클라이언트-서버시스템의 보안을 위한 통제모형

The Model of Security Controls for Client-Server System

남 성 우 (Seongwoo Nam) 한전정보네트워크(주) 개발사업단
한 인 구 (Ingoo Han) 한국과학기술원 테크노경영대학원
이 상 재 (Sangjae Lee) 한국과학기술원 테크노경영연구소

목 차

Ⅰ. 서 론
Ⅱ. 클라이언트-서버 보안통제 모형
Ⅲ. K은행의 사례연구
Ⅳ. 결 론

Keywords: *클라이언트-서버시스템, 관리통제, 아키텍처통제, 응용통제*

Ⅰ. 서 론

기업정보시스템은 현재 메인프레임(Mainframe) 환경에서 클라이언트-서버시스템환경으로 변화 발전되고 있다. 하드웨어 비용의 하락, PC의 성능 향상, 변화에 대한 대처 능력, 유연성 등의 향상으로 클라이언트-서버 환경으로 급속한 발전이 이루어지고 있고 이에 대한 효과적인 구현, 관리 및 통제방안에 대한 연구가 중요해지고 있다(Anandarajan and Arinze, 1998; Chengalur and Duchessi, 1999; Drury, 1997; Ryan and Bordoloi, 1997).

메인프레임컴퓨팅 환경에서 사용자들은 응용프로그램을 하나의 컴퓨터상에서 실행시킨다. 주 컴퓨터에 한번 로그인함으로써 응용프로그램에 접근할 수가 있다. 클라이언트-서버 컴퓨팅 환경에서는 사용자들은 그들이 가지고 있는 클라이언트용 컴퓨터를 이용하여 업무를 처리한다. 서버는 별도의 프로세스를 가지고 요청에 대하여 답변을 하거나 작업을 하여 결과를 다시 클라이언트에게 보내 준다. 분산된 클라이언트-서버시스템의 가장 큰 특징으로는 응용프로그램의 분리에 있는 것으로 말할 수 있고 응용프로그램이 클라이언트와 서버사이에 다양한 비율로 분리된다(MASP Consulting staff, 1994a, 1994b). 응용프로그램을 모듈 단위로 나누어지고 각 모듈이 가장 효율적으로 수행될 수 있는 플랫폼 상에서 수행되도록 한다(Runge, 1994). 즉 응용프로그램은 둘 이상의 실행모듈로 변환하여 하나는 클라이언트 모듈로, 다른 하나는 서버 모듈로, 즉, 각기 하나 이상의 컴퓨터 상에서 실행된다. 클라이언트-서버는 서로 상호작용하면서 또한 클라이언트와 서버 각각의 분명한 처리를 수행한다. 이때 클라이언트와 서버는 종종 서로 다른 컴퓨터 플랫폼에서 수행되기도 한다. 따라서 클라이언트-서버 구조는 최소한 둘 이상의 다중플랫폼에서 운영된다. 그리고 클라이언트-서버 구조는 일정한 형태를 갖는, 그리고 다양한 복잡성을 갖는 네트워킹을 포함한다. 결국 클라이언트-서버는 단일의 집중된 응

용시스템 보다 더욱 복잡하다. 이러한 시스템의 효과성 및 신뢰성을 증진시키기 위하여 시스템의 통제의 중요성은 매우 크다고 할 수 있다.

분산된 서버와 클라이언트를 가진 클라이언트-서버 환경 하에서는 보안관리 방법이 달라져야 한다. 클라이언트-서버에서 보안통제를 구현하기 위해서는 클라이언트-서버가 가지고 있는 특수한 환경을 인식하여야 한다(Jess, 1995). 메인프레임환경 하에서는 주 전산기가 있고 운영 요원이 집중된 전산실 위주의 보안관리(전산실 설비, 인원에 대한 보안관리)가 주를 이루었다면, 클라이언트-서버 환경 하에서는 설비 및 운영 요원의 다양화, 복잡화로 인해 보다 많은 통제요소가 필요하게 되었다. 예를 들면 메인프레임 환경하에서는 주 전산기에 대한 주기적인 백업만이 요구가 되었으나, 클라이언트-서버 환경하에서는 각 파일서버 또는 데이타베이스 서버에 대한 백업 및 클라이언트용 PC에 대한 백업관리가 필요하게 되었다(Runge, 1994). 클라이언트-서버 환경하에서는 LAN에 대한 보안정책, 각종 통신용 응용프로그램에 대한 논리적 접근통제, 복잡해진 통신경로 및 방법에 대한 통제가 필요하게 되었다(Belden, 1995). 또한 메인프레임환경하에서는 주 전산기가 존재하는 전산실 위주의 재난복구계획이 요구되었으나, 클라이언트-서버 환경하에서는 각 서버 중심의 재난복구계획이 존재해야 하며 또한 각 서버들간의 연계성을 갖는 계획이 필요하게 되었다. 또한 클라이언트-서버 환경 하에서는 각 서버에 따라 사용자 ID와 패스워드가 다를 수 있으므로 여러 개의 사용자 ID와 패스워드의 등록, 수정 및 관리가 요구된다.

이와 같이 클라이언트-서버 시스템환경의 성격을 고려한 통제의 중요성이 증대되고 있는데도 불구하고 메인프레임환경에서의 사용되는 기존의 시스템통제 모형이 클라이언트-서버 시스템 환경에서도 계속 사용되고 있어서 클라이언트-서버 환경에 적합한 새로운 통제 모형을 제시할 필요가 있다. 기존의 보안 및 통제에 관련된 문헌들은 실제로 일반적인 정보시스템 통제모형이나 가이드라인을 제시하고 있어서 클라이언트-서버 시스템의 구조적인 특성을 고려하지 못하고 있다. 본 연구는 클라이언트-서버시스템 환경에서 현업의 실무자들이 보다 효과적인 보안시스템을 개발 및 유지할 수 있도록 시스템을 개발 및 운영시 고려해야 할 통제요소 들을 제공하여 하는데 목적이 있다. 그리고 이러한 통제모형이 현업에 실제로 적용이 가능한 지 여부를 판단하기 위하여 사례 연구를 실시하여 적용 가능성을 검증하였다.

Ⅱ. 클라이언트-서버 보안통제 모형

정보시스템의 통제는 크게 조직내 관리통제와 응용통제로 구분될 수 있다(Weber, 1999). 관리통제는 정보시스템개발 및 유지, 보안관리, 및 운영관리 등을 포함하는 것으로서 전반적인 응용시스템의 개발, 유지 및 운영을 위한 모든 정보시스템 및 조직내의 절차를 의미한다. 응용통제는 각 응용시스템의 보안 및 무결성을 증진시키기 위한 것으로서 입력, 처리, 출력 통제를 포함한다. 관리통제는 전반적인 모든 응용시스템의 보안관리를 다룬다는 점에서 특정 응용시스템에 대한 통제인 응용통제와 차이가 있다. 또한 관리통제는 정보시스템조직 전반에 영향을 미치므로 이에 대한 점검은 응용통제보다 먼저 이루어져야 한다(Moeller, 1989; Weber, 1999). 이와 같은 분류이외에 통제목적에 따라서 통제를 분류할 있는데 예를 들면 정보의 정확성, 프라이버시(privacy)나 기밀성, 가용성을 각각 증진시키는 정확성통제, 기밀성통제, 적시성통제가 있을 수 있다. 또한 오류를 예방(prevent), 발견(detect), 혹은 정정(correct)하는 목적을 갖는 여부에 따라서 예방통제, 발견통제, 정정통제로 나눌 수도 있다. 최근에 미국 정보시스템 통제 및 감사협회에서는 COBIT 이라는 통제분류체계를 제시하였는데 이는 통제를 계획 및 조직(Planning and Organization), 시스템 구현(Acquisition and Implementation), 시스템 서비스제공 및 지원(Delivery and Support), 시스템 성과 모니터링(Monitoring)으로 크게 네가지 영역으로 나누었다(ISACF, 1996).

본 논문에서는 기본적으로 아직 학계 및 실무계에서 가장 보편적으로 사용되는 분류체계인 관리통제와 응용통제를 사용하고 이를 확대 응용하여 클라이언트-서버 시스템 통제모형을 제시하고자 한다. 즉 클라이언트-서버통제모형으로서 조직 내 보안정책을 수립하는 관리통제(administrative controls), 실제 응용프로그램의 입출력, 처리통제를 담당하는 응용통제(application controls), 그리고 이 두가지 통제외에 클라이언트-서버환경 등과 같은 고유의 컴퓨터 구조에 맞는 보안정책을 수립하는 아키텍처통제(architectural controls) 를 제시한다.

