공공 및 민간부문의 사이버침해사고 현황분석에 따른 대응방안

Countermeasure by Cyber Infringement Accident Present Condition Analysis of Public and Private Section

조호대, 신동일
순천향대학교 경찰행정학과

Ho-Dae Cho(jhd30@sch.ac.kr), Dong-Il Shin(adamatos@hanmail.net)

요약

우리가 살아가는데 있어서 인터넷이란 일상생활에서 없어서는 안 될 중요한 인프라가 되었다. 그러나 이러한 사이버 공간이 확장되고 일상화 되면서 여러 가지 역기능을 동시에 가져다주었다. 이러한 역기능을 최소화하기 위해서는 사이버공간에 적용될 새로운 질서가 정립되어야 한다. 사이버침해는 정보사회가 초래한 가장 심각한 문제 가운데 하나이다. 사이버 상에서는 상대방이 보이지 않으므로 그에 대한 죄의식이 희박하고 불안함도 적으며, 사이버 범죄의 처벌에 대한 무지도 생각할 수 있다.

본 연구에서는 공공부문과 민간부문에 대한 사이버침해정도를 알아보고, 공공부문과 민간부문의 사이버침해현황을 분석하고 이를 바탕으로 사이버침해사고에 대한 대응방안을 제시하고자 한다.

■ 중심어 : | 사이버침해사고 | 사이버공간 | 사이버범죄예방 | 인터넷 |

Abstract

We live was operates the life which is the Internet and became infra is very important. In order minimizes like this disfunction from will be applied the new order must take a position in cyber space. The cyber infringement most the information society brings about is serious concern middle one. The biggest thing is anonymous characteristic with cause of cyber crime. Also well cannot know becomes the cause where commits a crime that about cyber crime. Cyber crime the guilty conscience is thin. And the criminal who commits a cyber crime sense of insecurity is few.

This paper which sees cyber infringement accident dividing came in public section, and analyzed presented a present condition and a confrontation plan.

■ keyword : | Cyber Infringement Accident | Cyber Space | Cyber Crime Prevention | Internet |

Ⅰ. 서 론

인터넷 사용인구가 증가하면서 이제 사이버공간은 우리 생활에서 중요한 인프라가 되었다. 사이버공간이 우리에게 있어서 중요한 생활공간으로 등장한 것이다. 더욱이 21세기를 맞이하여 새로운 패러다임의 변화를 요구하는 정보화시대의 도래와 아울러 정보인프라가 전 세계적인 국가산업의 원동력 내지 지상목표로 인식

접수번호 : #081201-008
접수일자 : 2008년 12월 01일
심사완료일 : 2008년 12월 12일
교신저자 : 조호대, e-mail : jhd30@sch.ac.kr

될 정도로 그 중요성이 점차 증대되고 있으며, 정보통신산업이 세계경제의 핵심 산업의 역할을 다할 것이라는 기대와 인식이 높은 때이다.

하지만 이러한 정보통신망의 파급으로 인한 협조의 용이함과 편리함이라는 순기능 못지않게 지식과 정보에 대한 역기능 측면에서 불법적인 침해행위가 다양하게 발생하고 있고, 사이버공간이 우리 생활에서 차지하는 비중이 높아지면 높아질수록 사이버공간에서의 안전한 생활보장과 새로운 질서정립에 대한 욕구도 늘어나고 있다. 따라서 하루 빨리 인터넷을 중심으로 급속히 형성되고 있는 사이버공간에 적용될 새로운 질서가 정립되어야 할 것이고, 이러한 질서의 기초가 될 사이버 법제의 정비, 대응기구의 설치 및 운용이 필요할 때라고 생각한다.

본 연구에서는 사이버침해사고를 사이버 세상에서 일어날 수 있는 모든 침해이며, 사이버범죄로 규정되고 있는 범죄와 범죄로 규정되어 있지 않은 행위까지 포함하여 정의 한다. 여기에서는 사이버침해 유형과 사이버침해 현황을 공공부문과 민간부문으로 구분하여 살펴보고 이러한 사이버침해에 대한 대응방안에 관하여 연구하고자 한다.

