「악성프로그램 확산방지 등에 관한 법률(안)」의 주요내용 및 발전방향에 관한 소고

한정연*

최근 인터넷 기술 및 서비스 발달로 DDoS 공격, 개인정보 유출 등 사이버 침해사고가 단순 해킹에서 국가안보를 위협하고 사회혼란을 조장하는 조직적 · 지능화된 사이버테러로 변화함에 따라, 침해사고에 대한 효율적 예방 및 대응 체계를 규율하는 법제 마련의 필요성이 지속적으로 제기되고 있다. 이에 본고에서는 기존 사이버보안 법제의 문제점과 한계를 살펴보고 「악성프로그램 확산방지 등에 관한 법률(안)」(통상 "좀비PC법(안)"이라 함)의 제정 필요성과 바람직한 입법 방향을 제시해 보고자 한다.

* 한국인터넷진흥원 법제연구팀 연구원(hjy@kisa.or.kr)

Ⅰ. 서론

IT 기술이 발전함에 따라 인터넷을 통한 해킹, 개인정보 유출 등 사이버보안 침해 사고는 점차 지능화된 사이버테러 형태로 변화하고 있다. 최근 악성 코드의 제작에도 새로운 기술과 개념이 도입되고 있으며, 피해 범위도 컴퓨터 시스템에서 태블릿 PC, 스마트폰, RFID태그 등 네트워크로 상호 연동되는 스마트 기기 전반으로 확장되고 있다.

악성프로그램은 단순히 사이버 공간을 어지럽히는 것에 그치는 것이 아니라 국가나 기업체, 이용자에 대한 개인정보 유출 등 국가 전체의 재산과 이익에 막대한 피해를 야기한다. 하지만, 이를 규율하는 현행 정보보호 법제는 기존 네트워크와 기반시설 중심의 대응조치를 규정하고 있어 다양한 정보처리장치를 대상으로 새롭게 발생하는 악성코드에 효율적으로 대응하기에는 다소 한계가 있다는 지적이 지속 제기되어 왔다. 물론, 사이버 공격의 특성상 이를 근본적으로 막기는 쉽지 않은 것이 사실이다. 그러나 정부와 사업자, 이용자가 함께 협력하여 공격에 선제적으로 대응하고 정보보안 강화를 위한 체계적인 대응 절차를 법제화하는 것은 사이버 침해사고 대응체계를 효율화하는 측면에서 의미가 있을 것으로 본다.

이에 본고에서는 사이버보안 체계의 강화를 위한 「악성프로그램 확산방지 등에 관한 법률(안)」(이하 "좀비PC법(안)")의 제정 필요성을 제시해 보고자 한다. 특히, 기존의 침해사고 대응에 있어서 현행 정보보호 법제가 가지는 한계와 문제점을 확인해 보고, 이를 통해 제정안의 주요내용과 향후 추진 방향을 검토해보기로 한다.

Ⅱ. 사이버보안 법제 개선 필요성

1. 사이버 침해사고 발생현황

2013년 6월 25일 주요 정부기관 웹사이트를 대상으로 한 사이버 테러가 발생하여 우리 사회를 큰 혼란에 빠트렸다. 이는 얼마 전에 주요 금융기관 서버를 대상으로 했던 3.20 사이버 테러가 잊혀지기도 전의 일이었다.[1] 사이버 테러는 초기의 단순한 해킹사고에서 분산서비스

1 정 완, "한·미 사이버보안 법제 동향에 관한 고찰", 「경희법학」 제48권 제3호, 2013.9, 213면.

거부(DDoS) 공격 등으로 진화하며 주요 기업 및 정부기관을 대상으로 확대되고 있다. 우리나라 최초의 사이버 테러사건인 2003년도 1.25 대란 이후, 7.7, 3.4 DDoS 공격, 농협 전산망 해킹, 중앙일보 해킹사건, 방송사 · 금융기관 전산망 마비 사건 등에 이르기까지 정부기관 및 주요 기업을 대상으로 한 DDoS 공격 등 사이버 테러는 지속 증가하는 추세이다.

