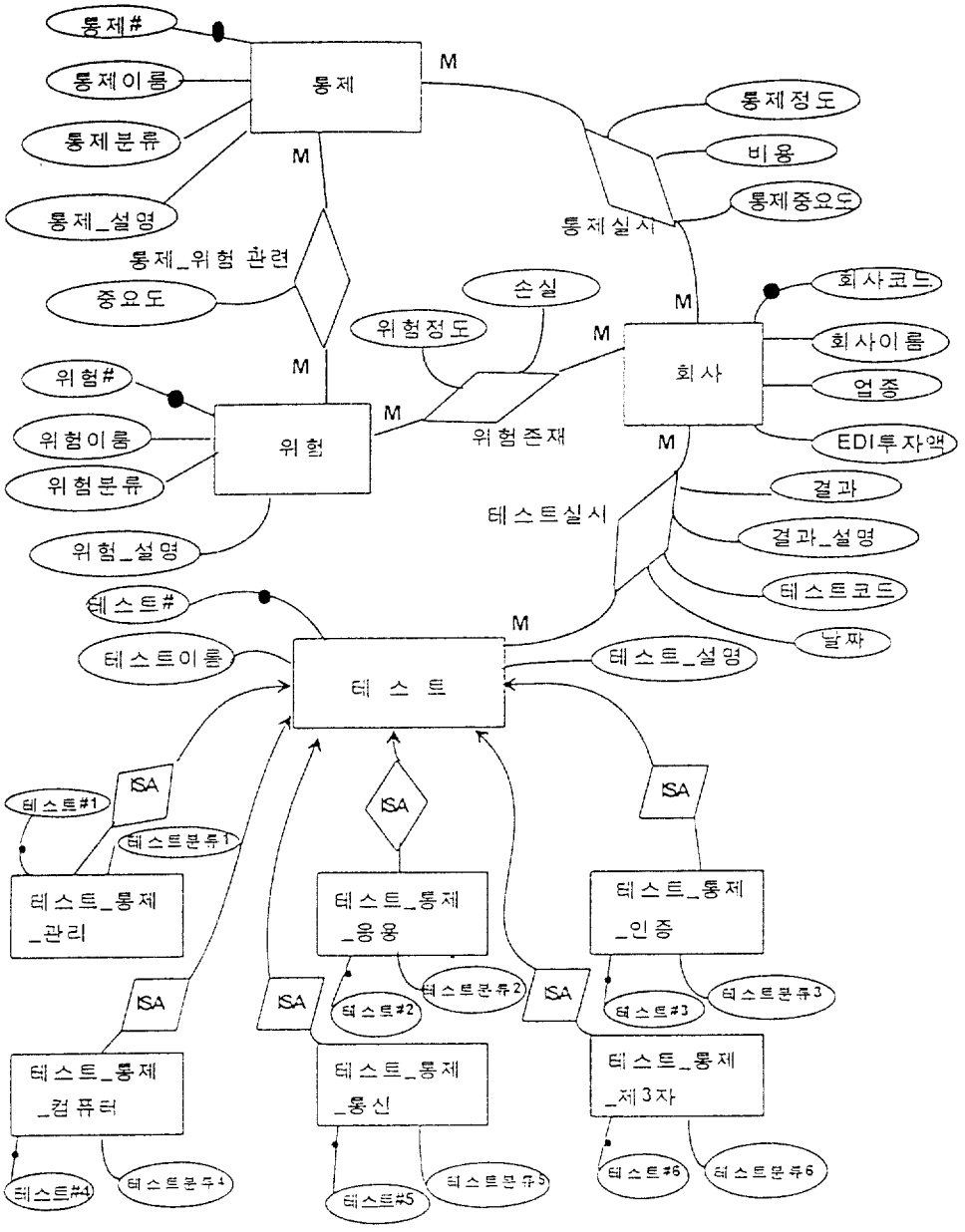
〈 그림 7 〉 은 시스템에서 생성되는 몇몇 테이블의 예를 보여준다.

V. 지능형 의사결정지원시스템의 개념적 틀

이 시스템은 데이타베이스시스템으로 개발되었으나 모델 및 규칙베이스 부분을 첨가시키면 지능형 의사결정지원시스템이 될 수 있을 것이다. 이와 같은 지능형 의사결정시스템의 구조가 〈 그림 8 〉에 제시되어 있다. 이러한 규칙베이스의 예로서 가능한 위험상황에 대한 통제방안이 무엇인지에 관한 규칙을 생각할 수 있다. 이러한 규칙은 UNIK-RULEGEN과 같은 자동 규칙생성도구에 의해 개발되어 질 수 있다(이재규, 1994). EDI통제위험과 가능한 통제방안에 관한 규칙을 생성하는 것을 UNIK-RULEGEN에 의해 보이기 위해서 지식분석도를 먼저 제시하면 〈 그림 9 〉, 〈 그림 10 〉, 〈 그림 11 〉과 같다. 이것은 가능한 위험에 대해 통제방안을 제시하는 규칙을 〈 표 2 〉에 제시된 상관 관계에 따라 만들기 위한 것이다. 〈 표 2 〉는 EDICA and EDPAA(1991a)에서 분류한 통제와 위험리스트를 통제와 위험 관련성 규칙을 생성하기 위해서 서로 관련시켜 놓은 것이다. 우선 〈 그림 9 〉는 개괄적인 지식분석도이다. 특히 여기서는 관리통제에 대한 위험과 통제방안을 나타낸다. 〈 그림 10 〉과 〈 그림 11 〉은 응용, 네트워크통제 각각에 대한 위험 및 위험에 대한 통제방안을 나타낸다. 각각 위험과 통제사항에 대해서는 편의상 문자 및 숫자를 사용해서 간략히 표기했다. 생성된 규칙의 예는 다음과 같다.

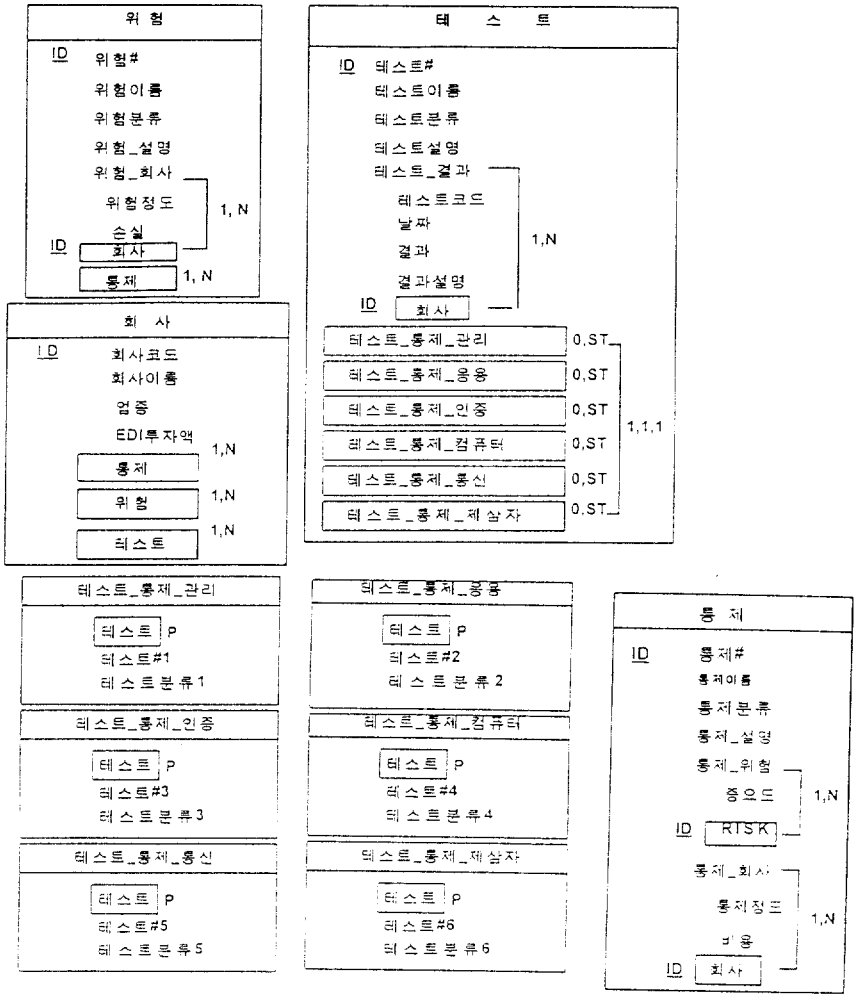
```
(TITLE '"EDI Auditing EXPERT System")
(GOAL "Control_Risk")

(Rule Rule110
IF
   (IS "다음 중 어떤 통제를 감사하겠습니까?"
    '"제3자 네트웍(VAN) 통제")
   (IS "제3자 네트웍(VAN) 보안통제에서 다음
    중 어떤 사항을 감사하겠습니까?" '"메일 박
    스 및 네트웍 데이타 보안")
   (IS "메일 박스 및 네트웍 데이타 보안에 관
    하여 다음 중 어떤 사항을 감사하겠니까?"
    '"제3자에 의해 제공된 네트웍 및 메일 박
```



