

컴퓨터 범죄의 현황 및 대책 연구

임 명 순*

◇ 목 차 ◇

-
- I. 서 론
 - II. 컴퓨터 범죄의 의의와 유형
 - III. 컴퓨터 범죄의 특성과 현황
 - IV. 컴퓨터 범죄의 대책
 - V. 결 론
 - 참고문헌
 - ABSTRACT
-

I. 서 론

정보사회의 발달과 더불어 컴퓨터의 활용이 여러 분야로 확대됨에 따라 컴퓨터 네트워크는 국내·외적으로 급속히 확산되고 있다. 그리고 업무나 정보처리의 합리화와 정보통신서비스를 위해 도입되고 있는 컴퓨터시스템은 하드웨어기술과 소프트웨어 기술의 발달과 더불어 중요한 역할을 하고 있다. 뿐만 아니라 컴퓨터는 단순한 과학기술의

* 대구대학교 경찰행정학과 강사, 동대학 박사과정.

차원을 넘어 정치, 경제, 사회, 문화, 군사 등 여러 분야에 걸쳐 엄청난 영향을 미치고 있다. 이처럼 사회의 여러 분야에서 보다 구체적이고 실제적인 정보를 이용하고 있다. 새로운 컴퓨터 시스템이나 기술이 도입됨으로 해서 많은 일 처리 가능하게 되었지만 이에 반하여 역기능적 측면도 나타나 사고나 재해 등을 받을 범위가 넓어지고 컴퓨터범죄에 의한 피해도 점차 증가하고 있는 추세이다. 컴퓨터범죄의 역기능으로 등장한 신종범죄로서 정보화가 발전될수록 여러 분야에서 발생하고 있으며 그 범죄 양상도 점차 심화되어가고 있는 실정이다. 컴퓨터범죄를 효과적으로 방지하지 못한다면 정보화의 진전은 相殺될 위치에 놓이게 될 우려까지도 예상된다고 할 수 있다. 이러한 상황은 컴퓨터범죄연구와 그 방지를 위한 노력이 더욱 필요하다고 하겠다. 이러한 시점에서 본 논문은 컴퓨터범죄의 내용과 현상을 살펴보고 그 확산방지를 위한 방안을 제시하고자 한다.

본 논문은 컴퓨터범죄의 앞으로의 경향을 예측하기 위하여 컴퓨터범죄의 유형과 컴퓨터범죄의 특성과 현황 및 수법 등을 살펴보고 분석한 후, 컴퓨터범죄의 심화현상 및 확산을 방지할 수 있는 방안을 제시하는데 연구의 목적을 두고 있으며 연구방법으로는 문헌연구 및 범죄통계자료를 활용하고자 한다.

Ⅱ. 컴퓨터 범죄의 의의와 유형

1. 의의

정보화사회란 규범적으로는 인간의 삶의 질을 향상시키며, 민주화·복지화·합리화의 여러 가치를 실현시킴을 목적으로 하며, 정보·지식이 중요한 자원의 하나로 인식되어 사회의 핵심적 역할을 담당하며, 고도로 발달된 정보기술을 기반구조로 하여 정보의 이용이 보편화되고 이의 생성, 전달, 가공, 축적이 활발해져 정보통신시스템의 응용분야가 복잡·다양화되고 광범위하게 확대된 사회를 말한다.¹⁾

정보의 가치가 물질의 가치보다 상대적으로 증대된 사회로의 전환을 가능케 한 것은 바로 컴퓨터와 통신기술의 진보에 있다. 인류가 산업혁명으로 새로운 에너지를 공급받아 인간의 육체적 한계를 극복하였듯이 정보혁명은 인류에게 새로운 두뇌와 신경을 제공하여 인간의 정신적 영역을 무한히 넓혀주고 있다. 그러나 정보화사회를 실현함으로써

1) 캐나다의 文化史學者 마샬 맥루한(Marshall McLuhan)은 통신의 발달에 의해 지구상의 모든 인간이 한 마을의 일원이라는 의식을 갖게 되었다고 하고 지구촌(Global Village)이라고 하는 조어를 제창하였는데, 이것도 정보화사회의 또다른 표현이라 할 수 있다.

써 금세기 최대문명의 이기로 각광을 받게 된 컴퓨터도 사회적 편익의 증진이라는 인류에 대한 유익적 측면을 제공하는 반면 그의 오용 및 남용으로 인류에게 피해를 초래하는 역기능적 측면도 있다. 우리 나라에서 컴퓨터는 1960년대 도입된 후 고도의 효율성으로 인하여 급속히 확대 보급되어 은행의 온라인예금, 각종 공과금, 고지서, 기차표예매, 증권시장, 부동산정보, 학력고사의 채점, 컴퓨터 세탁기, 화상회의, 전자사서함, 비디오텍스 등 이제 컴퓨터는 우리의 생활과 밀접 불가분의 관계를 맺게 되었다.