〈표 1〉 국내 주요 사이버 침해사고 발생현황

구 분	발생원인 및 내용
국가기관 해킹	원격 명령 실행
7.7 DDoS 공격	웹하드 업데이트 서버를 통해 악성프로그램 유포 및 DDoS 공격
3.4 DDoS 공격	
농협 전산망 해킹	유지보수업체 직원 노트북에 악성프로그램을 설치하여 정보유출
중앙일보 해킹	악성프로그램을 이용하여 해당 서버 파괴 및 정보유출
3.20 사이버 테러	악성프로그램 유포 등을 통해 금융사 및 방송사 전산 마비

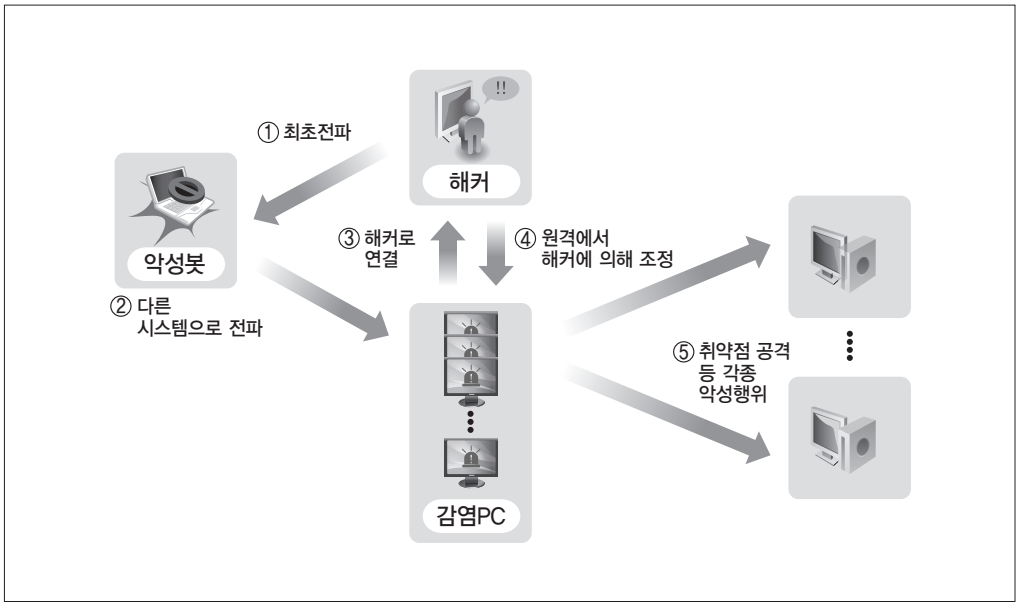
DDoS(Distributed Denial of Service Attack) 공격은 '분산'이라는 용어에서도 알 수 있듯 해커가 사전에 악성프로그램을 유포하여 이른바 좀비PC를 만든 다음, 악성프로그램에 감염된 좀비PC를 일제히 동작하게 하여 특정사이트나 시스템을 공격하는 방식이다. 공격 시나리오를 전체적으로 살펴보면, 컴퓨터를 해킹하여 사용자 몰래 악성프로그램을 설치해 놓거나 이메일 등을 통해 악성프로그램 유포하여 좀비PC를 만든 다음, 좀비PC로 하여금 공격 대상 서버에 대량의 신호 또는 데이터를 전송하여 서버의 정상적인 서비스를 마비시켜 해당 기관의 고유 업무를 방해하도록 하는 진화된 해킹 공격 방법이다.[3]

이러한 일련의 공격 행위로 발생하는 DDoS 피해액은 2003년 1.25. 대란 때에는 1,675억원, 2009년 7.7. DDos 공격 때에는 544억원, 2013년 3.20. 사이버공격 때에는 8,800억원으로 추정[4] 되고 있어 사이버 공격으로 인한 국가나 기업체, 개인의 유 · 무형의 경제적 피해

2 3.4 DDoS 공격은 사용자 개인 PC가 DDoS 공격에 이용된 점과 악성코드 유포지가 국내 P2P 사이트들을 이용했던 점 등에서 이전 7.7 DDoS 공격과 많은 유사점이 있지만, 한층 더 진화된 공격 방식을 사용하였다는 점에서 차이가 있다. 7.7 DDoS의 경우, 악성코드를 유포한 웹하드 업체가 3곳이었던 것에 반해 3.4 DDoS 악성코드는 6곳을 통해 유포되었으며, 보다 진화된 악성코드를 사용하여 청와대, 국방부, 외교통상부, 국회, 네이버블로그, 네이버메일, 옥션, 농협공격 대상 사이트가 3배 이상 증가하였다. 이러한 공격 형태는 사이버 공격이 갈수록 정교화, 지능화되고 있음을 잘 보여주는 사례라고 할 수 있다.(염흥열, "3.4. DDoS 공격과 7.7. DDoS 공격은 어떻게 다르나", 2011.4.1, 방송통신위원회 웹진).

3 권양섭, "사이버 범죄 처벌규정의 문제점과 대응방안", 한국법학회, 「법학연구」 제53집, 2014.3.6., 186면.

