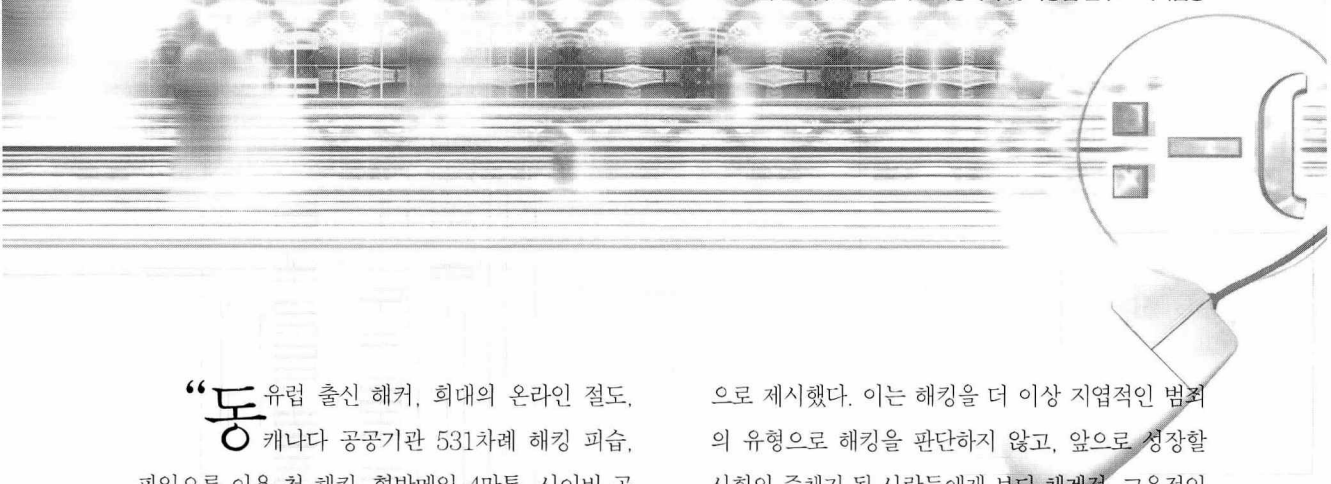
해킹@사이버월드, 새로운 법 감정(Legal Mind) 형성이 관건!

이태현/벤처법률지원센터 전자상거래 및 가상법 연구소 기획팀장



"동유럽 출신 해커, 희대의 온라인 절도, 캐나다 공공기관 531차례 해킹 피습, 파일오류 이용 첫 해킹, 협박메일 4만통, 사이버 공갈범 검거, FBI사이트 해킹으로 3시간 패쇄..." 사이버 공격에 관한 뉴스로 세계가 뜨겁다.

디지털 경제, 사이버 커뮤니티, 혁신적인 생활의 변화는 사이버월드(Cyber-world)를 창조하고 있다. 물리적 공간에 구애받지 않는 '생활'이 가능하다는 것은 무한한 기회를 제공하고 있음이 분명하다.

그러나, 세계적인 사이트에 대한 연속되는 해킹 공격은 어쩌면 인터넷 세계도 기존 사회와 같이 범죄로부터는 자유롭지 못함을 증명하며 건설중인 새로운 사회에는 새로운 규율체계와 가치관이 절실함을 일깨우고 있다. 이러한 시대적 환경에서 해킹에 대응할 효과적 대응책을 마련하기 위한 계획이 실행단계에 있다.

해킹에 대응한 국제적 공조체계 수립과 각종 법률의 보다 적극적인 집행을 골자로 정책 방향을 잡아가고 있으나, 최근 미국에서는 컴퓨터, 인터넷 시대에 적합한 '컴퓨터 윤리교육' 프로그램에 깊은 관심과 계획을 발표, 해킹에 대한 윤리의식 배양을 한 방법으로 제시했다. 이는 해킹을 더 이상 지엽적인 범죄의 유형으로 해킹을 판단하지 않고, 앞으로 성장할 사회의 주체가 될 사람들에게 보다 체계적, 교육적인 내용을 공급하여 안전한 사이버월드를 구축하기 위한 것으로 보인다.

디지털 시대에는 도덕이니, 윤리니 하는 말을 본능적으로 거부하는 사람들도 있겠지만 디지털 시대일수록 사이버월드를 건설하는 원동력은 인간의 의지, 창조력에 의존하는 만큼, 철학적 기반은 매우 중요한 문제가 아닐 수 없다.

이런 의미에서 해킹에 대한 실질적 해결책은 디지털 시대에 적합한 법 감정을 수립하는 문제에 달려 있다고 하겠다.