정보화사회에서 있어서의 컴퓨터는 인간생활의 거의 모든 영역에서 놀라운 기능을 수행하면서 법률 분야와도 밀접한 관련을 맺어가고 있다. 컴퓨터의 이용범위와 가능성은 실로 다양하고 무한한 것이므로 선진국에서는 각 대학의 부설연구소나 변호사협회 심지어는 개인적으로도 방대한 판례법과 복잡한 법령들을 체계적으로 컴퓨터에 기억·저장시켜 두었다가 필요시 사안에 적용될 수 있는 법규와 판례 등을 다시 끄집어내어 볼 수 있도록 하는 연구에 막대한 노력을 하고 있다. 그리고 금융기관, 회사, 증권거래소가 컴퓨터 시스템을 이용하게 됨에 따라 회사법규 및 거래법규의 수정이 불가피하게 되었으며, 자기 테이프, 자기 디스크, 자기 드럼, CD롬 등이 등장하게 됨에 따라 과연 그 증거능력이 인정될 것인지 증거법도 새로운 해석이 요청되고 있다. 이외에도 보험법, 특허법 및 저작권법 또는 노동법 등 컴퓨터의 영향이 방법론적 측면과 실체적 측면에 끼치는 것은 다대하다고 하겠다.²⁾

컴퓨터의 자연과학적 개념정의는 컴퓨터범죄에서 말하는 컴퓨터의 정의와 반드시 일치하는 것은 아니다. 왜냐하면 컴퓨터에 대한 법률적 개념정립은 특히 형벌에 의한 보호의 필요성이 큰 것으로 한정해야 하는데 범죄유형에 따라 그 대상이 되는 컴퓨터의 범위가 다를 수도 있고, 앞으로의 기술의 진보에 따라 현시점에서 예상하지 못한 형태가 생길 수도 있기 때문에 컴퓨터 범죄에서 말하는 컴퓨터의 개념을 一義적으로 정의하는 것은 쉬운 일이 아니다.³⁾

컴퓨터범죄에 대한 개념이 통일되지 않는 이유는, 그것이 하나의 카테고리로 묶을 수 있는 범죄가 아니고 수많은 유형의 범죄가 컴퓨터 시스템을 이용하거나 컴퓨터 시스템과 관련하여 발생하고 있기 때문이다. 또한 이들 범죄유형 중에는 절도, 사기 등 종래의 전통적 범죄에 흡수시켜 처벌이 가능한 범죄도 있다. 그것의 처벌을 위해서는 새로운 입법조치를 필요로 하는 유형들이 있다. 문제는 이러한 컴퓨터범죄의 개념에 재산적 침

2) Hans Peter Bull und Zentarō Kitagawa(Hrsg), Computer im Dienst der Gesellschaft?, Carl Heymanns Verlag KG, 1984참조 ; “컴퓨터技術의 활용이 法學 각 분야에 미치는 영향에 관한 小考”(서울대학교 법학, 제13권 1호), pp.35~36.

3) 이철, “컴퓨터범죄와 소프트웨어보호”, 서울: 박영사, 1996, p.8.

해행위와는 별도로 개인의 사생활에 대한 비밀의 침해나 국가적·정치적 기밀에 대한 침해를 포함시키느냐에 귀착된다. 컴퓨터 시스템과 관련하여 발생하는 범죄행위가 재산 침해행위가 중심이 되는 것은 사실이나 개인이나 국가의 비밀을 침해하는 행위도 무시할 수 없다. 특히 현대국가의 행정국가화 추세에 따라 개인의 각종 데이터가 컴퓨터 시스템에 수록되어 이용되고 있고 국가의 기밀도 컴퓨터 시스템에 저장되어 활용되고 있는 현실을 고려할 때, 이들 비밀을 침해하는 행위는 개인사생활의 평온과 국가의 안전에 크나큰 위협이 아닐 수 없다. 그러므로 컴퓨터범죄에 대한 개념정의는 작업 가설적인 의미가 더 크고 앞으로 입법화에 대비한다는 견지에서 형사상 처벌하거나 처벌할 만한 가치 있는 범죄들을 광범하게 포섭하는 의미로 사용함이 바람직하다 하겠다.

2. 컴퓨터범죄의 유형

컴퓨터 범죄의 유형은 각기 이를 파악하는 시각에 따라 여러 가지 차이가 있으나 지금까지의 대개의 유형은 다음과 같다.

1) 컴퓨터의 不正操作

컴퓨터의 부정조작이란 컴퓨터에 의해 처리, 전달, 보존되는 데이터를 부정하게 조작하는 일체의 행위를 말하며 컴퓨터에 대한 입력, 처리, 출력, 기억의 모든 단계에서 데이터나 프로그램의 부정입력, 변경, 소거, 부정작출의 행위 등을 포함한다. Ulrich Sieber는 컴퓨터의 부정조작이라는 개념은 탄력적이며, 정확성이 덜한 까닭에 자료변경을 “행위자가 컴퓨터의 처리결과 혹은 인쇄출력을 변경시켜 이로 인하여 자신의 재산적 이익을 얻기 위한 의도를 가지고 전자자료처리의 영역에 있어서 부분적인 자료변경을 시도하는 것⁴⁾이라고 한다.

컴퓨터부정조작은 피해회사나 내부의 컴퓨터 관련직원에 의한 범행이 대부분이지만, 컴퓨터 시스템의 네트워크가 광범하게 이루어지고 현금자동지급기 및 자동 입출금기의 설치가 급속히 늘어감에 따라 외부인에 의한 범행도 늘어날 것이다.⁵⁾

4) Ulrich Sieber, Computerkriminalität und Strafrecht, 2. 1980. S. 39ff.

5) 이철, 전게서, p.65.