보안시스템은 현재 운영 중인 시스템을 대상으로 구축되지만 전산환경의 급속한 발전에 따라 보안시스템 역시 변화 발전되어야 한다. 전산환경이 변화할 때마다 보안시스템을 다시 재구축해야 한다면 인력 및 비용의 막대한 지출이 필요하다(David, 1995). 따라서 보안시스템을 구축하는 단계를 모듈 단위로 접근하여 구축하는 것이 필요하다. 우선 보안시스템구축의 첫번째 단계로서 조직의 일반적인 전산운영에 대한 보안정책수립 즉 관리통제를 수립하고 두번째 단계로서 시스템 아키텍처에 대한 통제를 개발하며 마지막으로 응용통제를 구축하여 응용프로그램의 개발, 운영, 유지보수 및 프로그램 내에 갖추어야 할 보안요소 들을 관리한다. 관리 및 응용통제는 시스템의 아키텍처(Architecture)의 영향을 거의 안받는 모든 컴퓨팅 환경에 적용될 수 있는 것으로써, 시스템 운영환경 변화의 영향을 적게 받는 통제이다. 급속한 전산운영 환경의 변화가 있을 때에는 두번째 통제계층인 아키텍처통제 부분을 집중적으로 보완하거나, 새로이 구축함으로써 환경 변화에 대해 신속히 대응할 필요가 있다. 이러한 모듈 접근법에 의해 변화하는 전산환경 하에서 효율적인 보안시스템 구축이 가능하다. 관리, 아키텍처 및 응용통제의 세부적인 통제사항은 <표 1>에 요약되어 있다.

〈표 1〉 클라이언트-서버 통제모형

통제계층	통제사항
1. 관리통제	1.1 보안정책수립 (기업내 전반적인 IT환경) 1.2 재해복구계획(DRP) 1.3 전이시 보안정책수립 1.4 신규 하드웨어/소프트웨어 구입에 관한 보안정책수립
2. 아키텍처통제	2.1 클라이언트의 보안정책수립 2.2 서버의 보안정책수립 2.3 네트워크의 보안정책수립
3. 응용통제	3.1응용시스템 개발과정에서의 통제 3.2 유지 및 보수관리에서의 통제 3.3 입력, 처리, 출력상에서의 통제

2.1 관리통제

관리통제는 조직의 전산환경에 관련된 보안정책을 수립하는 통제계층이다. 기본적으로는 기업 또는 사업의 전략과 계획을 달성하는데 도움을 주며 그러한 전략과 계획에 포함된 정보시스템 전략과 계획을 구체적으로 정의해 준다(Weber, 1999). 본 논문에서는 관리통제의 목적을 크게 그리고 1) 정보시스템의 구현, 운영 및 관리를 위한 정보시스템 환경을 계획 및 조직하고 2) 화재, 홍수, 사고 등과 같은 재해와 해킹, 사기, 절도, 바이러스 등과 같은 고의적인 부정 등의 발생할 수 있는 모든 재해위협으로부터 기업 내 전산자원을 보호하며 3) 기업의 전략을 달성하고 업무요구사항을 만족시킬 수 있는 시스템 구현하는데 있다고 정의한다. 조직이 이러한 관리통제를 수립할 때 고려되어야 할 사항으로서 기업 내 전반적인 IT 환경에 대한 보안정책수립, 재해복구계획, 전이시 보안정책수립, 신규 하드웨어/소프트웨어 구입에 관한 보안정책수립의 4가지 통제사항을 제시한다. 다른 보안정책이 포함될 수 있겠으나 이 네가지 통제가 성공적인 클라이언트-서버 시스템의 개발 및 보안성 그리고 효과성 증진을 위해 가장 필요하다고 생각된다.

2.1.1 기업 내 전반적인 IT 환경에 대한 보안정책 수립

기업정보시스템 운영 전반에 대한 문서화된 보안정책을 의미한다. 이러한 통제의 내용은 기업의 사업

정책에 근거를 두고 있고 또한 다른 정보 보안정책의 기본이 된다. 기업 내 전반적인 IT 환경에 대한 보안 정책의 수립목적은 크게 다섯 가지가 있다. 첫째, 경영계획에 기반하여 전산화 작업에 대한 장·단기계획을 수립한다. 내외 경영 환경을 정확히 파악하고 전략적 정보계획수립에 따라 전산화의 중장기계획이 추진되도록 해야 한다. 또한 회사의 경영계획이 전산화계획의 작성 지침으로 활용되어야 한다. 둘째, 기업 내 전산 자원에 대한 물리적 보안정책이 수립되어 있음을 보장한다. 셋째, 공정하고 합리적인 인사 정책을 수립한다. 현재 및 장래의 요원에 대한 소요 필요성을 정확하게 파악하고 있어야 한다. 또한 요원보충을 위한 기준은 명확하고 구체적으로 표현되어 있어야 한다(Scott and Martin, 1995). 보충요원에 대한 교육프로그램이 준비되어 있어야 하며 계획에 반영되어 있어야 한다. 넷째, 모든 절차가 문서화되어 있고 표준화되어 있음을 보장한다. 예를 들어 조직구조와 책임분담, 백업 및 복구, 비상계획, 장비 및 소프트웨어의 유지 및 보수, 보안검토 및 감시, 시스템변경관리, 위험분석 및 위험관리, 각각에 대한 절차가 문서화되어 있어야 한다. 다섯째, 기술사항들이 문서화되고 표준화되어 있음을 보장하여 직원의 이직이나 전직으로 인한 기술적인 업무의 중단이 생기는 것을 방지한다.

2.1.2 재해복구계획

큰 재난이 발생하였을 경우에도 비지니스가 계속적으로 운영할 수 있도록 재해복구계획(DRP: Disaster Recovery Plan)을 수립하고 계획에 의거 테스트를 하며 계획이 주기적으로 검토, 갱신되도록 한다(Charles, 1995). 세부통제목적으로는 첫째, 재해복구계획에 포함될 내용과 재해의 수준을 명확히 설명할 수 있도록 문서화한다(Kenneth, 1995). 효과적인 재해복구계획의 요건들에는 비상재해시에 대처하기 위한 절차, 재해선언절차 관련자에게 통보를 위한 비상연락망, 재해인지를 확인하는 기준 등이 만들어져야 한다.

둘째, 정보시스템 처리와 사용자 업무기능에 영향을 줄 수 있는 모든 종류의 재해적인 사건을 고려하여 재해 상황시나리오를 작성한다. 민감성과 중요성에 따라 핵심적인 시스템에 우선순위를 정한다. 셋째, 재해로 인한 피해를 최소화하기 위하여 주요 설비 및 소프트웨어 등에 대하여는 보험을 가입하여 둔다. 예를 들어 전산장비와 설비, 정보처리시설과 장비에 대한 물리적인 피해보상, 미디어(소프트웨어) 재구성, 계속적인 운영에 소요되는 추가적인 비용에 대한 보험가입을 고려한다. 넷째, 타 지역의 정보처리시설은 원래의 장소와 마찬가지로 안전하게 보안이 되고 통제되고 있음을 보장하여야 한다. 예를 들어 물리적 접근통제가 이루어지고 쉽게 발견이 안 되는 곳에 위치해야 하며 원래의 장소에서 멀리 위치해야 한다.

2.1.3 전이시 보안정책수립

기존 메인프레임시스템 환경에서 클라이언트-서버 시스템 환경으로의 전이시 발생가능한 혼란을 최소화하고 보안을 유지하기 위한 정책이 필요하다(Hitchings, 1995). 세부통제목적으로는 첫째, 새로운 시스템에 대한 이해를 증진시키고 원활한 운영을 보장하는 것이다(Charles, 1995). 새로운 시스템환경에 대한 이해를 증진시키기 위해 새로운 어플리케이션, 새로운 사용자, LAN 운영 체계, 외부에서 전화선을 이용한 접근 등에 대한 교육 및 훈련을 실시한다. 둘째, 전이시 충분하고 엄격한 보안활동을 적용한다. 전이시 사전에 전이계획을 철저히 세우고 계획에 따라 각 부문의 역할분담이 이루어져 혼란을 최소화시킬 수 있음을 보장하여야 한다. 전이시 전문가를 새로이 고용하는 것보다는 계약관계를 유지시키는 것이 효과적인데 그 이유는 메인프레임관리자가 새로운 기술을 축적할 필요가 없이 분산된 환경에 대해 즉시 숙련된 보안기능을 제공하고 현재의 보안관리자가 새로운 환경에 필요한 새로운 기술을 습득할 시간적 여유를 가질 수 있기 때문이다.

2.1.4 신규 하드웨어/소프트웨어 구입에 관한 보안정책수립

통제목적은 신규하드웨어/소프트웨어 구입 시 적절

하고 합리적인 절차를 준수하여 구입의 효과성을 가지는 것이다(Charles, 1995). 세부통제목적으로는 첫째, 공급자로부터 구매 시에 취득정책에 의거하여 이루어지도록 한다. 예를 들어 취득정책에 고려할 사항에는 경쟁 입찰의 준비, 입찰자의 분석과 선택, 테스트와 인수절차, 공급자의 재정적 상태의 분석, 유지, 관리 및 교육을 포함하는 지원정책에 대한 분석, 설치일자, 하드웨어/소프트웨어의 승급 시에 호환성제공여부, 보안과 통제 기능의 분석, 가격, 계약조항, 감사요구 권리조항 등이 포함된다(Linda, 1995). 둘째, 구입절차가 문서화되어 있으며 이에 대한 준수를 보장해야 한다. 구입 절차를 상세히 문서화, 규정화 하여 이를 준수토록 하기 위하여 교육, 훈련 등을 실시한다. 셋째, 구매에 필요한 하드웨어/소프트웨어를 명세화 하여 공정한 구매행위가 이루어짐을 보장해야 한다. 넷째, 공급자의 제안서를 평가하기 위한 기준과 자료는 적절히 계획되고 있음을 보장한다. 평가 과정에서 고려해야 할 기준들에는 반환시간, 응답시간, 시스템반응시간, 처리량, 작업부하, 호환성, 용량, 이용도, 벤치마크 테스트 등이 포함된다.