4 신영웅 외 3인, "국가 사이버보안 피해금액 분석과 대안–3.20 사이버 침해사건을 중심으로", 「국가정보연구」 제6권 1호, 2013.6, 151면.



[그림 1] DDoS 공격 동작 원리

가 매년 지속적으로 증가하고 있음을 알 수 있다.

사이버 공격은 적은 비용으로도 막대한 경제적 피해를 야기할 수 있고, 그 공격 흔적을 찾기 어려운[5] 반면 피해 확산속도 및 침해규모는 일반 테러보다 훨씬 더 크다는 점에서 국가 전체에 심각한 위협으로 작용하게 된다. 따라서 사이버 공격에 대한 효율적 대응을 위해서는 단순한 침해 대응에 그치는 것이 아니라, 민 · 관이 긴밀하게 협력하여 고도화된 예방 · 대응 체계를 구축해야할 필요성이 있다.

2. 국내 사이버보안 법제의 문제점과 한계

현행법 상 사이버 공격 대응에 관한 법률로는 「형법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"), 「정보통신기반 보호법」, 「국가정보화 기본법」 등이 있다. 구체적으로 「정보통신망법」은 정보통신망의 보안을 위한 사업자의 보호조치 및 악성프로

5 DDoS 공격자는 대부분 상대적으로 해킹 등에 미온적인 중국 등을 이용하기 때문에 역추적이 쉽지 않고, 공격에 사용되는 좀비PC 역시 서버도 있지만 대부분 보안에 취약한 Windows 기반의 가정용 PC이며 더구나 DHCP를 이용하기 때문에 IP를 알아도 역추적하거나 처리하기가 쉽지 않은 것이 현실이다.(김범수 외 13인, 스마트 시대 정보보호 전략과 법제도, 한국학술정보, 2011.12.30, 188면 참고).

그램 유포 등 침해행위 금지와 이에 대한 정부의 대응조치 등[6]을 규율하며, 「정보통신기반 보호법」은 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위한 취약점 분석 및 평가, 사이버 공격 금지 등에 대한 사항을 규정하고 있다.[7]

하지만 이러한 기존 법체계는 정보통신망, 기반시설 등의 보호를 위한 정부 및 사업자의 사후 조치를 중점으로 규정되어 있어,[8] 일반 이용자 컴퓨터 자체의 보안 허점을 이용한 공격에는 법 적용상 한계가 있는 실정이다. 예를 들어, 첫째, 악성코드 감염 PC로 인한 침해사고 발생 시 원인분석 및 정보 수집을 위해서는 침해받은 시스템에 접근하여 신속한 대응조치를 취해야 하지만 현행 「정보통신망법」의 시스템 접근요청에 대한 규정만으로는 피해 입은 사업자의 동의와 협조를 구하는데 현실적인 어려움이 있다. 이로 인해 악성코드 샘플채집을 위한 가입자 섭외 거부가 빈번하여 감염 PC에 대한 접근이 지연되고 있으며, 이러한 시간 지연은 전체 침해사고 대응 절차를 지연시킬 위험이 있다.

둘째, 침해사고 발생에 대한 적극적 대응에도 한계가 있다. 「정보통신망법」 제47조의3제2항은 침해사고 발생시 정보통신서비스 제공자가 이용약관에 따라 이용자에게 보호조치를 요청하고 미이행시 접속을 제한할 수 있도록 규정하고는 있으나, 정보통신서비스 제공자는 접속 제한 등의 조치로 인해 부담할 수 있는 손해배상책임 등의 문제로 적극적인 대응을 하지 않기 때문에 그 규정의 실효성에 한계가 있는 실정이다.

셋째, 감염 PC의 상당수는 일반 이용자 PC임에도 불구하고 현행 「정보통신망법」 및 「정보통신기반 보호법」은 정보통신망, 주요정보통신기반시설 보호를 위한 정부 및 사업자의 조치를 중점으로 하고 있다. 대다수 PC 이용자들이 자신의 컴퓨터가 감염된 사실을 몰라 피해가 확산되고 있는 현실을 고려해볼 때, 백신프로그램 이용 활성화, 소프트웨어 보안패치 등 보안조치, 웹사이트를 통한 악성프로그램 유포 방지 등 이용자 컴퓨터 보안 강화를 위한 실효성 있는 법체계 마련이 시급하다고 할 것이다.[9]

---

6 정보통신서비스 제공자 및 집적정보통신시설 사업자의 보호조치(제45조제1항 및 제46조제1항), 정보보호 관리체계 인증(제47조), 정보통신망 침해행위 등의 금지(제48조), 정부의 침해사고 대응 및 원인분석(제48조의2, 제48조의3, 제48조의4) 등.