(1) 컴퓨터 입력조작

입력조작이란 불법적인 목적을 달성하기 위하여 입력될 자료를 조작하여 컴퓨터로 하여금 거짓 처리결과를 만들어 내게 하는 것이다. 이러한 입력조작은 일부 은닉된 자료, 변경된 자료, 허위의 자료 등을 컴퓨터에 공급함으로써 잘못된 출력을 생성케 하여 발생하는 범죄로서, 가장 기본적인 컴퓨터 범죄의 형태라고 할 수 있다. 입력조작은 입력자료에 변경을 가하거나, 입력장치를 이용하여 컴퓨터에 허위의 정보를 제공함으로써 이루어지는데, 컴퓨터의 자료입력의 유형에 따라 그 조작의 태양과 행위자의 범위가 달라지게 된다.⁶⁾

(2) 콘솔조작

콘솔(Konsol)이라 함은 컴퓨터 시스템 전체를 총괄, 조정, 운영하는 조작장치를 말한다. 콘솔은 컴퓨터시스템을 점검·감시할 수 있으며 처리하고 있는 정보처리내용과 방법을 변경, 수정, 대치할 수 있다. 이러한 콘솔조작은 콘솔 타자기에 의하여 컴퓨터에 공급되는 자료를 허위로 입력시키거나, 컴퓨터의 내부 혹은 외부기억장치에 기억된 자료를 변경시킴으로써 가능하며, 프로그램 진행과정 중 표현을 방해하거나 이를 반복하거나 빠뜨리는 형태 등을 그 예로 들 수 있다.⁷⁾

(3) 프로그램 조작

프로그램이란 컴퓨터를 작동하도록 하거나 어떤 결과를 얻기 위하여 컴퓨터에 주어지는 복합명령의 표현이다.⁸⁾ 즉, 컴퓨터를 작동하도록 하거나 특정한 결과를 얻기 위하여 컴퓨터 등 정보처리장치 내에서 직접 또는 간접으로 사용되는 일련의 지시, 명령 등의 군이라고 할 수 있다.⁹⁾

(4) 출력조작

출력은 단말기의 스크린이나 특별한 인쇄용지를 제외하고는 입력이 행하여진 것과 동일한 매체, 즉 카드, 종이 테이프, 마그네틱 테이프, 디스크, 마그네틱 판 등에 의하여 행하여진다. 따라서 출력조작은 원칙적으로 입력조작과 똑같은 자료매체에 대하여 발행

6) 장영민, 조영관, "컴퓨터범죄에 관한 연구", 한국형사정책연구원, 1993, p.25.

7) Ulrich Sieber, a. a. O., S. 60.

8) Ulrich Sieber, a. a. O., S. 54.

9) 컴퓨터프로그램보호법, 제2조 제1항.

할 수 있다. 출력조작이란 컴퓨터에 의하여 올바르게 출력된 출력인쇄를 사후에 변조하는 것이다.¹⁰⁾

2) 컴퓨터 파괴

컴퓨터파괴란 자료나 프로그램이 저장된 매체를 없애거나 교란시키는 행위를 말하며 컴퓨터방해라고도 한다. 형법상의 컴퓨터업무방해죄에서의 정보처리장치 등 손상행위와 전자기록 등 손괴죄에서의 특수매체기록 은닉행위 등이 이러한 유형에 해당된다. 컴퓨터의 물리적인 구성물, 즉 하드웨어와 소프트웨어인 각종 프로그램과 컴퓨터 장비 내에 포함된 데이터를 파괴하는 행위이다.¹¹⁾

(1) 행위태양

컴퓨터가 개발되던 초기에 하드웨어의 경제적 가치가 높았으나 현재에는 소프트웨어가 크게 발전한 컴퓨터 이용의 효율에 미치는 영향이 하드웨어의 영향을 앞지르기 때문에 컴퓨터 산업의 투자액도 거의 80%가 소프트웨어에 대한 투자이다. 이제는 컴퓨터 파괴의 대상도 소프트웨어가 하드웨어보다 훨씬 주목을 끌고 있다. 따라서 컴퓨터 파괴의 방법도 하드웨어 자체를 파괴시키는 것보다는 강력한 자석을 사용하거나 기억된 자료를 무효화시킬 수 있는 새로운 프로그램을 짜 넣는 등의 방법이 주로 이용된다.¹²⁾

(2) 행위자태양

행위자의 태양은 대체로 세 가지로 분류할 수 있다. 첫째, 타국의 비밀첩보원으로 또 는 각종 지하조직의 테러리스트들이 파견되어 범하는 경우와, 둘째, 정치적 동기에서 자국의 과격파 청년들에 의한 경우, 셋째, 회사 내에서 임금인상 요구나 처우개선에 관한 요구를 거절당한 데 대한 복수심에서 경영주에 대한 경고나 카드로서 범하는 경우, 그리고 어떤 단체나 개인에 대한 사적 원한이 있어 범행하는 경우 등이다.¹³⁾

10) Ulrich Sieber, a. a. O., S. 65.

11) 최규태, "컴퓨터범죄와 이에 대한 형법적 대응에 관한 연구", 전남대학교 박사학위논문, 1994, pp.12~13.

12) 신각철, 김문일, "컴퓨터범죄론", 서울: 법영사, 1997, p.111.

13) 신각철, 김문일, 전게서, p.111.

3) 컴퓨터 스파이

컴퓨터스파이란 컴퓨터에 의하여 처리, 보관, 전송되는 자료나 처리결과 또는 프로그램을 권한 없이 획득, 이용하는 것을 말하며 자료의 부정취득이라고도 한다. 형법상의 기술적 수단에 의한 비밀침해죄에서의 특수매체기록의 내용을 기술적 수단을 이용하여 알아낸 경우가 이러한 유형에 해당된다. 컴퓨터 시스템의 자료를 권한 없이 획득하거나 이용·누설하여 타인 하에 재산적 손해를 야기시키는 행위를 말한다.¹⁴⁾

(1) 컴퓨터프로그램

컴퓨터의 우열을 소프트웨어, 즉 프로그램의 우열에 의하여 판가름되어진다. 따라서 오늘날의 컴퓨터 산업부분에서는 이 방면에 대한 연구·개발이 극히 중요시되고 있다. 중요한 프로그램을 개발하는 데에는 전문인력과 많은 시간, 비용이 소요되기 때문에 타인이 개발해 놓은 프로그램을 상당한 대가없이 취득·사용한다는 것은 피해자가 입은 손실만큼 재산적 이익을 얻게 되는 것이다.¹⁵⁾

(2) 데이터

컴퓨터의 기억장치에 기억되어 있는 데이터(자료)도 컴퓨터 스파이의 행위객체가 된다. 즉 연구자료나 고객의 명단, 경영·산업데이터, 건축데이터, 개인신상에 관한 데이터 등의 그것이다. 이들 데이터는 그 양이 방대함에도 불구하고 매우 용적이 작은 자기 테이프, 자기 디스크, 칩 등에 압축·수록되어 있어 적은 노력으로도 취득이 가능하므로 컴퓨터 스파이의 공격대상으로는 매우 적합한 것이다.

