「法과 政策」 第19輯 第1號, 2013. 2. 28.
濟州大學校 法과政策硏究所

「정보통신망법」 개정안에 대한 입법정책*

- 침해사고와 관련하여 -

A Legislative Policy on a Revision of 「Information and Communications Network Law」

이 부 하**
Lee, Boo-Ha

목 차

국문초록

현행 정보통신망법에는 일정수준 이상의 침해사고 발생시 긴급대응조치를 취할 법규정이 없다. 정보통신망법을 개정하여 대규모 분산 서비스 거부(DDoS) 공격 등 중대한 침해사고에 대비할 수 있는 법적 근거조항을 마련하는 것이 시급한 과제이다. 첫째, 신속한 침해사고의 원인분석 및 악성프로그램의 확산방지를 위해 악성코드 감염이 확인된 PC에 한하여, 방송통신위원회가 접속요청을 할 수 있는 법적 근거가 필요하다. 둘째, 웹사이트에 은닉된 악성

논문접수일 : 2012.12.20
심사완료일 : 2013.01.22
게재확정일 : 2013.01.24
* 본 논문은 한국인터넷진흥원에서 개최한 정보통신망법 개정안 검토회의 내용을 반영한 것임.
** 법학박사 · 영남대학교 법학전문대학원 교수

프로그램에 대해 해당 웹사이트 운영자가 정기점검하고 악성프로그램을 발견할 경우 삭제 조치할 수 있는 법적 근거가 필요하다. 셋째, 긴급한 조치로서 방송통신위원회는 주요 정보통신서비스 제공자(ISP)에게 침해사고 확산에 이용가능한 접속경로(도메인, IP주소, 포트번호 등)를 차단조치하도록 명령할 수 있어야 한다. 넷째, 악성프로그램에 감염된 PC의 인터넷 접속제한 명령을 통해 중대한 피해확산을 방지할 수 있는 조치가 필요하다. 다섯째, 침해사고의 원인분석을 위해 주요 정보통신서비스 제공자(ISP) 등 특정한 사업자들은 침해사고 관련 정보를 방송통신위원회나 한국인터넷진흥원에 제공하도록 해야 한다.

주제어 : 정보통신망법, 악성프로그램, 감염PC에 대한 접속요청, 정보통신서비스 제공자(ISP), 디도스(DDoS : 분산 서비스 거부)

Ⅰ. 문제의 제기

헌법국가는 보다 폭넓게 논쟁할 여지가 있는 소재들을 회피한다.[1] 이러한 범주에 해당하는 것이 인터넷상 디도스(DDoS : 분산 서비스 거부) 공격 등에 대비한 입법논의이다. 일반적으로 법이 추구하는 공익을 위해 입법상 사용되는 수단이 헌법에서 보장하는 기본권인 사익을 제한하는 경우, 이를 판단하기 위해 공익과 사익간의 비교형량이 이루어진다.[2] 그런데 요즘 빈번히 발생하는 인터넷상 디도스 공격은 우리 헌법이 보장하는 기본권이나 법적 이익에 해당되지 않으며, 오히려 공익을 심각하게 해치는 행위에 해당된다. 인터넷상 디도스 공격 등에 의한 중대한 침해사고는 국가적·사회적으로 큰 혼란을 일으키며 국민 개개인의 기본권적 법익에 심각한 침해를 일으키는 결과를 낳는

1) Josef Isensee (이승우 역), 「국가와 헌법」, 세창출판사, 2001, 48면.

2) 비례성 원칙에 관하여는 이부하, "비례성원칙과 과소보호금지원칙", 「헌법학연구」 제13권 제2호, 2007. 6, 275면 이하; 이기철, "헌법재판소는 비례의 원칙에 목적의 정당성을 포함시켜도 좋은가?", 「공법연구」 제35집 제1호, 2006. 10, 377면 이하 참조.

다. 기존 정보통신망법 등 법률 규정에는 디도스 공격 등에 의한 중대한 침해사고 발생시 이에 대한 법적 대비 방안이 불비한 상황이고 중대한 공익을 위해 헌법상 입법의무가 있음에도 입법부작위 상태에 있었다.

과거에 증가추세였던 정보통신범죄로서 사이버 명예훼손, 사이버 스토킹, 사이버 음란정보유포, 사이버 성폭력 등의 범죄행위는 감소 전망이고, 사이버 사기, 스팸메일, 사이버 저작권 침해, 해킹, 디도스 공격 등 범죄행위는 증가 전망에 있다.[3] 우리나라 정보통신사업이 새로운 도약을 하려면, 한편으로는 가상세계에 대한 기반형성이나 산업활성화를 위한 정책을 실현하기 위한 법제도적 기반이 마련되어야 하며, 다른 한편으로는 정보통신이나 인터넷 발전에 저해가 되는 법제도적 장애물을 제거함과 동시에 이용자 컴퓨터의 보호 및 침해사고 대응에 필요한 실효성있는 수단이 법제도적으로 마련되어야 한다.[4]

최근 컴퓨터, PDA, 스마트폰 등 다양한 정보처리장치를 통해 언제 어디서나 인터넷에 접속할 수 있는 IT환경이 구축되면서, 일반 이용자 컴퓨터를 대상으로 한 악성프로그램[5]이 확산·증대되고 있다. 특히 악성프로그램에 감염된 이른바 '좀비PC'가 디도스[6](DDoS : 분산 서비스 거부) 공격 등 침해사고에 악용되고 있어 일반 이용자 컴퓨터를 보호할 수 있는 법제도적 대응체계 확립이 절실하게 되었다.

현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다)은 정보통신서비스를 이용하는 자의 개인정보 보호 및 정보통신망의 건전하고 안전한 이용 환경을 조성하는데 그 입법목적이 있다. 또한 「정보통신기반 보호법」의 주요한 입법취지는, 국가안전보장·행정·국방

3) 홍승희, "정보통신범죄의 전망", 「형사정책」 제19권 제1호, 2007, 9면 이하.

4) 최경진, "가상세계에 대한 법적 고찰", 「문화 미디어 엔터테인먼트 법」, 중앙대 문화미디어 엔터테인먼트법연구소, 2011, 126면.

5) "악성프로그램"이란 정당한 사유 없이 컴퓨터·데이터 또는 컴퓨터에 설치된 프로그램을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 컴퓨터프로그램(특정한 결과를 얻기 위하여 컴퓨터 내에서 직접 또는 간접으로 사용되는 일련의 지시·명령으로 표현된 전자적 정보를 말한다. 이하 같다)을 말한다.