7 주요정보통신기반시설 침해행위 등의 금지(제12조), 취약점 분석 및 평가(제9조), 침해사고 대응 및 복구조치(제11조, 제14조) 등.

8 「정보통신망법」에서 규정하는 제46조의2(집적정보통신시설 사업자의 긴급대응), 제48조의2(침해사고 대응 등) 대응조치의 적용범위는 주요정보통신서비스 제공자, 집적정보통신시설 사업자 등에 한정되어 있다.

9 김중권외 8인, "정보통신망법 개정 연구", 방송통신위원회 연구결과보고서, 2012.12, 35면.

3. 별도 입법의 필요성

앞서 살펴본 바와 같이, 현행 정보보호 법제는 주로 체제(네트워크) 중심의 보호를 중점으로 규정되어 있음을 알 수 있다. 하지만 최근 사이버 침해사고는 컴퓨터 뿐 아니라 이용자의 PDA, 스마트폰 등 다양한 정보처리장치를 통해 확산 · 증대되고 있다. 따라서 정보처리장치가 악성프로그램으로부터 공격을 받거나 공격기지로 악용되는 것을 막기 위해서는 보다 근본적인 대응체계를 마련할 필요가 있다.

〈표 2〉 현행 「정보통신망법」과 「좀비PC법(안)」 비교[10]

구 분	정보통신망법	좀비PC법(안)	비 고
적용범위	• 정보통신망(제2조제1항제1호) – 정보통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터 이용기술을 활용한 정보통신체제	• 컴퓨터(안 제2조제1항제1호) – 개인PC, 서버컴퓨터, 셋톱박스, 스마트폰 등 모바일 휴대단말기	• 체제(네트워크) 중심의 「정보통신망법」으로는 규율하기 어려웠던 이용자 컴퓨터에 특유한 법규 제정
적용대상	이용자		
	• 이용자(제2조제1항제4호) – 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자	• 이용자(안 제2조제1항제2호) – 컴퓨터 등 정보처리장비를 이용 · 관리하는 개인, 법인, 단체(행정기관 등 제외)	• 정보통신서비스 이용자만 포함되는 「정보통신망법」과 달리 컴퓨터를 이용 · 관리하는 개인, 법인, 단체 등이 규율 대상에 포함
	사업자		
	• 정보통신서비스 제공자 (제2조제1항제3호) – 전기통신사업자 및 전기통신역무를 이용하여 정보를 제공하거나 매개하는 자 • 주요정보통신서비스 제공자 (제46조의3제1항제1호) – 전국적으로 정보통신망서비스를 제공하는 자	• 인터넷접속서비스 제공자 (안 제8조제1항) – 전기통신사업자로서 인터넷접속서비스를 제공하는 자 • 포털서비스 제공자 (안 제8조제1항) – 전기통신사업자로서 검색, 정보제공 등 서비스를 제공하는 자 • 컴퓨터 제조 · 수입 · 판매자 (안 제8조제2항) • PC방 사업자 등 (안 제8조제3항) • 웹사이트 운영자(안 제10조)	• 「정보통신망법」 상 주요정보통신서비스 제공자에는 전화 등 인터넷과 무관한 사업자도 포함되는 대신 지역인터넷망 사업자인 종합/중계유선방송 사업자는 불포함 • 「좀비PC법(안)」은 인터넷접속서비스를 제공하는 모든 사업자가 대상

10 제19대 국회 미래창조과학방송통신위원회 수석전문위원 검토보고서, 2013.6.3, 7면 참고.

「좀비PC법(안)」은 정부, 사업자, 이용자가 책임과 의무를 분담하고 상호 긴밀하게 협력 · 지원하는 민관 협력적 거버넌스를 규율하고 있다. 컴퓨터를 이용 · 관리하는 개인, 법인, 단체 등을 폭넓게 규율하고 정보통신서비스 제공자 뿐 아니라 지역인터넷망사업자인 종합 · 중계유선방송사업자 등 인터넷접속서비스를 제공하는 모든 사업자를 대상으로 함으로써 새로운 보안 위협에 대한 보다 강화된 대응체계를 구축한다. 또한, 침해사고 긴급 대응조치 뿐 아니라, 사전예방을 통한 피해 최소화 방안을 규율하고 있다는 점에서 기존 정보보호 법체계와 구별된다.

인터넷 상의 좀비PC 상당수가 일반 이용자PC라는 점을 고려해볼 때, 이용자에 대한 정보보호를 강화하는 새로운 사이버 보안법제 정립이 필요한 시점이라고 본다. 이에 따라, 이하에서는 보다 구체적으로 「좀비PC법(안)」의 주요내용과 법 적용에 따라 예상되는 법적 쟁점에 대하여 살펴보기로 한다.