II. 이론적 배경

1. 사이버침해사고의 의의

사이버 침해사고는 사이버상에서 범죄로 규정되고 있는 행위뿐만이 아니라, 법적으로 규제하고 있지 않은 행위들 중 침해하는 모든 행위를 포함한다. 사이버범죄는 수많은 유형의 범죄가 컴퓨터시스템을 이용하거나 그와 관련하여 발생하고 있기 때문에 단적으로 정의하기가 매우 곤란하다[1]. 만약에 사이버공간이 범죄의 발생 공간이나 매개가 되는 것이 아니라 물품구매의 과정에 불과하다면 이것은 사이버범죄라고 할 수 없다[2]. 즉 사이버범죄란 사이버공간에서 발생하는 모든 범죄적인 현상이라고 말할 수 있다.

2. 사이버침해사고의 특징

2.1 비대면성과 익명성

사이버 범죄는 발생하는 장소가 사이버공간이라는 가상공간에서 이루어지므로 피해자는 가해자가 누구인지 정확히 알 수 없는 익명성과 비대면성이 생긴다. 현실세계의 범죄가 서로간의 대면을 통해서 이루어지는 반면에 사이버범죄는 당사자 간의 대면 없이도 발생하기 때문에 범죄자들은 보다 과격하고 대담하게 행동하게 되며, 범죄를 반복적으로 행할 가능성이 많다[3]. 사이버공간에서 자신의 신분을 숨기고 익명성이 보장되면 일반 범죄를 생각하고 있는 자들은 그 범죄의 유혹에 쉽게 빠질 수 있다.

2.2 전문적인 기술성과 국제적인 광역성

사이버범죄는 사이버공간에서 정보의 형태로 신속하게 이루어지므로 빠른 전파성과 천문학적인 재산피해를 가져올 수 있다. 최근에는 간단한 바이러스를 유포하기도 하지만 상당한 전문성을 갖춘 사람이 행할 수 있다.

또한 인터넷은 전 세계를 하나로 연결하고 있기 때문에 오늘날에는 국가 간의 경계와 지리적인 개념이 사라지고 있다. 인터넷시대의 국제범죄는 그 심각성에 비하여 대비책을 강구하기가 더욱 어렵게 되어있고, 인터넷의 확산으로 인하여 사이버범죄의 국제화가 급증하고 있다[4].

2.3 잠재성과 전파성

사이버범죄는 현실공간에서 벌어지는 범죄와 달리 피해자나 수사기관이 인지하기가 상당히 곤란하고 그것의 원인을 규명하기가 쉽지 않아 증거가 인멸될 가능성이 높은 범죄이다[5]. 사이버 공간에서 벌어지는 범죄에서는 현실공간에서 일어나는 범죄보다 평균적으로 높은 암수범죄(hidden crime)가 발생하고 있다[6].

컴퓨터가 네트워크화 되면서 시간과 공간의 제한을 거의 받지 않는 상황에서 모든 정보는 사람들 사이에서 매우 빠르게 전파된다. 사이버범죄는 빠른 시간 내

에 전 세계로 전파될 수 있으며, 그에 따라 사이버범죄도 매우 광범위하게 발생할 수가 있다.

2.4 동시성과 시간적 · 공간적 무제한성

인터넷상에서는 의사소통을 매우 빠르게 실시간으로 할 수 있다. 이러한 동시성으로 인하여 사이버상에서는 기존의 공간과 시간에 대한 제약을 받지 않게 되었다. 사이버공간에서의 인터넷은 개인이 컴퓨터를 클릭하는 즉시 그 사람의 의사를 전달하거나 표현할 수가 있다. 사이버범죄는 현실과 달리 인터넷이 연결된 컴퓨터가 있는 곳이라면 어디에서든지 범할 수 있으므로 범죄 장소나 시간이 제한이 없다.