4) 현행 형법의 분류

현행 형법상 컴퓨터범죄에 관련된 규정은 첫째, 컴퓨터 부정조작 범죄의 범주에 속하는 것으로 전자기록위작·변작 등 죄(공전자기록위작·변작, 공정증서원본부실기재, 위조공문서등행사, 사전자기록위작·변작, 위조사문서등행사)와 컴퓨터 등 사용사기죄가 규정되었고, 둘째, 컴퓨터 파괴범죄의 범주에 속하는 것으로는 컴퓨터 파괴 등 업무방해

14) Ulrich Sieber, a. a. O., S. 98 ; Thomas Fischer, Computerkriminalitat, Bern, 1979, S. 21f. : Theodor Lenckner, Computerkriminalitat und Vermögensdelikte, (Heidelberg · Karlsruhe ; C. F. Muller Juristischer Verlag. GmbH, 1981), S. 17.

15) 신각철, 김문일, 전계서, p.115.

죄, 공전자기록 등 무효죄, 사전자기기록과괴죄가 규정되었고 셋째, 데이터의 부정입수(컴퓨터스파이)범죄의 범주에 속하는 것으로서 비밀침해죄와 공무상 비밀내용탐지죄가 규정되었다. 또한 컴퓨터 등 사용자기죄를 보완, 그 처벌범위를 제한하는 규정인 편의시설 부정이용죄가 있다. 그러나 현행 형법은 컴퓨터범죄 유형 가운데 컴퓨터의 무권한사용에 대하여는 직접적으로 규정하지 않고 있다.

Ⅲ. 컴퓨터 범죄의 특성과 현황

1. 컴퓨터 범죄의 특성

1) 발각과 원인규명의 곤란

범죄의 발각과 원인규명이 곤란하다는 점도 특성이다. 대상이 물건이 아니라 데이터로서 可視性和 可讀性이 없어 발각이 어려우며, 데이터의 처리가 매우 고속으로 이루어지고, 범죄수단에 의한 에러 등의 影響이 단시간에 광범위하게 전달되기 때문에 원인규명이 곤란하다.

2) 범행의 국제성과 광역성

네트워크를 이용하여 遠隔地 間에서 이루어지는 경우가 많아 행위지와 결과 발생지가 다른 지방 또는 다른 국가가 될 수 있는 바, 이러한 문제는 수사관할권에 관한 문제, 다른 지역, 또는 국가 간의 컴퓨터범죄의 근거법 선택문제 등 새로운 문제점을 파생시키고 있다.

3) 피해액의 과다성

컴퓨터 범죄의 특징은 전통적인 범죄인 횡령죄, 사기죄와 비교해서 피해액이 크다는 것을 알 수 있고, 피해액이 커지는 이유는 컴퓨터가 가지는 연속성과 자동성의 특징인 컴퓨터 범죄로 인한 피해액을 증대시키는 한 원인이다.

컴퓨터의 기계적 특성인 자료의 압축성을 들 수 있다. 컴퓨터 조작의 대부분이 예금구조를 대상으로 하고 있다는 점이다.

4) 범죄의식의 희박화

컴퓨터는 20세기 인류가 창출해 낸 최고 걸작품의 하나로 지적되고 있고 그 효과가 지대한 만큼 이를 이용한 범죄는 타인을 살해하거나 상해하는 것 등 전통적인 범죄의식 보다는 컴퓨터에 대한 고도의 조작기술을 즐기는 경우가 많고 단순한 遊戱의 동기에서 비롯되는 경우가 있으며, 범죄의식이 희박한 경우가 많다. 그러나 최근에 이르러서는 점차 경제적 동기에 의한 범행으로 변모하고 있다.

5) 범행의 자동성과 반복, 연속성

컴퓨터 범죄는 어떤 행위는 한번 행위를 명령하고 나면 그것을 다시 정지시키지 않는 한 그 행위는 자동적이며 연속적으로 계속된다. 행위자가 어떤 다른 행위를 하지 않더라도 일단 불법 변경된 고정자료를 呼出하거나 불법한 프로그램을 삽입할 때마다 자동적으로 범죄행위가 유발되기 때문이다.¹⁶⁾ 금융기관의 종사자들이 예금계좌를 조작하여 범행하는 경우가 가장 많이 발견되는 사례이다.

6) 전문가 또는 경영내부자의 범행이 많음

컴퓨터범죄는 컴퓨터의 조작, 사용방법 및 소프트웨어에 대한 평가 등 컴퓨터에 대한 기초 내지 전문지식이 필요하므로, 전문가 또는 내부경영자 등에 의하여 범하여지는 경우가 많다.

2. 컴퓨터범죄의 현황과 문제점

컴퓨터범죄가 최초로 발생한 것은 1950년대부터이며, 1960년대에 접어들면서부터 컴퓨터 범죄는 미국을 중심으로 점차 사회 문제화되기 시작하였다. 특히 70년대 들어서면서 발생건수가 급격히 증가함과 아울러 다른 나라에서도 여러 종류의 범죄가 발생하였다. 국내에서 최초로 발생한 컴퓨터 범죄는 1973년 10월 AID차관 아파트 입주권자의 추첨프로그램을 변조하여 부정 당첨시킨 것이다.