주) ● : 객체와 속성을 연결하는 선의 검정 동그라미는 주키(primary key)임

〈그림 1〉 실체관계 모형



〈그림 2〉 의미론적 객체모형(Semantic Object Model)

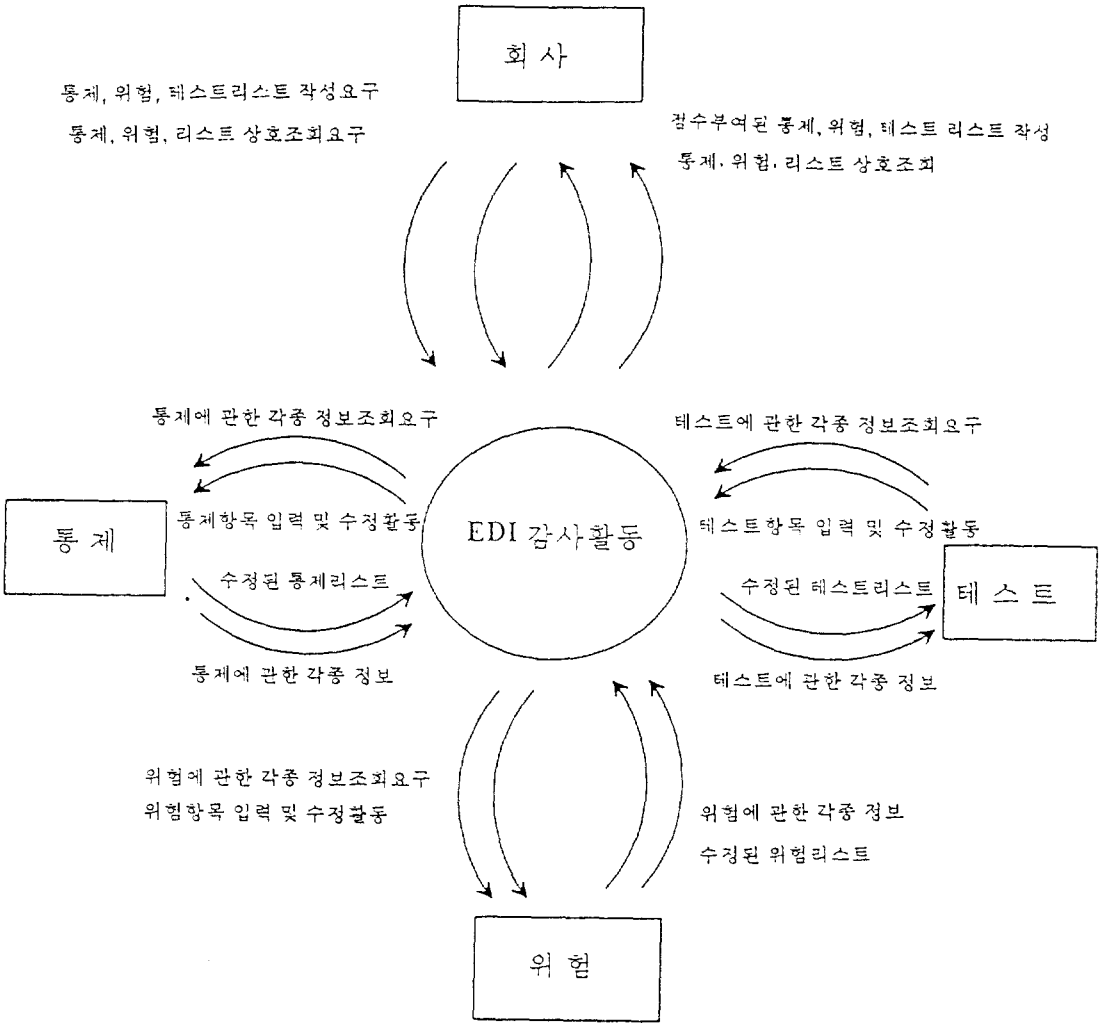
주) 1) Dewitz and Olson(1994)의 의미론적인 객체모형에 기반을 둠

2) 1, N(0, N 및 1, 1 등) : 한 객체의 원소(instance)가 다른 객체의 원소에 대해 관계를 맺을 수 있는 최대 및 최소 원소수(예: 위험 객체의 하나의 원소에 대해 최소 한개이상(1, N) 통제객체 요소가 관련된다)