3. 사이버침해사고의 유형 및 사례

3.1 개인정보 유출

개인정보란 개인의 정신, 신체, 사회적 지위, 신분 등에 관한 사실판단·평가를 나타내는 개인에 관한 정보이고 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 개인을 식별할 수 있는 정보를 말한다. 인터넷상에서 사업을 하고 있는 각 회사들은 자신의 회원수를 늘리기 위해 경쟁적으로 경품을 제공하고 있다. 일반인이 이러한 인터넷사이트에 가입을 하기 위해서는 개인의 신상정보를 기입해야 하는 과정으로 되어 있기 때문에, 이러한 사이트에서는 해당 사이트에 가입한 사람들의 개인정보를 메인 서버에 소유하게 된다. 그러나 이러한 메인서버의 보안체계가 완벽하지 못한 경우가 대부분이기 때문에 일반인의 개인정보가 유출되고, 일부 악의적인 사이트에서는 그들이 소유하고 있는 개인정보를 돈을 받고 넘기는 경우까지 발생하고 있다[7].

3.2 사이버 음란물

사이버공간을 통하여 유통되는 음란물과 국경을 초월하여 접속되는 음란사이트의 폐해로 인해 사이버공간은 신종윤락의 온산지로 변질되어가고 있다. 음란물 인터넷의 사이트의 주소를 알면 자신의 신분을 공개하지 않고도 쉽게 접근하여 이를 시청할 수 있다. 이는 날이 갈수록 인터넷이 신종윤락의 온상으로 변질되도록 하고 있으며, 청소년들이 범죄에 빠져드는데 있어서의 기회를 제공하고 있는 셈이다. 사이버음란물 유통과 관련된 사이버범죄도 국경을 넘어서 발생하고 있으며 그 범죄율도 증가하고 있다[7].

3.3 사이버 명예훼손

개인의 사생활에 관한 인터넷범죄 가운데 가장 자주 논의가 되는 범죄는 명예훼손에 관한 죄이다. 우리나라는 명예훼손의 경우 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에서 처벌하고 있지만 모욕의 경우 처벌조항이 없어 법 개정이 요구된다. 최근 인터넷 사이트를 통하여 허위사실을 유포하거나 명예훼손이 이루어지는 경우가 많다. 사이버공간의 비대면성과 익명성 때문에 사이버상에서는 타인에 대한 비방이나 언어폭력이 현실보다 심각하게 발생하고 있다.

3.4 저작권 침해

인터넷환경이 점점 발전하면서 저작권에 대한 침해행위도 증가하고 있다. 컴퓨터 소프트웨어는 서적과는 달리 복사와 배포가 쉽기 때문에, 이것은 프로그램 개발자들이 투자한 시간과 비용을 순식간에 절도해가는 행위라고 볼 수 있다. 개인 홈페이지 사용자들이 증가하면서 다른 사람의 홈페이지나 다른 사이트에 게시된 자료를 복사하여 마치 자신의 자료인 것처럼 사용하는 행위가 증가하고 있다.

3.5 사이버 사기

사이버 사기행위는 지능범들이 행하는 범죄인 화이트칼라의 한 범죄로 분류한다. 사이버사기는 전자상거래와 관련하여 사이버 공간에서 이루어지는 사기행위의 한 유형을 말한다. 사이버상에서 사기는 고학력이나 많은 지식을 요구하기 보다는 컴퓨터와 관련된 전문지식만 가지고 있으면 누구나 가능하다. 통신을 이용한 사기는 인터넷을 범행 장소로 이용하여 물품을 판매하겠다고 한 후 돈을 송금 받고 물품을 보내주지 않는 경우가 대표적이다. 전자상거래는 기존의 가게를

이용하지 않고도 소비자와 생산자간에 거래가 이루어질 수 있다는 점으로 인하여 급진적으로 증가하고 있다.

3.6 사이버 절도

사이버공간에서의 게임이 급속한 인기를 보이면서 최근 인터넷게임 사업은 나날이 발전하고 있다. 인터넷게임에서는 사람들이 자신의 아이템을 획득하여 보유할 수 있으며, 게임 마니아들은 이러한 아이템을 사이버공간에서의 매매를 통하여 거래하고 있다.