6) 디도스(DDoS : 분산서비스거부 공격(Distribute Denial of Service)) 공격은 다수의 좀비 PC(바이러스에 감염된 다수의 개인컴퓨터)를 이용해 특정사이트에 과도한 트래픽을 발생시켜 시스템을 마비시키는 사이버 공격의 일종이다.

·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망법」의 규정에 의한 정보통신망 등 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 공격하는 행위를 대비하고 주요정보통신기반시설을 보호하고자 함에 있다. 「정보통신기반 보호법」에 의하면, 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.[7] 또한 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 보호진흥원에 그 사실을 통지하여야 한다. 이 경우 관계기관 등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다고 규정하고 있다.[8]

그러나 현행 우리나라 정보보호법들은 네트워크(망) 또는 정보통신기반 보호를 중점으로 하고 있어 이용자 컴퓨터의 보호 및 실효성 있는 침해사고 예방·대응에 한계가 있으며, 일정 수준 이상의 침해사고 발생시 긴급대응조치에 대한 법적 규율이 부재한 상태이다. 이용자 컴퓨터가 악성프로그램에 감염된 경우 해당 이용자에게 감염사실과 치료방법을 알리고 치료를 지원하는 근본적 대응이 필요하며, 악성프로그램 감염 예방을 위해 백신소프트웨어 등 보안프로그램 이용을 활성화하고 인터넷 게시판 등을 통해 유포·확산되는 악성프로그램을 삭제하는 조치를 할 수 있는 법적 근거가 필요하다. 또한 일정 수준 이상의 중대한 침해사고 발생시 피해확산을 최소화할 수 있는 실효성 있는 긴급대응조치가 확보되어야 한다. 컴퓨터보안프로그램 이용·보급 활성화, 웹사이트에 은닉된 악성프로그램 삭제, 악성프로그램 감염컴퓨터의 치료지원, 심각한 침해사고 발생시 실효성있는 대응체계 확립 등 이용자 컴퓨터의 보안 강화를 위한 새로운 입법이 필요하다. 침해사고와 관련하여 기존의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정하여 침해사고에 신

7) 정보통신기반 보호법 제8조.
8) 정보통신기반 보호법 제13조 제1항.

속히 대응하기 위한 조치의 법적 근거를 마련해야 한다.

먼저 본고에서는, 정보통신망법의 개정 배경 및 필요성을 살펴본다(이하 Ⅱ). 또한 법률 개정의 방법과 관련하여, 새로운 법률 제정 방식과 기존의 정보통신망법 개정 방식이 가능한데, 현실적인 면을 고려하여 기존의 법률을 개정하는 방식을 취하여 개정안을 제시해 본다(이하 Ⅲ).

Ⅱ. 법률 개정의 배경 및 필요성

1. 악성 프로그램의 확산 및 디도스 공격 등 침해사고 현황

수시로 또는 여러 차례 다음과 같은 사건들이 발생하고 있다. "인터넷을 실행하는 순간 엉뚱한 포털창이 뜨고, 바탕화면에는 내려받지도 않은 쇼핑몰 창이 서너 개 생기더니 잘 삭제되지도 않습니다. 이는 컴퓨터 이용자가 미디어 재생 프로그램이나 백신 등을 내려받을 때 함께 침투한 겁니다. 아무런 확인 없이 이같은 프로그램을 내려받은 컴퓨터 270만 대는 순간 좀비PC로 변했습니다." 이러한 사건의 발생은 인터넷 광고 일을 하던 20대, 30대 4명이 쇼핑몰 등 특정사이트에 강제접속하게 만드는 악성프로그램들을 무차별 유포했기 때문이다.[9]

"2009년 7월 7일 18시 50분을 기하여 국내 청와대 등 16개 기관 사이트, 미국 백악관 등 14개 사이트에 대한 대규모 분산 서비스 거부(DDoS) 공격이 발생했다. 이 공격은 보안이 허술한 다수의 감염PC(일명 좀비PC)를 이용하여 대량의 허위 유해 트래픽을 전송하여 시스템상의 과부하를 발생시켜 해당 시스템의 정상적인 서비스를 방해하는 사이버 공격을 의미한다. 또한, 2009년 7월 8일 오후 6시 이후 국정원, 안철수 연구소 등에 2차적인 공격이 이루어졌다. 이는 사이버 공간에 큰 지진이 일어난 후, 몇 개의 여진이 발생하는 현상이다. 이번에 발생한 분산 서비스 거부 공격은 국내PC 12,000여대와 해외PC

9) http://imnews.imbc.com/replay/nwtoday/article/3095792_5782.html (2012년 7월 13일 MBC 뉴스)

8,000여대가 악용되었다고 하며 기존에 널리 알려진 분산서비스 공격 형태와 달리 중간 명령 제어 서버가 없이 이루어져 금융권에 까지 피해를 받고 있어 2003년 1.25 인터넷 대란 이후에 최대의 사이버 테러가 발생하였다."[10]

2012년 12월 정부는 인터넷을 통한 해킹이나 디도스 공격도구 유통을 집중적으로 단속한다고 공지하였다. 방송통신위원회와 한국인터넷진흥원은 2012년 12월 4일 인터넷을 통한 해킹이나 디도스 공격도구 유통 및 청부해킹 관련 게시물을 정기적으로 단속한다고 밝혔다. 해킹도구나 청부해킹 유도 게시물을 인터넷에 올리는 행위는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 따라 처벌 대상이다. 하지만 카페나 블로그의 비공개 게시판을 통해 여전히 공격도구 제작이나 판매 등이 이루어지고 있다. 방송통신위원회는 2012년 9월 말 기준으로 해킹대행 27건, 해킹도구 판매 및 배포 30건 등 약 60여건의 불법 게시물이 파악됐다고 밝혔다. 방송통신위원회 관계자는 "청소년 등 일반인들이 단순한 호기심과 영웅 심리 때문에 범죄행위라는 인식 없이 불법해킹이나 디도스 공격을 저지르는 사례가 계속 발생하고 있는데, 이는 해킹프로그램을 인터넷에서 쉽게 구할 수 있는 것도 주요 원인 중 하나"라며 "수사기관 등 관계기관과 협조하여 사이버범죄 예방활동을 강화해 나가겠다"고 말했다.[11]

최근 컴퓨터, PDA, 스마트폰 등 다양한 정보처리장치를 통해 언제 어디서나 인터넷에 접속할 수 있는 IT환경이 구축되면서, 일반 이용자 컴퓨터를 대상으로 한 악성프로그램이 확산되고 있다. 특히 악성프로그램에 감염된 이른바 '좀비PC'가 디도스(DDoS : 분산 서비스 거부) 공격 등 침해사고에 악용되고 있다. 국가기관과 언론사 및 은행들이 이러한 디도스 공격을 받는 경우가 빈번한데, 이 경우 국가 및 사회 전체의 정치, 경제, 행정에 심각한 영향을 줄 뿐만 아니라 이로 인해 발생하는 피해도 막대하다. 또한 개개 국민의 PC가 디도스(DDoS) 공격을 받는 경우 통신의 자유를 침해받을 뿐만 아니라 그 피해도 심각하다.