Ⅲ. 「좀비PC법(안)」의 주요 내용

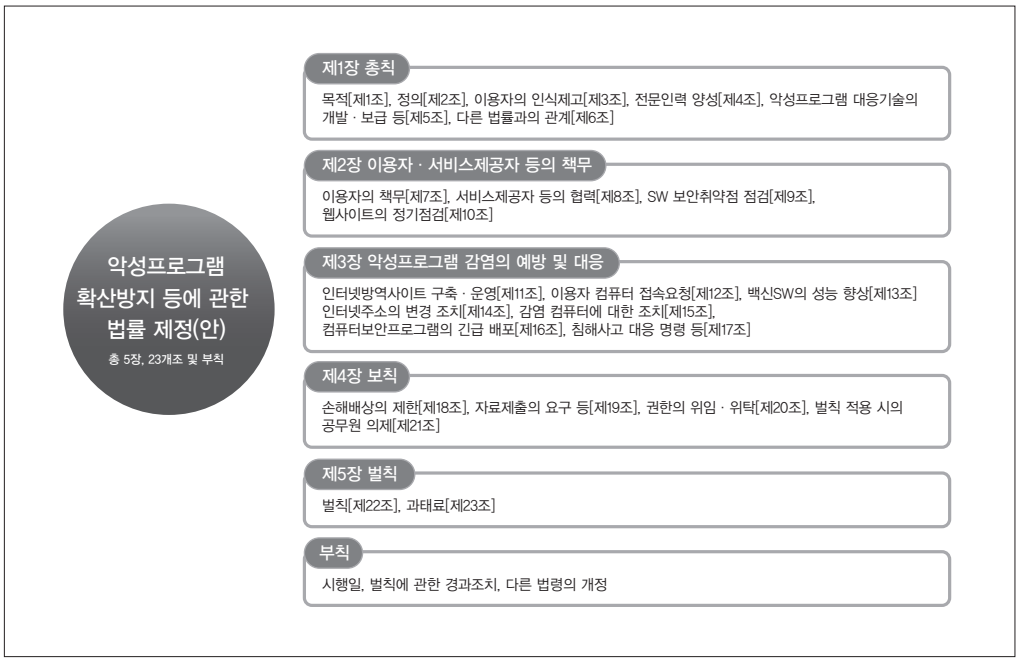
1. 구성 체계 및 주요내용

「좀비PC법(안)」은 총5장 24개 조문으로 구성되어 있으며, 제1장은 총칙, 제2장은 이용자 · 서비스제공자 등의 책무, 제3장은 악성프로그램 감염의 예방 및 대응, 제4장은 보칙, 제5장은 벌칙에 대한 내용을 규정하고 있으며, 부칙은 제정에 따른 경과규정 등 3개 조문으로 구성되어 있다.

그 주요 내용을 ①악성프로그램 확산방지를 위한 대국민 인식제고, ②정부의 침해사고 예방조치 규정, ③이용자의 책무와 사업자의 협력 및 지원을 위한 근거규정 마련, ④악성프로그램 확산방지를 위한 체계 구축, ⑤악성프로그램 감염에 대한 대응조치 강화 등으로 구분해 볼 수 있다.

1) 악성프로그램 확산방지를 위한 대국민 인식제고(안 제3조 및 제4조)

인터넷 침해사고는 네트워크를 통해 신속히 전파되어 단시간에 광범위한 피해를 입을 수 있는 만큼, 침해사고 발생 시 정부와 사업자가 미리 준비된 매뉴얼에 따라 신속하게 이용자



[그림 2] 「좀비PC법(안)」의 구성 체계

에게 침해사고 상황을 알림으로써 피해 발생을 최소화하는 것이 중요하다. 이에 대하여 안 제3조는 정부에서 실시하는 대응훈련에 대하여 ISP, 포털, 언론 등 필요한 범위의 모든 사업자가 모두 참여할 수 있도록 규정하고, 이용자가 침해사고 위험성에 대해 인식하고 컴퓨터를 안전하게 이용할 수 있도록 정보보호수칙 및 기준[11]을 제정하여 권고할 수 있음을 명시한다. 이는 정부가 시행하는 각종 사업과 활동에 대한 명확한 법적 근거를 마련함으로써 보다 적극적인 교육 · 홍보 활동을 추진하기 위한 것이라고 할 수 있다.

또한, 안 제4조는 최근 등장한 새로운 유형의 악성프로그램과 다양한 형태의 침해사고 발생에 대응하기 위해 정부가 전문 인력 양성에 대한 시책을 수립하고 시행할 수 있음을 규정하였는바, 이는 상대적으로 정보보안 전문 인력에 대한 대우가 열악한 현실[12] 을 개선하고 정부의 체계적인 지원을 통해 우수한 인력을 확보하려는 목적으로 보인다.