인터넷게임에서 획득한 아이템에 대하여 재산적 가치의 인정여부와 관련하여 게임에서 타인의 아이템을 부당한 방법으로 자신의 소유로 변경하거나 훔쳐오는 사이버 절도의 사례가 증가하고 있다.

3.7 사이버 도박

사이버도박이란 사이버공간에서 일정한 재물을 걸고 우연성에 기초하여 블랙잭·포커와 같은 카드 게임이나 슬롯머신·룰렛 등 각종 도박을 즐길 수 있도록 고안된 프로그램을 이용한 도박행위를 말한다[8]. 부산경찰청에 의하면 사이버범죄 중에서는 사이버 도박이 505명으로 가장 많았고 인터넷 사기가 321명, 개인정보 유출 212명, 해킹사범 11명, 스팸 발송 36명 등의 순이라고 한다. 이처럼 경찰청의 자료를 보아도 사이버 도박의 심각성을 알 수 있다.

3.8 해킹

해킹은 컴퓨터 시스템의 취약점을 이용하여 타인의 사이버 공간에 불법적으로 접근한 후 자료의 유출, 위·변조 및 삭제, 시스템 장애 및 마비를 유발시키는 장애행위를 말한다[9]. 법률적인 의미에서 해킹이란 시스템의 관리자가 구축해놓은 보안망을 어떤 목적에서든지 무력화시켰을 경우 이에 따른 모든 행동을 말한다. 하지만 네티즌 간에는 보통 시스템 관리자의 권한을 불법적으로 획득한 경우, 또는 이를 악용해 다른 사용자에게 피해를 준 경우를 해킹이라고 정의한다[10].

3.9 바이러스 유포

컴퓨터 바이러스는 자기복제를 하여 전파되면서 시스템에 잘못된 동작을 일으키거나 하드디스크에 저장된 귀중한 자료를 지워버리는 등의 파일을 손상시키는 프로그램을 말한다. 이러한 부작용으로 인해 재산상으로 또는 정신적으로 막대한 피해를 초래한다[11].

Ⅲ. 사이버침해사고의 현황

연도별 사이버 범죄 발생 건수를 보면 지난 2006년 82,000건에서 2007년 88,000건, 올 상반기에는 57,000건 등 매년 증가하고 있어 정부 차원의 강력한 대책 마련이 요구된다.

1. 공공부문 사이버침해 현황

2007년에 국가사이버안전센터에서 접수•처리한 침해사고를 분석한 결과 전체 공공기관에서 발생하는 사이버침해사고 건수는 총 7,588건으로 전년도의 4,286건에 비해 크게 증가한 것으로 나타났다. 특히 자치단체와 교육기관을 목표로 한 사이버 침해사고 발생 건수가 급증하여 지방자치단체에서 발생한 사이버침해사고 건수는 총 3,827건으로 전년 1,470건에 비해 3배 가까이 늘었고, 교육기관도 1,464건에서 2,148건으로 2배 증가하였다[12].

표 1. 공공부문 사이버침해사고 발생 현황[17]

기 관	웜·바이러스 감염	경유지악용	홈페이지변조	자료훼손 및 유출	기타	합 계
국가기관	498	29	21	55	22	625
지자체	3,583	94	111	24	15	3,827
연구소	145	20	8	19	6	198
교육기관	1,504	513	91	18	22	2,148
산하기관	448	85	143	26	4	706
기 타	16	26	5	34	3	84
합 계	6,194	767	379	176	72	7,588

1.1 월별 사이버침해사고

침해사고는 꾸준히 감소세를 보이고 있는데, 이는 주로 악성코드 감염과 홈페이지 변조사고가 감소한 데 기인한다. 일 년 평균으로 볼 때 매월 632건이 발생한 것으로 나타났다.

