경영정보학연구
제8권 제2호
1998년 9월

국내 주요그룹의 정보보안관리 체계에 관한 사례 연구

선 한 길*, 한 인 구**

A Case Study on the Information Security Management System for Major Korean Businessn Groups

Sun, Han-Gil, Han In-Goo

As the first step to information security, the security policy and organizational control need to be established. The purpose of this study is to investigate the policy and management of information security of five major Korean business groups. The results of case study on five giant groups can be summarized as follows. There exists a basic policy for information security. But it is outdated and not realistic in the present. The security audit and education need to be upgraded. It is also necessary to use security tools actively. The security level is low in companies which do not have independent information security divisions. Therefore, it is desirable to build information security teams. The number of security personnel is not enough for the task although there exist an information security team in the company. It is important to check if the team has the ability of perform information security task.

The interview with security managers reveals that the total security management should be integrated with physical and computer security. It is suggested that an Information Security Center play the major role for information security. The study on the information security management for industry level is expected to be performed in the future.

* 한국사회경제연구소
** 한국과학기술원 테크노경영대학원

Ⅰ. 서 론

정보보안 관리의 연구 동향을 살펴보면, 그동안 공공기관이나 금융기관 등에서 논문이나 세미나 등을 통해 부분적으로 발표한 적은 있으나 일반 기업체, 특히 우리나라 재계를 대표하는 재벌 그룹들에 대한 정보보안 관리 연구는 찾아보기가 힘들다. 그 이유는 아마도 '보안'이라는 말 뜻 그대로 감추어져 있어서 연구자료를 구하기가 쉽지 않기 때문일 것이다.

정보보안이라고 하면 당연히 고도의 기술과 값비싼 장비를 떠올리기 쉽지만 업무를 보고 있는 책상 주변의 정리, 서류함의 시건장치, 출입인원 관리, 컴퓨터의 패스워드 설정 등 가장 기본적이고 하기 쉬운 일부터 그 시작이 되고 있다. 본 연구에서는 정보보안의 기본을 이루고 있는 정책과 조직의 모델에 대해서 연구하고자 한다. 우리나라 기업체들, 특히 대기업군의 관리 실태를 조사하여 모범적인 기업 정보보안 체계의 사례를 연구해 보려고 한다.

본 연구의 목적은 재계 순위4위 안에 드는 L그룹, S그룹, H그룹, D그룹 등과 P그룹을 포함한 5대 국내 주요그룹에 대한 정보보안 관리 사례를 조사함으로써 보다 발전적이고 바람직한 정보보안 관리 시스템을 연구하고자 하는 것이다. 우선 연구 대상업체는 그룹별, 업종별로 18개 회사를 선정하였다. 업종은 그룹들이 가장 많이 진출해 있는 시스템 통합업(SI), 화학제품 제조업, 전자제품 제조업, 금속산업, 금융서비스업, 무역유통업, 건설업, 중공업 등 8가지이다. 이 18개 회사들에 대해 정보보안 관련 부서에 접촉을 해 본 결과 긍정적인 반응을 얻어 인터뷰를 하였다.

보안성에 영향을 주는 정책/조직적 모형을 만들어 보안 정책적 요인들과 보안 조직적 요인들을 도출해 내었으며, 대상 회사별로 지수를 내어 비교 분석해 보았다.

본 논문의 구성은 제2장에서 정보보안 관리체계, 제3장에서 보안성에 영향을 주는 정책/조직적 모형을 설명하고 제4장에서 정보보안 관리시스템 사례연구를 한 후 제5장에서 결론을 내는 것으로 되어 있다.

Ⅱ. 정보보안 관리체계

2.1 정보보안 관리 및 정책

최근 정보시스템의 사회적 중요성은 한층 높아지고 있으며 이의 정상적 기능의 유지는 건전하고 효율적인 사회를 유지하는 데에 무엇보다도 중요한 요소로 자리잡게 되었다.

1960년대 초 시분할 시스템과 멀티 프로그래밍의 등장과 더불어 정보시스템의 보안에 대한 필요성이 인식되기 시작하였으며[Wilkes, 1991], 1967년에 미국에서 개최된 National Joint Computer Conference 에서 컴퓨터 보안이 최초로 공개적으로 논의되기 시작하였다[Ware, 1988].

정보보안이란 '정보를 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐서 보안하는 것'을 말하며, '시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터의 보안'이라고도 정의한다.

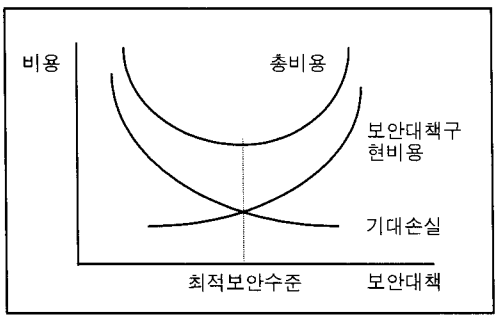
정보보안 위협의 형태에 대해 살펴보면 크게 형태별, 장소별, 의도적 분류로 나눌 수 있으며 형태별 분류로는 범죄, 부정행위, 자연재해, 인적재해, 고장, 오류 등, 장소별 분류로는 컴퓨터 시스템의 내부, 외부 등, 의도적 분류로는 의도적, 비의도적 등으로 분류할 수 있다.

정보보안에 대한 공격의 종류는 방해(Interruption), 가로채기(Interception), 불법수정(Modification), 위조(Fabrication) 등이 있다[Stallings, 1995].

보안정책이란 보호 될 필요가 있는 것과 그것들을 보안하기 위하여 지원되어야 하는 자원

의 수준을 결정하기 위한 판단과 그에 따른 대책을 미리 수립하는 것이다[임채호 외, 1994].

정보시스템의 안전한 운용을 위한 보안대책의 선정은 개별 시스템의 특성 및 운용 환경에 따라 다르나, 보안대책의 구현 및 운용 비용과 구현된 보안 대책에 의해서도 보안되지 않는 위험에 의한 기대 손실의 합계인 총비용이 최저가 되는 수준에서 보안대책을 강구한다. 아래 그림에서와 같이 최적 보안 대책 결정 모형은 가장 비용 효과적인 보안대책이 먼저 고려된다는 가정을 전제로 하며, 따라서 한계효용과 한계비용이 일치되는 점에서 최적화 된다[Solms, et al., 1990].