해킹 현황

해킹침해사고대응협의회(www.certcc.or.kr)의 통계를 보면, 2000년 2월 한달 동안 해킹사건이 115건이 접수, 90건을 종결하였다. 기업이 피해기관의 53%, 대학이 23%를 구성하고 있어 기업이 피해가 가장 큰 것으로 나타났다.

해킹수법 또한 복잡하게 진행되고 있으며, 백오리

피스, 트로이목마 등의 악성 프로그램이 유통되면서 전문적 기술(?)을 가진 일부 컴퓨터 마니아들의 해킹이 아닌 경우가 많아 졌다. 이러한 악성 프로그램은 컴퓨터 바이러스, 변종들을 수반하기 때문에 심각성은 높아지고 있다. 불법행위의 내용으로는 침입시도가 77건에 이르고, 불법침입이 52건이어서 네트워크 자원에 대한 침입이 가장 큰 비중을 차지했다.

얼마 전 미국의 야후, 이트레이드, 이베이 등을 공격했던 방식이라 보이는 '서비스 거부' 공격도 7건 정도 있었다.

해킹 관련 통계를 보면, 1998년에는 158건의 해킹사건이, 1999년에는 572건의 해킹사건이 보고되었는데 이는 인터넷 사용의 폭발적 증가와 상관관계를 갖는 것으로 판단된다. 그리고, 해킹의 경로를 보면 총 115건의 사고 중에 64건이 경로가 밝혀지지 않았다는 점에서 해킹에 대한 기술적 대응이 과연 가능한가 의문을 가진다. 해킹의 대상이 되는 컴퓨터도 중대형 컴퓨터 혹은 네트워크 시스템에서 개인용 컴퓨터 등으로 확산되고 있다.

또한 인터넷 PC방이 해킹의 경로로 사용되는 사례가 점점 많아지면서 청소년층의 개입이 늘고 있다.

해킹 처벌, 강한 윤리의식을 심어야 한다

해킹사례에 대한 형사처벌의 역사는 얼마 되지 않는다. 그러나 해킹의 유형은 하루가 다르게 다양하고 복잡한 양상을 띄고 있다. 주로, 인터넷을 통한 시스템 침입으로 불법적 계좌이체, 업무 방해 등의 단조로운 공격에 머물었던 초기 해킹은 개인 컴퓨터의 공격으로 프라이버시 침해, 시스템의 오작동, 정보의 위조 등 복잡한 불법 관리업무를 하는 형태로 변화하고 있다.

그럼에도 불구하고, 해커 처벌은 전통적인 처벌기준에 별다른 변화를 갖고 있지 않다. 예를 들어, 해커들은 경찰관들이 연행할 순간에야 죄의식을 가지게 되는 경우가 대부분이며 해커들의 처벌은 대부분 벌금형을 받으며 청소년이 범인인 경우가 많아 높은 재범률에도 불구하고, 효과적인 개선 프로그램 없이 표면적인 처벌만 반복되는 실정이다.

이와 같이 해커들이 죄의식을 느끼지 못하는 것은 윤리적으로 매우 큰 결함을 갖고 있음을 의미한다. 해커들에게 해킹에 대한 법 감정을 교육하기 위하여 해커의 처벌은 보다 획기적인 윤리교육이 수반되어야 한다. 단기적으로는 법의식의 개선을 위한 집중적인 프로그램과 함께 정책적 변화를 도모하여야 할 것으로 보인다.

예를 들어, 해킹은 단순히 키보딩으로 인한 기술과 지적 호기심의 잘못된 행위에 불과한 것이 아닌 심각한 불법행위이며 타인의 네트워크를 침해, 막대한 사회적, 재산상의 피해를 동반하는 죄임을 각인시키는 프로그램이 필요하다고 하겠다.