---

10) http://economy.hankooki.com/lpage/opinion/200907/e20090709174542480 90.htm (2009년 7월 10일 서울경제-기고: 김광조 교수)

11) http://biz.chosun.com/site/data/html_dir/2012/12/04/2012120401374.html (검색일: 2012년 12월 10일)

"2009년 7월 7일 오후 6시 대한민국은 일대 혼란에 빠졌다. 약 20만개의 PC가 동원된 분산서비스거부(DDoS) 공격이 청와대, 백악관, 국방부, 주요 언론사, 주요 정당, 포털 등 26개 사이트로 무차별적으로 쏟아져 홈페이지가 마비됐다. 이같은 공격은 2009년 7월 8일과 9일 오후 6시에 반복됐고, 제대로 된 방어체계를 갖추지 못한 정부는 허둥지둥하며 무려 72시간동안 곤혹을 치렀다. 7.7 DDoS는 당시 우리 정부의 사이버방어 시스템의 현주소를 여실히 노출시켰고 현대경제연구원은 7.7 DDoS의 피해액을 363억~544억원 가량으로 추산했다."[12]

또한 2012년 4.11 총선 하루 전날 중앙선거관리위원회 서버에 디도스(DDoS·분산서비스거부) 공격이 발생하였다.[13] 중소기업과 금융권 등 보안예산 투자가 어려운 영세기업을 겨냥한 DDoS 공격은 여전하다. 이에 대비해 정부는 영세기업의 DDoS 공격 방어를 위해 KISA에 사이버대피소를 운영하고 있다. DDoS 공격을 당하고 사이버대피소를 이용한 기업의 수는 2010년 52건, 2011년 101건, 2012년 상반기까지 75건으로 매년 두 배 가까이 늘고 있다.[14] 이렇게 디도스(DDoS) 공격이 심각한 상황임에도 불구하고, 현행 정보통신법제는 네트워크 또는 정보통신기반보호를 중심으로 한 법규율이 중심이 되고 있으며,[15] 침해사고의 원인분석을 위한 시스템 접근권이나 악성프로그램의 주기적 점검 및 삭제 등 필요한 조치를 할 법적 근거가 미흡하여 기업과 개인 이용자 컴퓨터의 보호 및 침해사고에 대한 실효적 대응에 있어서 한계에 직면하고 있다.

2. 법률 개정의 필요성

최근 헌법재판소 결정에 의하면, "인터넷게시판을 설치·운영하는 정보통신

12) http://www.dt.co.kr/contents.html?article_no=2012070602010860785001

13) http://www.yonhapnews.co.kr/bulletin/2012/06/28/0200000000AKR20120628101700004.HTML?did=1179m

14) http://www.dt.co.kr/contents.html?article_no=2012070602010860785001

15) 손승우, "사이버 보안의 예방 수단을 위한 법제 분석", 「연세 의료·과학기술과 법」 제2권 제2호, 2011. 8, 28-29면.

서비스 제공자에게 본인확인조치의무를 부과하여 게시판 이용자로 하여금 본인확인절차를 거쳐야만 게시판을 이용할 수 있도록 하는 본인확인제를 규정한 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제44조의5 제1항 제2호, 같은 법 시행령 제29조, 제30조 제1항이 과잉금지원칙에 위배하여 인터넷 게시판 이용자의 표현의 자유, 개인정보자기결정권 및 인터넷게시판을 운영하는 정보통신서비스 제공자의 언론의 자유를 침해를 침해한다"고 판시하였다.[16] 이는 게시판 이용자의 표현의 자유를 사전에 제한하여 의사표현 자체를 위축시킴으로써 자유로운 여론의 형성을 방해하기 때문이다. 이처럼 인터넷 이용자의 표현의 자유를 직접적으로 제한하는 법률 조항은 위헌이 될 가능성이 높다.

또한 헌법재판소는 "정보통신망을 통하여 일반에게 공개된 정보로 말미암아 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자가 삭제요청을 하면 정보통신서비스 제공자는 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 30일 이내에서 해당 정보에 대한 접근을 임시적으로 차단하는 조치를 하여야 한다고 규정하고 있는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제44조의2 제2항 중 '임시조치'에 관한 부분 및 제4항의 입법목적이 정당하고 수단 또한 적절하며, 침해의 최소성 및 법익균형성 요건도 충족한다"고 판시하였다.[17]

현행 정보통신망법은 정보통신서비스 제공자에게 이용자의 행위에 대해 일정한 조치를 하도록 하고 있으나, 실효성있는 조치를 취하기도 어려운 실정이다. 또한 중대한 침해사고가 발생할 경우 정보통신서비스 제공자와 이용자 모두에게 심각한 피해가 발생하는데 이에 대한 입법이 불비한 상황이다.

컴퓨터보안프로그램 이용·보급 활성화, 웹사이트에 은닉된 악성프로그램 삭제, 악성프로그램 감염컴퓨터의 치료 지원, 심각한 침해사고 발생시 실효성 있는 대응체계 확립 등 이용자 컴퓨터의 보안 강화를 위한 새로운 입법이 절실히 필요한 상황이다. 디도스(DDoS) 공격 등 침해사고 예방을 위한 법적 조

16) 헌재 2012. 8. 23. 2010헌마47 등, 공보 제191호, 1631, 1631-1632.
17) 헌재 2012. 5. 31. 2010헌마88, 판례집 24-1하, 578, 578-579.

치, 침해사고 상황전파, 침해사고의 교육·홍보 등을 통한 대국민 인식 제고, 컴퓨터보안프로그램개발자 및 감염컴퓨터의 치료 전문인력 양성, 악성프로그램 대응기술 개발·보급 등 컴퓨터의 안전한 이용·관리 및 악성프로그램의 확산방지를 위해 정부의 촉진 및 지원 기능을 법률에 규정할 필요성이 있다.