정보화시대가 도래한지는 얼마 되지 않았으나 그 전파속도는 빠른 것이 현실이다. 정

16) 김문일, "정보화 사회에 있어서의 컴퓨터범죄와 그 방지대책에 관한 연구", 중앙대학교 박사 학위논문, 1998, p.57.

보화시대의 부산물인 컴퓨터 관련 범죄는 컴퓨터 기술의 발전양상과 보급정도에 비례하여 그 유형이 변화하여 왔는데, 1960~1970년대에는 대형 컴퓨터를 중심으로, 1980년대에는 개인용 컴퓨터를 이용한 컴퓨터 범죄 유형이 생겨나기 시작했으며, 1990년대에는 데이터베이스산업과 통신망의 발전에 따른 네트워크 범죄로 그 동향의 변화를 가져왔다. 전세계를 연결시키고 있는 인터넷과 관련된 범죄의 등장은 바로 눈앞에 펼쳐지고 있는 현실이다.¹⁷⁾

<표 1> 컴퓨터범죄의 검거상황

단위 : 건, %, 명

구 분		1997년	1998년	1999년
발생건수		582	100	1,421
검거건수		531	96	1,401
검거율		91.2	96.0	98.6
검거인원	계	544	128	1,484
	남	497	122	1,305
	여	47	6	179
성년	계	537	123	1,472
	남	491	117	1,297
	여	46	6	175
미성년	계	7	5	12
	남	6	5	8
	여	1	0	4
법인체		94	15	219

※ 출처 : 경찰청, 범죄분석, 1997~1999 자료재구성.

컴퓨터범죄의 최근 3년 동안의 검거상황을 보면 <표 1>과 같이 나타났다. '97년도에는 발생건수가 582건, 검거건수는 531건으로써 검거율이 91.2%이며 '98년도 범죄발생건수가 100건, 검거건수는 96건으로써 검거율이 96.0%으로 나타났다. 그리고 '99년도에는 발

17) 박범규, “개정형법의 컴퓨터범죄에 관한 연구”, 연세대학교 석사학위논문, 1996, pp.14~15.

생건수가 1,421건, 검거건수는 1,401건으로 98.6%로 나타났다. 발생율과 검거율이 해가 갈수록 큰 폭으로 증가함을 알 수 있다. 검거인원을 성별로 보면 '97년도에 남자가 497명, 여자가 47명이고 '98년도에는 남자가 122명, 여자가 6명으로 나타났으며 '99년도에는 남자가 1,305명, 여자는 179명으로 나타났다.

남자가 여자에 비해 컴퓨터 범죄자가 월등히 많은 것으로 드러났다. 미성년 컴퓨터 범죄자의 등장도 주목할 만한 변화이며, 해가 갈수록 증가하고 있는 것으로 나타났다.

<표 2> 컴퓨터 범죄의 동기별 현황 단위 : 명

구 분		1997	1998	1999
총 계		37	65	128
이 목	소 계	22	30	42
	생활비	1	5	6
	유흥비	5	5	4
	도박비	0	0	0
	허영사치	2	0	1
	치 부	4	4	2
	기 타	10	16	9
사행심		1	2	1
보 복		0	1	1
가정불화		0	0	1
호기심		0	4	14
유 혹		1	0	0
우발적		0	1	1
현실불만		0	0	0
부주의		0	2	0
기 타		13	25	68

※ 출처 : 경찰청, 범죄분석, 1997~1999 자료재구성.

컴퓨터범죄의 동기별 현황을 보면은 기타를 제외하고 이욕범죄의 빈도가 '97년도에는 22명, '98년도에는 30명, '99년도에는 42명으로써 가장 높은 것으로 나타났으며 계속해서 증가하고 있는 추세이다. “유홍비” 마련을 위해서 '97년도에 5명, '98년도 5명, '99년도에 4명으로 나타났으며 “생활비”를 위해서 '97년도에 1명, '98년도에 5명, '99년도에 6명으로 나타났다. 이욕 중에서 유홍비 마련이 높게 나온 것은 물질만능풍조와 배금사상의 영향을 받은 것이다.

<표 3> 컴퓨터범죄의 시간별 현황 단위 : 건

구 분	1997	1998	1999
계	34	56	106
심야 00:00~04:00	1	0	2
새벽 04:00~07:00	0	0	0
오전 07:00~12:00	6	16	22
오후 12:00~18:00	10	9	20
초저녁 18:00~20:00	1	1	2
밤 20:00~24:00	0	1	4
미 상	16	29	56

※ 출처: 경찰청, 범죄분석, 1997~1999 자료재구성.

컴퓨터 범죄의 시간별 현황을 보면은 미상을 제외하고 '97년도에는 오후(12:00~20:00)가 10건, 오전(07:00~12:00)이 6건, '98년도는 오전이 16건, 오후가 9건으로 나타났으며, '99년도에는 오전이 22건이고 오후에는 20건으로 드러났다. 그리고 밤(20:00~24:00)을 보면은 '97년도가 0건, '98년도가 1건, '99년도가 4건으로 증가하는 추세를 보이고 있다. <표 3>에서 입증하듯이 '98년도부터는 오후보다는 오전에 컴퓨터 범죄가 더

많이 나타나고 있다.