11 현재 한국인터넷진흥원(KISA)은 「정보보호 실천수칙」, 「메신저 이용가이드」, 「온라인 게임 이용시 주의사항」, 「무선랜 안전하게 이용하기」, 「패스워드 선택 및 이용 안내서」 등 이용자가 준수해야 할 정보보호 수칙 또는 기준 등을 제공하고 있다.

12 현재까지 우리나라의 경우 정보보안에 대한 전문인력의 절대적 필요성을 인식하고 있는 수준은 미국, 일본 등에 비하여 매우 낮은 수준이며, 미국·일본을 비롯한 여러 나라에서 시스템 및 정보보안제도를 이미 법제화, 제도화하여 시행하고 있는 만큼, 우리나라도 이에 부응하여 적절한 제도적인 장치를 마련할 필요가 있다.(박재용, "정보보안 전문인력 양성을 위한 교육과정 분석", 경영정보연구 제31권 제1호, 2012.3, 162면 참고).

2) 정부의 침해사고 예방조치(안 제5조, 제9조제2항 및 제3항, 제10조제2항, 제14조)

국내 DDoS 공격은 세계 최고 수준의 정보통신 인프라를 기반으로 점차 지능화되고 고도화되고 있기 때문에 효과적인 대응조치뿐 아니라 사이버 공격에 능동적 대처하기 위한 사전 조치가 필수적이다. 「좀비PC법(안)」은 정부가 컴퓨터 보안프로그램의 이용 및 보급을 촉진하고 악성프로그램의 삭제 원격지원, 유해트래픽 차단 기술 등 대응기술의 개발과 보급 등을 지원할 수 있도록 하여 침해사고 예방을 위한 정부 예방조치의 효율성을 높이고 있다.

구체적으로 정부는 우수 컴퓨터 보안프로그램을 선정하여[13] 이용자에게 관련 정보를 제공함으로써 이용자가 우수한 품질의 보안프로그램을 사용할 수 있도록 장려하고 보안프로그램의 품질을 제고할 수 있도록 규정한다. 또한 좀비PC를 효율적으로 관리할 수 있는 기술 개발을 위한 시범사업을 실시할 수 있음을 명시하여 이용자의 프라이버시(Privacy)나 통신권을 침해하지 않으면서도 보안프로그램의 이용 및 보급을 촉진하는 등 정부의 예방조치를 강화하여 규정하고 있다.

3) 이용자의 책무와 사업자의 협력 및 지원(안 제7조, 제8조, 제9조, 제10조)[14]

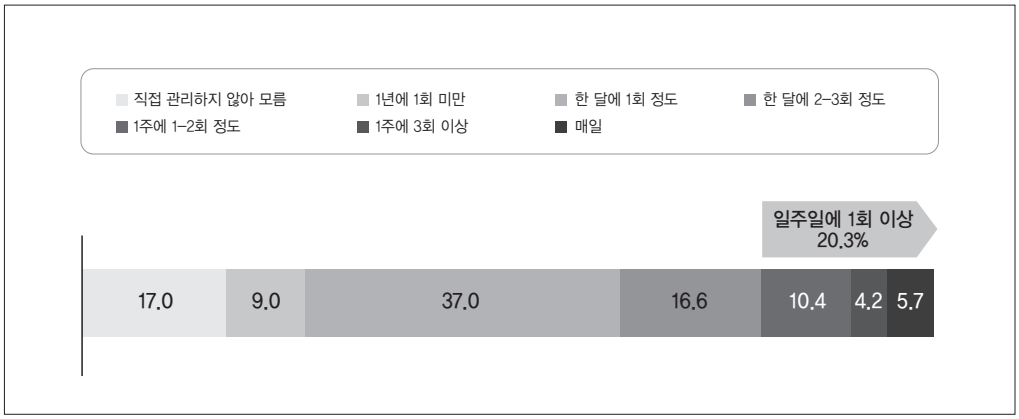
(1) 이용자의 책무(안 제7조)

최근 발생하는 침해사고의 주요 원인 중 하나는 이용자가 백신설치 등 기본적인 보안수칙을 지키지 않아 악성프로그램에 감염된 컴퓨터가 좀비PC가 되어 DDoS 공격에 악용되는 것으로 파악되고 있다.[15] 이에 따라 백신프로그램 설치 등을 더 이상 이용자의 임의적인 판단에만 의존할 수 없다는 사회적 공감대가 형성되고 있으며, 「좀비PC법(안)」은 이러한 판단에서 정보보호를 위하여 이용자가 준수하여야 할 책무를 규정하고 있다. 물론, 백신 프로그램을