백신소프트웨어 설치·이용 및 정기적 갱신, 소프트웨어 보안취약점보완프로그램의 확인 및 설치 등 이용자가 자신의 컴퓨터를 악성프로그램으로부터 안전하게 보호하기 위하여 지켜야 할 책무를 규정해야 할 필요성이 있다. 감염컴퓨터로부터 악성프로그램의 전파 및 확산을 방지하고 침해사고의 확산방지 및 침해사고의 효과적인 대응을 위해 방송통신위원회가 악성프로그램에 감염된 컴퓨터의 소유자 또는 이용자에게 접속요청을 할 수 있는 법적 근거조항이 필요하다.

일정한 수준의 웹사이트 운영자에게 웹사이트 게시자료의 정기점검 및 악성프로그램 발견시 삭제조치를 할 수 있도록 하고, 방송통신위원회가 악성프로그램이 숨겨진 게시판 발견한 경우 해당 게시판의 운영자에게 삭제 명령 등 필요한 조치를 할 수 있도록 법적 근거조항을 둘 필요성이 있다. 한국인터넷진흥원은 이용자의 컴퓨터 보호를 위하여 긴급배포용 백신소프트웨어 보급, 상담 및 원격지원 등 기능을 갖춘 인터넷방역사이트를 구축·운영하도록 해야 한다.

방송통신위원회가 침해사고 원인 조사 및 분석을 위하여 필요한 경우 이용자의 동의를 얻어 악성프로그램 감염 컴퓨터에 대한 접속 및 자료의 수집·조사를 할 수 있도록 해야 한다. 침해사고의 원인분석을 위해 주요 인터넷서비스 제공자(ISP)[18] 등 특정한 사업자들은 침해사고 관련 자료를 방송통신위원회나 한국인터넷진흥원에 제출하도록 해야 한다. 중대한 침해사고의 발생으로 급속한 피해확산이 우려되는 경우에 침해사고 원인이 되는 악성프로그램 등을 치료·복구할 수 있는 컴퓨터보안프로그램을 이용자에게 긴급 배포할 수 있도록 해야 한다. 방송통신위원회가 일정 수준 이상의 심각한 침해사고가 발생한 경우 인터넷접속서비스 제공자에게 인터넷주소의 차단 등의 조치를

18) 인터넷서비스 제공자(ISP)의 법적 책임, 특히 관리책임에 관한 연구로는 박정훈, "인터넷서비스제공자의 관리책임", 「공법연구」 제41집 제2호, 2012. 12, 511면 이하 참조.

명할 수 있도록 하기 위해 법적 근거조항이 필요하다.

III. 개정안 제안

1. 악성코드 감염PC에 대한 접속요청권

현행 정보통신망법 제48조의4[19]에 의하면, 침해사고[20]의 원인을 분석하고 침해사고의 피해 확산을 방지하기 위해 민·관합동조사단을 구성하여 원인분석 하도록 규정하고 있다. 이러한 법조항으로는 침해사고의 확산 방지에 한계가 있고 침해사고의 원인 분석이 사실상 어렵다. 실제로 침해사고가 발생한 경우 침해사고의 대응에 있어서 신속한 조치를 요하지만, 악성코드 샘플채집을 위한 가입자의 섭외 거부 등이 빈번하여 샘플 채집이 지연되고 있다. 가입자의 섭외시간 지연은 전체 침해사고의 대응을 지연시키게 된다. 현재 실무상 감염 PC 이용자 또는 소유자의 협조를 얻어 샘플을 수집하고 있으나, 이러한 행위

19) 정보통신망법 제48조의4(침해사고의 원인 분석 등) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다.
② 방송통신위원회는 정보통신서비스 제공자의 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위하여 정보보호에 전문성을 갖춘 민·관합동조사단을 구성하여 그 침해사고의 원인 분석을 할 수 있다.
③ 방송통신위원회는 제2항에 따른 침해사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.
④ 방송통신위원회는 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.
⑤ 방송통신위원회나 민·관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.
⑥ 제2항에 따른 민·관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.

20) "침해사고"란 전자적 침해행위로 발생하는 모든 사태를 말한다.

의 법적 근거 미비로 인해 샘플수집에 많은 애로사항이 존재한다.

【악성프로그램 조치거부 유형】

거부 유형	거부 업체수	거부 비율	상세 거부 사유
무시 및 근거부족	81개	81%	o 법적 근거가 있습니까? o 관리업체가 별도 잘하고 있다 o 우리일에 신경쓰지 마라 o 전화 통화 거부(대화중 중단) o 메일 주소 요청 거부 o 홈페이지가 정상인데 무슨 소리? (악성프로그램 인지 부족)
연락 불가	11개	11%	o 1회 통화 후 연락두절(전화불통)
조치능력 부재	8개	8%	o 조치할 수 있는 담당자 부재 o 담당자 퇴사 o 담당자 장기간 출장
합 계	100개	100%	

[통계기간 : '10.06월 ~ '10.12월, 100개 업체 대상]

신속한 침해사고의 원인분석 및 확산방지를 위해 악성코드 감염이 확인된 PC에 한하여 접속요청을 위해 법률상 법적 근거를 마련해야 한다. 악성코드 감염PC에 대한 접속요청권 조항 신설은 감염PC의 가입자를 섭외하여 악성코드 샘플을 신속히 채집하기 위함이다. 접속요청시 헌법이 요구하는 적법절차원칙[21]의 준수가 요구되므로 컴퓨터 이용자에게 적절한 고지 및 동의를 구하는 절차를 법률에 명시할 필요성이 있다.

21) 적법절차원칙에서 도출할 수 있는 가장 중요한 절차적 요청 중의 하나로, 당사자에게 적절한 고지를 행할 것, 당사자에게 의견 및 자료 제출의 기회를 부여할 것을 들 수 있겠으나(헌재 1994. 7. 29. 93헌가3등, 판례집 6-2, 1, 11; 헌재 1996. 1. 15. 95헌가5, 판례집 8-1, 1, 16-17; 헌재 2002. 6. 27. 99헌마480, 판례집 14-1, 616, 634 참조), 이 원칙이 구체적으로 어떠한 절차를 어느 정도로 요구하는지는 일률적으로 말하기 어렵고, 규율되는 사항의 성질, 관련 당사자의 사익(私益), 절차의 이행으로 제고될 가치, 국가작용의 효율성, 절차에 소요되는 비용, 불복의 기회 등 다양한 요소들을 형량하여 개별적으로 판단할 수밖에 없을 것이다(헌재 2003. 7. 28. 2001헌가25, 판례집 15-2, 1, 17-18; 헌재 2006. 5. 25. 2004헌바12, 판례집 제18권 1집 하, 58, 66-67).