<표 4> 컴퓨터범죄의 연령별 현황

단위 : 명

구 분		1997	1998	1999
계		37	65	128
소 년	소 계	17	10	58
	14세 미만	0	0	0
	14~15세	9	1	6
	16~17세	4	0	20
	18~19세	2	9	32
성 인	소 계	20	54	69
	20~21세	1	3	8
	22~23세	1	0	12
	24~25세	3	9	5
	26~30세	5	11	21
	31~35세	5	19	5
	36~40세	3	8	8
	41~50세	2	3	8
	51세 이상	0	1	2
	미 상	0	1	1

※ 출처 : 경찰청, 범죄분석, 1997~1999 자료재구성.

'97년도에는 컴퓨터 범죄의 연령을 보면 14~15세가 9명으로 가장 많고 26~30세와 31~35세가 각각 5명으로 나타났다. '98년에는 31~35세가 19명으로 가장 높게 나타났으며, 그 다음으로는 26~30세가 11명이고, 18~19세도 9명으로 나타났다. '99년도를 보면 18~19세가 32명으로 급증하였으며, 26~30세가 21명으로 나타났다.

이와 같은 분석결과는 컴퓨터범죄의 평균연령이 점차 낮아지고 있음을 시사해 주는 것이다.

IV. 컴퓨터 범죄의 대책

1. 컴퓨터 시스템 안전 대책

컴퓨터 시스템에 대한 각종의 범죄나 사고는 국민의 사회활동이나 국가의 경제활동에 커다란 타격을 주기 때문에 그 예방과 방지대책이 수립되어야 한다. 컴퓨터범죄에 대한 예방과 방지에 있어서는 먼저 컴퓨터 시스템에 대한 안전대책을 들 수 있는데, 여기에는 대체로 물리적 대책, 관리적 대책, 기술적 대책으로 나누어지는 바 이를 고찰하면 다음과 같다.¹⁸⁾

1) 물리적 대책

물리적 대책이란 고의적이거나 우발적인 위협에 대처하기 위한 보호조치를 의미하며 이것은 컴퓨터 시스템 전체와의 관련성을 가지고 있어야 한다. 컴퓨터 시설에 대한 완전한 보안대책수립이란 현실적으로 어려운 점이 많으나 화재, 홍수, 사보타지, 폭동, 폭탄장치 및 불가항력적 천재지변과 같은 재해에 신속히 대처할 수 있도록 강구되어야 하며 또는 데이터센터에 대한 모든 위협과 위협발생 가능성을 최소화하고 긴급 시 사람과 재산을 보호할 수 있도록 해야 한다. 첫째, 컴퓨터실의 위치를 선정할 때 고려해야 할 중요사항은 화재, 홍수, 폭발 또는 이와 유사한 주변의 위협과 침입자에 의한 위협으로부터의 안전성을 검토하는 것이다. 둘째, 물리적 재해란 사람이나 자연적 현상에 의해 발생되는 재해를 의미한다.

발생원인이 무엇이든지 간에 물리적 재해에 대한 최선의 방안은 효과적인 백업절차를 준비하여 미 처리 업무량이 가급적 적은 상태에서 복구할 수 있도록 해야한다. 셋째, 컴퓨터실은 허가 받은 자만이 출입하도록 엄격히 통제해야 한다. 가장 이상적으로는 오퍼레이터, 기계실 관리책임자 등 컴퓨터 시스템 운영요원만이 컴퓨터실 내에 근무하도록 하며 컴퓨터실은 항상 잠겨 있고 키가 없이는 내부에서만 열 수 있도록 되어 있어야 한다. 넷째, 예기치 못한 사태의 발생으로 컴퓨터의 사용을 중단해야 할 경우에 대비한

18) 신각철, 김문일, 전계서, pp.297~300.

계획으로 컴퓨터 기기, 프로그램, 도큐멘테이션, 처리절차에 관한 매뉴얼, 데이터 파일을 주요 대상으로 한다.

2) 관리적 대책

컴퓨터범죄를 예방·방지하기 위하여서는 물리적인 보안대책과 병행하여 컴퓨터 업무에 대한 관리체제의 강화 등의 관리적 대책이 필요하다. 첫째, 데이터의 수정을 의도하는 프로그래머가 있다 해도 오퍼레이터와 공모하거나, 컴퓨터실에 불법적으로 침입하여 조작하지 않는 한 범행을 하기란 상당히 어려움이 있다. 따라서 프로그래머는 기기 조작을 하지 않고 오퍼레이터는 프로그래밍하지 않는다는 원칙을 철저히 준수하고 프로그래머는 컴퓨터실에 출입하지 않도록 해야 한다. 둘째, 프로그램을 작성하기 전의 시스템 설계 단계에서는 그 관계 회의에 감사 요원을 참가시켜 사고방지의 시점에서 프로그램에 억제기능을 가진 특수 루틴을 삽입하도록 설계하게 하고 필요한 프로그램은 전부 시스템 감사팀의 심의를 거친 후 실제업무에 사용하도록 해야 한다. 셋째, 문서화를 하는 데 있어, 특히 업무흐름도와 프로그램의 내용이 상치되지 않도록 하는 것이 중요하다. 넷째, 컴퓨터실에는 기억장치와 입력장치의 가동상황을 점검하고 각 오퍼레이터에게 작업을 할당하는 스케줄러가 있다. 스케줄러는 프로그래머에게 건네진 프로그램 테이프와 디스크의 내용을 면밀히 점검하여 부정이 있는지 여부를 체크하도록 한다. 다섯째, 데이터의 경우 특정 직급 이상이어야만 해독할 수 있도록 키나 패스워드를 부여하는 등 일정한 기준을 설정하도록 해야 한다. 여섯째, 통신회선을 감청하려면 패스워드를 사용하지 않으면 안되므로 패스워드는 부장급이 철저히 관리하여 권한 없는 사람은 해독할 수 없는 시스템을 도입하여야 한다. 때로는 파일이나 데이터베이스도 패스워드를 부여하여 이중화, 즉 파일을 등급화하여 보호하여야 한다.

