□ 기술해설 □

정보화 역기능 현황 및 분석

한국전산원 신순자* · 김홍근* · 이재우*

● 목 차 ●

1. 서 론

가속화되는 정보통신 기술의 발전은 우리 생활의 질을 높여주는 순기능적 측면이 대부분이었으나 몇 년전부터 그에 반하는 역기능적 측면이 급속히 증가하고 있다. 정보 사회에서 정보 자산이 중요한 가치를 갖게 되면서 이를 노리는 범죄적 역기능이 날로 늘어나고 또한 이에 대한 보호 대책도 중요한 문제로 떠오르게 되었다.

정보화 역기능 사례는 정보통신 기술 및 정보통신기기를 오·남용한 경우가 대부분인데, 이들의 특성상 공개된 사례보다는 비공개 사례가 더 많을 것으로 추측된다. 일단 여기서는 언론에 공개된 역기능 사례들만 다루었으므로 이점을 염두하기 바란다.

본 연구의 주된 목적은 증가하는 정보화 역기능 사고를 방지하고 그에 대한 대책을 세우기 위해 현 상황에 대한 정확한 진단 및 그 동향 파악에 있다. 이를 통해 역기능 사례의 심각성을 인식하고 이에 대한 새로운 보안 기술이나 제품, 거시적인 대책 등을 알아 볼 수 있다.

*비 회 원

2. 정보화 역기능 사례 분류 기준

체계적인 분류 기준을 마련하는데 목적을 두고 95년에 분류 기준을 새롭게 재정리하였다.

정보시스템 감사를 그 발전 단계 및 접근법에 따라 컴퓨터 주변 감사, 컴퓨터 처리 과정 감사, 컴퓨터 활용 감사의 세가지로 분류하는데 착안하여 ATW식 컴퓨터 범죄 분류법[박태희, 1992]을 바탕으로 표 1과 같이 분류하였다.

대 분류에 해당되는 컴퓨터 주변 역기능 행위, 컴퓨터 처리 과정 역기능 행위, 컴퓨터 활용 역기능 행위는 ATW식 분류에 의거하였고, 여기에 기타 컴퓨터 관련 역기능 행위를 추가하였다. 세부 분류는 자체적으로 결정 하였다. 컴퓨터 주변 역기능 행위는 컴퓨터와 직접적으로 관련된 역기능 사례로서 컴퓨터내에 보관된 민감한 자료의 유출과 정보기기 관련 장비 및 부품 관련 사고를 말한다. 컴퓨터 처리 과정 역기능 행위는 컴퓨터 시스템을 운영하는 과정에서 이루어지는 사고로서 주로 내부인에 의해 발생된다. 내부 자료 변조 및 파괴와 부정 정보 처리가 이에 해당한다. 컴퓨터 활용 역기능 행위는 조직의 내부, 외부에서 통신망을 통해

표 1 정보화 역기능 사례 분류 코드

A 컴퓨터 주변 역기능 행위	00. 자료 유출	01 개인 자료
		02. 학교, 연구소 자료
		03. 기업 자료
		04. 공공 기관 및 국가 자료
	10. 정보기기 관련 장비 및 부품 관련 범죄	11. 절도
		12. 밀반입, 출
		13. 물리적 파괴
T. 컴퓨터 처리 과정 역기능 행위	00. 내부 자료 변조 및 파괴	01. 고의적 변조
		02. 실수에의한 변조
		03. 고의적 파괴
		04. 실수에의한 피괴
	10. 부정 정보 처리	11. 관리 태만
W. 컴퓨터 활용 역기능 행위	00. 해킹	01. 단순 침입
		02. ID 도용
		03. 자료 절취
		04. 자료 변조 및 파괴
E. 기타 컴퓨터 관련 역기능 행위	00. 금융 범죄	01. 카드 위조
		02. 수표(지폐)위조
		03. 증권(채권)위조
	10. 비윤리적 행위	11. 음란물 유포
		12. 사기 행위
		13. 협박, 폭력
	20. 컴퓨터 바이러스	21. 피해
		22. 제작 및 유포
	90. 기타	

타인의 시스템에 침입하여 자료를 절취, 파괴하는 행위와 타인의 S/W나 프로그램의 암호를 변조 또는 해독하는 행위를 말한다. 이는 흔히 해킹이라고 알려져 있다. 기타 컴퓨터 관련 역기능 행위에는 위의 세 가지 범주에 포함시키기 어려운 내용들을 담았다. 정보기술을 이용한 신용카드나 수표 등의 위조를 포함하는 금융 사고와 컴퓨터를 이용한 비윤리적 행위, 그리고 컴퓨터 바이러스등이 여기에 해당된다. 94년까지 역기능으로 분류했던 불법 복제는 95년도 역기능 사례에서 제외시켰다.