1.2 악성코드 감염사고

악성코드 감염사고는 전체적으로 감소세를 보였는데, 이는 지방자치단체에서의 악성코드 감염사고 감소(18.1%)에 기인한다. 일 년 평균으로 보면 매월 516건이 발생한 것으로 나타났다.

또한 악성코드 감염사고의 기관별 발생비율을 살펴보면, 지방자치단체가 전체 악성코드 감염사고의 54.8%를 차지하였다. 이는 2006년 지방자치단체의 악성코드 비율인 62.2%보다 감소된 수치로 해당 기관에 대한 지속적인 악성코드 감염예방 조치에 기인한 것으로 보인다[12].

표 2. 악성코드 감염기관 분포[17]

기 관	지방자치 단체	교육기관	산하기관	국가기관	연구기관	기타
발생비율	54.8 %	30.5 %	6.0 %	5.2 %	3.3 %	0.2 %

1.3 홈페이지 변조사고

홈페이지 변조사고는 다른 유형의 사고들과 달리 해커들이 자신의 실력을 과시하기 위해 변조한 내용을 인터넷에 공개하고 있는데, 2007년 6월 이후 공공기관의 사고가 증가추세에 있었으나, 10월부터 산하기관 등에서 집중적으로 홈페이지 취약점을 제거하여 12월에 다시 연간 평균 31.6회 이하로 감소하였다[12].

2. 민간부문 사이버침해 현황

2007년 한국정보보호진흥원에서 접수•처리한 민간부문 침해사고 통계를 분석한 결과 해킹사고 접수•처리는 21,732건으로 2006년(26,808건) 대비 18.9% 감소하였으며, 웜•바이러스피해신고는 총 5,996건으로 2006년(7,789건)대비 23.0% 감소하였다.

2.1 해킹사고 현황

2.1.1 해킹사고 전체 추이

침해사고 유형별로는 스팸릴레이, 피싱 경유지, 기타 해킹, 홈페이지 변조는 2006년 대비 각각 17.0%, 13.5%, 48.4%, 28.5% 감소하였으며, 단순침입시도는 2006년 대비 16.3% 증가 하였다.

표 3. 민간부문 해킹사고 발생현황[17]

구 분	2006년 총계	2007년 총계
스팸 릴레이	14,055	11,668
피싱 경유지	1,266	1,095
단순 침입시도	3,711	4316
기타해킹	4,570	2,360
홈페이지변조	3,206	2,293
합계	26,808	21,732

2.1.2 운영체제별 현황

2007년에 발생한 해킹사고를 피해 운영체제별로 분류한 결과, [표 7]과 같이 윈도우 운영체제가 전체의 88%로 가장 많았으며, 리눅스 운영체제는 전체의 10%로 2006년 대비 3%감소한 것으로 나타났다.[12].

표 4. 해킹사고 운영체제별 발생현황[16]

운영체제	윈도우	리눅스	기타
발생비율	88%	10%	2%

2.1.3 기관별(대상별) 현황

피해 기관별로 분류한 결과 [표 5]와 같이 기타(개인)가 차지하는 비율이 79%로 가장 많았으며, 다음으로 기업 14%, 대학 5% 순으로 나타났다.

표 5. 해킹피해 기관별 분류[17]

기 관	기타 (개인)	기업	대학	네트워크
발생비율	79 %	14 %	5 %	1 %

2.2 웜・바이러스 현황

2007년 한 해 동안 웜・바이러스 신고건수는 5,996건으로 월 평균 499.7건에 해당하며, 2006년(7,789건) 대비 23% 감소한 수치다. 주요 감소 이유로는 이메일 바이러스로 인한 피해신고가 크게 감소하였기 때문이다. 반면 웹 사이트를 통하여 감염되는 악성코드 의한 피해신고가 증가하였으나 자체 전파력이 없어 전체 건수는 전년도에 비하여 감소한 것으로 파악되었다[12].