2.2 아키텍쳐통제

관리통제는 조직 또는 기업 내 전산환경의 일반적인 보안정책에 대한 것인 반면에 아키텍쳐통제는 클라이언트-서버의 특수한 전산환경에서의 보안정책에 관한 것이라고 할 수 있다. 관리통제는 전산을 도입하고 운영 중인 조직이나 기업들간에 그 내용에 있어서 별 차이가 없겠으나 아키텍쳐통제는 해당 조직이나 기업의 전산환경, 즉 기본플랫폼에 의존하여 보안정책이 수립될 것이다. 메인프레임환경, 분산처리환경, 클라이언트-서버환경 등 여러 환경에 따른 아키텍쳐통제가 제시될 수 있겠으나 본 논문에서는 클라이언트-서버 환경에서의 아키텍쳐통제를 다룬다. 아키텍쳐통제는 클라이언트-서버 구성부분별로 통제사항을 구성한다. 즉 클라이언트-서버시스템의 각 구성부분을 크게 클라이언트, 서버, 네트워크로 구분하고 아키텍쳐통제는 이 세가지 구성부분 각각에 대한 보안정책으로 구성된다.

2.2.1 클라이언트에서의 보안정책수립

클라이언트 쪽에서의 보안정책을 정의한다. 이는 기업의 정책과 기업의 전반적인 전산환경의 정책에 의거하여 내용이 구성된다. 세부통제목적으로는 첫째, 기업 또는 부서의 정책이 클라이언트 쪽의 관리와 통제를 위하여 명확하게 수립되어 있음을 보장한다(MASP Consulting staff, 1994). 둘째, 클라이언트 워크스테이션의 승인된 사용자명부가 유효한 지를 보장한다. 셋째, 오직 승인된 사용자만이 데이타를 입력하거나 변경할 수 있음을 보장한다, 넷째, 워크스테이션 수준에서의 표현 기능에 대한 보안을 위하여 표현계층이 보안에 대한 규정을 준수하고 있음을 보장해야 한다. 예를 들면, 한 워크스테이션으로부터 LAN 통신 환경을 이용해 다른 워크스테이션 및 설비로 데이타를 라우팅 시켜봄으로써 통제상태를 검사할 수 있다(라우팅이 되면 표현계층의 통제가 제대로 이루어지지 않다는 것임). 다섯째, 오직 승인된 워크스테이션 만이 클라이언트-서버네트워크에 설치될 수 있음을 보장한다. 여섯째, 비 승인된 워크스테이션에 의한 갱신으로부터 마스터 데이타베이스를 보호한다. 일곱째, 워크스테이션장비에 남아 있는 다운로드된 데이타를 보호한다. 여덟째, 워크스테이션에서 소프트웨어의 사용이 합법적이고 승인된 정책에 의거하여 이루어지도록 한다.

2.2.2 서버에서의 보안정책수립

불법적인 접근권한을 최소화하고 클라이언트 워크스테이션에 대한 인증통제를 제공함으로써 서버의 데이터베이스에 대한 무결성을 보장한다(MASP Consulting staff, 1994a, 1994b). 세부통제목적으로는 첫째, 서버의 데이타베이스가 오직 승인된 워크스테이션과 사람에게만 접근이 허용되도록 한다. 예를 들어 데이타베이스로 질의접근을 허용할 수 있는 적절한 SQL 언어를 구현한다. 또한 데이타베이스에의 접근, 다운로드된

데이터 등을 기록한다. 둘째, 통제된 메카니즘 하에서 워크스테이션의 접근이 이루어지도록 한다. 예를 들어 워크스테이션이나 개인에 대한 인증, 권한통제 및 워크스테이션 접근통제를 위하여 라우터나 게이트웨이를 사용한 방화벽을 구축하는 것을 고려한다. 셋째, 서버의 데이타베이스로부터 다운로드된 데이타의 무결성과 신뢰성을 보호할 통제규정을 마련한다. 예를 들어 서버 데이타베이스로부터 다운로드된 데이타의 조작, 저장, 유포에 대하여 엄격한 규정을 수립한다. 넷째, 워크스테이션으로부터 서버의 데이타베이스로의 업로딩에 대한 통제를 제공한다. 예를 들어 서버의 중요한 마스터 데이타로의 업로딩시 엄격한 제한 규정을 수립한다.

2.2.3 네트워크 관리에 대한 보안정책수립

네트워크상에서 문제가 될 수 있는 위협을 사전에 방지하여 네트워크의 안전성을 높이는데 통제의 목적이 있다(Edwin, 1995; Jack, 1995). 세부통제목적으로는 첫째, LAN에 대한 통제가 신뢰할 수 있는 수준임을 보장한다. 예를 들어 LAN으로 연결된 환경에서 한 컴퓨터에서 다른 컴퓨터의 파일로 접근하는 것을 통제하는 보안 장치를 마련한다. 또한 LAN 서버를 포함한 LAN의 기기와 문서는 안전한 지역에 위치하여야 하며 LAN 파일서버의 키는 인가된 사람에 의해 발급되어야 한다(Ralph, 1995). 둘째, 접근통제소프트웨어에 의한 자동화된 네트워크통제가 바람직하다. 예를 들어 접근통제소프트웨어는 정보처리실에서 쓰이는 모든 종류의 파일과 프로그램을 통제할 수 있어야 한다. 또한 접근통제소프트웨어는 조직 전체의 요구수준과 일치하는 접근규칙을 제공하는 유연성을 지녀야 한다. 셋째, 네트워크 통제가 보다 잘 작동되도록 보장한다. 예를 들어 네트워크 관리 소프트웨어의 도입, 운영은 문서화된 경영자의 승인서를 획득한다. 또한 네트워크관리소프트웨어는 산업 표준으로 정의된 프로토콜을 지원해야 한다. 넷째, 자동화된 네트워크관리소프트웨어를 사용하는 것이 바람직하다. 다섯째, 공중회선을 통한 접근통제가 적절히 시행되도록 보장해야 한다. 여섯째, 네트워크운영체제(NOS: Network Operating System)의 구매 단계에서 여러 조건이 고려되어야 한다.

2.3 응용통제

실제사용 가능한 응용 시스템의 개발 및 운영은 클라이언트-서버 시스템에 있어서 가장 중요한 기능이다. 응용 시스템의 개발, 유지, 운영, 입출력, 처리에 대한 통제가 응용통제 영역이다. 본 논문에서는 응용통제를 종전에 응용통제의 구성항목인 입출력 및 처리통제뿐만 아니라 응용시스템 개발, 유지, 운영통제도 포함시켰다. 이는 분산화된 응용프로그램에 대한 통제가 중요해짐에 따라 응용시스템 개발, 유지, 운영, 입출력, 처리등에 대한 통제를 일관되게 하나의 범주로 분류하여 관리하는 것이 필요하기 때문이다.

2.3.1 응용 시스템 개발 과정에서의 통제

기업의 사업목표, 정보시스템 전략을 달성하고 정보시스템 정책과 절차, 정보시스템 운영을 지원하기 위하여 효과적이고 효율적으로 자원을 사용하여 서비스를 제공하도록 하는 것이 통제목적이다(Murphy and Parker, 1994; Weber, 1999). 세부통제목적으로는 첫째, 프로젝트 관리의 효과성 및 효율성을 증진하도록 해야 한다. 예를 들어 프로젝트일정을 통제하기 위해 마스터 플랜 검토, 절차의 적합성 검토, 마스터플랜의 이행정도 검토, 미래의 요구사항변경의 확인 등이 이루어져야 한다. 둘째, 시스템수명주기(System Development Life Cycle) 의 각 단계에서 적절한 통제가 이루어 짐을 보장한다. 예를 들어 요구사항정의단계에서 사용자의 정보 요구사항을 명확히 정의하여야 하고 개념적인 단계에서 통제의 유무를 결정하며 필요하면 설계 과정에 감사루틴삽입을 요구한다. 설계단계에서 입력, 처리, 출력요구사항의 정의, 문서화 및 통제가 잘 반영되어 있어야 한다. 테스트단계에서는 검증, 평가, 시험을 하기 위한 계획 및 기준이 설정되어 있어야 하고 그 테스트결과는 사용자 부서의 승인이 이루어진 후에 반드시 문서로 보존하여야 한다.

2.3.2 정보시스템의 유지 및 관리과정에서의 통제

시스템의 유지 및 관리란 응용프로그램의 수정과정을 말한다. 계속적인 보수 유지를 원활히 하기 위하여 변경 및 변경기록관리에 대한 표준 방법론을 설정하여 유지 및 관리에 대한 통제 지침으로 삼는다(Moeller, 1989). 세부통제목적으로는 첫째, 실운영프로그램에 대한 변경은 허가 절차에 따라 이루어지고 유지 및 관리 기록이 보존되도록 한다. 사용자의 변경요청서는 최소한 요청자성명, 요청일자, 완료일자, 우선순위, 변경내역 및 변경으로 인한 타 시스템에 미치는 영향 등이 포함되어 있어야 한다. 둘째, 시스템의 효과적인 이용과 유지 및 관리를 위해서 시스템 관련 문서들은 최신의 것으로 갱신되어 있어야 한다. 시스템 관련 문서들은 프로그램 및 시스템 흐름도, 프로그램 설명서, 데이타 목록(Data Dictionary), E-R 모듈, 데이타 흐름도, 운영자설명서, 사용자운영매뉴얼 등이 있다. 셋째, 시스템관리자에 의해서 수정된 프로그램은 실제 사용을 위한 설치 전에 철저하게 시험되어야 한다. 사용자가 시험 결과에 만족하면 사용자부서의 관리자로부터 승인을 얻고 그 증빙은 시스템 관리자에 의해 잘 보관되어야 한다. 테스트 환경에서 실제 사용 환경으로의 이관은 프로그래밍 팀과는 독립된 조직에서 행하여야 한다.