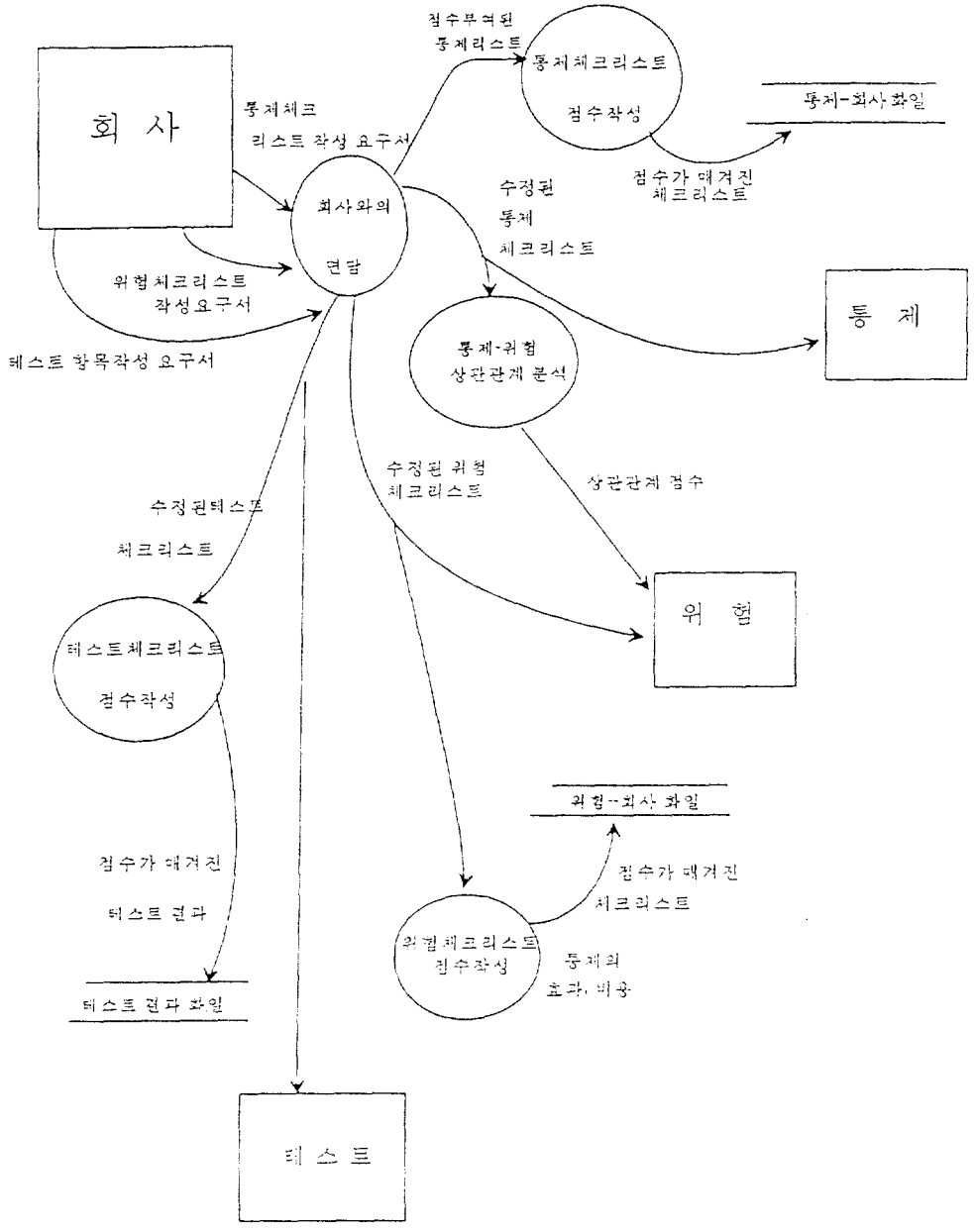
3) 0, ST : 앞의 숫자는 그 객체의 최소 한 필요한 원소수이고 뒤의 ST는 하위객체(subtype)임을 표시

4) P : 객체가 상위(parent)객체임 표시

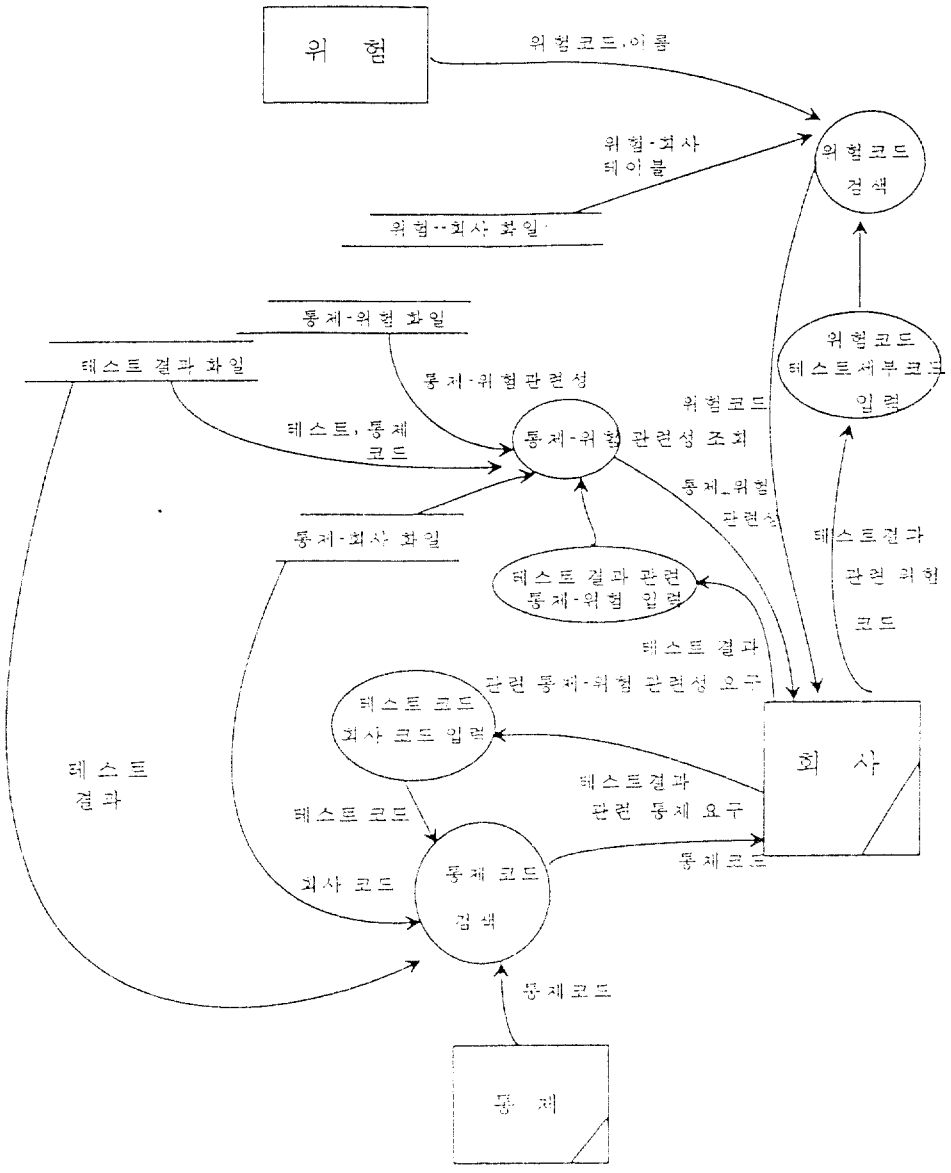
5) 1, 1, 1 : 제일 처음 숫자는 각각의 상위객체의 원소에 대해서 적어도 하나의 하위객체의 원소가 존재한다는 것이고(0이면존재할 필요가 없음) 두번째 및 세번째 숫자는 각각의 상위객체의 원소에 대해서 관계를 맺을 수 있는 최소 및 최대로 원소수(예: 테스트객체의 각각의 원소는 6개의 하위객체중 하나에 반드시 속하고 반드시 한개의 하위객체 원소값을 갖는다)



〈그림 3〉 기본다이어그램(Context Diagram)