Ⅳ. 사이버침해사고에 대한 대응방안

1. 정책적 대응

1.1 법체제의 정비와 보완

사이버 공간이 생활공간으로 자리를 잡아가면서 이제는 법과 규범이 사이버공간에도 필요하게 되었다. 이에 대응하여 사이버공간상의 법규위반자에 대한 경찰의 수사여건보장과 법집행의 효율성을 향상시키는 방향으로 법과 제도가 정비되어야 할 것이다. 사이버공간에서의 사이버범죄에 대해 현행법은 부분적인 직접적 규정을 하고 있을 뿐이고 그것도 여러 곳에 산재되어 있다. 현재 부분적인 범죄에 대해서만 법적용이 가능하며, 또한 산재성으로 인하여 예방적인 효과도 떨어진다. 그러므로 이제는 사이버공간의 특수성에 걸맞게 사이버범죄에 대한 특별한 법체제의 정비와 보안이 필요하다.

물론 현재 사이버범죄를 규제하고 있는 법들이 있지만 근본적으로 사이버범죄에 적용할 법률의 제정이 필요하다[13].

1.2 사이버전담 수사경찰의 인력충원

현재의 사이버 수사 인원으로 급증하는 사이버범죄에 대응한다는 것은 역부족으로 보인다. 수사기관에게 사이버화를 요구하면서 범인검거를 위한 사이버수사요원을 보강해야 한다. 경찰청에서는 컴퓨터관련 전문가들을 경찰관으로 특별 채용하여 사이버범죄에 대응하고 있으나 그것으로 급증하는 사이버범죄에 대응한다는 것은 부족하다. 장기적으로는 정보보호 전문가 양성 및 현직 수사관 전문 인력의 훈련을 위하여 대학이나 지정된 센터에서 정보보호를 위한 전문교육을 시행토록 하여 단계적으로 양성할 수 있도록 지원하여야 하며, 정보보호 교육프로그램을 개발하는 것도 필요하다[14]. 우선 경찰공무원 신임순경 가운데 컴퓨터 관련 학과 전공자를 선발하여 사이버범죄 수사요원으로 양성하는 방안이 있을 수 있다. 특히 여자 경찰관들을 사이버범죄 수사요원으로 선발하여 전문가로 육성하는 방안이 바람직할 수 있다. 그러나 이러한 전문능력을 사이버수사능력으로 발전시키지 못한다면 오히려 고급인력이 낭비되는 결과를 초래하므로 신중히 대응책을 마련해야 할 것이다.

1.3 경찰의 외부 전문 인력 활용

현재의 경찰인력은 일선 현장범죄에 초점이 맞추어져 있다. 그러나 현재 일어나고 있는 사이버범죄의 유형을 살펴보면 현장에서 일어나는 범죄유형이 사이버공간에서도 많이 일어나고 있다[15]. 현실적으로 사이버범죄를 수사하기 위해서는 컴퓨터와 관련된 전문적인 지식과 기술이 요구된다. 이러한 전문적인 인력을 수사기관 내부에서만 선발하여 교육시킨다면 많은 시간과 비용이 수반되므로 외부로부터 전문 인력을 활용하는 대응책을 마련해야 할 것이다. 전문적인 인력을 활용하기 위해서는 일반적인 특별채용 방식만을 통하여 전문 인력을 확보할 것이 아니라, 관련된 전문회사나 기업체로부터 그 특정분야에 관련된 전문 인력을 활용할 필요성도 있다.

1.4 국제공조수사의 활성화

사이버범죄는 범행의 효과가 국제적으로 영향을 미치는 경우가 많고 새로운 범죄수법이 만들어지면 국경을 초월하여 광범위하게 전파 되므로 이에 대한 공동연구와 수사기관에 대한 훈련을 위한 공동대처는 물론 수사공조와 범죄인의 인도 등에 대한 국제협약의 체결이 요구된다. 특히 인터넷 사용의 편리성이 증가하면서 국외로부터 침입되는 사례도 증가하고 있다. 사이