<그림 2-3> 최적 보안대책 결정 모형

조직관리 측면에서 전문기술 분야의 업무를 한 사람만이 담당하지 않도록 하며 조직 내의 중요한 기능일수록 직무의 분담이 이루어지도록 한다. 정보처리부문의 부서장은 반드시 부서의 보안관리 책임을 지도록 한다. 조직관리자는 조직에서 마련한 안전관리를 위한 지침 등이 제대로 지켜지고 있는지 확인한다. 또한 응용시스템이 사용자 부서의 개발 계획과 합치하여 개발되는지를 감시할 수 있는 관리나 통제 기법을 만든다[Banks, 1990].

소프트웨어와 데이타에 관하여는 보안관리요원이나 감사요원, 전산시스템 운영요원이 직접적으로 데이타에 대한 수정을 하지 못하게 하고 시스템이나 데이타에 관한 지식은 진정 알 필요가 있는(Need to know) 사람에게만 알려지도록 제한되어야 한다. 실행 라이브러리 안의 모든 소프트웨어와 Procedure의 수정은 공식적인 인가를 필요로 하도록 하며 프로그램과 데이타에 대한 승인되지 않은 복사는 금지한다. 전산자원 공급자와의 계약, 합의 등의 행위는 반드시 기록되어 보관되어야 한다.

정보보안을 위하여 컴퓨터를 사용하려는 사람을 바로 인식(Identification)하고, 정당한 사용자인지 그 실체의 신분을 인증(authentication)한 후, 사용자 번호와 패스워드를 입력한 자가 요구한 프로그램이나 데이타 이용을 인가(Authorization)하는 절차를 모두 거치게 하는 것이 바람직한 패스워드 관리 정책이라 할 수 있다[김세헌, 1990, 정보통신진흥협회, 1989].

재해로 인해 컴퓨터시스템이나 데이타 파일이 파괴된 경우 생산라인이 중지되거나 파일이 재생불능이 되어 오랫동안 연구 개발해 온 실적을 잃게 될 수 있으며, 데이타의 재생에 장기간의 시간을 필요로 하게 되어 기업의 존속에 관계되는 사태도 있을 수 있을 것이다. 재해의 종류로는 화재, 수해, 지진, 풍해, 염해, 낙뢰, 화산의 분화, 쥐의 피해 등을 들 수 있다. 이에 대비하여 재해대책을 수립해야 한다[일본청산감사법인, 1993].

2.2 정보보안 관리 조직

정보보안 관리 조직은 전산자원의 불법적인 사용과 비상상태에 대비하기 위하여 다음 기능을 반드시 갖추어야 한다[한국전산원, 1993].

① 보안통제의 권고와 통제 방법의 제안과 통제 시행에 있어서의 보조
② 조직이나 특정 시스템의 보안 정도 평가
③ 조직 구성원에 대한 정보보안 교육의 시행
④ 예상되는 긴급상황에 대처하는 비상계획의 작성

⑤ 불법적 행위의 예방과 적발

정보보안 담당부서의 조직설계는 부서의 역할을 명확히 하고 정보시스템 조직 전체 내에서 어떤 위치에 부서를 위치 시키는가가 중요한 고려 사항이다. 정보보안 담당부서의 기본기능은 다음과 같다[김세헌, 백인섭, 1992].

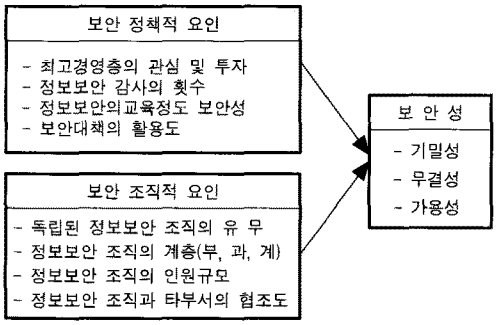
① 안통제에 관한 제안
② 보안 자체 평가
③ 통제의 시행에 있어서의 보조
④ 사용자, 관리자의 보안 교육
⑤ 보안정책, 기준, 가이드라인의 제공
⑥ 시스템 개발에의 참가
⑦ 비상계획(Contingency Plan)
⑧ ID 및 Password 관리
⑨ 불법적 행위, 횡령들의 발견과 사전대비
⑩ 보안에 관한 책임과 직무를 설정, 유지, 변경

Ⅲ. 보안성에 영향을 주는 정책/조직적 모형

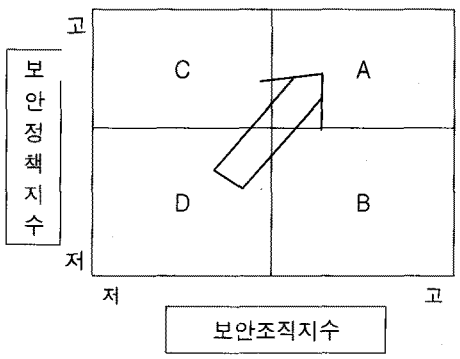
정책에 있어서 사용자 및 관리자의 시스템 보안에 대한 인식은 보안체계를 효과적으로 유지하기 위한 중요한 성공요인으로 꼽힌다[Post & Kievit, 1991]. 조직이 크면 작은 조직보다 전산보안 관련 스탭 수가 조직 크기의 비례보다 더 많음에도 불구하고 더 심각하고 더 많은 보안 위반 사고를 경험한다고 한다[Hoffer & Straub, 1989]. 즉, 조직이 클수록 더 큰 규모의 정보보안 조직이 필요하다. 정보보안 관리는 정보의 기밀성, 무결성, 가용성 등을 확보하는 것을 목적으로 한다. 기밀성(Confidentiality)은 비인가자와 불법 침입자의 접근을 제어하여 자료의 비밀성이 노출되지 않도록 하는 기능이며, 무결성(Integrity)은 비인가자와 불법 침입자의 파일에 대한 기록, 삭제, 생성, 변경 등의 접근으로부터 자료를 보호하는 기능을 말한다. 또한 가용성(Availability)은 인가된 자가 언제든지 자료를 효율적으로 사용하도록 하는 기능이다.

정보의 보안성에 직접적으로 영향을 주는 정책 및 조직적 요인을 도시해 보면 다음과 같다. 정책 및 조직적 요인들은 실무자들의 의견을 수렴 후 정리해서 가장 빈도수가 많은 순서대로 정리한 것이다. 이 요인들의 달성지수를 최대한 높임으로써 보다 높은 정보보안성을 확보할 수 있다.

<표 3-1> 보안성에 영향을 주는 정책/조직적 요인 모형



상기의 정책 및 조직적 요인들을 항목별로 지수화하여 모델을 만들면 다음과 같다. 본 연구에서는 사례연구를 통해 조사대상 회사들이 이 모형의 어느 위치에 어떻게 분포 되는지를 알아보고 그에 따른 분석 및 평가를 하려고 한다.