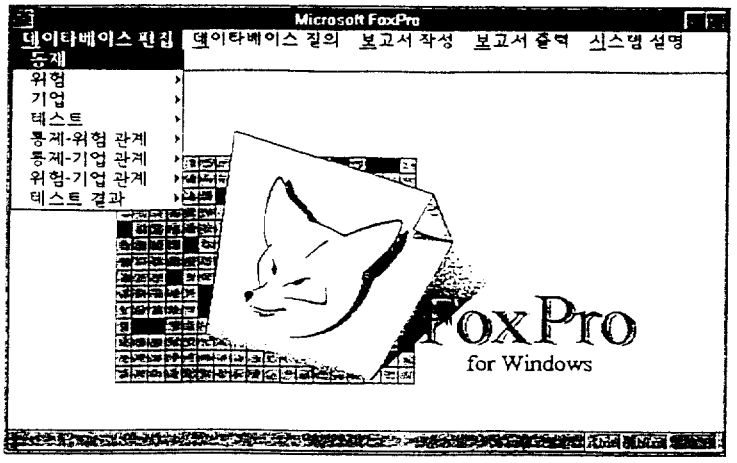


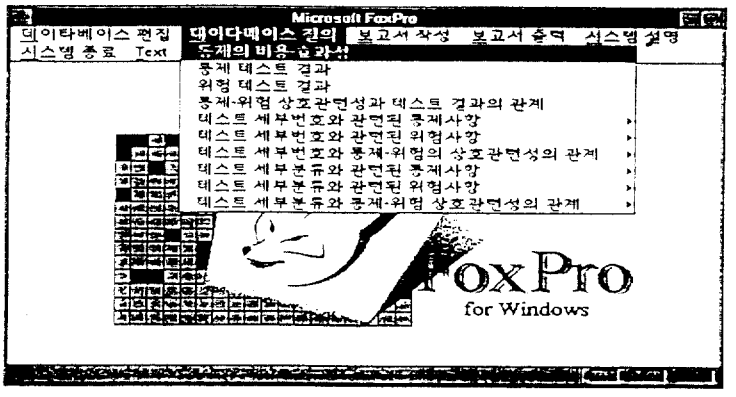
〈그림 4〉 수준 1 (level-1) 데이터흐름 다이어그램(DFD) : 체크리스트 작성

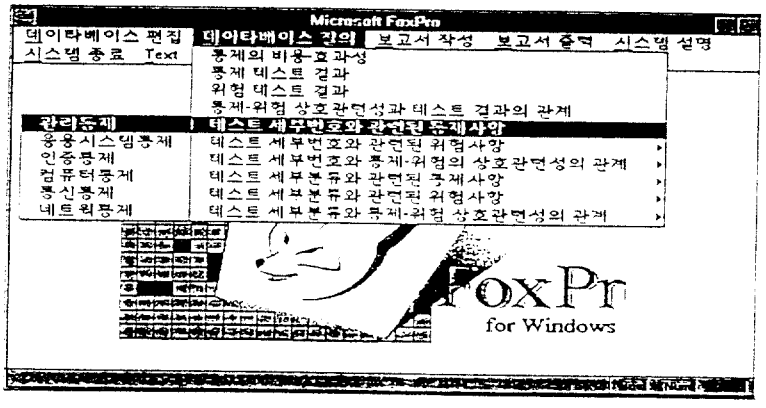


〈그림 5〉 수준 1 DFD : 테스트 결과에 대한 통제, 위험, 그리고 통제-위험 상관관계 조회

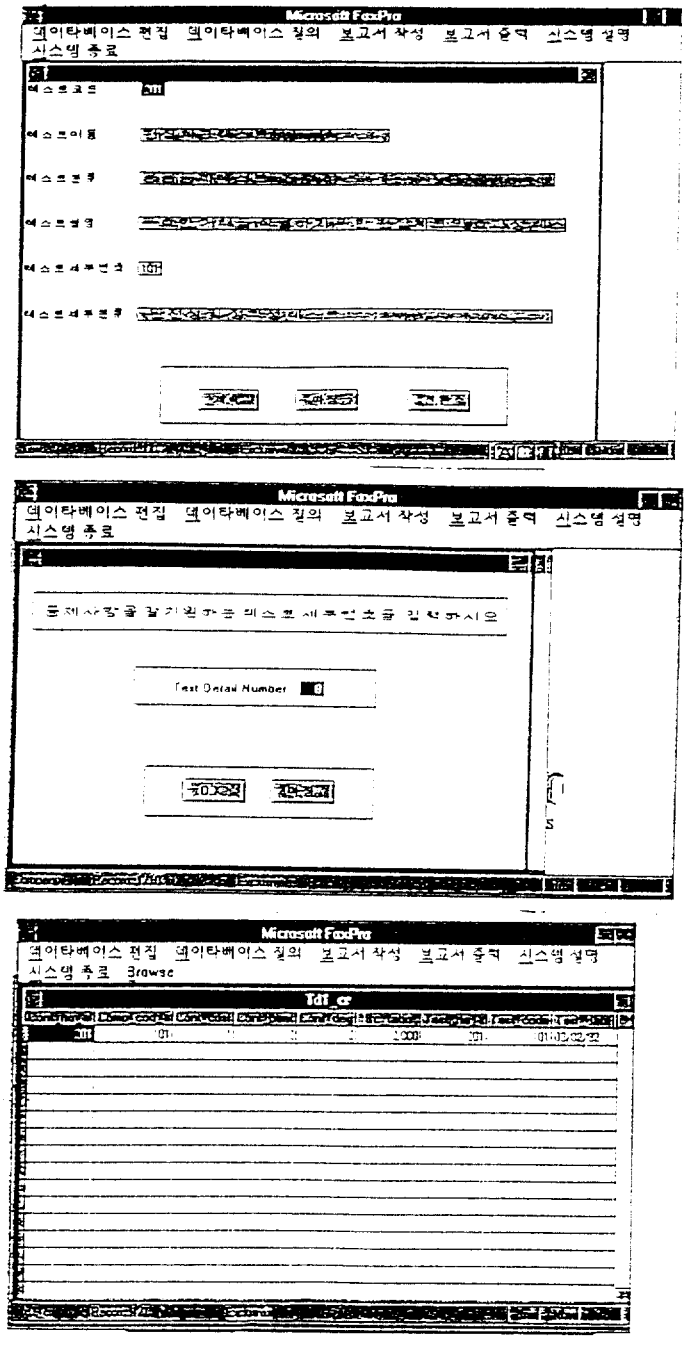
주) 본 DFD는 전체 DFD의 일부분으로서 회사와 통제의 객체 기호에 붙인 빗금은 그 객체가 다른 DFD에 이미 존재하고 있음을 시사함.







〈그림 6〉 시스템 초기 및 메뉴화면



〈그림 6〉 시스템 초기 및 메뉴화면(계속)

〈그림 7〉 몇가지 테이블의 입력 혹은 출력된 예

■ 통제(통제#, 통제이름, 통제분류, 통제_설명)

통제#	통제이름	통제분류	통제_설명
110	EDI 대표	EDI 계획 및 관리	EDI산업에 대표단을 파견
120	EDI 계획	EDI 계획 & 관리	EDI실행을 계획하고 기존의 시스템과의 통합이 되도록 함
420	논리적 접근 제한	컴퓨터에 대한 보안	EDI에 논리적 접근이 제한됨
670	제3자 체킹	제3자 보안	메시지 체킹과 서비스 비용책정에 관한 정보가 제3자로부터 전달되어야 함
231	화일 연속성	응용 통제	응용시스템으로 전달되기전에 화일이 보전되어야 함

■ 위험(위험#, 위험이름, 위험분류, 위험_설명)