3. 정보화 역기능 사례 현황 및 분석

3.1 1973년~1994년 사이에 발생한 역기능 사례

국내의 정보화 역기능 사고는 1973년 10월 서울 반포 AID 차관 아파트 입주자의 추첨 프로그램을 관계자들이 변조하여 특정인을 부정 당첨시킨 사례를 효시로 하여 매년 증가되어 왔다.

역기능 사고의 특성상 개인이나 조직을 막론하고 공식적인 노출을 회피해 왔음으로 신문지상이나 방송 매체에 발표된 경우 이외의 사고 현황은 정확히 파악하기가 어려웠다. 그러나 그동안 몇 분의 현직 검사와 학자들이 개인적인 연구나 논문을 통해서 부분적으로 집계해 온 자료가 있고, 비교적 최신 자료로 대검찰청 전산실의 통계 자료가 있어 집계의 근거를 마련할 수가 있었다. 따라서 1973년부터 1992년 10월 23일 이전까지의 통계 자료는 대검찰청 전산실장 노연후 씨의 저서 "컴퓨터 범죄—실태와 사례 유형"[노연후, 1992]을 참고하기로 하고 그 이후의 사례는 언론에 발표된 분명한 자료를 근거로하여 분석 검토하기로 하였다. 1992년 10월 23일까지 발생한 역기능 사례는 51건이었다. 그 후 1994년 12월 31일까지 추가로 118건이 발생함으로써 그동안 발생한 역기능 사례는 총 169건에 이르고 있다. 그 중 58건은 금융기관에서 발생함으로써 금융관련 역기능 사례가 34%로 가장 높은 비율을 차지하고 있다.

94년까지의 사례를 사례유형별, 발생기관별, 연령별, 피해액별로 다음과 같이 통계표를 산출하였다. 참고로 사례유형별 분류기준은 노연후 씨의 분류기준에 따랐다.

표 2 사례유형별 발생현황

사례 유형	73. 1. 1~92.10.23	92.10.24~94.12.31	소 계
자료 유출	0	12	12
자료 및 프로그램 변조	5	5	10
자료 부정 입력	38	17	55
컴퓨터 부정 사용	0	10	10
시스템 파괴 및 절도	0	3	3
자료 및 프로그램 절도	0	4	4
CD 범죄	4	2	6
기 타	0	65	65
(자료 부정 입수)	3	0	3
(콘솔 부정 조작)	1	0	1
합 계	51	118	169

표 3 발생기관별 발생현황

발생기관	73. 1. 1~92.10.23	92.10.24~94.12.31	소 계
공공기관 및 학교	6	34	40
금융기관	41	17	58
기업체	4	42	46
기 타	0	25	25
합 계	51	118	169

표 4 연령별 발생현황

연 령	73. 1. 1~92.10.23	92.10.23~94.12.31	소 계
60세 이상	0	0	0
50~60	0	4	4
40~50	6	4	10
30~40	16	16	32
20~30	29	20	49
20세 미만	0	5	5
미 상	0	69	69
합 계	51	118	169

표 5 피해액별 발생현황

피해액	73. 1. 1~92.10.23	92.10.23~94.12.31	소 계
1백억원 이상	2	3	5
1억원 이상	17	7	24
5,000만원~1억원	4	3	7
1,000만원~5,000만원	15	6	21
500만원~1,000만원	4	3	7
500만원 미만	9	1	10
미 상	0	95	95
합 계	51	118	169

3.2 1995년 1월 1일~12월 31일 사이에 발생한 역기능 사례

1995년 한해 동안 발생한 정보화 역기능 사례는 총 100건으로 나타났으며, 각 관점별 분석표를 보면 다음 표와 같다. 사례유형별 통계는 표 1에 소개된 분류기준에 따른 것이다.