<그림 3-1> 보안 정책/조직 지수 모형

A면에 속한 회사들은 보안정책 및 조직이 가장 잘 되어 있는 회사들이고, B면은 조직은 잘 되어 있으나 정책이 약한 회사들, C면은 정책은 잘 되어 있으나 조직이 약한 회사들, D면은 정책과 조직이 모두 잘 안되고 있는 회사들임을 나타낸다. 당연한 결론이겠으나 B, C, D면에 속한 모든 회사들이 A면에 들어갈 수 있도록 노력해야 하며, D면에 속한 회사들은 형편에 따라 B면이나 C면을 거쳐 A면으로 들어갈 수도 있겠다.

Ⅳ. 정보보안 관리시스템 사례연구

4.1 연구범위 및 방법

연구 대상업체는 그룹별, 업종별로 다음과 같이 18개 회사를 선정하였다.

<표 4-1> 연구 대상 업체

그룹 / 업종	L그룹	S그룹	H그룹	D그룹	P그룹
SI업체	L시스템	S시스템	H정보기술		P데이타
화학제조업	L화학				
전제제조업	L전자	S전자	H전자		
금속산업					P제철
금융서비스업	L증권			D증권	
무역유통업	L상사	S물산(무역)	H건설		
건설업	L건설	S물산(건설)	H중공업		
중공업		S중공업			

위 18개 계열사들의 정보보안 관련 부서에 접촉을 해 본 결과 긍정적인 반응을 얻어 인터뷰를 하였으며, 시간이 맞지않는 일부 회사들은 설문지를 받아 처리하였다. 인터뷰 및 설문 내용에는 정보보안 실무자들이 가지고 있는 정책과 조직에 대한 주관적인 내용들이 반영되어 객관성은 떨어지는 감도 없지 않다. 그러나 이러한 주관적인 자료가 각 회사의 정보보안 정책 및 조직을 이해하고 적절한 대책을 세우는 데는 많은 도움이 될 것으로 본다.

설문의 구성내용은 크게 나누어 요인 측정, 보안성 평가, 일반적인 내용 등 3개 부문이며 요인 측정은 정보보안의 정책적 요인과 조직적 요인으로 구분하였다.

<표 4-2> 설문의 구성

구 분		내 용
요인측정	정보보안 정책적요인	대상회사에 대한 최고 경영층의 관심 및 투자, 정보보안감사의 횟수, 교육 정도, 보안대책의 활용도 등의 요소
	정보보안 조직적요인	대상회사에 대한 정보보안 조직의 유무, 정보보안 조직의 계층, 인원규모, 타 부서와의 협조도 등의 요소
보안성 평가		일반보안성, 기밀성, 무결성, 가용성 등의 컴퓨터 보안성에 대한 측정
일반적인 내용		응답자의 회사, 직위 및 소속부서에 대한 질문

측정요소를 구체적 항목으로 나누면 다음 표와 같다. 각 항목당 5점 리커트 방식으로 하여 1점부터 5점까지 점수를 매겼다. 최고경영층의 관심 및 투자 항목은 두 점수를 평균 내었으며, 정보보안 감사의 횟수와 교육정도는 연간 총횟수를 점수화 하였다. 보안대책의 활용도는 사용되는 대책이 7가지 이상이면 5점, 6가지이면 4점, 5가지이면 3점, 4가지 이하이면 2점을 부여하였다. 정보보안 조직의 유무 항목에서는 별도의 조직이 있을 경우에 5점, 없을 경우에는 1점을 부여하였다. 정보보안 조직의 계층은 팀장의 직위에 따라 점수를 주었다.

<표 4-3> 측정 요소 및 점수

측 정 요 소		점 수	내 용
정책적요인	최고경영층의 관심 및 투자	1~5	
	정보보안 감사의 횟수	1~5	연간 총횟수
	정보보안의 교육 정도	1~5	연간 총횟수
	보안대책의 활용도	1~5	
조직적요인	정보보안 조직의 유무	1~5	무이면 1, 유이면 5
	정보보안 조기의 계통	1~5	팀장의 직급
	정보보안 조직의 인원규모	1~5	
	타 부서와의 협조도	1~5	
보안성	일반 보안성	1~5	물리적 보안
	기밀성	1~5	
	무결성	1~5	
	가용성	1~5	

4.2 L그룹

1) 그룹 및 SI업체의 개요

L그룹은 1997년도 대규모 기업집단 지정 순위 3위로서, 48개 계열사를 거느리고 있으며 자산총액 약 31조 4천억원이다.

L그룹 내 시스템 통합업체는 L시스템이다. 1987년 미국 최대의 시스템통합 업체인 E사와 각각 50%의 지분으로 합작하여 설립되었다. L시스템은 1997년에 매출액 3,912억원이며, 1998년 매출목표는 4,100억원, 현재인력은 3,700명(1998년 3월 기준)이다.

2) 정보보안 대책

L그룹은 회장실 전략지원팀에서 그룹 전체의 보안현황을 관리하고 있다. 비상설 조직으로 그룹 보안진단팀을 만들어 전 계열사에 걸쳐 보안진단을 실시한다. L그룹은 보다 확실한 보안환경 구축을 위하여 신분증, PC보안, 전자지갑 등 다양한 기능을 수행할 수 있는 IC 카드 형태의 그룹 통합카드를 도입, 운영하고 있다. L정보통신이 중심이 되어 그룹 통합카드를 도입한다는 방침 아래 1996년부터 1997년 7월까지 모두 4단계로 IC카드를 도입하였는데 우선 ID 기능, 출입보안, PC보안, 주차관리 등에 사용하고 단계적으로 도서 및 자료관리, 식당관리, 자판기이용, 의료정보카드, 신용카드, 증권카드, 전자지갑, 홈쇼핑, 무선전화 과금업무 등까지 적용 범위를 확대해 나갔다.

그룹 내 시스템 통합업체인 L시스템의 보안대책은 시스템 및 네트워크 보안으로 크게 구분된다. 시스템 보안에는 기존의 메인프레임용 정보처리 보안을 위한 SW인 ACF2가 핵심역할을 담당한다. ACF2는 미국방성의 자료취급통제 SW로 권한이 부여되지 않은 자는 특정 데이타를 사용하지 못한다. 또 비밀번호를 모르는 외부침입자가 6번 이상 틀린 비밀번호를 입력하면 자동으로 시스템 연결이 끊어진다. 중요 프로그램 사용 후에는 사용자의 ID와 시간이 기록되고 시스템별로 중요도에 따라 사용할 수 있는 이용자를 제한 시킨다. 이는 부평에 있는 L정보기술센터의 보안대책으로 마련된 것이다. 시설보안으로는 카드 엑세스 시스템에 의한 출입통제를 실시하고 있으며 이러한 시스템 보안은 정보보안팀에서 관장한다.