3) 기술적 대책

기술적 대책은 컴퓨터 처리에 의하여 데이터의 취급자를 규제·건제하여 데이터를 보호하는 것을 의미한다. 데이터의 감청, 무단복제, 파괴, 개변, 그리고 가공하여 데이터를 교묘히 컴퓨터 시스템에서 유출시키는 행위 등에 대처하는 방법은 고도의 기술적 연구로 데이터를 가능한 한 암호화하는 방법이다. 최근 암호기법은 단순히 정보내용의 위장뿐만 아니라 전송중의 데이터 암호화, 기록매체상의 데이터의 암호화, 전문의 인증, 디지털 서명, 전문 오배달시의 데이터 보호 등의 분야에서 응용되고 있다.

2. 형사정책적 대책

컴퓨터범죄의 대부분은 전문인에 의하여 범하여지고 범죄의 발각과 증명이 어렵고 극히 범죄암수가 많기 때문이다. 또한 범죄가 발각된다 하더라도 컴퓨터에 대한 지식의 결여로 수사기관 또는 법원에서 불기소 또는 무죄로 되는 사례가 많이 나타나고 있다. 이에 따라 수사관의 수사능력의 배양, 검사·법관의 컴퓨터지식배양문제는 오늘날 범죄의 극복을 위한 중요한 과제의 하나이며, 또한 수사력의 강화, 수사장비의 현대화, 컴퓨터 요원의 윤리적 교육이 필요하고 컴퓨터 안전대책기구의 신설, 컴퓨터범죄 연구기관(산·학·연의 합동)의 설치가 바람직하다.

1) 컴퓨터 시스템 안전대책기구의 설치

컴퓨터범죄의 사전 억제책으로 컴퓨터 시스템의 안전이용을 위한 컴퓨터 시스템 안전대책기구의 설치가 요청된다. 컴퓨터 회사, 수사기관, 대학교수 등을 주축으로 이를 구성하여 컴퓨터 시스템이 범죄에 이용되는 취약점을 조사·분석하고 이에 대한 기술적인 개선책이나 컴퓨터 시스템 안전에 관한 일반기준 등을 제시함으로써 컴퓨터범죄를 사전에 예방하는데 기여하도록 한다.

2) 컴퓨터범죄 연구기관의 설치

컴퓨터범죄에 대하여 효과적이고 적절한 대책을 수립하기 위해서는 범죄실태의 파악과 분석이 기본적인 과제이다. 이를 위하여 검찰·경찰 등 수사기관 안에 또는 별도로 컴퓨터범죄 연구기관을 설치하는 것이 바람직하다.

3) 수사능력의 향상

컴퓨터범죄는 기술적인 요소 때문에 범죄의 발각과 증명이 어렵고 증거인멸도 다른 범죄에 비하여 아주 간단할 뿐 아니라, 또한 범죄자가 발각되었다 하더라도 컴퓨터 시스템에 관한 지식의 결여로 수사기관 또는 법원에서 불기소 또는 무죄로 되는 경우가 많다. 따라서 과학적인 수사를 위해 수사관이나 검사·법관들에게 컴퓨터 지식의 배양으로 법관·수사요원들의 전문화가 필요하다.

4) 재범방지를 위한 행형제도의 개선

우리 나라 행형법상의 문제점의 하나로서 소내에서의 처우로 행하는 인격교화를 위한 제도로서의 학과교육·집업보도(직업훈련)·인격개화(치료)·생활습관의 교정 등 모든 문제에 관한 기본적인 규정이 체계적으로 담겨져 있지 못하고 미흡한 상황이다.

5) 컴퓨터 종사자의 윤리교육

1981년 미국의 IBM사는 컴퓨터의 안전의 문제와 관련하여 낸 광고에서 “The computer didn't do it (crime)”을 그 헤드라인으로 썼는데 이것은 컴퓨터범죄는 컴퓨터 자체의 문제가 아니라 인간자신의 문제임을 강조한 것이라 하겠다. 컴퓨터범죄에 대한 보다 근본적인 대책은 컴퓨터와 관련하는 인간들의 윤리관의 확립에 노력이 경주되어야 한다고 본다.

6) 정보범죄수사센터 설립¹⁹⁾

검찰에서는 이와 같이 서울에 정보범죄수사센터를 설치하여 컴퓨터 해킹범죄 뿐 아니라 각종 유형의 첨단 정보시스템 범죄에 대한 종합대책을 강구하고 있으며, 각 지방 검찰청에 컴퓨터범죄 전담검사를 두어 정보시스템범죄에 대한 대응체제를 구축하고 있다. 정보범죄수사센터에서는 컴퓨터범죄에 관한 각종 압수물과 증거자료 및 정보들을 계속 수집하고 있으며 각종 대규모 경제범죄수사 등에서 컴퓨터로 처리된 각종 증거물들에 대한 분석업무도 지원하고 있고 각 지방의 컴퓨터범죄 등 첨단범죄수사를 지원하는 기능도 담당하고 있다.

검찰에서는 이러한 정보시스템범죄에 대한 직접 수사활동을 수행하고 있을 뿐 아니라, 첨단 컴퓨터범죄에 대처하기 위한 종합적인 법적, 제도적 조치들도 강구하고 있다.

7) 정보보호센터의 설립²⁰⁾

정보센터는 법인형태로 설립되어 각 부처에서 파견된 공무원들과 전문직원들로 구성되어 정보보호 관련업무를 담당할 예정으로 되어 있다. 정보보호센터의 기능과 임무는 정보보호 정책 및 제도조사, 연구, 정보화 역기능 분석 및 대책연구, 정보보호시스템의

19) 한봉조, “정보시스템범죄 대응체계동향”, 한국전산원, 1996, pp.156~157.