표 6 '95년 사례별 발생건수

사례 유형	발생건수(비율)
자료 유출	14 (14%)
정보기기 관련 범죄	9 (9%)
내부 자료 변조 및 파괴	14 (14%)
부정 정보 처리	2 (2%)
해 킹	17 (17%)
금융범죄	8 (8%)
비윤리적 행위	20 (20%)
컴퓨터 바이러스	6 (6%)
기 타	10 (10%)
합 계	100

표 7 '95년 발생기관별 발생건수

발생기관	발생건수(비율)
개 인	34 (34%)
공공기관	15 (15%)
일반기업	15 (15%)
금융기관	13 (13%)
대 학	10 (10%)
학 교	5 (5%)
기 타	8 (8%)
합 계	100

표 8 '95년 연령별 발생건수

연 령 별	발생건수(비율)
50대 이상	5 (5%)
40~50	6 (6%)
30~40	10 (10%)
20~30	24 (24%)
10~20	5 (5%)
기 타(미상)	50 (50%)
합 계	100

표 9 '95년 피해액별 발생건수

피 해 액	발생건수(비율)
10억 이상	5 (5%)
1억~10억	10 (10%)
5,000만원~1억	5 (5%)
1,000만원~5,000만원	7 (7%)
500만원~1,000만원	3 (3%)
500만원 미만	10 (10%)
기 타(미상)	60 (60%)
합 계	100

3.3 1973년부터 1995년까지 정보화 역기능 사례 발생 추이

전체 기간(73년부터 95년까지) 동안 정보화 역기능 사례의 발생 추이를 살펴보면, 1973년부터 1992년 10월까지 약 20년간 51건, 1992년 10월부터 1994년까지 약 2년간 118건으로 무려 같은 기간에 비해 20배가 넘는 증가율을 보였다. 1995년 한해에는 100건의 역기능 사례가 발생했는데, 이는 94년까지 포함했던 불법복제를 제외한 사례이므로 그 발생건수는 매우 크다고 할 수있다. PC보급 및 교육의 확대

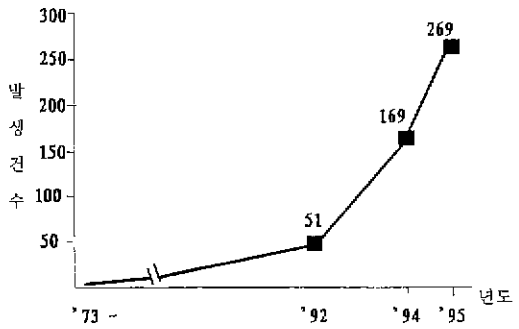

그림 1 '73~'95년까지 역기능 사례 증가율

표 10 '73~'95년까지 전체 역기능 사례 발생건수

연 도	'73년~92년 10월	'92년 10월 ~'94년	'95년(1.1 ~12.31)	총 계
발생건수	51건	118건	100건	269건

로 이용자들이 늘어났고, 그에 따른 역기능 사례도 빠른 속도로 증가추이를 보였다.

3.4 역기능 사례 발생 특징

3.4.1 1973년 1. 1~1994. 12. 31

73년부터 94년까지 대표적인 역기능 사례를 살펴보면 청와대를 사칭하여 패스워드를 변경시킨후 각 은행망에 침투하여 휴면계좌의 금액을 부정 인출하려던 해킹사건, 소프트웨어의 불법 복제로 15개 업체가 미국 사무용 소프트웨어 협회(BSA)로부터 서울지방검찰청에 고소당한 사건, 은행과 대학에서 최고관리자가 자료의 변조를 지시한 사건, 몇 개 기관에서 불법 흥신업소에 개인 정보를 유출시킨 사건, 하드웨어와 소프트웨어의 절도 사건, 국제 카드 위조범의 국내 침투 범행, 기타 증명서 부정 발급, 예금의 부정 인출을 위한 자료 변조 사건, 공공 기관에 대한 해킹사건 등이 있다. 이들 사례들의 세부적인 발생 특징을 살펴보면 다음과 같다.