버범죄에 대한 주권과 관할권의 문제, 다른 나라에 존재하는 증거물에 대한 압수·수색 문제, 수사기법에 관한 기술적 협력, 네트워크상의 상시연락체제유지, 사이버범죄관련 자료의 공유 등에 관한 국제공조가 원활하게 이루어져야 국제화되어가고 있는 사이버범죄에 효율적으로 대응할 수 있을 것이다. 국제 공조체제의 원활한 운영을 위해서는 우선 수사공조보다는 정보공조를 강화하는 게 중요하다. 일반적으로 국가 간 수사공조는 사람이나 증거물 같은 것을 다른 국가로 보내야 하는데 이것은 절차가 번거롭고, 제한이 따를 수밖에 없다. 그러나 정보공조는 사람이나 증거물을 넘겨주는 문제가 생기지 않기 때문에 상대적으로 절차가 간편하다. 정보공조가 활성화되면 수사공조의 수요가 감소하는 효과도 기대할 수 있으므로 국제성이 강한 사이버범죄를 효과적으로 규제하려면 경찰의 정보공조수사를 활성화해 나가야 할 것이다.

2. 기술적 대응

2.1 사이버범죄에 대한 전문적인 기술의 개발

사이버범죄는 전문적인 기술을 통하여 이루어지는 범죄이므로 각 범죄양상에 대한 연구와 그에 대한 보안적인 대책이 필요하다. 사이버범죄는 전문성을 요하는 범죄이므로 이를 예방하기 위해서는 범죄의 전문성에 대응하는 경찰의 전문적 기술의 개발이 요구된다. 또한 과학이 점점 발전하면서 사이버공간에서는 그에 따르는 신종범죄가 발생하고 있으며, 이에 경찰수사기관은 이러한 신종범죄를 예견하고 예방할 수 있는 보안기술을 지속적으로 개발해야 한다.

2.2 방화벽 시스템 도입

방화벽이란 기업이나 조직의 모든 정보가 컴퓨터에 저장되면서, 컴퓨터의 정보 보안을 위해 외부에서 내부, 내부에서 외부의 정보통신망에 불법으로 접근하는 것을 차단하는 시스템이다[1]. 기업이나 조직에서 이러한 방화벽을 설치하고 이를 담당할 전문 인력을 보강하여 신경을 쓴다면 사이버범죄에 대하여 효과적인 대책을 강구할 수 있을 것이다. 또한 각 공공기관에서도 방화벽 시스템을 도입하여 이를 의무화해야 할 것이다.

3. 환경적 대응

3.1 예방활동

사이버범죄는 그 기술적인 특성으로 인해 예방활동이 매우 중요하다. 범죄를 예방하는데 있어서 범죄의 기회를 제거하는 것은 중요한 부분이다. 사이버범죄의 기회를 줄이기 위해서는 우선 국민들의 방범의식을 환기시키는 것이 필요하다. 사이버범죄는 발생하는 순간 이미 회복하기 피해를 발생시키기 때문에 이에 대하여 범죄가 발생하기 전에 예방활동을 하는 것은 매우 중요하다. 이러한 위험성에 대하여 사전에 인식하고 발견하는 것은 어려운 일이므로 예방활동이 가장 경제적이고 효율적인 대응책이라 할 수 있다.

3.2 주기적인 보안교육 및 홍보활동 강화

최근에는 해킹이 개별 PC를 대상으로 이루어지고 있음에도 불구하고 여전히 내부망 PC에 대한 보안대책은 부실한 실정이다. 일반적으로 기관의 정보보호 담당자는 극소수인데다 있다 하더라도 정보통신 시스템의 운영요원이 중복하여 보안을 담당하고 있어 기관 내 모든 PC에 대한 보안관리를 완벽하게 수행하기는 사실상 불가능하다. 따라서 개별 PC에 대한 보안관리는 각 사용자가 직접 수행할 수 있도록 주기적인 보안교육을 실시하여야 한다.

또한 사이버공간을 위한 효율적인 정책이 지속적으로 효과를 나타내기 위해서는 국민들을 대상으로 홍보활동이 이루어져야 한다. 사이버공간에서의 지켜야할 규범에 대하여 홍보를 한다는 것은 그 자체로 중요성을 가지고 있을 뿐 아니라, 범죄예방적인 측면에서도 필요하다.[16].