2.3.3 적용 업무 시스템의 입력, 처리, 출력 통제

각각의 적용업무시스템이 자산을 보호하고, 자료무결성을 유지하며, 그들의 목적을 달성하고 있고, 효율적으로 자료가 처리될 수 있도록 한다(Donn, 1994). 세부적인 통제목적으로는 첫째, 입력통제로써 데이타 입력작업 시 비 승인된 사용과 클라이언트 PC의 잘못된 사용을 판단할 수 있는 절차가 수립되어 있음을 보장한다. 또한 입력 데이터를 검증하는 절차를 수립한다. 예를 들면 입력 시 사용되는 클라이언트 PC는 물리적으로 안전한 장소에 위치하여야 하며 데이타 입력은 오직 승인된 권한을 가지고 있는 사람에 의해 수행되어야 한다. 클라이언트 PC의 비 승인된 사용을 방지하기 위하여 자료입력절차가 관리되며 패스워드를 사용해야 한다(Marro, 1995). 둘째, 처리통제로써 각 응용프로그램에 의해 처리되는 데이타가 처리 도중 추가, 삭제 및 변경되지 않도록 한다. 이를 위해 데이타처리에 대한 감사증적을 갖고 이를 유지하며 처리가 도중에 비정상적으로 종료된 작업은 반드시 기록되고 책임자에게 정기적으로 보고되어야 한다. 응용 시스템의 분리가 이루어진 서버와 클라이언트 쪽의 역할과 책임이 문서화되어야 한다. 셋째, 출력은 적절히 승인된 클라이언트 PC만이 가능하며 출력물도 적절히 통제되어야 한다. 사용자와 클라이언트 PC의 적절한 보안등급이 사전에 설정되어 있어 정해진 보안등급의 자료만이 출력될 수 있도록 한다.

Ⅲ. K은행의 사례연구

3.1 사례연구의 배경 및 설계

사례연구방법은 연구변수나 가설을 새롭게 탐색하고 몇가지 대상실체에 대한 심층적인 연구를 수행하기에 적합한 연구방법이다(Yin, 1993a, 1993b). 클라이언트/서버 환경으로의 이전사례 중 규모나 업무의 성격상 보안에 민감한 기업이나 클라이언트/서버 전산환경 하에서 보안시스템을 구축한 기업의 사례가 국내에서는 많지 않고 클라이언트-서버구축 사례에 대한 심층적인 연구를 위해서 사례연구방식을 연구방법으로 선택하였다. 규모나 업무의 성격상 보안에 민감한 금융산업에 속하면서 클라이언트-서버시스템 환경을 성공적으로 구축한 K 은행을 사례대상기업으로 선택하였다. 이러한 사례의 연구 목적은 클라이언트-서버통제가 현업에서 얼마나 이루어지는지를 점검하여 모형의 실제 적용가능성을 높이는데 있다.

K은행은 1991년 6월 다운 사이징의 일환으로 클라이언트-서버시스템 구축을 위한 검토에 착수하여 개발을 수행 후 1994년 1월부터 정상적인 업무를 개시하였다. K은행이 이러한 작업을 추진하게 된 배경에는 기존 시스템의 문제점들을 파악한 것이 계기가 되었는데 그러한 기존 시스템의 문제점들은 다음과 같다.

〈표 2〉 클라이언트-서버통제항목

통제계층	통제사항	통제항목	세부통제항목
관리통제	보안정책수립	전산화 장단기계획수립 정도	• 경영계획과 전산화계획의 상호연관성정도 • 회사의 경영계획이 전산화계획에 반영정도 • 계획수립의 표준화 및 절차 수립정도 • 부문(Interface) 설명정도 • 제 3자에 의한 검토정도 • 수립 방법의 수립정도
		전산자원에 대한 물리적 보안정책	• 빌딩이나 전산실 내로의 접근통제 수립정도 • 환경적 통제 장치 수립정도 • 설비관리계획 (3세부항목)
		인사정책	• 채용 및 승진 정책의 수립정도 • 계약직 사원의 보안관리에 대한 문서 수립정도 • 요원관리계획 (채용계획) (4 세부항목)
		기술사항들에 대한 문서화정도	• 검사기준의 문서화정도 • 평가기준의 수립정도 • 시스템구조에 대한 기술명세서의 수립정도 • 컴퓨터통신 및 네트워크구조에 대한 기술명세서의 수립정도
	재해복구계획	포함 내용 및 재해의 정의 기술 정도	• 복구계획의 문서화정도 • 재해의 분류정도 (어디서부터 재해인가를 구분하는 기준)
		재해 상황 시나리오	• 재해의 등급설정의 정도 및 각각의 시나리오 또는 전체 시나리오의 수립정도 • 테스트시행정도
		보험	• 형태 및 보증정도
		타 지역저장소	• 수립정도 • 보안통제정도 • 보관 중인 문서 및 소프트웨어의 갖춘 정도
	전이시 보안정책 수립	새로운 시스템에 대한 이해	• 교육훈련내용 및 종업원의 이해정도
		전이시 적용한 방법	• 전이방법에 대한 문서화정도
	신규 하드웨어, 소프트웨어 구입에 관한 보안 정책수립	구매정책	• 구매시 취득정책의 수립정도
		구입절차	• 구입절차의 문서화의 수립정도
		구매제도	• 공정한 구매 행위가 이루어질 수 있는 제도적 장치
		제안서 평가	• 공급자의 제안서를 평가하기 위한 기준의 문서화 수립정도
아키텍쳐 통제	클라이언트의 보안정책수립	클라이언트쪽 부서 정책의 수립정도	• 클라이언트에서의 서비스기능에 대한 접근제한정도 • 클라이언트의 원본사용지침에 관한 문서수립정도 • 업로드시 바이러스 체크를 위한 소프트웨어의 수립정도 • 원격지 서버에 대한 업로드, 다운로드절차의 문서화정도 • 클라이언트 사용시 의무사항에 대한 정책 (6세부항목)
		클라이언트 접속에 대한 기록보유	• 변경에 관련된 기록의 검토정도 • 논리적 접근권한에 대한 승인정책수립정도

〈표 2〉 클라이언트-서버통제항목(계속)

통제계층	통제사항	통제항목	세부통제항목
아키텍처 통제	클라이언트의 보안정책수립	접근통제	• 사용자에 대한 인증통제정도 (패스워드 등) • 민감한 수준에 따른 워크스테이션의 분류정도 • 물리적 접근통제에 대한 규정정도
		표현 기능에 대한 보안	• 서로 다른 기능의 접근 형태에 대한 승인 기능의 분류정도 • 승인을 위한 별도의 서버사용정도 • 기밀을 요하는 데이터에 대한 안전장치 제공정도 (3세부항목) • 외부통신망과의 연계관계 (3세부항목) • 워크스테이션의 작업로그의 보관정도 • 워크스테이션으로 다운로드된 데이타의 기록정도 • 클라이언트 관리자의 역할 -- 민감한 데이타의 PC내 존재를 파악할 수 있는지 정도 • 민감한 데이타에 대한 처분, 폐기 절차의 수립정도 • 보안 기능의 위임정도 (사무실 또는 지역 관리자에게) • 콜백 (Callback) 장치의 수립정도 • 부서차원의 LAN 운영에 대한 정책의 문서화정도 (3세부항목)
	서버의 보안정책수립	승인자만의 접근제한 정도	• 워크스테이션이나 개인의 인증, 권한에 대한 통제절차수립정도 • 방화벽의 설치정도
		통제된 메카니즘 활용 정도	• 데이터베이스로의 질의접근허용언어의 사용제한정도 • 감사증적기능의 수립정도
		다운로드된 데이타에 대한 통제규정	• 다운로드, 업로드에 대한 정책수립정도 • DB로부터 다운로드된 데이타의 조작, 저장, 유포에 대한 규정의 수립정도 (4세부항목)
		DB서버로의 업로드 통제 규정	• 서버DB로의 업로드에 대한 엄격한 통제규정수립정도
	네트워크의 보안정책 수립	LAN에 대한 통제	• 한 컴퓨터에서 다른 컴퓨터의 파일로의 접근을 통제하는 보안장치의 수립정도 • LAN서버 및 기기에 대한 물리적 보안장치 수립정도 • LAN 파일서버의 키 보관방법의 문서화정도 • 외부에서의 접속시 통제 방법의 문서화정도
		네트워크통제	• 운영오퍼레이터의 기술 자격조건에 대한 문서화정도 • 통제기능의 분류정도 • 네트워크 통제소프트웨어의 감사증적기록의 유지정도 • 감사 증적의 주기적 검토정도 • 통제단말기 설치정도 및 운영메뉴얼의 수립정도 • 네트워크 운영표준 및 프로토콜의 문서화정도 • 모니터링 기능의 수행정도 • 시스템의 효율성을 분석할 수 있는 방법의 수립정도 • 서브 시스템에 데이타 전송 시 물리적인 방벽의 수립정도 • 데이터에 대한 암호화기법의 수립정도
		자동화된 네트워크 관리 소프트웨어사용정도	• 도입에 대한 승인절차의 문서화정도 • 변경을 위한 문서화정도 • 자료 전송의 무결성을 제공하는 기능의 수립정도