- ○ 발생한 역기능 사례들을 발생기관별로 살펴 보면 금융기관에서 높은 발생률을 보이고 있으며 금전상의 피해액도 점점 상승하여 수 천만원대에서 수 억대 이상의 고액화 사고로 확대되고 있다.
- ○ 사례유형별로 살펴보면 자료의 부정 입력이 주종을 이루고 있으며 다음이 자료의 부정 유출 순으로 집계되었다. 자료 부정 유출의 경우 특정 기관이나 단체 뿐 아니라 개인 정보의 유출이 늘어나고 있어 이에 대한 대책이 조속히 마련되어야 할 것이다.
- ○ 기술적인 면에서는 컴퓨터의 단순 조작 또는 자료의 변조와 같은 수법들로 아직 기초적인 단계 이거나 저수준에 머무르고 있다. 그러나 전문 기술자가 범죄에 적극 개입하고 있음은 주목할 만한 특징이다.
- ○ 범인 신분별로 볼 때 금융계와 학계의 최고 관리자의 지시에 의한 자료 변조 사고가 몇건 발생 하였다. 이와 같이 최고 관리자가 큰 죄책감 없이 직접 또는 간접적으로 범행을 지시하거나 종용하여 전산 전문가들로 하여금 범행을 저지르게 하는 행위는 국내 역기능 사례의 특징으로써 외국에는 유례가 드문 특수 위법 사례로 분석된다.
- ○ 컴퓨터 부정 사용의 거의 전부를 차지한 해킹과 기타로 분류된 바이러스에 의한 피해가 증가하고 있다. 향후에는 국제전산망을 통한 해커의 침투와 국가기간전산망의 해킹 피해가 예상된다.
- ○ 범죄자의 연령층은 20~30대가 많았으나 20대 이하의 청소년 들에 의한 PC 및 디스켓의 절도사건 등이 증가하고 있다. 컴퓨터 시스템의 큰 방해 요인인 바이러스에 의한 피해는 20대들에 의해 작성 유

포되었다고 생각할때 이들에 대한 윤리 의식 교육이 절실히 필요하다.

- ○ 종전에는 생각할 수 없었던 컴퓨터 관련 범죄 행위가 생겨나고 있다. 일례로 컴퓨터의 고장을 빙자하여 업무를 수작업으로 조작 처리한 경우가 있었다.
- ○ 기타로 분류된 내용의 70%이상이 불법 복제였고 그 나머지는 바이러스에 의한 피해였다.

3.4.2 1995년 1. 1.~12. 31

1995년 한해 동안 발생한 역기능 사례중 대표적인 것을 살펴보면, 비윤리적 행위중에서는 PC대화방을 통한 사기행위와 그 외 통신상에서 타인 비방행위등이 있었다. 해킹 행위중에서는 PC통신상에서 타인의 ID와 패스워드를 도용하거나 이들 통신업체를 직접 해킹하여 자료 변조 및 삭제한 경우가 있었고, 대학과 연구소를 해킹한 사례가 있었는데, 이들중 단순 침입 이외에 자료 파괴와 같은 악의성을 지닌 행위가 더욱 두드러졌다. 공공기관 및 개인정보를 다루는 기관에서 내부인에 의해 개인 정보가 유출돼 개인 사생활을 침해한 경우가 있었고, 관공서의 서류나 자료가 유출돼 범죄에 악용된 경우와 학교에서 디스켓에 담겨있던 시험문제가 유출돼 선의의 학생이 피해를 본 경우도 있었다.

은행에서 내부인이 단말기를 이용해 데이터를 조작하는 수법으로 고객의 예금을 횡령하는 사례도 많았다. 또한 신용카드를 암호 해독기 등을 이용하여 위조한 행위와 스캐너와 컬러 프린터기로 증권 및 채권 등을 위조한 사례들도 있었다. 이 사례들의 발생 특징을 살펴보면 다음과 같다.

- ○ 시기 별로는 학생들의 방학과 휴가철이 포함된 3/4분기, 특히 8월에 14건으로 그 발생 빈도가 높았는데, 이때 해킹이 6건으로 가장 많았다.
- ○ 연령별로는 20대가 24건으로 가장 많았고, 10대에서 발생한 사례도 5건이나 되었다. 20대에서 발생한 사례는 주로 해킹과 PC통신상에서 사기 행위들이다. 30대에서 발생한 사례는 주로 은행원 들에의한 단말기 조작이 대부분 이었다. 10대는 PC통신상에서 남의 ID를 도용하여 사기 행위를 한 사례가 많았는데, 10대 청소년들이 부모들의 무관심 아래 PC통신을 이용하여 음란물을 접하거나 이를 판매하는 수법으로까지 지능화 되고 있다.
- ○ 발생 기관별로는 개인이 34건으로 가장 많았고, 공공기관과 일반기업이 각각 15건, 금융기관 13건이었다. 개인에게서 발생된 행위의 대부분은 PC통신상에서 사기 행위이고, 공공기관은 일선 관공서의 내부인에의한 자료 유출, 바이러스 감염, 선거철의 선거자료 유출 및 절도가 있었다. 기업에서는 통신 서비스 업체의 해킹 피해 사례와 컴퓨터 부품 관련 사기 행위가 많았으며, 금융기관에서는 내부인에 의한 단말기 조작이 대부분 이었다.