감염PC에의 접속은 이용자의 '자유롭고 진정한' 동의에 의해서만 실시 가능하므로 기본권 침해가능성은 적다. 이용자의 동의 없는 감염PC에 대한 접속은 현행법상 해킹에 해당하고 타인의 감염PC에 침입시 주거침입죄에 해당된다. 또한 현행 정보통신망법상 패킷감청은 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 되어 있다. 따라서 PC에 대한 접속요청을 빙자하여 패킷감청을 한다면, 법적으로 금지되는 범죄행위로 처벌받게 된다. 이용자의 컴퓨터에 접근하여 원인분석 등 목적 외로 악용할 경우, 개정 법률안에서 "해당 업무 종사자를 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다"라고 규정하면 해결된다.

침해사고와 관련된 소유자 또는 이용자의 컴퓨터에 대한 접속요청과 감염PC 치료를 위한 IP 제공 등이 컴퓨터의 소유자 또는 이용자의 프라이버시권 침해, 기업의 영업비밀 노출, 패킷감청 등의 남용이 우려된다는 지적이 있다.[22] 그런데 최근 사이버침해의 특징은 '이용자'를 공격할뿐 아니라 '공격도구'(좀비PC)를 이용하여 공격하는 경우가 많으므로 이용자에 대한 조치없이는 침해사고 대응은 실효성을 거두기 어렵다. 감염PC에 대한 신속한 조치를 취하지 않을 경우, 다른 사람에게 피해를 줄 수 있어 공동체 사회에 해가 되는 결과를 초래하게 되므로 감염PC의 가입자를 섭외하여 악성코드 샘플을 신속히 채집하여 조치를 취하는 것이 필요하다. 침해사고의 확산 방지 및 침해사고의 효과적 대응이라는 중대한 공익을 달성하기 위하여 이용자의 컴퓨터에 대한 접속요청이라는 기본권 제한 수단보다도 기본권을 보다 덜 제한하는 다른 방법이 현실적으로 존재하지 않는다. 이러한 침해사고와 관련된 소유자 또는 이용자의 컴퓨터에 대한 접속요청이라는 기본권 제한은 수인한도를 넘는 과잉적 제한이라 보기 어렵기 때문에 비례의 원칙에 위반될 가능성이 낮다. 이 경우에도 정부의 판단이나 정책 결정에 의한 접속요청이 아니라, 침해사고를 받았거나 감염이 확인된 PC에 한해서 악성프로그램 샘플 수집을 위해 접속요청이 실시되는 것이다. 이러한 악성프로그램 샘플 수집은 신종플루 백신 개발의 경우와 같이 악성프로그램 확산방지를 위해 매우 중요한 절차이다.

22) 안정상, "악성프로그램 확산방지 등에 관한 법률안(좀비PC법) 평가", 국회, 2011, 6-7면.

유형	개정안	주요 내용
1안	제48조의5(감염 컴퓨터에 대한 접속요청 등) ① 방송통신위원회는 침해사고의 대응, 원인조사 등의 조치가 필요한 경우에는 전자적 침해행위[23]를 받거나 악성프로그램에 감염된 컴퓨터에 대한 접속요청을 해당 컴퓨터의 소유자 또는 이용자에게 요청할 수 있다. ② 방송통신위원회는 제1항에 따라 컴퓨터에 접속하는 경우에는 컴퓨터의 소유자 또는 이용자의 동의를 받아 침해사고 발생 원인의 조사 및 분석을 위하여 필요한 자료를 수집하거나 조사할 수 있다. ③ 제1항 및 제2항에 따른 업무를 수행하는 자는 해당 컴퓨터에 의하여 처리되는 정보를 해당 업무 목적 외로 열람·이용하거나 침해·훼손·누설하여서는 아니된다. ④ 제1항에 따른 해당 컴퓨터에 대한 접속요청의 방법·절차, 제2항에 따른 자료의 수집·조사 범위 등에 필요한 사항은 대통령령으로 정한다.	○ 별도의 조문으로 신설하여 감염PC 이용자에게 동의를 구하는 절차를 명시하고, 접속요청의 대상 및 범위를 구체적으로 규정함
2안	제48조의4(침해사고의 원인 분석 등) ① (현행과 동일) ② 방송통신위원회는 침해사고의 대응, 원인조사 등의 조치가 필요한 경우에는 침해사고와 관련된 컴퓨터의 소유자 또는 이용자에게 알리고 접속에 대한 동의를 받아 침해사고 발생 원인의 조사 및 분석을 위하여 필요한 자료를 수집하거나 조사할 수 있다. ③~⑦ (현행 ②~⑥과 동일) ⑧ 제2항에 따른 침해사고와 관련된 컴퓨터에 대한 접속요청의 방법·절차 및 자료의 수집·조사 범위 등에 필요한 사항은 대통령령으로 정한다.	○ 현행 정보통신망법 제48조의4를 개정하여 감염PC에 대한 접속요청을 통해 원인 분석할 수 있도록 접속요청에 대한 법적 근거를 마련

2. 웹사이트에 은닉된 악성프로그램 삭제조치

웹사이트를 통해 유포되고 있는 악성프로그램의 삭제를 강제할 법적 근거가 없고, 이를 방치할 경우 단시간내에 웹사이트를 방문하는 이용자가 감염될 수 있다. 현실에서는 해당업체에게 방송통신위원회가 공문발송을 통한 삭제조

23) "전자적 침해행위"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 컴퓨터를 공격하는 행위를 말한다.

치를 요청하지만 해당업체가 협조하지 않을 경우 악성프로그램 유포가 지속되고 있다.

웹사이트에 은닉된 악성프로그램에 대해 해당 웹사이트 운영자가 정기점검하고 악성프로그램을 발견할 경우 삭제 조치를 위한 법적 근거를 마련하면 악성프로그램의 유포가 방지될 수 있다. 모든 웹사이트 운영자에게 이러한 정기점검 등을 요구할 수 없기 때문에 일일 평균 이용자 수가 10만명 이상이면서 대통령령으로 정하는 기준에 해당되는 자에게 정기점검 의무를 부과해야 한다. 또한 악성프로그램 뿐만 아니라 악성프로그램을 유포하는 접속경로(URL)도 삭제할 수 있도록 '악성프로그램 및 유포접속경로'로 삭제대상을 명확히 규정하는 것이 필요하다.