〈표 2〉 클라이언트-서버통제항목(계속)

통제계층	통제사항	통제항목	세부통제항목
아키텍처 통제	네트워크의 보안정책 수립	공중회선을 통한 접근통제	• 접속을 승인하는 절차의 수립정도 • 콜백기기의 수립정도 • 자동화된 적절한 소프트웨어의 사용정도 • 접근 시도의 기록 및 이상 접근에 대한 보고체계정도
		NOS 구입에 대한 고려 사항	• 하드웨어 환경 검토항목 (5세부항목) • 기능면에서의 접근방법 (5세부항목)
응용통제	응용시스템 개발과정통제	프로젝트관리통제	• 목적에 대한 명확화된 문서화정도: 수행 원인, 환경, 범위, 제약 조건, 효익의 내용 등의 기록정도 • 팀원의 구성 및 책임분담의 문서화정도 • 적절한 관리자에 의한 타당성 분석, 대체안 검토, 수행정도의 결정에 대한 문서화정도 • 일정을 통제키 위한 마스터플랜수립정도
		시스템개발 각 단계에서의 통제	• 각 단계에서의 문서화정도 (6세부항목): 요구사항의 정의단계; 타당성검토; 설계단계; • 프로그래밍단계; 개발환경에서 실행환경으로의 전환; 테스트단계
	정보시스템 유지 및 관리과정에서의 통제	실운영프로그램에 대한 변경 관리	• 변경에 대한 허가절차수립정도 • 변경에 대한 유지 및 관리기록의 수립정도 • 변경 요청서의 수립정도 및 기록 보관정도
		시스템문서보유	• 최신 시스템 관련 문서의 보유정도
		프로그램에 검사	• 변경된 프로그램에 대한 검사방법
	정보시스템 입력, 처리, 출력통제	입력통제	• 입력 데이타의 검증방법의 수립정도 (3세부항목): 필드수준; 레코드수준; 파일수준
		처리통제	• 처리 도중 추가, 삭제, 변경에 대한 통제수립정도 (3세부항목)
		출력통제	• 승인된 클라이언트 만이 출력물이나 화면을 볼 수 있도록 하는 통제절차수립정도

첫째, 시스템규모의 확대 시 기존 시스템을 폐기해야 하므로 전산투자비용이 과다해진다. 둘째, 중요한 소프트웨어를 전산화하기 힘들고 공급업체에 예속되는 경향이 있어 보다 많은 비용을 지불해야 한다. 셋째, 시스템의 운영에 많은 전산인력을 필요로 하며 유지보수비용이 투자비용에 비례하여 확대된다. 넷째, 중앙 집중식 처리방식에 의한 금융시스템은 장애발생 시 전지역, 전지점의 시스템마비로 직결되어 고객의 손실뿐 아니라 사회적 기회비용 및 손실이 막대하다 (이대용. 및 안태주, 1994).

이러한 분석의 결과 UNIX 운영체제를 이용하여 지역분산 및 다운사이징시스템을 구축하였고 특정 하드웨어 공급업체에 예속되는 상태에서 탈피하고 소프트웨어 개발의 생산성을 향상시켰으며 시스템 규모의 확대시 투자비용 최소화를 통한 전산 투자비용 절감의 효과가 있었다.

K 은행의 전산감사담당자와 면담해 본 결과 보안시스템 구축에 있어서 다음의 사항들이 주요이슈가 되어 있음을 알 수 있었다. 첫째로는 조직차원의 문제로 새로운 시스템에 대한 이해부족 및 적응에 대한 거부감 그리고 조직구성원의 오해 내지는 반발이다. 둘째로는 클라이언트에서의 보안 문제로서 클라이언트에서의 패스워드 관리 및 클라이언트 PC에 대한 보안관리 문제이다. 세째로는 보안정책을 수립하는데 있어서 필수적인 문서화에 대한 어려움이었다. 국내 대부분의 기업에도 적용되는 문제로서 문서화에 있어

서의 미진한 수준이 전반적인 보안시스템 구축의 어려움으로 존재하고 있다.

본 연구에서 언급한 통제모형의 어느 부분이 반영되었으며, 또한 반영이 안 된 부분이 있으면 그 이유는 무엇인가에 대한 분석을 위해 전산팀장을 대상으로 면담을 실시하였다. 클라이언트-서버통제모형의 각 통제계층에 대한 체크리스트를 기존의 정보시스템 보안에 관한 문헌을(한국전산원, 1994; 1995; Bruce, 1995; Christine, 1995; Hale, 1996; Mark, 1995; Murphy and Parker, 1994) 참고하여 작성하였다. 클라이언트-서버시스템 통제항목은 <표 2>에 제시되었다. 각 세부항목에 대하여 5점척도로 통제의 수행정도를 측정하였다.

3.2 설문조사결과

클라이언트-서버 통제에 대한 조사의 전반적인 결과가 <표 3>에 제시되어 있다. <표 3>에 의하면 전반적으로 메인프레임환경에서도 중요한 통제요소인 관리통제와 응용통제에 대하여는 상대적으로 통제수행정도가 높게 나타나지만 클라이언트-서버 컴퓨팅 환경에서 특히 중요한 아키텍처통제는 상대적으로 통제수행정도가 낮다. 이것은 K 은행의 클라이언트-서버 시스템 환경의 아키텍처통제를 강화할 필요가 있다는 것을 나타낸다. 각각의 통제사항 및 항목에 대하여 통제수행정도를 나타내면 <표 4>와 같다.

세부항목별로 분석을 하여 보면 다음과 같다.

3.2.1 관리통제 측면

전반적인 측면에 비해 전이시 보안정책수립 부문이 취약하다. 조직 내 보안정책수립은 전체평균보다 높지만 인사정책부문은 상대적으로 낮은 수준(평균 2.1) 이다. 이는 조직이 현재까지의 주요이슈였던 시스템안정화에 치중함으로 인해 인사관리부문에 대한 통제를 강화하지 못했음을 나타낸다. 특히 필요한 인력의 선발기준을 아직껏 정립하지 못하고 있다. 관리통제에 대한 분석결과를 세분하여 제시하여 보면 다음과 같다.

1) 보안정책수립(기업 내 전반적인 IT 환경)

먼저 전산화 장단기계획 수립정도와 관련된 문항 중 총 6개의 세부질문에 대한 응답은 평균 3.8점을 받았으며, 전산 자원에 대한 물리적 보안정책수립 정도에 대한 부문에서는 총 5개의 세부질문에 대하여 점검을 한 결과 평균 3.8을 받아 보안정책수립 부문

〈표 3〉 K 은행의 통제요소점수

통제계층 및 통제사항	총점 및 세부항목 수	평 균
1. 관리통제	129점/35항목	3.7점
1.1 보안정책수립 (기업 내 전반적인 IT환경)	72점/21항목	3.4 점
1.2 재해복구계획	34점/8항목	4.3점
1.3 전이시 보안정책수립	5점/2항목	2.5점
1.4 신규 하드웨어, 소프트웨어구입에 대한 보안정책수립	18점/4항목	4.5점
2. 아키텍처통제	220점/74항목	2.9점
2.1 클라이언트의 보안정책수립	94점/32항목	2.9점
2.2 서버의 보안정책수립	28점/11항목	2.5점
2.3 네트워크의 보안정책수립	98점/31항목	3.2점
3. 응용통제	72점/22항목	3.3점
3.1 응용시스템 개발과정에서의 통제	31점/10항목	3.1점
3.2 유지 및 보수관리에서의 통제	20점/5항목	4.0점
3.3 입력, 처리, 출력상에서의 통제	21점/7항목	3.0점
종 합	421점/131항목	3.2점