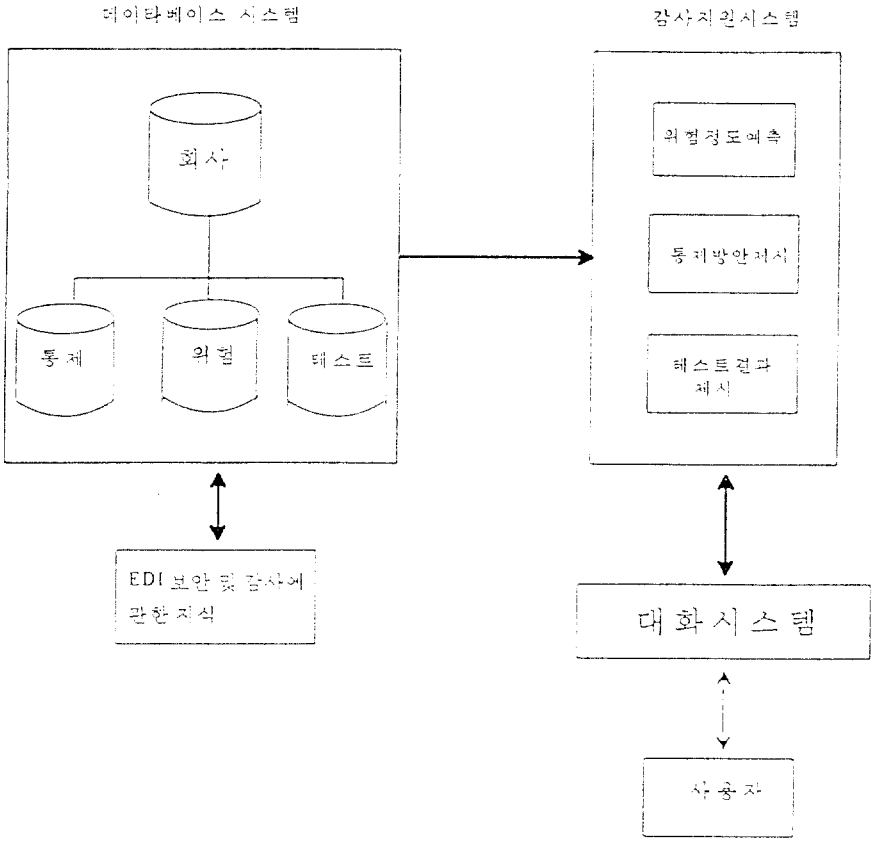
위험#	위험이름	위험분류	위험_설명
211	거래 오류	응용통제위험	거래파트너로부터 송신된 거래의 유실 및 중복
320	데이타의 비인가가 되어 있음	인증통제위험	거래데이타의 비인가된 입력 혹은 변경
233	부정확한 거래	응용통제위험	상호교류문서의 응용시스템 데이타로의 혹은응용 시스템 데이타의 상호교류문서로의 부정확한 변환
140	비인가된 거래	관리통제위험	거래파트너로부터 온 비인가된 혹은 부적절한 거래의 처리
440	비인가된 변경	컴퓨터통제위험	비인가된 거래파트너의 추가와 같은 데이터화일에 대한 비인가된 변경

■ 테스트(테스트#, 테스트이름, 테스트_설명)

테스트#	테스트이름	테스트_설명
201	편집 체크(Edit Checks)	무효한 거래를 식별하기 위한 편집 체크의 효과성 테스트
342	예외 보고 (Exception Procedure)	시스템 오류(failures)에 대한 사후예외보고서와 절차에 대한 테스트
312	디지탈 서명	각거래에 대해 전자서명을 제공할수 있는 기능
421	물리적 보호	물리적 통제와 접근제한에 대한 테스트
521	메시지 암호화	중요메시지가 암호화가 되었는지에 대한 테스트

■ 테스트 결과(테스트코드, 날짜, 결과, 결과 설명)

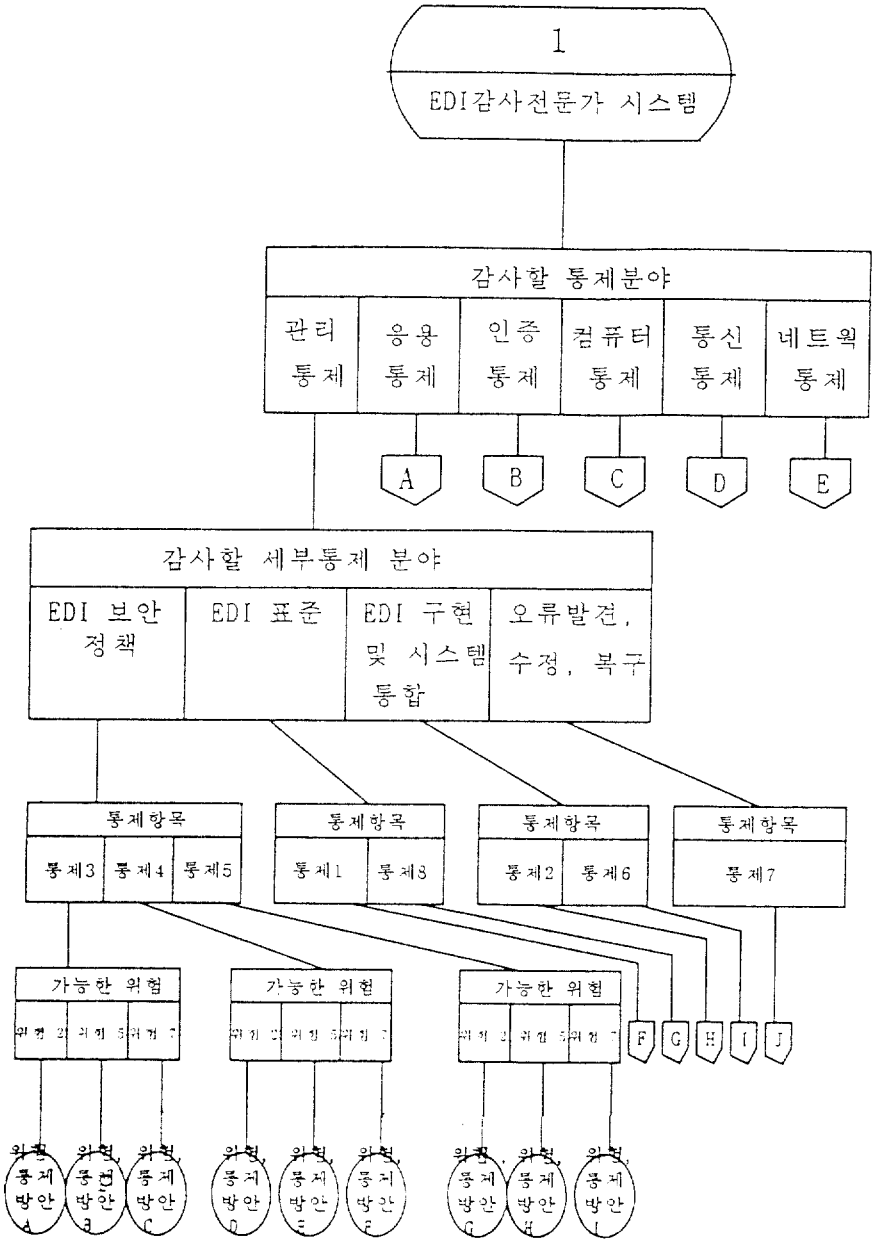
테스트#	테스트코드	날짜	결과	결과 설명	회사코드
201	2911	1994 3.2	좋다	데이타 입력시에 데이타 무결성을 체크하기 위한 유효성 체크등이 이루어진다	102
342	2111	1994 2.2	매우좋다	시스템 오류사후예외보고서가 작성되어 이에 대한 처리가 이루어지고 처리결과는 인가를 받는다	111
312	1992	1994 1.24	중간	디지탈 서명 체계가 기존의 수작업 서명 절차를 보완하고 있으나 구체적인 기술적 지원이 더 필요하다	330
421	0323	1993 12.20	매우나쁘다	EDI 시스템에 전반적인 물리적 보안이 취약하여 시스템 자원에 대한 손실우려가 있다	321
521	3232	1994 6.18	나쁘다	중요 메시지에 대한 암호화가 안되어 있고 데이타 노출위험이 크다.	121