L시스템이 최근 들어 집중 강화하고 있는 부문은 인터네트와 연결된 네트워크 보안문제이다. 1996년 1월부터 미국 안스(ANS)사로부터 '인터로크(Interlock)' 라는 파이어월(방화벽)을 도입, 네트워크 보안체계를 구축했다. 이를 위해 1년 전부터 통신운영팀을 가동하여 통신보안체계에 대한 준비 작업을 해왔다. L시스템은 보안관련 제품 판매와 함께 보안컨설팅 비즈니스도 전개해 나갈 예정이다. L시스템은 L전자 등 별도로 인터넷에 접속하고 있는 4개 계열사 전산망에 이 시스템을 구축하는 한편 나머지 계열사로 하여금 이 시스템을 설치한 자사의 망을 이용해 인터넷에 접속하도록 해 그룹전체의 인터넷 보안시스템을 구축했다.

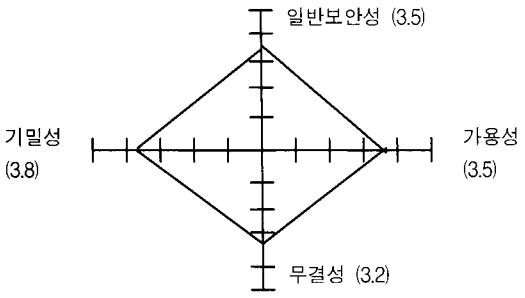
3) 분석 결과

L그룹은 정보보안 관리가 가장 잘 되고 있는 기업군으로 꼽힌다. 계열사에 따라 약간씩 차이는 있겠으나 출입인원 관리 등의 물리적 보안으로부터 컴퓨터 보안에 이르기까지 꼼꼼히 관리되고 있다. 특히 L그룹 시스템 통합업체인 L시스템은 합자회사인 미국E사로부터 1987년 설립이래 줄곧 보안 지도 및 감사를 받아와 정보보안에 가장 일찍 관심을 가질 수 있었다.

설문에 의한 연구결과를 보면 조직면에서는 만족할만한 지수가 나오지만 정책면에서는 보안실무 담당자들이 만족하지 못하고 있는 것으로 나타나고 있다. 특히 보안교육 및 보안감사의 실시도가 약한 실정이다.

보안성에 있어서는 기밀성은 양호, 가용성과 일반보안성은 보통, 무결성은 비교적 낮게 나타났다. 출입인원 관리라든가 출력물 관리 등 기본적인 물리적 보안에 더욱 신경을 써야 한다

는 의미로 보인다.



<그림 4-1> L그룹 보안성 평균지수

<표 4-4> L그룹의 보안정책 및 조직 지수

측정요소 \ 회사명		L-1	L-2	L-3	L-4	L-5	L-6
정책적 요인	관심 및 투자	4	3	4	4	3	3
	보안감사횟수	4	3	2	3	2	3
	보안 교육	3	5	1	2	4	4
	보안툴 활용도	5	5	2	2	2	3
	계	16	16	9	11	11	13
조직적 요인	보안조직의유무	5	1	1	5	1	5
	보안조직의계층	5	5	4	5	5	4
	보안조직의계층	4	4	3	2	4	1
	조직간의협조도	3	4	3	4	4	4
	계	17	14	11	16	14	14
보안성	일반보안성	3	3	4	4	3	4
	기 밀 성	4	4	3	4	4	4
	무 결 성	4	3	3	3	3	3
	가 용 성	4	3	3	4	4	3
	계	15	13	13	15	14	14

4.3 S그룹

1) 그룹 및 SI업체의 개요

S그룹은 1997년도 대규모 기업집단 지정 순위 2위로서, 계열사 수는 55개, 자산총액은 약 40조 7천 6백억원이다.

S그룹의 시스템 통합 업체는 S시스템이다. S시스템은 1985년에 한국 IBM과 3대 1지분으로 설립되었다. L그룹이 그룹 통합 전산화를 실시한 후 추이를 지켜보던 S그룹은 1991년과 1992년에 그룹 전산화 통합을 실시하였다. 1993년 말 합작회사인 I사와 결별을 하고 독자노선을 걷고 있다.

S시스템은 1997년에 매출액 8,400억원이며, 1998년 매출목표는 8,800억원, 현재인력은 6,200명(1998년 3월 기준)이다.

2) 정보보안 대책

S그룹은 그룹 차원의 정보관리가 아주 잘 되어있다. S그룹은 토픽스(TOPICS)라는 그룹 공유의 정보시스템을 운영중이다. TOPICS는 계열사별로 다소 차이가 있으나 거의 비슷한 형태로 운영되고 있다. S그룹 내에서도 특히 정보관리가 잘 되고 있는 회사로는 S전자와 S항공 등이다. S전자는 항상 정리정돈, 불요불급한 출입을 최대한 억제 등의 보안수칙 10훈을 제정해 시행중이다. S항공은 공장 출입구 통로에 자기선을 설치해 디스켓을 갖고 나올 경우, 디스켓의 데이타가 모두 파괴되도록 장치를 해 놓았다.

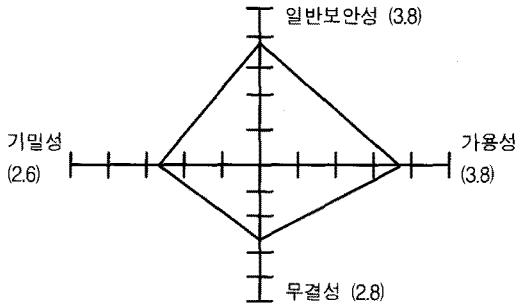
S그룹은 초고속 통신망을 이용한 인트라넷을 1996년 6월 구축하여 문서 없는 사무실을 구현하였다. 그룹 통합 정보시스템인 '싱글'을 이용, 그룹 내 12만대의 컴퓨터를 연결해 전자우편, 정보공유, 전자결재, 문서관리 기능 등을 인터넷 방식으로 운영하였다. 이에 따라 전세계 S그룹사 직원들은 웹 브라우저를 통해 해당지역의 시내전화요금으로 시간과 공간에 구애 받지 않고 필요정보를 공유하며 전자결재를 받을 수 있다. 방화벽 소프트웨어로는 S전자가 공급하는 '밀키웨이 블랙홀'을 이용해 그룹 전산망을 관리한다.

S시스템은 1995년3월 보안팀을 공식 출범시켰는데 접근통제와 사후 추적성 확보라는 기본임무로 S그룹의 시스템 보안에 대한 책임을 총괄하고 있다. S시스템은 1996년 초부터 그룹 계열사의 보안시스템을 적극 구축하고 있는데 이어 현재는 그룹 외 정보보안 수주활동도 본격화하고 있다.