악성프로그램 정기점검은 사람에 의해 특정 PC에 접속하여 실시되는 것이 아니라, 보안프로그램에 의해서 수행되는 것이다. 악성프로그램의 삭제도 대부분 프로그램에 의해서 자동적으로 이루어진다. 일반 이용자의 게시된 자료에 악성프로그램 등이 포함된 경우 해당 악성프로그램만 삭제되는 것이며 게시물 자체는 삭제대상이 아니다.

다만, 인터넷에 유통되는 정보에 대한 과도한 규제일 수 있다는 우려를 제거하기 위하여 악성프로그램 등만을 삭제하는 것이 곤란하여 게시된 자료에 대한 접속을 차단해야 하는 경우에는 이용자들이 알 수 있도록 1개월 이상 기존의 게시된 자료를 공개하도록 하는 개정안을 마련하는 것도 하나의 방안이다.

유형	개정안	주요 내용
1안 (별도 조문 신설)	제48조의6(악성프로그램 방지 등) ① 웹사이트를 운영하는 자로서 일일 평균 이용자 수가 10만명 이상이면서 대통령령으로 정하는 기준에 해당되는 자(이하 "웹사이트 운영자"라 한다)는 자신이 운영하는 웹사이트에 게시된 자료에 악성프로그램 또는 악성프로그램 감염을 유인하는 전자적 정보(이하 "악성프로그램 등"이라 한다)가 포함되어 있는지를 월 1회 이상 주기적으로 점검하는 기술적 조치를 하여야 하며, 게시된 자료에 악성프로그램 등이 포함된 사실을 발견한 경우에는 이를 즉시	○ 별도의 조문으로 신설하여 악성프로그램 점검 및 필요한 조치를 하도록 규정함

	삭제하는 등 필요한 조치를 하여야 한다. ② 방송통신위원회는 악성프로그램 등이 포함된 게시판을 발견한 경우 해당 게시판 관리·운영자에게 악성프로그램 등의 삭제 등 필요한 조치를 명할 수 있다. ③ 제1항에 따른 조치 및 그 밖에 필요한 사항은 대통령령으로 정한다.	
2안 (현행 제48조 개정)	제48조(정보통신망 침해행위 금지 등) ①~③ (현행과 동일) ④ 웹사이트를 운영하는 자로서 일일 평균 이용자 수가 10만명 이상이면서 대통령령으로 정하는 기준에 해당되는 자(이하 "웹사이트 운영자"라 한다)는 자신이 운영하는 웹사이트에 게시된 자료에 악성프로그램 또는 악성프로그램 감염을 유인하는 전자적 정보(이하 "악성프로그램 등"이라 한다)가 포함되어 있는지를 월 1회 이상 주기적으로 점검하는 기술적 조치를 하여야 하며, 게시된 자료에 악성프로그램 등이 포함된 사실을 발견한 경우에는 이를 즉시 삭제하는 등 필요한 조치를 하여야 한다. ⑤ 방송통신위원회는 악성프로그램 등이 포함된 게시판을 발견한 경우 해당 게시판 관리·운영자에게 악성프로그램 등의 삭제 등 필요한 조치를 명할 수 있다. ⑥ 제4항에 따른 조치 및 그 밖에 필요한 사항은 대통령령으로 정한다.	○ 현행 정보통신망법 제48조를 악성프로그램 전달·유포 금지 규정과 악성프로그램 점검 및 필요한 조치를 하도록 내용을 추가하여 개정

3. 침해사고 확산방지를 위한 접속 경로 차단 명령

침해사고의 확산에 이용가능한 접속경로(도메인, IP주소, 포트번호 등)에 대한 차단이 안되거나 지연될 경우 2차 피해 등 추가적 피해가 발생한다. 긴급한 조치로서 침해사고 확산에 이용되는 접속경로(도메인, IP주소, 포트번호 등)에 대해 주요 정보통신서비스 제공자(ISP)에게 차단조치 명령이 필요하다. 이러한 조기 대응을 위한 해당 접속경로에 대한 차단조치 명령의 법적 근거를 마련할 필요성이 있다.

유형	개정안	주요 내용
현행 법 제48조의2 개정	제48조의2(침해사고의 대응 등) ① (현행과 동일) ② 방송통신위원회는 침해사고에 대한 긴급한 조치로서 정보통신서비스 제공자 및 집적정보통신시설 사업자에게 침해사고의 확산에 이용되는 접속경로(도메인이름, 인터넷 프로토콜 주소, 포트번호 등을 말한다)의 차단을 명할 수 있다. ③~⑦ (현행 ②~⑥과 동일)	○ 현행 법 제48조의2에 침해사고에 대응하기 위한 추가적인 조치로서 침해사고 확산에 이용되는 접속경로에 대한 차단조치 명령 근거 마련

4. 악성프로그램 감염PC의 인터넷 접속제한 명령

근본적 문제해결을 위해 감염PC를 임시 차단하는 것이 가장 효과적인 조치이며 중대한 피해확산을 방지할 수 있는 조치이다. 좀비PC의 DDoS 공격은 특정 1~2개 사이트만을 대상으로 이루어지기도 하지만, 동시에 다수 사이트를 대상으로 이루어지기도 하여 정부가 모든 피해사이트에 악성프로그램에 감염된 좀비PC의 IP주소를 알려주는 것은 실효성도 없고 현실적으로 불가능하다. 좀비PC의 DDoS 공격은 공공의 안녕질서에 대한 직접적인 위협이 명백하게 존재하는 경우로서 이에 대응하기 위해서는 인터넷 차단 이외에 다른 수단이 없다. 또한 악성프로그램 감염PC의 인터넷 접속제한 조치도 여러 법적 절차를 통해 엄격한 조건하에서 가능하도록 구체적으로 규정한다면 기본권 침해의 최소성 원칙에도 부합할 수 있다.

악성프로그램 감염PC에 대한 인터넷 접속제한 명령은 좀비PC가 다른 정보시스템·정보통신망에 위해를 가하거나 급박한 위험이 있는 때에 한정하는 조치이며, 1차적으로 침해사고 상황, 치료방법 등 보호조치를 요청한 후에, 이를 이행하지 않는 경우에 한하여 2차적으로 인터넷 접속을 일정 기간을 정하여 제한하고 있기 때문에, 이는 대다수 국민의 통신권을 보호하기 위한 최소한의 조치이다.