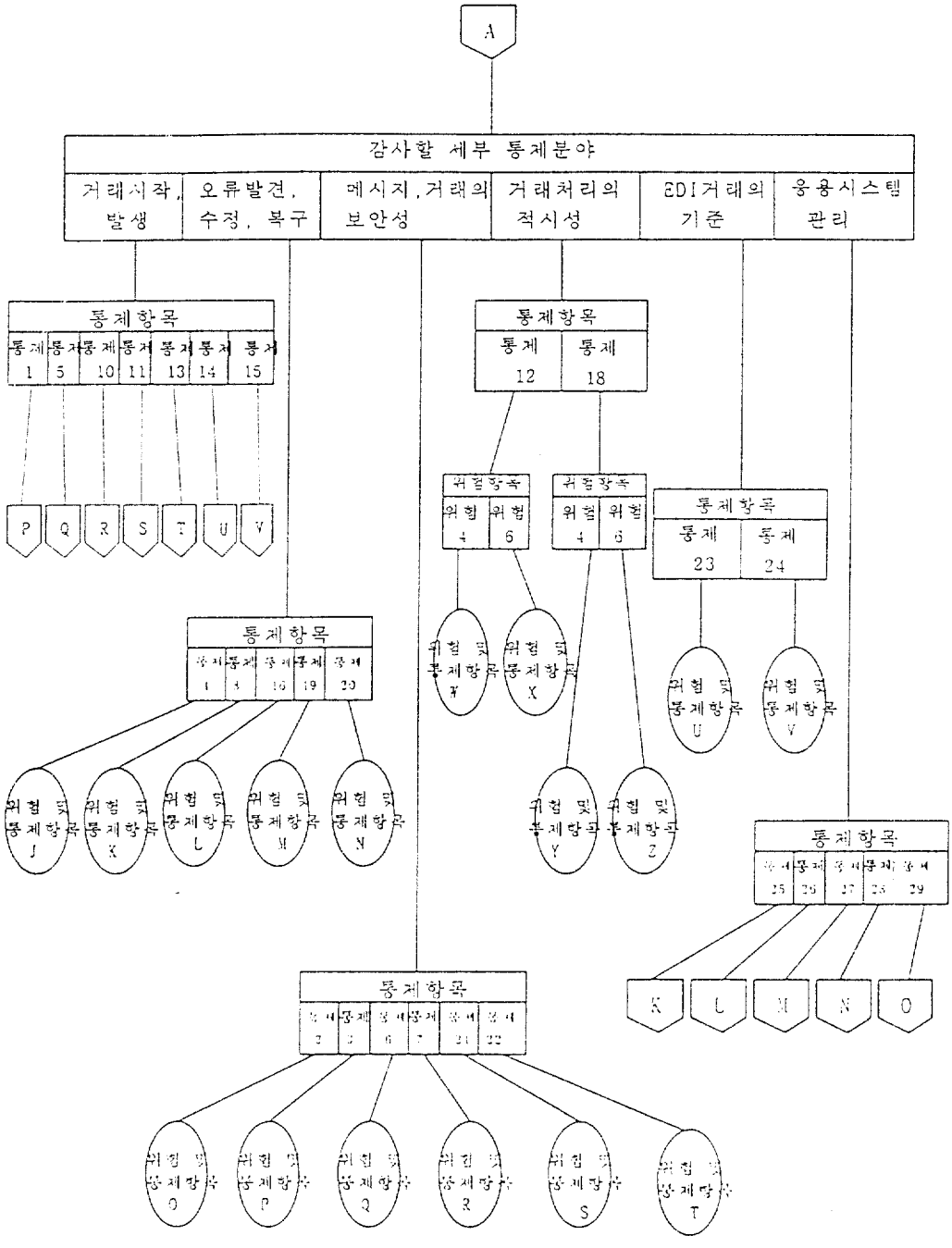
〈그림 8〉 EDI 감사용 지능형 의사결정지원시스템의 구조

〈표 2〉 EDI 통제(EDICA and EDPAA, 1991)와 관련된 위험항목

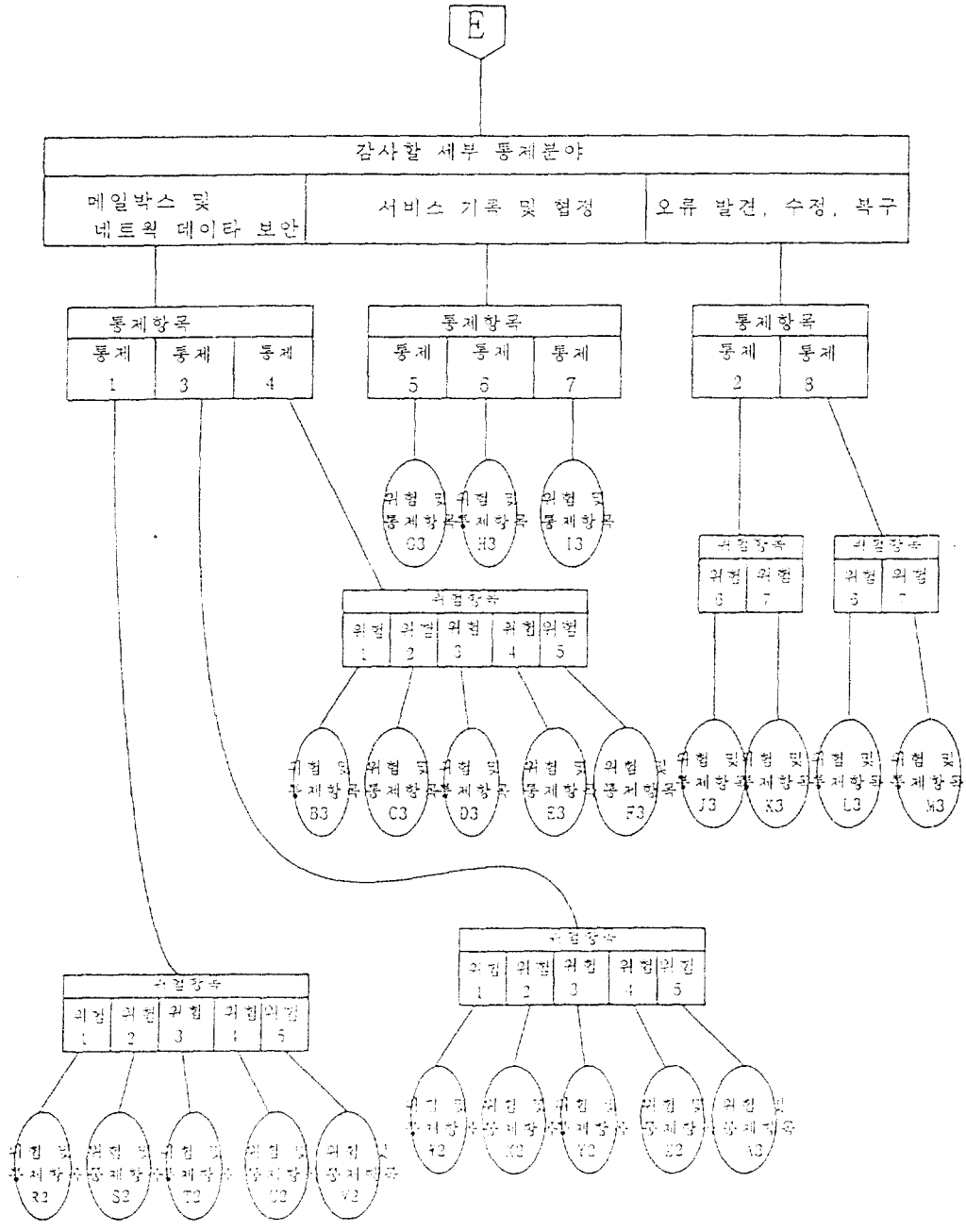
통제분류	세부분류기준	통제항목	위험항목
관리통제	EDI보안정책	3,4,5	2,5,7
	EDI표준	1,8	1
	EDI 구현 및 시스템 통합	2,6	6
	오류발견, 수정, 복구	7	3,4
응용통제	거래시작, 발생	1, 5, 10, 11 13, 14, 15	1,7
	오류발견, 수정, 복구	4, 8, 16, 19, 20	5
	메시지, 거래의 보안성	2, 3, 6, 7, 9, 17, 21, 22	8
	거래 처리의 적시성	12, 18	4, 6
	EDI 거래의 기준	23, 24	9
	EDI및 관련 응용시스템 관리	25, 26, 27, 28, 29	2, 3, 10
EDI 인증통제	메시지 보안성	3, 7	3
	거래 개시시 보안성	5, 6	2, 4
	오류에 대한 책임	2, 4	1
컴퓨터 내부통제	데이타 접근, 보안 통제	1, 2, 3, 5	2, 3, 4
	오류발견, 수정, 복구	4, 6	1, 6
통신보안 통제	통신메시지 보안 통제	1, 5	3
	오류발견, 수정, 복구	3, 4, 6, 7	1, 2, 4, 5
	메시지 지연 및 중복	2	6, 7
제3자 네트워크 보안	메일 박스 및 네트워크 데이타 보안	1, 3, 4	1, 2, 3, 4, 5
	서비스 기록 및 협정	5, 6, 7	8
	오류발견, 수정, 복구	2, 8	6, 7