13 다만, 우수 보안프로그램 선정 등에 대한 신뢰성·공정성의 문제가 제기될 수도 있는 만큼, 전문 기관이나 이용자 단체 또는 사업자 단체를 통하여 실시하도록 하는 것도 하나의 방법이다. 특히, 독일의 경우 「연방 정보기술의 보안 강화를 위한 법률(Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes)」('09.8.14)에서 '연방정보기술보안청(BIS)'이 악성프로그램의 예방과 탐지를 위하여 정보기술 제품과 서비스의 보안상의 하자에 대한 경고를 할 수 있도록 하고, 이용자에게 특정한 보안프로그램의 설치를 추천할 수 있는 권한을 규정하고 있다.

14 제19대 국회 미래창조과학방송통신위원회 수석전문위원 검토보고서, 2013.6.3, 10–19면 참고.

15 SK커뮤니케이션즈 개인정보 유출사태, 3·20 사이버 테러, 6·25 사이버 테러 등과 같은 일련의 사고의 주요 원인은 악성프로그램으로 파악되며, 사용자(또는 직원)의 컴퓨터가 악성프로그램에 감염되고 감염된 컴퓨터를 이용하여 외부 악의적인 공격자가 내부 시스템에 침투하고, 정보를 탈취하는 결과로 이어지고 있음을 보여준다.(최상용, 인터넷을 통해 유포되는 악성 프로그램 대응전략", 전자공학회지, 2014.4, 319면 참고).



출처 : KISA, 2013 「정보보호 실태조사 개인편」

[그림 3] 이용자의 바이러스 검사 빈도

적극적으로 활용하는 인터넷 이용자가 점차 증가하고 있는 추세이기는 하나, 그럼에도 주 1회 이상 바이러스 검사를 실시하는 경우는 20.3%에 불과한 실정이다.[16] 따라서 법률에 정보보호를 위한 이용자의 책무를 규정하여 준수를 유도하는 것 역시 의미가 있을 것으로 보인다.

안 제7조는 이용자가 자신의 PC를 악성프로그램으로부터 보호하는 방법을 숙지하고 실천(제1항) 하고, 백신소프트웨어를 주기적으로 갱신하며(제2항), 소프트웨어 보안취약점 보완 프로그램을 정기적으로 확인하고 설치(제3항)하는 등 정부가 권고하는 이용자보호수칙 등을 준수(제4항)하여야 함을 규정한다. 다만, 이와 같이 이용자에게 강제적으로 백신을 설치하도록 의무화하는 것은 개인의 자유를 지나치게 제약할 우려가 있을 수 있으므로 이용자의 책무는 규정하되, 벌칙이나 시정명령 대상에서는 제외하도록 하고 있다.

(2) 서비스제공자 등의 협력(안 제8조)

DDoS 공격 예방을 위해서는 이용자 컴퓨터의 백신 설치가 매우 중요하지만 사실상 이용자의 컴퓨터 이용능력은 천차만별이고, 특히 정보 취약계층에 속하는 이용자는 백신의 중요성을 인지한다 하더라도 혼자서 백신 등 보안프로그램을 설치하거나 이용하지 못하는 경우가 많다. 따라서 이용자 개인의 책무를 규정하는 것에서 더 나아가 인터넷접속서비스 제공자[17]

16 KISA, 「2013 정보보호 실태조사–개인편」, 54면.

17 적용대상 사업자의 범위에 해당하는 "인터넷접속서비스 제공자"는 전기통신사업자로서 인터넷접속 서비스를 제공하는 자를 말하는 것으로, 전국적으로 인터넷접속서비스를 제공하는 (주)케이티, SK브로드밴드(주), (주)LG텔레콤, (주)온세텔레콤,

등 사업자가 이용자의 백신소프트웨어 설치 등의 조치를 지원할 수 있도록 하고 있다. ISP와 컴퓨터 제작 · 수입 · 판매업자에게 보안프로그램 설치 및 이용방법 등 정보보호조치에 관한 정보를 이용자에게 제공할 의무를 부과하며,[18] 특히 PC방, 도서관 등 일정한 물리적 장소에서 컴퓨터를 갖추고 다중이 정보통신망에 접속하여 서비스를 이용할 수 있도록 하는 사업자에게는 백신프로그램 설치를 의무화하였다. 실제로 PC방의 경우 접속하는 웹사이트나 다운받은 프로그램이 개인이 이용하는 컴퓨터보다 위험에 노출되기 쉽기 때문에 백신소프트웨어 설치에 대한 사항을 법률에서 규정하여 사업자의 경각심을 높일 수 있을 것으로 기대된다. 다만, 다중이용업소에 대해서만 백신소프트웨어 설치 및 업데이트를 의무화하는 것은 일반 사업자와의 형평성 문제와 사업자 비용 부담의 문제가 제기될 우려가 있으므로 과태료 대상에서는 제외하도록 규정하였다.