3) 분석 결과

설문에 의한 연구 결과를 보면 정보보안 정

책이나 조직면에서 S-5 회사의 지수가 낮은 것을 제외하고는 비교적 만족한 상태인 것으로 나타나고 있다. 보안성 측정에 있어서는 일반 보안성은 높게 평가되는 반면 기밀성, 무결성 등의 컴퓨터 보안성은 약간 낮게 나타나고 있다. 이는 정보 시스템을 맡고 있는 SI업체에 대한 계열사 실무자들로부터의 정보보안 신뢰도가 낮은 데에 기인한 것으로 보인다. S시스템은 최근 활발한 정보보안 구축을 하고 있어 인지도는 곧 높아질 것으로 예상된다. S그룹에서도 전산실을 독자 운영하는 회사에서의 보안에 대한 우려가 나타나고 있어 그룹차원의 조정이 필요해 보인다.



<그림 4-2> S그룹 보안성 평균 지수

<표4-5> S그룹의 보안정책 및 조직 지수

측정요소 \ 회사명		L-1	L-2	L-3	L-4	L-5
정책적 요인	관심 및 투자	4	5	4	5	3
	보안감사횟수	5	4	5	2	4
	보안 교육	2	4	4	4	2
	보안툴 활용도	3	3	2	4	2
	계	14	16	15	15	11
조직적 요인	보안조직의유무	5	1	1	5	1
	보안조직의계층	5	5	5	4	5
	보안조직의계층	3	3	2	4	2
	조직간의협조도	3	4	3	4	3
	계	16	13	11	17	11
보안성	일반보안성	4	3	4	4	4
	기 밀 성	2	3	2	4	2
	무 결 성	2	3	2	4	3
	가 용 성	5	4	3	3	4
	계	13	13	11	15	13

4.4 D그룹

1) 그룹 및 SI업체의 개요

D그룹은 1997년도 대규모 기업집단 지정 순위 4위로서, 계열사 수는 25개이며 자산총액은 약 31조 3천억원이다.

D그룹의 시스템 통합업체는 D정보시스템이다. D정보시스템은 1989년에 자본금 13억원과 인원 400명으로 설립되었다. 그룹 통합 전산화는 타 그룹에 비해 다소 늦게 시작되어 1993년에 22개 계열사 중 증권, 금융 부문을 제외한 12개 계열사부터 전산시스템 재구축 작업에 들어가 1995년에 이르러 그룹 통합 전산화 작업이 마무리 되었다.

D정보시스템은 1997년 매출액이 1,800억원이며, 1998년 매출 목표는 1,900억원, 현재인력은 1,766명(1998년 3월 기준)이다.

2) 정보보안 대책

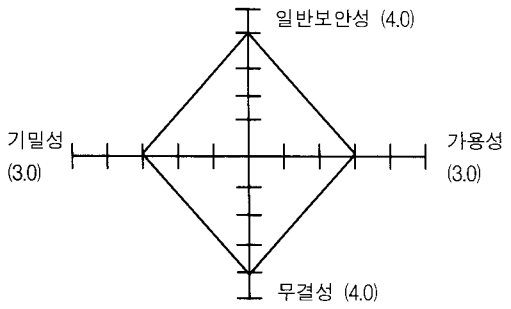
D정보시스템도 최근 정보보안의 중요성을 감안, 이분야 비즈니스에 적극적으로 뛰어들고 있다. 보안관련 문제는 시스템서비스부 내의 보안 전담팀이 총괄한다. 지난 1988년 메인프레임용 보안SW인 ACF를 도입, 메인프레임 센터에서 호스트 보안 솔루션으로 적용해 왔다. 도입 초기 뚜렷한 보안전략을 세우지 못해 패키지와 시스템이 별개로 운영되는 시행착오를 겪기도 했으나 1993년부터 시스템 보안에 관한 본격 연구의 결과로 현재까지는 ACF로 호스트의 보안 문제를 해결하고 있다.

D정보시스템이 최근 들어 주력하고 있는 부문은 네트워크 보안인데, 기업의 MIS 인프라가 인터네트 접속으로 이루어져 인터네트 중심의 네트워크 보안은 필연적이라는 시각 때문이다. 이 회사는 이에 따라 그룹 인터네트 보안 정책을 수립하였으며, 네트워크 보안관련 파이어월

은 선 마이크로시스템즈의 솔루션과 함께 미 악센트(Axent)사의 옴니가드(Omni-Guard)를 채택하였다. D정보시스템은 자체망에 우선 시범 적용하다가 1996년 3월까지 1차적으로 D자동차, D중공업, (주) D무역부문에도 확대 적용하였다. 또, 독일의 보안 솔루션 개발업체인 슈만사로부터 '샘(SAM)'이라는 중앙 집중관리 툴을 도입, 1996년 말까지 20여개 그룹사를 대상으로 구축 완료하였다. D정보시스템은 '샘' 솔루션을 전략적으로 활용, 대외 비즈니스 사업에도 적극 참여할 계획이다.

3) 분석 결과

D그룹으로부터 응답한 회사는 금융 서비스업에 속한 회사로서 전산업무를 자사의 전산실에서 독자 운영하는 형태였다. 독립된 정보보안 조직이 없이 시스템지원부에서 보안업무를 담당하고 있으며, 감사 및 교육 항목이 낮은 지수로 나타났고 보안성은 비교적 높은 지수로 나왔다. 금융관련 회사인 만큼 보안에 관한 중요성이 강조되어 왔음을 보여주고 있다. 이 회사는 정보보안의 교육과 감사의 횟수를 더 늘리고 지금은 활용하지 않는 위험평가 분석 방법을 도입할 것을 권하고 싶다.



<그림 4-3> D그룹 보안성 평균지수

<표 4-6> D그룹의 보안정책 및 조직 지수

측정요소 \ 회사명		L-1				
정책적요인	관심 및 투자	4				
	보안감사횟수	2				
	보안 교육	2				
	보안툴 활용도	4				
	계	12				
조직적요인	보안조직의유무	1				
	보안조직의계층	5				
	보안조직의계층	3				
	조직간의협조도	3				
	계	12				
보안성	일반보안성	4				
	기 밀 성	3				
	무 결 성	4				
	가 용 성	3				
	계	14				

4.5 H그룹

1) 그룹 및 SI업체의 개요

H그룹은 1997년도 대규모 기업집단 지정 순위 1위로서, 계열사 수는 46개이며 자산총액은 약 43조 7천 4백억원이다.