4. 향후 전망 및 대책

4.1 향후 전망

- ○ 금융기관의 모든 업무가 전산화 되어 있어, 내부인이 단순히 단말기 조작으로 데이터를 변조하기가 쉬워 손쉽게 많은 돈을 횡령할 수 있기 때문에 금융기관 내에서 내부 자료 변조 및 파괴는 그 피해가 늘어날 것으로 보인다.
- ○ 주로 대학과 연구소, PC통신 업체에서 발생한 해킹 사례도 단순 침입 외에 자료의 삭제, 파괴 등 그 악의성이 점점 커지고 있다. 대학이나 연구소 뿐만 아니라 국가기간 전산망 그리고 산업 정보전이 치열한 기업 전산망도 해커의 목표가 될 수 있다. 특히, 전세계적으로 오픈된 인터넷을 통해 외국 해커의 침입도 빈번할 것으로 예상된다. 청소년 층에서는 언론의 해커 찬양론과 같은 왜곡된 보도와 각종 해킹 기법이 소개된 책들을 통해 호기심에서 해킹 행위를 할 가능성도 높다.
- ○ 정보의 재산 가치가 더욱 커지면서 정보를 얻으려고 부당한 수단을 이용하는 경우가 늘고 있다. 정보의 종류도 개인정보

뿐만 아니라 선거철의 선거 자료, 학교의 시험문제 등으로 다양화 되었다. 앞으로 기업 정보와 국가 및 공공기관의 정보도 그 중요성이 확대되어 유출 가능성이 더욱 커질 전망이다.

- PC의 증가와 각 학교에서의 컴퓨터 교육 확대로 일반인들과 청소년 층의 PC통신 이용이 매우 활발하다. 하지만, 통신상에서의 익명성을 악용한 각종 사기 행위나 ID도용은 다른 선의의 이용자들에게 큰 피해를 주고 있고, 이는 앞으로도 계속 증가할 전망이다.
- 각급 학교와 대학의 컴퓨터 교육이 확대되면서 교육장의 컴퓨터 내부 부품을 노린 절도 행위도 증가하고 있다. 컴퓨터 칩과 같은 고가의 부품은 부피가 작아 한번에 여러개의 부품을 도난 당할 수 있다. 일반 교육장과 실습실은 자물쇠 등으로 잠금 장치가 되어 있지만, 그것으로는 안전할 수 없다. 좀 더 철저한 관리와 보안장치가 마련되어 앞으로 늘어날 피해에 대비하여야 한다.
- 컴퓨터와 그 주변기기들이 날로 발전 하면서 이를 이용한 사건도 늘고 있다. 암호해독 프로그램을 이용한 신용카드 위조나 정교한 컬러 프린터기나 컬러 복사기 그리고 스캐너를 이용한 수표나 지폐 등의 위조는 첨단 기기의 단속이 보다 철저히 이루어지지 않는한 계속 불법적으로 유통되어 범죄 확산이 더욱 커질 전망이다.

4.2 역기능 방지 대책

날로 증가하는 정보화 역기능 사고를 미리 방지 하고 이에 대한 대책을 수립하기 위해서 관리적 측면을 중심으로 살펴보자.