1차적으로 요청하는 사항은 '침해사고의 구체적인 내용 및 정보통신망 등의 장애 발생 상황, 이용자에게 보호조치를 요청할 수 있는 사유 및 요청하는 방

법, 이용자가 하여야 할 보호조치의 내용, 이용자가 보호조치를 이행하지 아니할 경우 정보통신망으로의 접속제한 기간, 이용자의 보호조치 불이행에 대하여 부당한 접속제한을 한 경우 이용자의 이의제기 절차'로 규정할 수 있다.

국가위기수준의 침해사고가 발생한 경우, 감염PC에 대한 인터넷 접속을 제한할 수 있는 법적 근거를 마련할 필요가 있다. 인터넷 접속제한조치의 기본권 침해가능성을 고려하고 기존의 법률 조항에서 이와 유사한 내용을 담고 있지 아니하므로 별도의 조문으로 신설할 필요성이 있다. 정보통신망법 제47조의3 제2항에 의하면, 주요 정보통신서비스 제공자(ISP)는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다. 그러나 방송통신위원회가 침해대응을 위한 접속제한의 명령을 할 수 있는 법적 근거는 현재 존재하지 않는다. 따라서 인터넷 접속제한 조치에 대한 절차를 보완하여 악성프로그램 감염PC의 인터넷 접속제한에 관한 기본적인 사항만을 법률에서 규정하고, 단계별 조치에 대해서는 하위법령에 규정하는 것이 적절하다.

유형	개정안	주요 내용
별도 조문 신설	제48조의7(침해사고의 조치 등) ① 방송통신위원회는 정보통신망의 안정적 운영을 중대하게 방해하거나 심각한 장애를 초래할 위험이 있는 국가위기수준으로서 대통령령이 정하는 침해사고가 발생한 경우에는 정보통신서비스 제공자로 하여금 이용자에 대하여 다음 각 호의 조치를 취하도록 명할 수 있다. 1. 인터넷주소의 차단 2. 정보통신망으로의 접속 제한 3. 그 밖의 대통령령으로 정하는 침해사고 대응 조치 ② 정보통신서비스 제공자는 제1항에 따른 조치의 대상이 법인 또는 단체인 이용자의 경우에는 해당 법인 또는 단체의 침해사고 관련정보를 방송통신위원회에 알려	○ 국가위기수준의 심각한 침해사고가 발생한 경우에 한하여 감염PC에 대하여 인터넷 접속제한 등 조치

	야 한다. ③ 방송통신위원회가 제1항 및 제2항에 따른 필요한 조치를 하는 경우에는 이용자에게 접속 제한의 이유 및 근거, 접속 제한의 해제조건 등을 알려야 하고, 필요한 조치의 사유가 종료되었다고 인정될 때에는 지체없이 그 조치의 해제를 명하여야 한다.	

5. 침해사고의 원인분석을 위한 자료제출 요구

침해사고의 원인분석을 위해 주요 정보통신서비스 제공자(ISP) 등 특정한 사업자들은 침해사고 관련 자료를 방송통신위원회나 한국인터넷진흥원에 제출하도록 해야 한다. 일반 이용자에게 백신사용의무 또는 악성코드 제거의무 위반 혐의가 있다는 이유만으로 자료제출의 요구 및 검사를 받도록 하는 것은 불가능하다. 일반 이용자에 대한 자료제출 요구가 적용될 수도 있다는 오해의 소지가 있으므로, 개정안은 적용범위에서 제8조부터 제17조까지의 규정으로 한정함으로써 제7조(이용자의 책무)를 적용범위에서 배제하여 개정안을 작성할 필요가 있다. 개정안 제19조 제1항 제1호를 '제8조부터 제17조까지의 규정을 위반하거나 위반에 대한 신고 또는 민원이 접수된 경우'로 수정하여 혐의만으로는 자료제출을 요구하지 않도록 하여야 한다. 개정안은 PC방 등 다중을 상대로 영업을 하는 '사업자'가 백신을 미설치한 경우 시정을 명할 수 있는 권한을 부여하고 있고, 웹사이트 운영자가 악성프로그램 정기점검의무를 해태하거나, 악성프로그램 삭제명령을 위반한 경우 등에 한하여 시정조치 또는 과태료 처분을 할 수 있다. 사업자의 법위반 혐의가 포착된 경우 위반사실을 확인하기 위해 정부가 자료제출, 현장검사 등을 행하는 것은 중대한 침해사고로 확산되는 것을 방지하기 위한 필수적 절차이다.

정보통신망법 제48조의4 제4항에는 "방송통신위원회는 침해사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 침해사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민·관 합동조사단에게 관계인의 사업장에 출입하여 침해사고 원인을 조사하도록 할

수 있다. 다만, 「통신비밀보호법」 제2조 제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다."라고 규정하고 있다. 이 법률 조항은 침해사고의 대응을 위한 근거조항이지만, 실제적으로 필요한 공격 로그 수집(IP목록 등)에 대한 명확한 근거조항이 될 수 없다. 침해사고의 원인분석을 위한 사고관련 로그 기록 등은 통신사실확인자료에 해당될 수 있어 통신비밀보호법에 저촉될 수 있다. 현행 법률로서는 침해사고의 원활한 대응에 한계가 있다. 따라서 정보제공의 명확한 기준 마련을 위한 고시 제정에 대한 법적 근거를 마련하는 것이 필요하다. 방송통신위원회의 고시에는 정보제공 기관별 제공해야 하는 정보량, 정보의 유형 등을 구체적으로 명시하면 된다.

유형	개정안	주요 내용
현행 법 제48조의2 개정	제48조의2(침해사고의 대응 등) ① (현행과 동일) ② 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 침해사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 방송통신위원회가 정하여 고시하는 침해사고 관련 정보를 방송통신위원회나 한국인터넷진흥원에 제공하여야 한다.	○ 침해사고 관련정보에 대해 구체적으로 고시로 규정함 ○ 고시에서 침해사고 관련정보 제공자에 따른 정보제공 유형 및 범위를 구체적으로 규정

방송통신위원회 고시 제0000-000호
국가 정보통신망 안전에 필요한 침해사고 관련정보의 정의 및 정보제공 범위

1. 침해사고 관련정보는 **침해사고 이상징후 모니터링에 필요한 통계정보 및 대국민 침해사고 피해관련 통계정보**를 말하며 다음과 같다.
① 트래픽 소통량 통계 (BPS/PPS)
② 포트별 소통량 통계 (BPS/PPS)
③ 프로토콜별 소통량 통계 (BPS/PPS)
④ 사이버 공격유형 탐지 통계 (IDS, F/W, ESM 등 보안장비 로그 통계)
⑤ 악성코드 피해신고 및 탐지 통계

2. 침해사고 관련정보 제공자가 제공해야할 정보는 다음과 같음.