H그룹의 정보시스템 통합업체는 H정보기술이다. H정보기술은 H전자 및 그룹 전산실을 주축으로 40여개 계열사의 전산인력을 통합한 1천여명과 자본금 210억원 규모의 대형 시스템 통합 전문업체로 1993년에 설립되었다.

국내 대기업들의 그룹 통합 전산화에 조금 늦게 편승한 H정보기술은 다른 기업과의 경쟁을 위해 연간 매출의 10% 이상을 인재 양성과 기술 개발을 위해 투자하여 종합정보기술 회사로서 발돋움 하겠다는 의지를 갖고 있다

H정보기술의 1997년도 매출액은 3,637억원이며, 1998년 매출 목표는 3,850억원, 현재 인력은 3,229명(1998년 3월 기준)이다.

2) 정보보안 대책

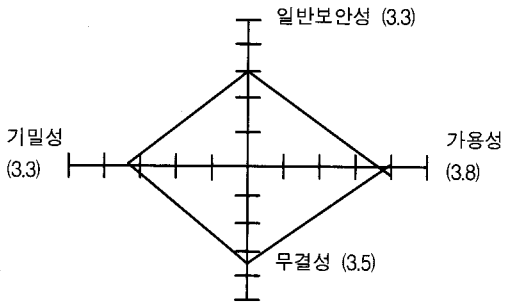
H그룹은 각 계열사 별로 품질보증실, 감사실, 정보기술실, 시스템운영부 등에서 보안 업무를

맡고 있다. 아직은 SI업체의 영향력이 약한 관계로 각 계열사 중심의 정보보안 대책이 이루어지고 있다. H정보기술에서는 IBM의 RACF라는 보안 툴을 사용하고 있다. 또한 전자우편 및 서버시스템 보안과 방화벽시스템 구성 기능이 포함된 망관리 소프트웨어를 사용해 자사의 인터넷 서비스인 '신비로'와 그룹 전산망 관리를 동시에 수행하고 있다. H전자는 사내 정보 인프라 구축의 일환으로 통합전산망인 '오피스21'을 자체 개발하여 가동 중인데 개인마다 부여할 수 있는 비밀번호를 통해 보안기능을 강화했다.

3) 분석 결과

H그룹은 타 그룹에 비해 최고 경영층의 관심 및 투자 항목의 지수가 높게 나타나고 있는 것이 특징이다. 후발 주자인만큼 SI에 대한 경영층의 관심이 크면서 정보보안에 대한 관심도 자연스럽게 높은 것으로 보인다.

정보보안 조직을 가지고 있는 전자제품 제조업체의 정책 및 조직 지수가 높으며 보안성도 양호한 것으로 나타나고 있다. 그러나 SI업체의 영향력이나 계열사들로부터의 신뢰성은 낮은 것으로 판단되어 이에 대한 대책이 요구된다.



<그림 4-4> H그룹 보안성 평균 지수

<표 4-7> H그룹의 보안정책 및 조직 지수

측정요소 \ 회사명		H-1	H-2	H-3	H-4
정책적요인	관심 및 투자	4	5	4	4
	보안감사횟수	1	2	1	1
	보안 교육	4	4	1	1
	보안툴 활용도	3	3	4	3
	계	12	14	10	9
조직적요인	보안조직의유무	1	5	1	1
	보안조직의계층	4	3	3	5
	보안조직의계층	3	3	3	2
	조직간의협조도	3	4	2	3
	계	11	15	9	
보안성	일반보안성	4	4	2	3
	기 밀 성	2	4	4	3
	무 결 성	3	4	4	3
	가 용 성	4	4	3	4
	계	13	16	13	13

4.6 P그룹

1) 그룹 및 SI업체의 개요

P그룹은 정부가 지정하는 30대 재벌 그룹에 포함되지는 않지만 세계 굴지의 철강회사인 P제철을 중심으로 하여 P스틸, P개발, P데이타, S통신 등의 계열사를 거느리고 있다.

P그룹의 시스템 통합업체는 P데이타이다. P데이타는 1989년에 200억원의 자본금으로 설립되었으며 P제철의 생산관리 전산화를 시작으로 전 그룹의 전산 통합화를 추진하고 있다.

P데이타는 1997년 매출이 1,585억원이며, 1998년 매출 목표는 1,500억원, 현재인력은 850명(1997년 12월 기준)이다.

2) 정보보안 대책

P그룹은 모회사인 P제철의 감사팀에서 계열사별 감사인원을 확보하여 통합적인 감사체계와 함께 그룹 차원의 정보보안 관리를 하고 있다.

P데이타는 기존의 메인프레임을 운영 관리해 온 RCS(리모트 컴퓨팅 서비스)팀에서 보안업무를 주관하고 있다. 시스템보안의 경우 메인프레

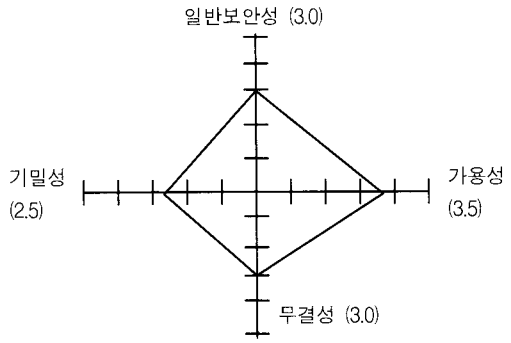
임용 정보처리 보안 소프트웨어인 ACF로 시스템 접근을 통제하고 있다. P데이타는 사내망으로 P제철 본사와 광양, P제철소, P센타 등 4개 지역을 네트워크로 묶는 한편 사외망은 인터네트로 연결시켰다. 이에 따라 네트워크 보안의 중요성을 절감, 그동안 P공대 연구팀과 에이텔을 통해 준비해오던 방화벽 구축작업을 최근 완료했다. P데이타의 보안대책은 주로 P그룹과 P공대 공동으로 추진된다. 1995년에 수립한 그룹정보망 구축작업의 경우, P공대 정보통신연구소와 공동으로 보안프로젝트를 수행중이다. 1998년 구축 완료 예정인 이 그룹 정보망에 대한 기획총괄은 P그룹의 정보화기획팀에서 주도하고 있었는데, 이 정보화기획팀이 P데이타로 흡수 통합되었으며 그룹사 보안업무도 P데이타로 이관되었다.

P데이타는 네트워크를 통한 정보 교류가 활발해지면서 정보보안 업무가 중요하다고 판단, IBM의 'RACF' 라는 보안 툴로 시스템 보안을 추진하는 한편 정보보안팀도 구성, 이의 사업화를 추진하였다. 정보보안팀에선 1차로 P공대 정보통신 연구소와 공동으로 인터넷 방화벽 시스템과 통합 보안관리 시스템 구축 프로젝트를 시행중이다.