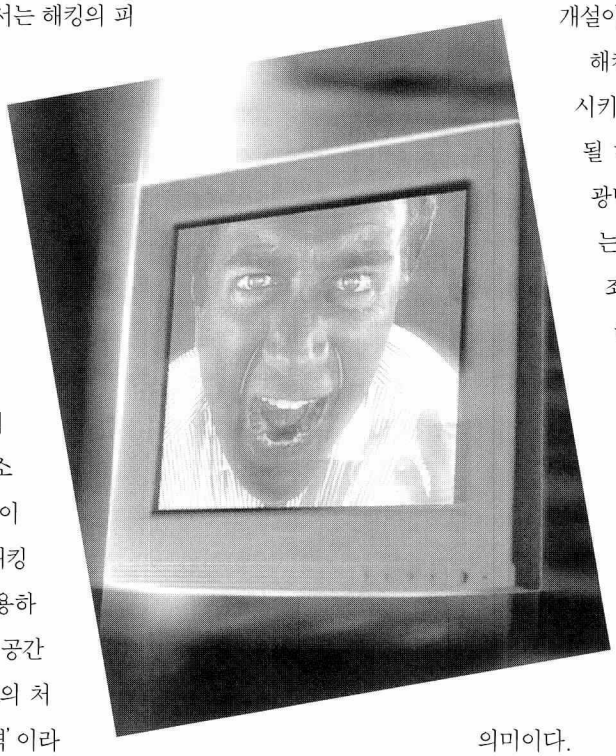
해킹 관련 법규

미국의 경우는 The Computer Fraud and Abuse Act를 통하여 부정한 컴퓨터 사용과 네트워크자원에 침입, 부당한 사용을 통일적으로 규율하는 법규를 가지고 있다. 이는 각 주법에 우선하여 적용되는 법률로써 관할분쟁의 경우도 규정하고 있다.

이와 함께, 컴퓨터 이용과 가장 많은 수의 인터넷 사용자를 보호하기 위하여 해킹사고에 대한 종합적 대책을 세우고 진행함에 최근 눈길을 끄는 것은 '사이버경찰의 창설'이다. 주요 내용은 해킹기술을 가진 컴퓨터 전사를 공식화하여 정보사회의 안전성 확보에 적극적인 활동을 펴나가기 위한 정책으로 판단된다. 그리고, 일본에서는 "부정 억세스 행위의 금지 등에 관한 법률"이 올해 2월 13일부로 시행에 들어갔다. 위 법률의 주요 내용으로는 전기통신회선을 이용하여 행해지는 컴퓨터와 관계된 범죄의 방지 및 억세스 제어기능에 의해 실현되는 전기통신에 관한 질서유지를 도모하고 정보통신사회의 건전한 발전에 기여하는 것이라는 목적을 가지고 있다.

이는 '부정한 억세스'라는 해킹을 단일한 법률로써 통제하고 통일적인 법체계의 일부로 판단된다. 한편, 우리나라의 경우에는 형법의 일부규정에서 '데이터 부정조작, 변조, 업무방해, 비밀침해, 전자기록 손괴 및 은닉, 컴퓨터 사기'의 경우를 규율하고 있고, 전산망보급확장과 이용촉진에 관한 법률에서 '전산망 보호조치 침해, 훼손' 등의 경우로 규율하는 등, 개별 법규에 산재되어 있는 형태이다.

그러나 현행 법규에서는 해킹의 피해와 처벌간의 균형을 잃고 있다는 평가를 받고 있으며, 산재된 규정만큼, 법적용에 있어서 어려운 점이 많다는 평가가 많다. 결국, 이러한 상황은 해킹에 대한 죄의식, 윤리의식의 형성에 장애요소로 작용하고 있는 것이다. 즉, 현행 법규상 해킹을 독립한 범죄로 수용하고 있지 못하며 사이버 공간에서 해킹이 어느 정도의 처벌을 받는 '불법적 공격'이라는 표시가 분명하지 않다는 느낌을 받게 된다.



이를 극복하기 위하여 최근 해킹, 정보보호에 대한 종합적 대응의 성격을 띄는 '정보통신기반보호법'을 올해 안에 제정하겠다는 발표가 있었다.

해킹에 대한 "인식과 참여"가 무엇보다 중요하다

해킹에 관한 새로운 법의식을 형성한다는 것은 정보화 사회성원들의 적극적 참여에서 가능하다. 사회적 공감대의 형성은 인터넷 환경에서 더 정확하고 신속하게 이루어질 수 있다. 실제로 인터넷을 통한 여론형성은 각종 인터넷 방송, 미디어의 등장과 함께 획기적인 발전의 길을 걸을 것으로 기대된다.

다시 말하면, 인터넷의 특성인 쌍방향성, 실시간 의사소통, 정보의 공유 등을 반영하는 해킹 대응책 마련이 기본이 되어야 한다. 이러한 맥락에서 좋은 예가 될 수 있는 것이 미국 법무부의 사이버범죄(www.cybercrime.gov)사이트 개설이다.

해킹에 관한 내용을 공식화시키고 여론 형성의 자료가 될 내용을 마련, 네티즌들의 광범위한 참여를 유도한다는 점에서 해킹에 대한 범죄의식을 객관화하기 위하여 사회성원들이 해킹 관련 사례와 내용, 정부정책 등의 내용을 실은 싸이트라는 점에서 실효성을 가질 것으로 보인다. 결국, "참여"를 보다 강화함으로써 해킹에 대한 법감정을 재고한다는 의미이다.