〈그림 9〉 지식분석도 : 개괄 및 관리통제



〈그림 10〉 지식분석도 : 응용통제



〈그림 11〉 지식분석도 : 네트워크통제

스에 대한 보안기능에 대한 독립적인 점검")
(IS "통제 부재의 위험은 다음과 같습니다. 통제방안을 알고 싶은 위험을 선택하십시요" "제3자 네트웍상에서 전송되는 데이타에 대한 고의적 수정 혹은 부정")
THEN
("제3자 네트웍상에서 전송되는 데이타에 대한 고의적 수정 혹은 부정에 대비한 통제방안")
(DISPLAY "" "다음과 같은 통제방안이 필요하다
- 데이타 전송시 안전성에 대한 독립적인 점검
- 제3자 네트웍에 대한 사용자 책임 설정
- 네트웍시설에 대한 물리적 보안
- 제3자 네트웍 제공자와의 데이타의 오류에 대한 책임 설정
- 네트웍 제공자의 감사증적 유지
- 거래메시지에 대한 합계통제 및 일련번호 부여
- 장비와 운영시스템에 대한 신속 복구절차
- 거래파일변환 프로그램의 점검
- 화일에 대한 기록유지
- 오류에 대한 경보기능
- 거래처리에 대한 법적 근거확보
- 화일에 대한 기밀성 부여
- 거래처리 사이클상의 처리로그 유지
- 통신되는 거래의 암호화
- 컴퓨터 물리적 접근 통제
- 기밀정보의 암호화
- 거래 데이타 입력에 대한 로그유지
- 운영업무에 대한 인증절차
- 입력거래 대한 일련번호 부여
- 운영 업무에 대한 정확성의 독립적인 검증
- 거래사이클 상의 감사증적유지
- 응용 프로그램에 대한 불법적
- 접근통제")

VI. 결 론

EDI의 보안 및 감사기법은 전통적인 기법과는 내용과 절차상에서 차이가 있으므로 보안 및 감사기법에 대한 전면적 재검토가 필요하다. EDI의 보안 및 감사업무의 효율성을 높이기 위하여는 데이타나 시스템의 보안문제를 진단해 주거나 적절한 통제절차를 제시하는 의사결정지원시스템을 구축하는 것이 필요할 것이다. 이 연구에서 EDI시스템의 감사를 지원해 주는 의사결정지원시스템을 개발하였다. 이 시스템을 통해서 감사나 보안문제에서 발생되는 반정형적(semi-structured) 또는 비정형적(unstructured)인 의사결정을 지원할수 있을 것이다. 또한 이 연구에서는 지능형 EDI감사 의사결정지원시스템을 제안하였다.

본 연구를 통해서 EDI감사용 의사결정지원시스템이 데이타베이스시스템을 기반으로 개발되었다. 이를 위해서 기존의 EDP감사용 의사결정지원시스템 및 감사전문가시스템분야의 연구를 고찰했다. EDI감사를 위한 의사결정지원시스템은 통제, 위험, 회사의 개요, 테스트 항목등의 데이타를 저장한 데이타베이스 시스템이다. 시스템개발을 위해서 E-R(Entity-Relation)및 DFD(Data Flow Diagram)분석을 통해서 논리적인 설계를 하였다. 시스템의 개발은 데이타베이스팩키지인 FoxPro를 사용하였다.

이 시스템을 통해서 감사인이 필요한 테스트결과, 통제, 위험점수등을 조회해 볼 수 있고 통제나

위험간의 관련성, 테스트 항목과 관련된 통제나 위험의 검토, 테스트 세부항목이나 분류와 관련된 통제, 위험등을 조사할 수 있다. 계속적으로 감사를 수행하는 경우에 각 회사에 맞는 체크리스트를 저장하여 이를 회사와 연결시켜서 조회해 볼 수 있어서 과거의 감사기록을 유지하는 기능도 가질수 있다. 본 시스템은 EDI감사뿐만 아니라 일반 EDP 감사분야에도 적용가능할 것이다.

본 연구를 통해서 개발된 EDI감사용 의사결정지원시스템에 지식베이스를 추가시켜 지능적 시스템의 방향으로 발전시킬 필요가 있을 것이다. 데이타베이스시스템을 기반으로 한 EDI감사용 의사결정지원시스템에 모델 및 규칙베이스 부분을 첨가시키면 지능형 의사결정시스템이 될 수 있을 것이다. 이러한 규칙베이스의 예로서 가능한 위험상황에 대한 통제방안이 무엇인지에 관한 규칙을 생각할 수 있다.이를 위해서 국내의 전문가 시스템 개발도구인 UNIK를 사용하여 통제와 위험의 관련성을 유추하는 규칙을 제시해 보았다.

EDI가 자동화된 통신시스템으로서 EDI감사는 전통적인 수작업으로는 충분하지 못하다. EDP감사시스템분야 국내 연구가 전무한 실정에서 EDI감사를 지원하는 시스템의 개발을 시도하였으며 앞으로 이 분야의 연구가 활성화하리기를 기대한다. 본 연구는 EDI의 보안 및 감사업무의 효율성을 높이고 EDI에 대한 위험에 효율적으로 대처하는데 기여할 수 있을 것이다. 그리고 이러한 보안 및 감사기법과 통제모형을 지식베이스로 구축해서 실제의 위험노출상황에서 가능한 보안을 위한 통제방안이 여러가지가 있는 경우에 비용/편익 분석, 효율성, 회사방침 및 법률적인 문제등을 고려해서 최적의 보안통제 및 감사기법을 선택하는 것을 지원할 수 있을 것이다.