P데이타가 최근 자체 개발한 보안 시스템을 P제철에 우선 적용하고 1997년 2월까지 전 계열사와 해외지사 사무소로 확대하였다. P데이타가 P공대 교수진 및 안기부 등과 공동 개발한 보안 시스템은 인증, 방화벽, 디지틀 서명, 스마트카드용 프로토콜, 암호화 프로토콜 등 5개 분야로 구성되어 있다. P데이타는 이들 구성요소를 상호 연계한 보안 체제를 갖추었다.

3) 분석 결과

P그룹도 최고 경영층의 관심 및 투자 지수가 높게 나오고 있다. P-1회사는 보안감사와 교육의 횟수가 적고, 보안대책의 활용이 패스워드 관리, 접근 제어, 신분 확인 등 3가지 뿐으로 정책지수가 낮게 나타났다. P그룹의 주력기업인 P-2회사는 정책 및 조직에 있어서 높은 지수를 나타내고 일반 보안성은 양호, 컴퓨터 보안성은 보통으로 나타났다.



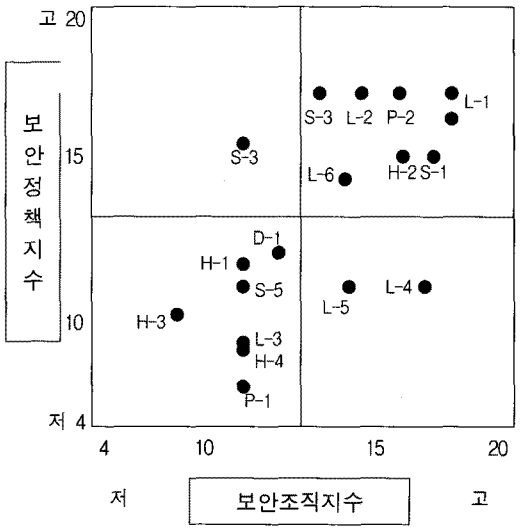
<그림 4-5> P그룹 보안성 평균지수

<표 4-8> P그룹의 정책 및 조직 지수

측정요소 \ 회사명		P-1	P-2			
정책적요인	관심 및 투자	4	4			
	보안감사횟수	1	4			
	보안 교육	1	5			
	보안툴 활용도	1	3			
	계	7	16			
조직적요인	보안조직의유무	1	5			
	보안조직의계층	4	3			
	보안조직의계층	3	3			
	조직간의협조도	3	4			
	계	11	15			
보안성	일반보안성	2	4			
	기 밀 성	2	3			
	무 결 성	3	3			
	가 용 성	4	3			
	계	11	13			

4.7 사례연구의 종합분석

아래 그림은 각 회사별 지수를 제3장에서 제시한 보안 정책/조직 지수 모형에 넣어서 도시화 해 본 것이다. 실제 회사명은 무작위 부여한 기호로 표시하였다. 모형에서 저점을 4로 잡은 이유는 설문의 항목별 최저점수가 1점이고 정책/조직 부문별로 각 4개 항목으로 최저점이 4점이기 때문이다.



<그림 4-6> 조사대상회사들의 정보보안 정책 및 조직 지수 위치도

기준을 어떻게 설정하느냐에 따라 차이가 있겠지만 지수 위치도를 살펴보면 정보보안 정책 및 조직이 잘 되어 있는 것으로 나타난 회사와 그렇지 못한 회사가 거의 반반이다. 또한 정책지수는 5점부터 20점까지 고르게 나타나 있는 반면 조직지수는 거의 10점 이상부터 시작되고 있다. 이는 대기업 계열사들이 대부분 정보보안 기능을 담당하는 조직은 갖고 있는데 반하여 정책적인 면은 아직 소홀히 하고 있는 데에 기인한 것으로 보인다.

V. 결 론

정보시스템의 발달이 정보사회라는 편리한 세상을 만들어 주면서 그에 대한 역작용으로 정보보안이라는 업무도 만들어 주고 있다. 정보보안을 위한 첫 단계로서 그것을 하고자 하는 의지, 규정, 방침 등의 정책이 있어야 할 것이고 그 정책을 수행할 조직이 있어야 할 것이다.

우리 기업 환경에 적합한 정보보안 정책 및 조직 체계를 제시하기 위하여 국내 5대 그룹을 대상으로 분석 연구한 결론은 다음과 같다.

1) 보안관리 규정 등 기본적인 정책은 있으나 실현 불가능하거나 시대에 뒤떨어져 신기술의 내용은 빠져있는 등 개정이 필요한 회사가 많았다.
2) 보안감사 및 보안교육이 전반적으로 부진하다.
3) 보안 툴의 활용도를 더욱 높일 필요가 있다. 디지탈 서명, 생체활용 기법 등 신기술에 관심을 가져야 한다.
4) 독립된 정보보안 조직이 없는 회사들은 대체적으로 보안성이 낮게 나타나고 있다. 정보보안팀의 결성이 시급하다.
5) 정보보안 조직이 있는 회사들도 그 규모에 비해 인원이 적은 편이다. 또 한 팀원들이 보안업무 수행능력을 갖추고 있는가도 점검할 문제이다.

연구자는 보안 담당자들과의 인터뷰 결과 기업의 정보보안 관리에 있어서는 일반보안과 컴퓨터보안이 통합된 '통합 정보보안 관리(Total Security Management)'가 이루어져야 한다고 생각한다. 특히 대기업에서는 '통합 정보보안 조직(Total Security Organization)'이 그룹차원에서 결성되어야 한다. 즉, 회장실 산하의 그룹 보안전담기구로서 전계열사 보안사고의 예방, 교육, 사고발생시 신고 및 처리, 사고 사례 및 대책의 전파, 전산보안감사 실시, 그룹 네트워크 통합관리 지원 및 관리 등의 업무를 수행하도록 한다. 명칭은 그룹의 성격에 따라 지으면 되겠지만 '(그룹명) 정보보안센타' 로 하면 무난할 것 같다. 이 통합조직을 통해서 '통합 정보보안 관리' 가 이루어질 때 그룹은 물론 각 계열사들의 '보안사고의 방지, 정보의 유출방지, 전산망의 안정성 확보' 라는 목표를 이룰 수 있을 것이다.

본 연구의 한계점은 정보보안에 관한 내용이라는 폐쇄성으로 인하여 관계자들의 협조를 얻기가 쉽지 않았다는 점이다. 따라서 설문에 참여하는 회사 수가 적고 설문 응답의 진실성을 확인하는 시간도 필요하였다. 미래의 연구과로는 업종별 정보보안 관리연구와 중소기업의 보안 사례연구를 들 수 있다. 특히 벤처 기업들의 정보보안은 무엇보다도 중요할 것이다.