4.2.1 자료 유출

자료 유출의 대부분은 개인정보의 유출이다. 이는 개인정보를 다루는 기관의 내부인들이 자신들이 다루거나 보관하고 있는 타인의 정보가 얼마나 중요하고, 유출시 큰 문제가 될 수 있다는 사실을 자각하지 못한 데서 비롯된 것이다. '각 개인의 정보는 그 개인의 돈이나 재산만큼 소중히 보호 되어야 하고 비밀이 유지되어야 한다'는 인식의 확산과 교육이 중요하다. 그리고 이를 다루는 기관의 정보 관리가 보다 체계적이고 철저하게 이루어져야 한다. 또한 일선 관공서와 학교의 자료도 관리 상태가 매우 허술하다. 관공서의 주민등록 등본 용지 등 일반 행정 자료도 유출돼 악용될 경우 범죄에 이용될 수 있고, 학교의 시험문제 유출 등은 선의의 학생들에게 피해를 줄 수 있다. 이를 방지하기 위해서는 관리상의 보안 문제를 등한시해 왔던 일선 관공서 및 학교의 문서 관리가 좀더 철저히 이루어져야 하며, 정기적으로 점검 되어야 한다. 참고로, 정부는 95년 12월 2일 국회에서 통과된 형법 개정안에 종전의 비밀침해죄 범위를 편지, 문서, 도서 외에 컴퓨터 디스크와 같은 특수 매체도 포함시키고, 형량도 상향 조정하여, 자료 유출 범죄를 좀더 강력히 단속 하고자 하였다.

4.2.2 정보기기 관련 장비, 부품 관련 범죄

정보기기와 관련한 범죄의 대부분은 컴퓨터 부품 도난 사례들이다. 특히 대학이나 초·중고교에서 그 발생 빈도가 높았는데, 주로 대학 및 학교의 컴퓨터 관리 상태가 허술한 점을 이용하므로, 좀더 철저한 물리적 보안과 관리가 필요하다. 대학의 경우 학생들의 출입이 잦은 학생회실이나 실습실 등의 통제와 야간의 관리가 보다 철저하게 이루어져야 하고, 일선 학교의 컴퓨터 교육 확대로 널리 보급된 각 PC 교육장에도 좀더 철저한 물리적 보안대책이 필요하다.

4.2.3 내부 자료 변조 및 파괴

대부분의 자료 변조는 은행에서 내부인이 단말기를 통한 데이타 조작이 대부분 이었다. 은행 내부인에 대한 철저한 윤리 교육과 자체 징계 처벌의 강화, 그리고 단말기 관리 및 데이타와 자료의 수시 점검이 중요하다. 아울러 개인정보를 다루는 관공서와 공공기관에서의 실수 또는 고의에 의한 자료 변조등은 선의의 국민들에게 큰 피해를 줄 수 있으므로 공공기관의 내부자료 보안을 위한 지침서를 현실에 맞

게 보완하여 배포, 숙지시켜야 하겠다.

4.2.4 부정 정보처리

올해 부정 정보처리중 관리태만에 해당하는 사례가 2건 발생했는데, 이는 정부 기관의 전산 정보 관리 소홀로 부적격자에게 운전 면허와 아파트 분양이 이루어진 경우와 정보서비스를 하는 통신업체에서 자료를 제때에 갱신하지 않아 이용자들이 피해를 본 경우다. 운전 면허 등과 같이 국민의 생명과 직결된 것일 때는 공무원들의 작은 실수로 큰 피해를 초래하므로, 보다 주의 깊은 관리 및 신중함이 요구된다. 정기적인 데이터 점검과 각 부처의 협조를 통한 자료의 무결성에 좀더 신중을 기해야 하며, 실수든 고의든 초래된 결과에 대해서는 철저히 책임을 묻고 징계 조치를 해야 한다.

4.2.5 해킹

해킹 사례의 대부분은 부가통신 서비스 업체를 통해서 대학이나 연구소 또는 이들 업체를 직접 해킹한 사례가 가장 많았는데, 통신을 이용한 해킹 사례는 주로 타인의 ID와 패스워드를 도용하여 이루어졌다. 이 사례들은 PC 통신을 주로 즐겨 하는 10대와 20대에서 빈번히 발생했는데, 이들은 주로 사설 BBS를 개설하고 등록된 ID와 패스워드 등을 도용하는 수법을 썼다. 그러므로, 가급적 건전하지 못한 사설 BBS 이용을 삼가고, 자신의 ID와 패스워드는 주기적으로 변경하며, 타인이나 친구에게도 알리지 말아야 한다. 또한 컴퓨터를 다루는 청소년들에게 윤리 의식을 좀더 철저히 교육시키고, 눈에 보이지 않는 '사이버스페이스'도 또 하나의 질서와 법이 존재하는 사회라는 인식과 그것을 위반 했을 경우 받는 처벌에 대한 홍보도 필요하다.