〈표 4〉 K 은행의 통제세부항목 점수

통제계층	통제사항	통제항목	세부 항목수	점수	평균
관리통제	보안정책수립	전산화 장단기계획의 수립정도	6	23	3.8
		전산자원에 대한 물리적 보안정책	5	19	3.8
		인사정책	6	13	2.1
		기술사항들에 대한 문서화정도	4	17	4.3
	재해복구계획	포함 내용및 재해의 정의의 기술사용정도	2	8	4.0
		재해상황시나리오	2	8	4.0
		보험	1	5	5.0
		타 지역저장소	3	13	4.3
	전이시 보안정책수립	새로운 시스템에 대한 이해	1	2	2
		전이시 적용한 방법	1	3	3
	신규 하드웨어, 소프트웨어 구입에 관한 보안정책수립	구매시 취득정책	1	4	4
		구입절차	1	5	5
		구매제도	1	6	6
		제안서평가	1	3	3
아키텍처통제	클라이언트의 보안정책수립	클라이언트쪽 부서에 대한 정책의 수립정도	10	31	3.1
		클라이언트 접속에 대한 기록보유	2	10	5.0
		접근통제	3	11	3.7
		표현기능에 대한 보안	17	42	2.5
	서버의 보안정책수립	승인자만의 접근제한정도	2	8	4.0
		통제된 메커니즘 활용정도	2	8	4.0
		다운로드된 데이타에 대한 통제규정	5	7	1.4
		DB서버로의 업로드에 대한 통제규정	1	5	5.0
	네크워크의 보안정책수립	LAN에 대한 통제	4	14	3.5
		네트워크통제	10	29	2.9
		자동화된 네트워크관리 소프트웨어사용정도	3	9	3.0
		공중회선을 통한 접근통제	4	7	1.8
		NOS구입에 대한 고려사항	10	39	3.9
응용통제	응용시스템 개발과정 통제	프로젝트 관리통제	4	17	4.3
		시스템개발 각 단계에서의 통제	6	14	2.3
	정보시스템 유지 및 관리과정에서의 통제	실 운영 프로그램의 변경에 대한 관리	3	15	5.0
		최신 시스템 관련 문서에 대한 보유정도	1	3	3.0
		변경된 프로그램에 대한 검사방법	1	2	2.0
	정보시스템 입력, 처리, 출력통제	입력통제	3	9	3.0
		처리통제	3	10	3.3
		출력통제	1	2	2.0

의 전체평균(3.4점) 보다 높다. 그러나 인사정책부문의 총 6개의 세부질문에 대한 응답은 평균 2.1점을 받음으로써 이 부문의 통제가 취약함을 보여 주었다.

이는 조직내 채용 및 승진정책은 수립이 되어 있으나 아직 클라이언트-서버시스템의 안정화에 치중한 결과 장래의 인원관리계획(채용계획) 이 다소 충실하지 못해진 것으로 해석된다.

그리고 마지막으로 기술사항들에 대한 문서화

정도에 관련된 총 4개의 세부질문에 대한 응답은 평균 4.3점을 받아 다른 부문들에 비해 이 부문에 대한 통제가 상대적으로 잘 되어 있음을 보여 준다.

2) 재해복구계획

재해의 정의에 대한 기술정도 및 재해계획의 포함 내용 부문에 관련된 총 2개의 세부질문에 대한 응답은 평균 4.0점을 받았으며, 재해상황시나리오의 존재 및 테스트 정도를 묻는 총 2개의 세부질문에 대한 응답은 평균 4.0을 받았다. 보험부문은 평균 5.0점을 받았고 마지막으로 타지역 저장소에 대한 부문은 총 3개의 세부질문에 대해 평균 4.3점을 받았다. 전반적으로 재해복구계획에 대하여는 높은 평균점(4.3점)을 받아서 재해복구계획이 잘 준비된 것을 나타낸다. 이는 K 은행이 속한 은행업의 특성상 재해복구계획이 잘 파악되고 준비된 것을 나타낸다.

3) 전이시 보안정책수립

새로운 시스템에 대한 교육 훈련 정도를 묻는 질문에 대한 응답은 평균 2.0점을 받았으며, 전이시 적용한 보안통제를 수립한 정도를 묻는 질문에 대한 응답은 3.0점을 받아 전이시 보안정책수립의 전체 평균은 2.5점을 기록하여 전이시 보안통제의 수립이 더 필요함을 나타내었다.

4) 신규 하드웨어, 소프트웨어 구입에 대한 보안정책수립

구매시 취득 정책의 수립정도 및 내용 확인, 구입절차의 문서화 수립정도, 공정한 구매행위가 이루어질 수 있는 제도적 장치의 수립정도를 묻는 질문에 대한 응답은 5.0점을 받았으나, 공급자의 제안서를 평가하기 위한 기준의 문서화 수립정도를 묻는 질문에 대한 응답은 3.0점을 받았다. 신규 하드웨어, 소프트웨어 구입에 대한 보안정책수립 부문은 전체 평균이 4.5점으로 전항목을 통해 가장 높은 점수를 받은 것으로 나타났다. 따라서 신규 하드웨어 및 소프트웨어 구입에 대한 보안정책은 잘 수립되어 있다고 볼 수 있고 공급자의 제안서 평가기준에 대한 문서화 작업이 이루어진다면 더욱 효과적일 것으로 여겨진다.

3.2.2 아키텍쳐통제 측면

다른 통제 영역보다 평균이 낮다(평균 2.9점). 이는 클라이언트-서버 특수한 환경을 고려한 보안통제는 아직 충분히 수립되지 못한 것을 나타낸다. 특히, 과거 메인프레임환경에서는 중앙의 호스트에 대한 통제만 치중하면 되었으나 클라이언트-서버시스템 환경에서는 클라이언트에 대한 통제가 주요 부문을 차지하는데도 불구하고 이러한 특성을 고려하지 못하고 통제가 구현되고 있음을 나타낸다. 특히 클라이언트 쪽으로 다운로드된 데이타의 관리에 대하여는 아직 명확한 관리 지침이 준비가 안되어 있는 것으로 나타났다.

1) 보안정책수립(클라이언트 측)

클라이언트 쪽의 관리와 통제를 위한 정책의 수립정도를 묻는 항목은 총 10 개로서 평균 3.1점의 점수를 받았다. 그리고 클라이언트에서 서버로 업로딩시 바이러스 체크를 위한 소프트웨어가 전혀 없다는 것이 문제로 지적되었다. 두번째 클라이언트에의 접속에 대한 기록 및 그 기록의 보관 정도에 관련된 총 2개의 질문은 평균 5.0점을 얻었다. 세번째 접근통제를 묻는 총 3개의 질문은 평균 3.7점을 받았다. 그리고 네번째 워크스테이션 수준에서의 표현기능에 대한 보안에 관한 총 17개의 질문은 평균 2.5점을 받았다. 특히 콜백(callback) 절차나 부서차원의 LAN 운영에 대한 정책의 문서화 정도는 0점을 받아 이 부문의 통제수립이 취약함을 나타내었다.

2) 보안정책수립(서버측)

오직 승인된 사람이나 워크 스테이션 만이 서버의 데이타베이스로의 접근이 제한되는지에 대한 2개의 질문은 평균 4.0점을 받았으며, 워크스테이션의 접근통제부문에 관련된 2개의 질문은 평균 4.0점을 받았다. 다운로드된 데이타의 무결성, 신뢰성을 보호할 통제규정에 관련된 총 5개의 질문은 평균 1.4점을 받아

이 부문에서 매우 저조한 통제수립정도를 나타내었다. 이는 다운로드된 데이타에 대한 통제나 다이얼-업에 대한 통제가 매우 취약함을 나타낸다.

3) 보안정책수립(네트워크 관리)

먼저 LAN에 대한 통제와 관련된 4개의 질문은 평균 3.5점을 받았으며, 네트워크통제에 관련된 10개의 질문은 평균 2.9점을 받았다. 반면에 서브 시스템에 데이타 전송시 물리적인 방호벽의 존재를 묻는 질문은 1점을 받아서 이 부분에 대한 보안이 필요함을 나타냈다. 자동화된 네트워크 관리 소프트웨어의 사용정도를 묻는 총 3개의 세부질문은 평균 3.0을 받았다. 그리고 공중 회선을 통한 접근통제에 관련된 총 4개의 질문은 평균 1.8을 받아 이 부문의 통제수립정도가 매우 취약한 것으로 나타났다. 특히 콜백장비의 보유정도(0점), 적절한 소프트웨어의 사용정도(0점), 접근 시도의 기록 및 이산 접근에 대한 보고 체계 정도(2점)는 취약한 상태임이 제시되었다. 다섯번째로 네트워크운영시스템(Network Operating System) 구입에 관련된 총 10개의 질문은 평균 3.9점을 받았다.

3.3.3 응용통제 측면

응용통제의 수립정도는 전체 시스템의 통제수립정도의 평균과 비슷한 정도이다(평균 3.3). 전반적으로 양호하나 시스템개발 각 단계에서의 문서화정도가 미비한 것으로(약 2.3) 평가되었으며. 클라이언트에 대한 출력물통제가 미비한 것으로 나타났다.

1) 응용 시스템 개발 과정에서의 통제

프로젝트 관리에서의 통제에 관련된 4개의 질문은 평균 4.3점을 받았으나 시스템개발(System Development Life Cycle) 각 단계에서의 통제에 관련된 총 6개의 질문은 2.3점을 얻어 이 부문에 대한 좀 더 적극적인 통제가 필요한 것으로 나타났다.

2) 유지 보수 관리에서의 통제

실제 운영 프로그램에 대한 변경관리부문에 관련된 3개의 질문은 평균 5.0점을 받았고 최신의 시스템 관련문서의 보유정도에 대한 질문은 3.0점을 받았다. 변경된 소프트웨어에 대한 검사절차는 다소 미흡하였다(2.0점). 따라서 변경된 소프트웨어에 대한 체계적인 검사절차를 수립할 필요가 있는 것으로 제시되었다.

3) 입력, 처리, 출력 상에서의 통제

입력통제에 관련된 문항은 3.0점을 받았고, 처리통제에 관련된 3개의 질문은 평균 3.3점을 받았다. 반면에 출력통제에 관련된 문항은 2.0점을 받아 출력통제에 대한 절차 수립 및 구현이 상대적으로 필요한 것으로 나타났다.