〈참 고 문 헌〉

[1] 김세헌, "정보통신망의 정보보안체계 설계에 대한 종합적 연구," '89 전기통신학술연구과제, 한국과학기술원 경영과학과, 1990.

[2] 김세헌, 박영호, 문상재, 강신각, 임주환, "컴퓨터 범죄 방지를 위한 정보 통신망의 보안방안에 관한 연구," 1994.

[3] 김세헌, *컴퓨터 범죄와 프라이버시 침해*, 희성출판사, 1989.

[4] 김영춘, 관세청, "패스워드 관리에 대한 실증분석," 1992.

[5] 김정덕, "정보시스템과 정보보안," *KMIS '94 추계 학술대회 논문집*, 한국경영정보학회, 1994.

[6] 백인섭, 김세헌, "정보보안을 위한 전산망 조직체계설계," 1992.

[7] 이재남, "SI업체를 가진 그룹내 계열사들의 정보시스템 외주 위탁 전략에 관한 연구," KAIST석사 논문, 1995.

[8] 이재창, "EDI에 있어서 내부 통제가 시스템 유용성 및 보안성에 미치는 영향," KAIST 석사 논문, 1995.

[9] 이필중, 정진욱, 박명순, 이재용, "전산망의 안전대책 개요," 1991.

[10] 일본정보처리 개발협회, *정보화 백서*, 1994.

[11] 일본 청산감사법인, *보안과 위험관리*, 1993.

[12] 임채호, 김동석, 오익균, 홍주영, "관리자를 위한 인터네트 보안 지침서," *통신정보보안학회지*, 제4권 제3호, 1994.9.

[13] 정보통신 진흥협회, "정보통신 안전체계 연구," 1989.

[14] 한국전산원, "국가기간전산망 시스템의 안전관리 체계에 관한 연구," 1991.12.

[15] 한국전산원, "전산망 안전을 위한 관리체계 및 조직연구," 1993.7.

[16] 홍주영, 임채호, "인터네트 보안관련 연구개발 현황," *통신정보보안학회지*, 제3권 제4호, 1993.12. pp. 50-55.

[17] C & C, "국내기업의 정보보안 실태," *컴퓨터와 커뮤니케이션*, 전자신문사, 1996. 6, pp. 13-52.

[18] Banks. S., "Security Policy," *Computer & Security*, Vol. 9, No. 7, 1990.

[19] Bessenhoffer, R., "Designing Security into a modern data processing center," *Computer Security Journal*, Vol. 5, No. 1.

[20] Fordyce, Samantha, "Computer Security : A Current Assessment," *Computer & Security*, North-Holland Publishing Company, 1982, pp. 9-16.

[21] Johnson, Normal. L., "Computer security and control," EDP *Auditor*, Smithkline Beckman Corporation, EDP Journal, Fall, 1983, pp. 59-72.

[22] Hoffer, J. A. & Straub, D. W., "The 9 to 5 Underground: Are You Policing Computer Crimes?," *Sloan Management Review*, Vol. 30, No. 2, 1989.

[23] Lynda M. Applegate, "Managing in an

information age, Transforming the Organization for the 1990s," IFIP, 1994.

[24] Parker, D.B., *Computer Abuse Assessment*, SRI, 1975.

[25] Porter, M.E. and Miller, V.E., "How Information Gives You Competitive Advantage," HBR, July-August 1985.

[26] Post, G. V. & Kievit, K., "Accessibility vs. Security: A Look at the Demand forComputer Security," *Computer & Security*, Vol. 10, No. 4, 1993.

[27] Schweitzer,J.A., *Computer Crime and Business Information* ; A Practical *Guide for Managers*, Elsevier, 1986.

[28] Sieber,U., *Computerkriminalitat und Strafrecht*, Carl Heymanns, 1980.

[29] Sieber, U., *The Internal Handbook on Computer Crime*, Jon Willey & Sons Ltd., 1986.

[30] Smith, M.R., "Computer Security - Threats, Vulnerabilities and Countermeasures," *Information Age*, Vol. 11, No. 4, Oct 1989, pp. 205-210.

[31] Solms, R., Eloff, J.H.P & Solms S.H., "Computer Security Management: A framework for Effective Management Involvement," *Information Age*, Vol. 12 No. 4, October, 1990, pp. 217-222.

[32] Stallings William, *Network & Internetwork Security*, Principles & Practice, 1995.

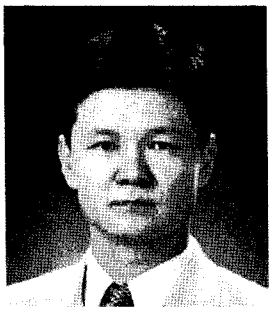
[33] Straub, D.W.Jr., "Effective IS Security : An Emperical Study," *Information Systems Research*, Vol. 1, No. 3, 1990, pp. 255-276.

[34] Ware, W.H., *Perspectives on Trusted Computer Systems*, RAND Corporation, September, 1988.

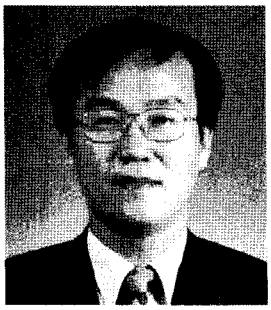
[35] Wilkes, M. V., "Revisiting Computer Security in the Business World," *Communications of the ACM*, Vol. 34, NO. 8, August 1991.

◈ 이 논문은 1998년 2월 11일 접수하여 2차 수정을 거쳐 1998년 9월 11일 게재확정되었습니다.

◆ 저자소개 ◆



선 한 길 (Sun, Han-Gil)
현재 한국사회경제연구소 정보통신 연구위원으로 재직 중이며, 제일제당 주식회사, ㈜ LG-EDS시스템 등에서 MIS구축, 정보시스템 감사 및 보안 업무를 수행하였다. 강원대학교 산업공학 학사, KAIST 경영정보공학 석사를 취득하였다. 주요관심분야는 정보시스템 보안 및 감사, 전자상거래 구현, 정보화 컨설팅 등이다.



한 인 구 (Han, In-Goo)
현재 KAIST 테크노경영대학원 부교수로 재직중이다. 서울대 국제경제학 학사, KAIST 경영과학 석사를 취득하고 Univ. of Illinois at Urbana-Champaign에서 회계정보시스템을 전공하여 경영학 석사 및 박사를 취득하였다. 주요 관심 분야는 회계정보시스템, 신용평가시스템, 정보시스템감사 등이다.