대학 및 연구소에서 발생한 해킹 사례는 타인의 ID를 도용하거나 시스템의 취약성을 이용한 불법적인 root권한 획득으로 일어난 사고들이다. 단순 침입 외에도 자료를 파괴하거나 삭제한 경우도 있었다. 각 시스템의 관리자들은 수시로 시스템 사용자들의 ID와 패스워드를 점검하여 쉬운 패스워드는 변경 조치를 하고, 주기적으로 패스워드를 변경 하도록 한다. 중요한 데이타와 파일은 반드시 백업 조치를 하고, 각 파일의 접근 권한이 올바른지 수시로 관리해야 한다. 주기적인 로그 파일의 검토를 통해 비인가된 자나 의심 가는 사람의 접근을 차단해야 한다. 점검 및 방지를 할 수 있는 진단 시스템, 방화벽, 경보장치와 같은 시스템 보안 장비를 설치, 운영하는 것도 사고 예방과 대처의 한 방법이다. 만약, 누군가에 의한 침입 사실이 의심될 때는 즉각 관계기관의 협조를 통해 계속 감시 및 추적이 이루어지도록 해야 한다.

그 외 소프트웨어의 암호해독과 같은 소프트웨어 변조는 몇몇 컴퓨터광의 호기심과 자신의 컴퓨터 실력을 과시하고자 하는데서 비롯될 수 있는데, 이것이 저작권 침해 및 불법행위에 해당한다는 것을 반드시 인식하고, 이들을 영웅이나 대단한 실력가로 인정해 주는 언론매체의 풍토도 하루 빨리 바뀌어야 한다.

4.2.6 금융 범죄

금융 범죄의 대부분은 암호해독 프로그램을 이용한 신용카드의 위조이고, 그 외 스캐너나 칼라 프린터기를 이용한 수표와 증권 위조 사고가 있었다. 암호 판독용 기계 및 프로그램에 대한 판매 단속과 규제가 보다 철저히 이루어져야 하며, 개인은 자신의 신용카드를 타인에게 잠시라도 건네주는 것을 삼가해야 한다. 정교한 인쇄가 되는 프린터기와 복사기 그리고 스캐너의 판매도 좀 더 신중히 이루어져야 하며 이에 대한 단속이나 처벌 규정이 시급하다.

4.2.7 비윤리적 행위

비윤리적 행위의 대부분은 PC 통신을 통한 음란물 판매 및 사기 행위 였다. 주로 윤리 의식이 불완전한 청소년들과 PC상의 익명성을 악용한 사람들에 의해 발생하였는데, 특히 방학과 휴가철인 8월에 집중적으로 발생하였다. 이 시기에는 좀더 강력한 대응책으로 PC통신 운영자 및 관계기관이 사이버 스페이스의 감시, 감독을 강화해야 한다. 청소년들에게 윤리 의식과 네티켓 교육을 강화하고, 각 개인도 단순히 PC통신을 통해 충동적 구매를 하기보다는 전화나 기타 확인 절차를 통한 후 그 대상이 확실할 때 구매를 하도록 한다.

4.2.8 컴퓨터 바이러스

컴퓨터 바이러스는 그 특징상 언론에 공개된 피해 사례 외에 그 몇 배 이상의 실제 피해들이 있을 것으로 추정된다. 일단 기본적인 예방책은 주기적으로 발생하는 바이러스에 대한 철저한 주의와 타인의 디스켓을 이용하기 전 백신툴로 미리 점검하는 습관을 기른다. 요즘 PC 통신이 널리 확대되면서 공개 소프트웨어를 통한 감염 사례가 늘고 있는데, 일단 그런 자료들은 PC통신에 올라온 지 1주이상 되어 안전하다고 평가된 것을 사용하고, 다운받아 사용하기 전에 백신툴로 진단해 보는 것이 안전한 방법이다. 통신 서비스 업체에서는 올라온 자료들을 좀더 체계적이고 철저하게 진단해 주는 것이 바람직하며, 일단 불량이나 악의성을 지닌 자료로 판명이 나면 그 자료를 올린 사람에게 적절한 조치를 취하여 다음에 재발하지 않도록 한다.