정보제공 기관	제공정보	정보제공자 근거
주요정보통신서비스 제공자(ISP)	트래픽, 포트, 프로토콜 소통량, 공격유형 탐지 통계	망법 제48조의2
집접정보통신시설 사업자(IDC 등)	공격유형 탐지 통계	망법 제48조의2
주요정보통신기반시설보호계획 및 보호지침의 적용을 받는 기관 (기반시설)	공격유형 탐지 통계	시행령 제57조
정보통신서비스 제공자의 정보통신망 운영현황을 주기적으로 관찰 및 침해사고 저오를 제공하는 자 (보안 관제업체)	공격유형 탐지 통계	시행령 제57조
기간통신사업자	트래픽, 포트, 프로토콜 소통량, 공격유형 탐지 통계	고시 제2008-122호
포털서비스를 제공하는 사업자	공격유형 탐지 통계	고시 제2008-122호
호스팅서비스를 제공하는 자	공격유형 탐지 통계	고시 제2008-122호
게임물을 정보통신망을 이용하여 제공하는 사업자	공격유형 탐지 통계	고시 제2008-122호
인터넷 멀티미디어 방송 제공사업자	트래픽, 포트, 프로토콜 소통량, 공격유형 탐지 통계	고시 제2008-122호
컴퓨터바이러스 백신소프트웨어 제조자 (백신업체)	악성코드 피해신고 및 탐지 통계	시행령 57조

※ 인터넷프로토콜 주소를 할당받아 독자적으로 저오통신망을 운영하는 민간사업자중 침해사고관련 정보 제공자의 범위(방통위고시 제2008-122호)

3. **제공정보의 규모는 각 기관의 회선대역폭, 시스템 규모 등을 감안하여 전체 제공 가능한 규모의 1/2 이상이어야 한다.**

Ⅳ. 결 론

1. 현행 우리나라 정보통신망법은 네트워크(망) 또는 정보통신기반 보호를 중점으로 하고 있어 컴퓨터 이용자의 보호 및 실효성 있는 침해사고 예방 및

대응에 한계가 있다. 이용자 컴퓨터가 악성프로그램에 감염된 경우 해당 이용자에게 감염사실과 치료방법을 알리고 치료를 지원하는 근본적 대응이 필요하며, 악성프로그램 감염 예방을 위해 백신소프트웨어 등 보안프로그램 이용을 활성화하고 인터넷 게시판 등을 통해 유포·확산되는 악성프로그램을 삭제하는 조치가 필요하다. 또한 일정 수준 이상의 중대한 침해사고 발생시 피해 확산을 최소화할 수 있는 실효성 있는 긴급대응조치가 확보되어야 한다. 컴퓨터 보안프로그램 이용·보급 활성화, 웹사이트에 은닉된 악성프로그램 삭제, 악성프로그램 감염컴퓨터의 치료 지원, 심각한 침해사고 발생시 실효성 있는 대응체계 확립 등 이용자 컴퓨터의 보안 강화를 위한 새로운 입법이 필요하다.

2. 최근 디도스(DDoS : 분산 서비스 거부) 공격 등 침해사고 등이 국내 인터넷 시스템을 심각하게 위협하고 있고, 경제적·정보적 피해가 급증하고 있는 실정이다. 이러한 침해사고에 대비한 개정된 법률이 새롭게 필요하며 이를 반영한 입법이 절실하다. 침해사고 확산 방지 및 조사를 위해서는 침해사고 발생 후 사후적 조치도 중요하지만, 사전 예방적인 조치를 강화하는 방향으로 입법화함이 필요하다.

3. 악성프로그램 등에 의한 침해사고에 대한 대응책으로서 법률상 조치가 국민의 기본권 침해를 최소화하는 방법을 선택해야 할 뿐만 아니라, 침해사고 발생 후 다른 추가적이고 광범위한 사고가 발생하지 않도록 하기 위해 신속하고 효과적인 법적 수단을 마련해야 한다.

참고문헌

김진섭, "위험관리 기반 침해사고 조기 대응 체계 구축 사례", 「정보보호학회지」 제20권 제6호, 2010. 12.

박정훈, "인터넷서비스제공자의 관리책임", 「공법연구」 제41집 제2호, 2012. 12.

손승우, "사이버 보안의 예방 수단을 위한 법제 분석", 「연세 의료·과학기술과 법」 제2권 제2호, 2011. 8.

안정상, "악성프로그램 확산방지 등에 관한 법률안(좀비PC법) 평가", 「국회」,

2011.
이부하, "비례성원칙과 과소보호금지원칙", 「헌법학연구」 제13권 제2호, 2007. 6.
이기철, "헌법재판소는 비례의 원칙에 목적의 정당성을 포함시켜도 좋은가?", 「공법연구」 제35집 제1호, 2006. 10.
최경진, "가상세계에 대한 법적 고찰", 「문화 미디어 엔터테인먼트 법」, 중앙대 문화미디어 엔터테인먼트법연구소, 2011.
홍승희, "정보통신범죄의 전망", 「형사정책」 제19권 제1호, 2007.
Josef Isensee (이승우 역), 「국가와 헌법」, 세창출판사, 2001.

[Abstract]

A Legislative Policy on a Revision of 「Information and Communications Network Law」

Lee, Boo-Ha
Professor, Law School, Yeungnam University

There are some limitations to protect computer users and prevent computer security incident. Because our law focuses on protection for network or information · communications. So we have to revise the law and make a clause to prepare for serious computer security incidents just like DDos (distributed denial of service) attack.

A revision should contain 5 clauses to prepare for those incidents.

First of all, a clause about request for access to a PC infected by malignant code should set up. Because it is important to promptly do causual analysis and nonproliferation of incidents.

Second, it is requested for a system operator to not only carry out a

regular inspection but also immediately eliminate malignant code when he found that in his website. If he did not, he might be imposed a penalty following a clause.

Third, there should be a clause of an order as emergency action. When a accident in the internet happens, internet service providers(ISP) should close up routes to spread of the accident(Domain, IP address, Port number, etc.).

Fourth, to prevent the spread of immediate damages, a PC infected by malignant code is limited to access. Therefore an order to limited to access is required.

At the end of these, it is essential to send incidents's information to Korea Communications Commission and Korea Internet & Security Agency. Because these organizations can analyze causes of incidents and to make a preparation for happening same incidents.

Key words : the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., malignant code, request access in PC infected by malignant code, internet service providers(ISP), DDoS(distributed denial of service)