3.3 사례분석 및 토의

K은행의 사례분석 결과가 <표 5>에 제시되어 있다. 이러한 사례분석결과, 본 연구에서 제시한 클라이언트-서버시스템 통제모형을 적용하고 통제의 수립정도를 체크하여 현재의 취약한 통제부문과 향후 대책방안을 제시할 수 있었다.

사례조사결과 보안 업무에 관계된 사람들은 보안대책의 필요성은 충분히 공감하고 있으나 전반적인 조직 구성원들은 아직 보안통제에 관한 의식을 많이 갖고 있지 못하고 있음이 제시되었다. 보안통제의 구현에 있어서도 구체적인 방법이 정립되지 못하였고 필요한 인원의 확보도 미진한 것으로 나타났다.

클라이언트-서버 환경에 맞는 보안정책수립정도도 미진한 것으로 보이며 클라이언트나 서버 쪽에서의 통제 지침이 아직은 부족한 것으로 나타났다(예: 서버에서의 업로드된 데이타에 대한 바이러스체크, 클라이언트에서의 다운로드된 데이타에 대한 폐기정책 등).

현재 분석된 결과를 토대로 대상 기업에 대한 효과적인 보안시스템 구축에 대한 제안을 하기 위해 본 연구에서 제시된 모델에 대하여 각 통제계층에서 대표적으로 미진한 부분에 대해 요약하면 다음과 같은 항목을 꼽을 수 있다. 관리통제에서는 장기적인 전산운영계획을 수립하고 그에 준하여 필요인원에 대한 인원채용계획을 수립하는 것과, 시스템환경의 변화에

〈표 5〉 K 은행의 각 통제 부문 분석 결과

통제계층	현재 취약한 통제부문	향후 강화해야 할 통제부문
관리통제	• 전이시 보안정책수립 부문이 취약 • 조직 내 보안정책수립은 전체평균보다 높지만 인사정책부문은 상대적으로 낮은 수준 • 조직이 현재까지의 주요이슈였던 시스템 안정화에 치중함으로 인해 인사관리부문에 대한 통제를 강화하지 못했음 • 필요한 인력의 선발기준을 아직껏 정립하지 못하고 있음	• 장기적인 전산운영계획을 수립하고 그에 준하여 필요인원에 대한 인원채용계획을 수립강화 • 시스템환경의 변화에 대비한 시스템변환과정에서의 보안정책을 수립하는 것이 필요 • 조직내 보안에 대한 이해를 높이는 방법으로 지속적인 교육 및 훈련강화
아키텍처통제	• 관리나 응용통제보다 통제수립정도 취약 • 클라이언트-서버 특수한 환경을 고려한 보안통제는 아직 충분히 수립되지 못함 • 클라이언트에 대한 통제가 충분히 수립되어 있지 못함 • 클라이언트 쪽으로 다운로드된 데이타의 관리에 대하여는 아직 명확한 관리 지침이 준비가 안되어 있음	• 클라이언트의 표현기능에 대한 보안관리강화 • 데이타베이스서버에서의 클라이언트쪽으로 다운로드된 데이타에 대한 통제규정수립강화 • 공중회선을 통한 접근에 대한 통제규정수립과 모니터링 기능의 확보
응용통제	• 전반적으로 통제 수립정도는 시스템 전체 평균보다 약간 양호한 편임 • 시스템개발 각 단계에서의 문서화정도가 미비한 수준 (약 2.3) 으로 평가 • 클라이언트에 대한 출력물통제가 미비	• 응용시스템 개발과정에서 시스템개발 각 계층에서의 문서화통제강화 • 정보시스템 유지 및 관리과정에서 변경된 프로그램에 대한 검사방법 수립 • 출력통제에 대한 규정의 수립 및 확보

대비하여 시스템변환과정에 적용되는 보안정책을 수립하여야 한다. 그외에 조직구성원의 보안에 대한 이해를 높이는 방법으로 지속적인 교육 및 훈련이 필요하다.

아키텍처통제에서는 클라이언트의 표현기능에 대한 보안관리, 데이타베이스서버에서의 클라이언트쪽으로 다운로드된 데이타에 대한 통제규정수립, 그리고 네트워크에 대한 보안정책수립 중 공중회선을 통한 접근에 대한 통제규정수립과 모니터링 기능의 확보가 중요하다.

응용통제계층에서는 응용시스템 개발과정에서 시스템개발 각 단계에서의 문서화수립, 변경된 프로그램에 대한 검사방법, 그리고 출력통제에 대한 규정을 수립하고 준수하는 것이 중요하다.

본 연구는 클라이언트-서버 컴퓨팅 환경에서의 보안시스템 구축에 있어서 일종의 가이드-라인을 제시하고자 하는 목적으로 연구되었다. 본 연구는 새로운 컴퓨터 운영 환경인 클라이언트-서버시스템에서의 보안 관련 연구를 초기 단계로 시도한 것이라고 할 수 있겠다. 본 연구에서 제시된 클라이언트-서버통제모형은 신속히 변화하는 전산운영 환경에서 효과적으로 통제체계를 구축하는데 도움을 줄 수 있을 것이다. 클라이언트-서버시스템을 구축한 기업 전산시스템관리자 들은 체계적인 통제모형을 통하여 클라이언트-서버시스템의 위험요소 및 통제취약점을 파악하여 보안관리를 효과적으로 수행할 수 있을 것이다.

Ⅳ. 결 론

클라이언트-서버시스템을 운영중인 각 조직에서는 이제 시스템의 안정화의 단계를 거치고 있다. 이러한 안정화단계에서 시스템 성과의 관리를 위하여 보안통제의 중요성은 크다. 특히 여러 사회적인 요인(컴퓨터 범죄의 증가, 해커로 인한 국가적인 피해의 증대

등) 으로 인해 클라이언트-서버 보안에 대한 필요성이 더욱 높아지게 되었다. 특히 클라이언트-서버시스템의 주요 특징인 응용프로그램의 분리로 인하여 보안통제의 어려움이 증가하고 있다. 과거중앙집중식의 보안관리에서 지역적으로 보안관리자를 선임하고 그들 간의 보안정보 공유체계가 필요하게 되었으며 기술적으로는 수작업에 의한 보안관리보다는 자동화된 보안관리가 필요하게 되었다.

본 논문에서는 클라이언트-서버통제모형을 관리, 아키텍쳐, 응용통제로 구분하였다. 관리통제는 조직차원의 보안정책수립과 관련된 부문으로써 이는 다른 두 부문의 기본이 되는 부문이라고 할 수 있다. 이에는 조직차원의 보안정책수립, 재해복구계획, 메인프레임에서 클라이언트-서버시스템으로의 전이시 보안정책, 신규 하드웨어/소프트웨어 구입에 관한 보안정책 등의 부문이 있다. 아키텍쳐통제는 시스템아키텍쳐에 대한 통제로서 각 조직의 전산환경에 따라 다를 수 있다. 이 부문통제는 클라이언트에 대한 보안정책, 서버에 대한 보안정책, 네트워크관리에 대한 보안정책 등으로 구성된다. 응용통제는 실제 운영되는 응용프로그램의 보안통제부문으로써 실제 프로그램 개발, 유지 및 운영에서 고려하여야 할 보안요소를 언급한다. 이에는 응용시스템개발과정에서의 통제요소, 유지보수관리에서의 통제요소, 입력, 처리, 출력에서의 통제부문이 있다.

본 연구의 통제모형의 적용가능성을 검증하기 위해 실제로 클라이언트-서버를 구축한 K은행을 대상으로 하여 사례연구를 실시하였다. 연구결과 관리, 아키텍쳐, 및 응용통제부문에서 현재 시스템의 통제취약점이 어느 부분인지를 파악할 수 있었고 필요한 세부통제항목 들을 제시할 수 있었다. 이러한 통제모형은 클라이언트-서버시스템의 보안관리 및 통제설계에 효과성 및 효율성을 증진시킬 수 있을 것이다.

클라이언트-서버 시스템은 데이터베이스, 네트워크, 응용시스템 등이 복합적으로 구성된 시스템이다. 시스템의 자산을 보호하고 정보의 정확성과 신뢰성을 높이기 위하여 본 논문에서 제시한 클라이언트-서버 시스템 보안통제모형이 적용되어질 수 있다. 관리, 아키텍쳐 및 응용통제는 서로 독립적으로 평가되어질 수 있으나 서로 연관관계를 가진다. 즉 관리통제는 전반적인 통제환경과 관련이 있고 아키텍쳐 및 응용통제는 각각 클라이언트-서버 시스템의 구조와 특정 응용프로그램의 통제와 직접 연결된다. 따라서 관리통제는 클라이언트-서버 시스템을 도입한 기업의 전산 업무처리에 공통으로 적용되는 통제로서 아키텍쳐 및 응용통제를 수립하기 위한 기초가 된다고 할 수 있다. 클라이언트-서버 시스템의 이러한 계층화된 통제모형은 여러 가지 다른 클라이언트-서버 통제구조를 평가하거나 벤치마킹하는데 유용하게 쓰일 수 있다.