이러한 시스템의 적용을 통해서 기업은 EDI시스템이 가질수 있는 위험, 즉 상호의존 및 노출성의 증가, 감사가능성에 대한 위험, 제삼자(third party) 네트웍 제공자의 위험, 응용시스템 고장, 그리고 통합의 위험 등의 다섯 가지 위험(Chan et al., 1991)을 줄임으로써 보안을 제고할수 있을 것이다. 그리고 중요한 자료 및 자금전달에 있어서 EDI를 활용할 경우 EDI시스템에 적합한 보안통제의 설계와 효율적인 감사기법의 개발을 통해서 보안상의 위험발생과 그것의 사후처리로 인한 비용을 줄일 수 있을 것이다. 이러한 지능형 의사결정지원시스템을 통해서 EDI가 가져다 줄 수 있는 본래의 이점을 보다 제고시켜 궁극적으로 고객에 대한 서비스를 향상시킴으로써 경쟁력을 향상시킬 수 있을 것이다.

참 고 문 헌

이재규 (1994), **UNIK사용자 설명서**, 한국과학기술원 지능정보시스템연구실.

이진주·박성주·이재규·김성희·정은상 (1994), **경영정보시스템**, 다산출판사.

Bailey, Jr., A., K. Hackenbrack, P. De, and J. Dillard (1987), "Artificial Intelligence, Cognitive Science, and Computational Modelling in Auditing Research: A Research Approach," *Journal of Information Systems*, Spring, 20-40.

Burns, David C. and James K. Loebbecke (1975), "Internal Control Evaluation: How the Computer Can Help," *Journal of Accountancy*, August, 60-70.

Caster, Paul (1987), "An analysis of techniques for assessing risk," *The EDP Auditor Journal*, Fall.

Chan, Sally, et. al. (1991), EDI for managers and auditors, Electronic Data Interchange Council of Canada..

Choi, Jong Uk (1994), "A constructive synthesis approach to a knowledge-based internal control evaluation system design," *Expert Systems with Applications*, 2, 357-372.

Date C. J. (1990), An introduction to database systems, Addison-Wesley Publishing Company, Inc..

Davis, A. Crowell, and Andrew Sundene (1989), "Data communications audit concerns," *The EDP Auditor Journal*, Fall.

De, Prabuddha, and Arun Sen (1988), "Semantic modeling of internal controls in database design," *Journal of Management Information Systems*, 5, 2.

Delisio, Jeff, Maureen McGowan, and Walter Mamscher (1994), "PLANET: an expert system for audit risk assessment and planning," *Intelligent Systems in Accounting Finance, and Management*, 3, 65-77.

Dewitz, Sandra and Michael, Olson (1994), Semantic object modeiing with SALSA, Mitchell McGraw-Hill.

Dijk, Van J.C. and Paul. A Williams (1990), Expert Systems in Auditing, Stockton Press,

Dungan, C. W. and J. S. Chandlers (1985), "AUDITOR: A microcomputer based expert system to support auditors in the field," *Expert System*, 2, 4, 210-224.

EDICA and EDPAA (1991a), EDI Control Guide, EDI Council of Austrailia._____ and _____(1991b), EDI Message Security Guide, EDI Council of Austrailia.

Everest, G. C., and Weber Ron (1977), "A relational approach to accounting models," *The Accounting Review*, April, 340-359

Gal, G., and McCarthy (1985), "Specification of internal controls in a database environment," *Computer and Security*, 23-32.

Gal, G. F. (1985), "Using auditor knowledge to formulate data model constraints: an expert system for internal control evaluation," Doctoral dissertation, Dept. of Accounting, Michigan State University.

Grace, T. Chu (1985), "Expert systems in computer based auditing," *The EDP Auditor Journal*, Spring.

Grundnitski, G. (1986), "A prototype of an internal control expert system for the sales/accounting receivable application," University of Texas at Austin Working Paper.

Han, I., and J. Choi (1993), "Selection of appropriate Tasks for the Expert Systems Development in Auditing," *Preceedings of '93 Korea/Japan Joint Conference on Expert Systems.*

Hansen, James V. and William F. Meisser, Jr. (1984), "A Relational Approach to Decision Support for EDP Auditing," *Communication of the ACM*, November, 1984, 1129-1133.

Hansen, James V, and William F. Meisser, Jr. (1986a), "A knowledge-based expert system for auditing advanced computer systems," *European Journal of Operational Research*, 26 371-379.

_____, and _____(1986b), "A preliminary investigation of EDP-XPERT," *Auditing: A Journal of Practice & Theory*, 109-123.

_____, and _____(1987), "A case study and field evaluation of EDP-XPERT," Working Paper; University of Florida, July.

Joseph, R. Pleier (1984), "Computer-assisted auditing," *The EDP Auditor Journal*, Summer.

Lefons, Ezio et al. (1989), "Architecture of a relational decision support system," *Decision Support Systems*, 5, 65-78.

Mai, Iskander, and Paul McMann (1989), "Expert systems in auditing: Advantages and applications," *The EDP Auditor Journal*, Winter.

McLeod, Jr. Raymond (1990), Management Information Systems, Macmillian Publishing Company, 4th ed..

Meisser, Jr., W., and J. Hansen (1987), "Expert Systems in Auditing: The State of Art", *Auditing: A Journal of Practice and Theory*, Fall, 94-105.

Morris, W. Bonnie (1994), "SCAN: a case-based reasoning model for generating information system control recommendations," *Intelligent Systems in Accounting, Finance and Management*, 3, 47-63.

Niv, Ahituv, and Lee Doretta (1986), "Control concepts and evaluation techniques for use in auditing of advanced EDP systems", *The EDP Auditor Journal*, Fall.

Peters M. James, and Barry L. Lewis (1989), "Assessing inherent risk during audit planning: the development of a knowledge based model," *Accounting, Organizations and Society*, 14, 4, 359-378.

Snodgrass, R. (1982), "Monitoring distributed systems: A relational approach CMU-CS-82-154, Dept. of Computer Science, Carnegie-Mellon Univ., Pittsburgh, Pa..

Steinbart, P. (1987), "The Construction of a Rule-Based Expert System as a Method for Studying Materiality Judgements," *Accounting Review*, January, 97-116.

Steve, Mar (1989), "Using expert systems to enhance the PC audit program," *The EDP Auditor Journal*, Spring.

Suh Eui-Ho, and Hirohide HINOMOTO (1989), "Use of a dialogbase for integrated relational decision support systems," *Decision Support Systems*, 5, 277-286.

Weber, Ron (1975), "Audit capabilities of some database management systems," Working Paper MISRC-WP-75-05, Management Information Systems Research Center, University of Minnesota, Minneapolis.

Weber, Ron (1980), "Some characteristics of the free recall of computer controls by EDP auditors," *Journal of Accounting Research*, 18, 1, spring, 214-241.

Weber, Ron (1988), EDP Auditing, MacGraw-Hill International editon.

William, J. Powers, and Thomas Carver (1990), "EDI: control and audit issues," *The EDP Auditor Journal*, Spring.

William, R. Edge and Wilson J. G. Edward (1989), "A prototype expert system for internal auditors," *The EDP Auditor Journal*, Spring.

Development of the Decision Support System for Auditing EDI System

Sang-Jae Lee* · Ingoo Han*

Abstract

In this paper, the decision support system for auditing the EDI system is developed. This system is based on the database system which has entities - control, risk, company, test, etc. E-R(Entity-Relationship) diagram and DFD(Data Flow Diagram) are drawn for logical system design. FoxPro, database package, is used as a development tool. An auditor can retrieve and store test results by using this system. An auditor can suggest required controls through cross-reference between control, risk, company, test result tables. Different controls, risks, and test checklists can be stored for different companies. This system can improve the efficiency and effectiveness of EDI auditing and can be applied to general EDP auditing.

* Graduate School of Management KAIST