V. 결 론

사이버공간은 앞으로도 계속해서 발전해 나갈 것이

다. 이러한 발전이 우리에게 정말 무엇을 의미할지는 아무도 모르는 일이다. 확실한 것은 우리 생활의 중요한 부분이 사이버공간으로 옮겨가고 있고, 이제는 사이버공간을 무시하고는 정상적인 생활을 하기가 어려운 지경이 되어 버렸다. 이러한 상황에 도달한 우리는 사이버공간에서의 생활이 보다 안전하고 편안한 생활이 되도록 노력해야 할 책무가 있다. 사이버공간의 안전을 위한 이러한 노력은 특정계층의 사람들만이 하는 것이 아니다. 사이버공간에 참여하고 있는 모든 사람들의 노력이 있어야 이러한 사이버공동체의 생활을 보다 안전하고 편안하게 유지할 수 있을 것이다. 사이버범죄는 해가 갈수록 새롭고 다양한 유형으로 나타나 우리에게 큰 피해를 입히곤 한다. 반면 사이버범죄와 관련된 대응법규는 이에 따라서 제대로 대응하지 못하고 있어 실질적인 단속을 어렵게 만들고 있다. 따라서 사이버범죄를 예방하고 보다 건전한 사이버문화를 조성하기 위해서는 실질적이고 효율적인 대응정책의 개발이 요구된다.

참 고 문 헌

[1] http://100.naver.com/

[2] 조철옥, *경찰학개론*, 대영문화사, p.504, 2008.

[3] 김상균, "사이버범죄에 대한 경찰의 수사력강화 방안", 법학연구, 한국법학회, p.403, 2001.

[4] 조병인, "인터넷시대의 국제범죄와 대응전략", 01년도 전반기 학술회의자료, 한국공안행정학회, p.6, 2001.

[5] 허만영, "사이버스페이스의 범죄현황과 경찰의 대응방안", 치안연구소 연구보고서, pp.50-51, 2000.

[6] 김상균, "사이버범죄에 대한 경찰의 수사력강화 방안", 법학연구, 한국법학회, p.405, 2001.

[7] http://www.netan.go.kr/

[8] 김연수, "사이버범죄 총람", 법률미디어, p.754, 2002.

[9] 조철옥, *경찰학개론*, 대영문화사, p.508, 2008.

[10] 김연수, "사이버범죄 총람", 법률미디어, p.220, 2002.

[11] 조철옥, *경찰학개론*, 대영문화사, p.509, 2008.

[12] *국가정보보호백서*, 국가정보원, 정보통신부, 2008.

[13] 김종세, "사이버범죄의 법적 쟁점에 관한 고찰", 한국경찰이론과실무학회, 경찰연구논집 제2호, 2008.

[14] 김상균, "사이버범죄에 대한 경찰의 수사력강화 방안", 법학연구, 한국법학회, 2001.

[15] 이황우, *경찰행정학*, 법문사, 2007.

[16] http://www.kisa.or.kr/

[17] http://www.ncsc.go.kr/

저 자 소 개

조 호 대(Ho-Dae Cho) 정회원

- 1999년 : 동국대학교 경찰행정학(석사)
- 2003년 : 동국대학교 경찰행정학(박사)
- 2000년 ~ 2003년 : 대불대학교 경찰행정학과 교수
- 2003년 ~ 현재 : 순천향대학교 경찰행정학과 교수

<관심분야> : 경찰의 재난관리, 경찰인사, 경찰조직

신 동 일(Dong-Il Shin) 준회원

- 2001년 ~ 2008년 : 순천향대학교 경찰행정학(학사)
- 2008년 ~ 2009년 : 순천향대학교 경찰행정학(석사과정)
- 2008년 ~ 2009년 : 순천향대 경찰행정학과 조교

<관심분야> : 경찰학