4.2.9 기타

기타로 분류된 사례는 주로 PC통신이나 인터넷의 익명성을 악용하여 여론조사를 왜곡 하거나 헛소문을 퍼뜨려 타인에게 피해를 준 사례들과 도청 장비로 개인의 사생활을 침해한 행위, 해킹기법을 책으로 출판하여 물의를 빚은 일 등이다. 이는 앞서 말한 인터넷 이용자들의 윤리 의식과 네티켓이 결여된 탓으로, 앞으로 이에 대한 교육 강화와 이를 지키지 않는 이용자 스스로가 수치심을 느껴 다시 그런 행동을 하지 않는 풍토를 조성해야 할 것이다. 또한 컴퓨터에 대한 전문가 일수록 단순히 자신의 능력에 대한 우월감에 사로잡히기 보다는 자신의 기술이 사회 전반적으로 어떤 영향을 끼칠 것인가를 좀더 신중하게 생각해 보아야 한다.

참고문헌

[1] Helen Collinson, Computer Fraud & Security, Elsevier Sicence, 1994.

[2] Simson Garfinkel & Gene Spaffo, Practical UNIX Security, O'Reilly & Associates, 1991.

[3] Tom Forester & Perry Morrison, Computer Ethics; Cautionary Tales and Ethical Dilemmas in Computing, The MIT Press, 1990.

[4] Charles P. Pfleeger, Security in Computing, Prentice-Hall, 1989.

[5] V.P. Lane, Security of Computer Based Information Systems, Macmillan Education, 1985.

[6] Bureau of Justice Statistics, Computer Crime - Criminal Justice Resource Mannual, Washington D.C., 1979.

[7] Richard H. Baker, Computer Security Handbook, Blue Ridge Summ, TAB Professional and Reference Books, 1991.

[8] 이재우외, 정보화 역기능 현황 및 분석, 한국전산원, 1994.

[9] 이재우외, 컴퓨터 보안관리 지침 연구, 한국전산원, 1990.

[10] 이재우외, 전산보안 어떻게 해야 하나, 한국전산원, 1995.

[11] 김세헌, 컴퓨터 범죄와 프라이버시 침해, 희성출판사, 1989.

[12] 김옥순, 최익선, 박혜진, 컴퓨터와 청소년 문화, 한국청소년문화연구소, 1994.

[13] 이서로, 파워 해킹 테크닉, 파워북, 1995.

[14] 노연후, 컴퓨터 범죄, 하이테크 정보, 1992.

[15] 신각철, 컴퓨터 범죄 처벌 형법 개정안 해설, 한국정보통신진흥협회, 1992.

[16] 한국전자통신연구소, 컴퓨터 범죄의 매카니즘, 1992.

[17] 김문일, 컴퓨터 범죄론, 범영사, 1992.

[18] 이형원, 정보시스템 안전대책, 영진출판사, 1993

신 순 자

1995 성균관대학교 정보공학과 학사

1995~현재 한국전산원 연구원

관심분야 : 정보화 역기능 사례 DB구축, 컴퓨터·네트워크 보안

김 홍 근

1985 서울대학교 컴퓨터공학과 학사
1987 서울대학교 컴퓨터공학과 석사
1994 서울대학교 컴퓨터공학과 박사
1994.5～현재 한국전산원 선임연구원
관심분야 : 컴퓨터 보안, 병렬처리, 알고리즘

이 재 우

1957 공군사관학교 학시
1979 서울대학교 행정대학원 국가정책과정 수료
1986 미 남가주대학교 대학원 정보체계 석사
1992 건국대학교 대학원 박사
1987～현재 한국전산원 기획조정실장, 본부장, 연구위원
1994～현재 정보시스템 감사통제협회 회장
1995～현재 검찰청 컴퓨터 범죄 수사센터 자문위원장
관심분야 : 컴퓨터 범죄 방지 연구, 정보시스템 보안, 전산망 관리

●'96 단동 첨단기술 국제 학술회의 및 신기술 신상품 전시●

- 일　　자 : 1996년 7월 28～31일
- 장　　소 : 中國, 丹東市(신의주對岸)
- 내　　용 : 심포지움, 전시회 및 백두산 관광 등
- 주　　최 : 중국 료녕성 민족과학가협회
- 문　　의 : 한국정보과학회 사무국
  T. 02-588-9246

●제23회 임시총회 · 춘계학술발표회●

- 일　　자 : 1996년 4월 19～20일
- 장　　소 : 계명대학교
- 내　　용 : 한국정보과학회
- 문　　의 : 학회사무국
  T. 02-588-9246
  F. 02-521-1352