이와 같이 우리가 보완해야 할 해킹 대응책은 해킹에 관한 단일한 법체계 수립과 함께 해킹에 관한 새로운 법감정 형성을 위한 자료공급에 최선을 다해야 한다. 민간부문에서 해킹에 공격적으로 대응하기 위해 일부 보안회사에서는 해커들을 양성하고 활성화하기 위한 해커 양성 프로그램을 실시하고 있어 긍정적인 평가를 받고 있다.

앞으로의 인터넷 환경에서는 적극적인 참여를 통한 여론을 형성하고 여론을 명확하게 반영하는 정책수립만이 기술의 발전을 효과적으로 소화해 낼 유용

한 해결책이 될 것이다.

윤리 형성과 법 집행력의 조화

해마다 한두 번 정도는 대규모 전산망에 침입하는 철없는 해커들이 있다고만 알려졌을 뿐, 그에 상당한 법의 집행을 받았는지, 피해복구에 따른 비용이 얼마나 심각한지에 대한 사회적 대응을 제시한 구체적인 움직임이 많지 않았다. 어쩌면, 일부에서는 '해커로 이름나거나 실력을 인정받으면, 새로운 전문가로 탄생할 수 있다는' 생각까지도 조장하고 있는 듯한 현실에서 해킹방지를 위해서는 컴퓨터 윤리 교육을 창출해야 한다는 것이 설득력 없어 보이기도 할 수 있다.

그러나, 우리가 건설하고 설계하는 사이버공간은 기존 세계를 반영하는 새로운 사회이자 현실에 긴밀하게 연결된 공간이다, 따라서, 안전하고 신뢰있는 사이버공간을 만들기 위해 적합한 윤리의식의 형성과 함께 현실세계에서 효과적으로 반영되는 법집행력은 필수이다. 전자정부를 구성하고 전자민주주의의 실현은 새로운 시대에 적합한 윤리의식 함양이 가장 필요한 내용이다.

우리는 현재 우리 인터넷 사용자 수의 폭발적 증가를 국가 경쟁력의 성장지표로 단순하게 비교하는 경우를 많이 본다. 그러나, 그 이면에는 세계적으로 가장 대중적인 해킹 경로를 제공하는 국가로 이름을 날리고 있다는 사실을 간과해서는 안 된다.

컴퓨터 사용자가 증가하는 만큼, 그들의 지적 호기심을 올바로 자기 제어할 전제가 필요하다는 것이다. 해킹을 막기 위한 대안으로 컴퓨터 윤리 교육을 중요시하는 이유는 재범률이 높다는 사실에서도 그 근거를 찾을 수 있다. 컴퓨터 윤리 교육을 통해 공유하는 '자기제어력' 은 범죄욕구를 억제하기 위한 기본적인 교육으로 자리잡을 수 있을 것이다.

결국, 해킹은 네트워크 자원의 관리를 방해하고 부정한 접근이자 사이버월드의 형성과 네티즌들의 의사형성, 활동에 광범위한 장애요소로 작용하는 만큼, 해킹방지를 위한 컴퓨터 사용 윤리 교육과 법집행의 실질화를 통해서 효율적인 대안을 마련할 수 있으리라 생각된다.

해킹 대응, 국경이 없다

해킹에 대한 대응은 국경을 초월하고 있다. 세계적인 사이트들의 해킹사례에서 해킹경로를 정확하게 파악하지 못함을 볼 때, 주요 정보 선진국들을 중심으로 전개되었던 '예전의' 국가별 해킹 대응 정책 수립은 더 이상 유효하지 않음을 알 수 있다.

해커의 키보딩만으로 국가간 전쟁이 일어날 수 있을 만큼 해커에 대한 통제력이 약해진다면 사이버월드의 형성은 매우 늦은 속도로 재정비의 과정을 겪을 뿐 아니라, 현실에서도 국제분쟁이 끊이지 않을 것이다. 이와 관련하여 각국에서는 '정보전' 시나리오를 짜고 이에 대비한 훈련이 진행중이어서 제4의 국가간 긴장상황을 만들지는 않을 것인지 우려된다.

얼마 전 타이완과 중국간의 정보전에서 보듯이 각국의 공공 전산망에 침입하여 정보자원을 파괴하고 치명적인 피해를 입게 한다면 주변 국가들도 이러한 대결 구도에 휘말리기 쉽다는 것이다. 이러한 대결구도에 효과적으로 대응하기 위해서는 해킹에 대한 국제적 협력체계의 수립이 무엇보다도 중요하다고 할 것이다.

특히 대형 해킹사고가 생길수록 수사공조, 피해 복구를 위한 효과적 협조체계를 구축해야 할 것이다. 국제적 협력 또한 국가를 초월한 해킹에 대한 법감정의 공유를 전제로 하여야 하며 통일적인 법집행력을 합의하는 것도 좋은 방안이 될 수 있을 것이다.