20) 한봉조, 전제서, pp.156~157.

연구·개발 및 시험·평가 등으로 되어 있으며, 구체적인 업무내용은 정보통신 보안 시스템 침투사례 분석, 대응조치 연구·개발, 정보통신 분야의 암호화 기법연구, 정보보호 시스템의 성능과 신뢰도에 관한 기준제정, 표준화 지원 등이 될 것이며, 전산망 보호를 위한 각 전산망의 보안시스템의 보안시설구축, 전산망 사고예방 및 사고발생시 대응조치 등의 기능도 담당할 것으로 전망된다.

V. 결 론

지금의 시대를 정보화시대라고 부르고 있으며, 이 정보화시대를 이끌어가고 있는 것이 컴퓨터이다. 컴퓨터범죄는 전문적, 지능적으로 이루어지기 때문에 범행의 포착이 어렵다. 따라서 그 대책이 치밀하지 않으면 소기의 성과를 거두기 어렵기 때문에 이를 막기 위해서는 다각적이고 종합적인 대책이 강구되어야 한다. 그러나 범죄란 항상 대책을 앞서가기 때문에 어떻게 보면 컴퓨터범죄대책은 성질상 궁극적인 것이 될 수 없다고 할 수 있다.

컴퓨터범죄의 발생동기는 어떤 범죄를 위한 목적도 있으며, 단순한 지적 호기심이나 장난일 수도 있다. 이와 같은 것이 사회전반의 위협에서부터 기업체의 영업비밀, 개인정보 유출로 인한 프라이버시의 침해에 이르기까지 포괄적이고 다양하다. 컴퓨터범죄의 태양과 법은 관련 컴퓨터 테크놀로지의 발달과 맞물려 계속 새로운 모습으로 나타나고 있다. 특히 악질적인 컴퓨터범죄자들은 전문적인 컴퓨터통신 지식으로 무장되어 있어 수시로 정보차단, 내용변경 등의 방법 등을 동원하여 수사기관의 추적으로부터 쉽게 달아나고 있다.

또한 우리 나라에서 전체 바이러스 가운데 3분의 2를 한국산이 차지하고 있고 외국산은 3분의 1에 그치고 있다고 하는 사실은 이에 대한 대처의 필요성이 절실하다 하겠다. 따라서 정부는 컴퓨터 및 네트워크를 이용한 컴퓨터 관련범죄에 대한 다각적이고 적극적인 대처방안을 마련해야 하지만 정부와 컴퓨터 전문가만이 행하여서 이루어지는 것이 아니고 컴퓨터 시스템을 운영하고 있는 운영자의 각성과 이를 관리하는 관리자의 역할, 그리고 이용자의 윤리 등이 중요한 부분들이라고 할 수 있다. 무엇보다도 보안의식의 확립이 필요하며, 보안기술을 통한 암호화로 정보의 유출이나 시스템에의 접근을 막아야 한다. 그리고 컴퓨터 범죄사태에 대한 실증적 조사요구가 선행되고 컴퓨터 및 컴퓨터 통신 전문가와의 협력적 연구가 필수 불가결하다고 본다.

끝으로 형법과 컴퓨터범죄관련특별법과의 체계적인 정비를 위한 노력이 요구된다.

參 考 文 獻

■ 국내문헌

- 박상기, 형법각론, 서울: 박영사, 1998.
- 신각철, 김문일, 최신컴퓨터 범죄론, 서울: 법영사, 1997.
- 이철, 컴퓨터 범죄와 소프트웨어 보호, 서울: 박영사, 1996.
- 최영호, 컴퓨터와 범죄현상, 서울: 컴퓨터 출판, 1995.
- 김문일, “정보화사회에 있어서의 컴퓨터 범죄와 그 방지대책에 관한 연구”, 중앙대학교 박사학위논문, 1998.
- 박범규, “개정형법의 컴퓨터 범죄에 관한 연구”, 연세대학교 석사학위논문, 1996.
- 장영민, 조영관, “컴퓨터 범죄에 관한 연구”, 한국형사정책연구원, 1993. 컴퓨터프로그램 보호법
- 최규태, “컴퓨터 범죄와 이에 대한 형법적 대응에 관한 연구”, 전남대학교 박사학위논문, 1994.
- 한봉조, “정보시스템범죄 대응체계 동향”, 한국전산원, 1996.

■ 외국문헌

- Hans Peter Bull und Zentaro Kitagawa(Hrsg), Computer im Dienst der Gesellschaft?, CarHeymanns Verlag KG, 1984.
- Ulrich Sieber, Computerkriminalitat und Strafrecht, 2. 1980. S. 39ff.
- Ulrich Sieber, a. a. O., S. 98 ; Thomas Fischer, Computerkriminalitat, Bern, 1979, S. 21f. : Theodor Lenckner, Computerkriminalitat und Vermögensdelikte, (Heidelberg · Karlsruhe ; C. F. Muller Juristischer Verlag. GmbH, 1981), S. 17.
- Frederick B. Cohen, A Short Course on Computer Viruses, 2nd Ed, John Willey and Sons Inc., 1994.
- Ph. D. Thesis, Vesselin Bonthodology of Computer Anti-Virus Research, University of Hamburg, 1994.

ABSTRACT

A Study on Computer Crime

by Lim, Moungh Soon

Computers have produced significant benefits to society.

Industrialized countries rely on their continuous availability and integrity,

Computers have introduced innovations into the business world, communications media, and scientific community.

In additions, as computers have developed, new categoris and methods of perpetrating crime have emerged that employ them.