본 연구가 제시하는 앞으로의 연구방향에 대한 시사점은 다음과 같다. 우선 정보시스템의 통제모형 및 체계에 대한 미래의 연구에서는 정보시스템의 구조적 특성뿐 아니라 도입 목적 및 통제목적 등에 따라 상이한 통제모형을 제시해줄 필요가 있다. 정보시스템의 통제는 정보시스템의 도입 목적에 따라 다르게 적용되어야 하고 이에 따라 각 통제가 어떻게 다라져야 하는지를 제시해주어야 할 것이다. 예를 들면 정보의 신속성이 강조되는 시스템은 정보의 기밀성이 보다 강조되어야 하는 시스템과 요구되는 통제항목이 달라질 것이다. 두번째로 클라이언트-서버 시스템에 대한 본 연구의 통제모형에서는 보다 구체적인 클라이언트-서버 시스템 아키텍쳐 특성(예: 클라이언트-서버 시스템의 중요수행프로그램의 분포) 에 따라 어떻게 통제가 달라져야 하는지를 제시해줄 필요가 있을 것이다. 예를 들면 아키텍쳐 통제부분에서 클라이언트, 서버, 그리고 네트워크 보안통제에 대한 중요성은 응용시스템, 데이터베이스관리시스템, 프레젠테이션서비스 등의 클라이언트-서버 시스템의 중요수행프로그램이 클라이언트와 서버에 분리된 정도에 따라 달라질 수 있을 것이다. 즉 클라이언트에 응용시스템, 데이터베이스관리시스템, 프레젠테이션서비스 등이 집중되어 있으면 클라이언트 통제에 대한 중요성이 높아져야 하고 분산된 사용자 및 프로그램, 데이터에 대한 통

제가 필요하다. 반대로 서버에 클라이언트-서버 시스템의 중요수행프로그램이 집중된 경우에 상대적으로 통제관리가 수월해지지만 집중된 데이터 및 프로그램에 대한 비상계획 및 복구계획의 중요성이 커질 것이다.

참 고 문 헌

이대용, 안태주, "광주 은행의 분산처리 시스템," 추계 한국경영정보시스템학술 대회논문집, 1994, pp.403-423.

한국전산원, *전산망 안전 보안 구축 실무 지침*, 제1호, 1994.

한국전산원, *전산망 안전 보안 구축 실무 지침*, 제2호, 1995.

Anandarajan, M. and B. Arinze, "Matching Client/ server Processing Architectures with Information Processing Requirements: A Contingency Study," *Information & Management*, 34, 1998, PP.265 -274.

Belden, M., "Too Many Client/Server Systems Ignore Security, Quality, and Auditability," *EDPACS*, Vol. 22, No. 7, January 1995.

Bruce, M. C., "PC Security Criteria A to Z," *IS Audit & Control Journal*, Vol. V, 1995, pp.27-32.

Cairo, L. and F. Alan, "Security Client/Server: Authen- tication Issues," *IS Audit & Control Journal*, Vol. V, 1995, pp.48-53.

Charles, C. W. and S. Karen, "ISO 9000 Information Security," *Computer & Security*, Vol. 14, No. 4, 1995, pp.287-288.

Charles, C. W., "Shifting Information Systems Security Responsibility from User Organizations to Vendor/ Publisher Organizations," *Computer & Security*, Vol. 14, No. 4, 1995, pp.283-284.

Chengalur-Smith, I. and Duchessi, P. "The Initiation and Adoption of Client-server Technology in Organiza- tions," *Information & Management*, 35, 1999, pp.77-88.

Christine, A., "The OECD Guidelines for the Security of Information Systems," *EDPACS*, Vol. 22, No. 10, April 1995.

David, E., "Marketing the Information Systems Security Program," *EDPACS*, Vol. 23, No. 2, August 1995.

Donn, B. P., "A Guide to Selecting and Implementing Security Control," *IS Security*, Summer 1994, pp.75-86.

Drury, D.H., "Chargeback systems in client/server environments," *Information & Management*, 32, 1997, pp.177-186.

Edwin, B. H., "Principles of Information System Secu- rity," *Computer & Security*, Vol. 14, No. 3, 1995, pp.197-198.

Hale, R., "End-User Computing Security Guidelines," *IS Security*, Winter 1996, pp.49-64.

Hitchings, J., "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology," *Computers & Security*, Vol. 14, No. 5, 1995, pp.377-383.

ISACF (Information Systems Audit and Control Foun- dation), COBIT (Control Objectives for Information and Related Technology) Framework, Illinois USA, April 1996.

Jack, J. C., "Is Your Wire Transfer System Secure?," *Internal Auditor*, June 1995, pp.56-59.

Jess, B., "Auditing Client/Server Information Processing," *EDPACS*, Vol. 22, No. 8, February 1995.

Kenneth, Y., "A Model for Disaster Recovering Planning," *IS Audit & Control Journal*, Vol. V, 1995, pp.45-51.

Linda, L. L., "Third Party Software," *Internal Auditor*, April 1995, pp.44-47.

MASP Consulting staff, "Distributed Client/Server Archi- tectures - Security and Control Implications - Part 1," *COM-SAC*, Vol. 21, No. 2, 1994a.

MASP Consulting staff, "Distributed Client/Server Archi- tectures - Security and Control Implications - Part 2," *COM-SAC*, Vol. 21, No. 3, 1994b.

Mark, B., "Developing End-User Computing Guidelines," *EDPACS*, Vol. 22, No. 12, June 1995.

Marro, P. E., "Overview of Computer Crime and Secu- rity," *IS Audit & Control Journal*, Vol. V, 1995, pp.20-25.

Moeller, R. R., *Computer Audit, Control, and Security*, John Wiley & Sons, 1989.

Murphy, M. A., and X. L. Parker, *Handbook of EDP Auditing*, Warren Gorham Lamont, 1994.

Ralph, P. M., "Single Sign-on and Security in a Client/ Server Environment," *IS Security*, Fall 1995, pp.38-45.

Runge, L., "Security and Data Integrity in a Client-Server Environment," *IS Security*, Spring 1994, pp.45-56.

Runge, L., "Security and the Transition to Client/ Server Computing," *IS Security*, Spring 1996, pp.49-57.

Ryan, S. D. and B. Bordoloi, "Evaluating Security Threats in Mainframe and Client/server Environments," *Information & Management*, 32, 1997, pp.137-146.

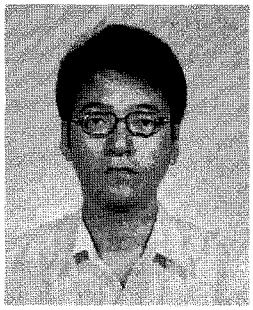
Scott, H. and S. Martin, "Risk Management & Corpo- rate Security: A viable Leadership anBusiness Solution Designed to Enhance Corporations in the Emerging Marketplace," *Computer & Security*, Vol. 14, No. 3, 1995, pp.199-204.

Weber, R., *Information Systems Audit and Control*, Mc- Graw-Hill, 1999.

Yin, R. K., *Application of Case Study Research*, SAGE Publications, 1993a.

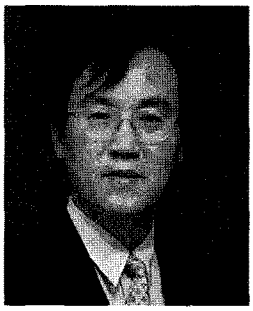
Yin, R. K., *Case Study Research*, SAGE Publications, 1993b.

◐ 저 자 소 개 ◑



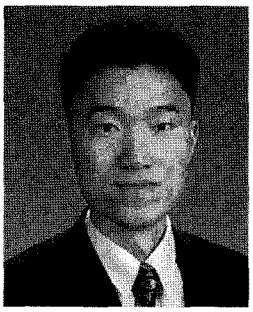
남 성 우 (seongwoo@www.kdn.com)

공동저자 남성우는 고려대학교에서 지질학 학사를 받고 한국과학기술원에서 경영정보공학 전공으로 석사학위를 받았다. 삼보지질(주)에서 기획팀장을 역임하였고 현재 한전정보네트워크(주)에서 컨설팅 분야 차장으로 근무하고 있다. 특히, Y2K 문제 해결 프로젝트에 1997년부터 한국전력, 에너지관리공단, 지역난방공사, 금융결제원등의 프로젝트관리자로 활동하고 있다. 저서로는 '컴퓨터 2000년 문제해결 방법론(1998.9, 진한도서)'이 있다.



한 인 구 (ighan@kgsm.kaist.ac.kr)

공동저자 한인구는 서울대학교에서 국제경제학 학사를 받고 한국과학기술원에서 경영과학 전공으로 석사학위를 받고 University of Illinois at Urbana-Champaign 에서 회계정보시스템을 전공하여 경영학박사학위를 취득하였다. 국민대학교 회계학과 조교수를 역임하였고 현재 한국과학기술원 테크노경영대학원 부교수로 재직하고 있다. 주요관심분야는 인공지능을 이용한 주가예측, 신용평가 및 도산예측, 정보시스템감사 및 보안등이다



이 상 재 (sangjae@kgsm.kaist.ac.kr)

공동저자 이상재는 한국과학기술원에서 경영정보공학으로 공학박사를 취득하였다. 현재 한국과학기술원 테크노경영연구소 연구원으로 재직하고 있다. 그는 국제공인정보시스템감사사 (CISA)이다. 주요연구분야는 Electronic Data Interchange (EDI)를 포함한 전자상거래시스템의 확산, 통제 및 감사 그리고 인공지능을 이용한 감사 및 통제제안 지원시스템 등이다.