(3) 소프트웨어 보안취약점 점검 등(안 제9조)

소프트웨어 사업자에게도 정보보호를 위한 근본적인 침해사고 예방조치가 필요함을 규정한다. 사이버 공격은 윈도우 OS 등 소프트웨어의 보안취약점을 이용하는 경우가 많다. 실제로 2003년에 발생한 1.25 인터넷 침해사고의 경우, 호주, 미국 등에서 유입된 슬래머 웜(Slammer worm)[19]이 보안업데이트를 하지 않은 MS-SQL 서버를 공격하여 한국의 8,800대 PC를 다운시켰다.[20] 정보통신망의 안전성을 확보하기 위해서는 보안프로그램과 소프트웨어 보안 취약점을 보완하는 프로그램(보안패치)의 설치가 필수적임에도, 영세 소프트웨어 제작자나 수입 소프트웨어의 경우 소프트웨어를 배포만 하고 보안취약점에 대한 보완 없이 방치하는 경우가 많았던 것이다. 이에 따라 안 제9조는 침해사고 발생 여부와 상관없이 소프트웨어사업자에게 자신이 제작한 소프트웨어[21]의 보안취약점을 점검하고 보안패치를 제작하고

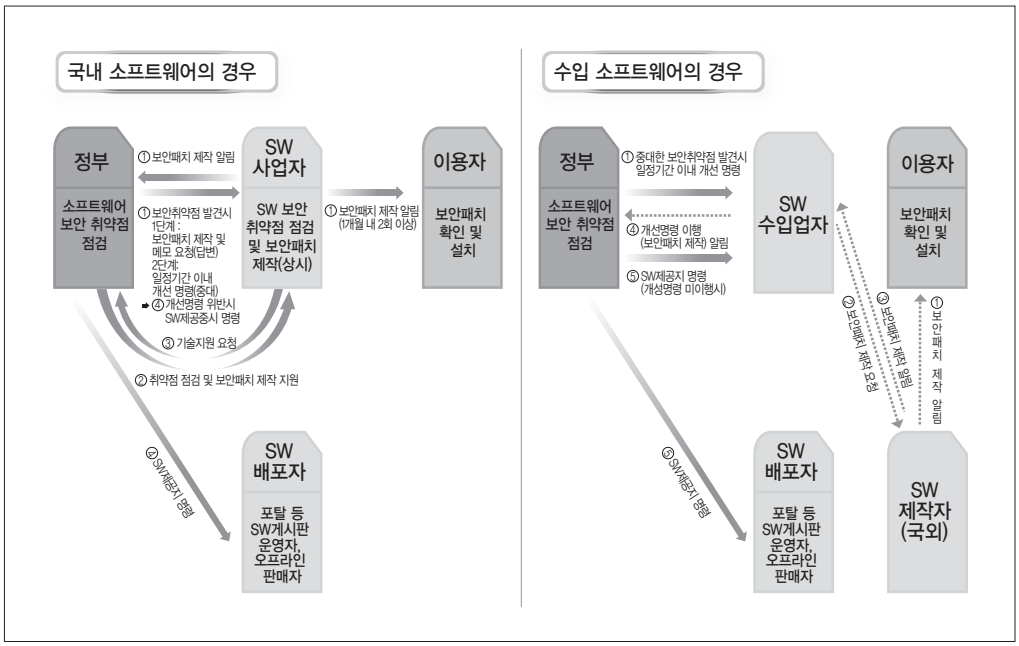
(주)세종텔레콤, 드림라인(주) 등 11개 사업자 외에 종합유선방송사업자(SO) 및 중계유선방송사업자(RO)도 포함한다.

18 이용자가 최초 인터넷서비스 접속시(ISP) 또는 컴퓨터 구매시 안내문 제공 등 정보제공방법은 대통령령으로 정하도록 하였으며, 위반 시 2천만 원 이하의 과태료를 부과하여 사업자의 의무를 강화하였다.(안 제24조제1항제1호).

19 슬래머 웜은 컴퓨터 바이러스의 일종으로, 전파가 빠른 UDP 프로토콜을 이용해 초당 50,000여회의 트래픽을 유발시켜 해당 취약점을 가진 서버를 공격해 8.5초마다 감염규모를 2배로 늘려가면서 사고 발생 10분 만에 전 세계 약 75,000여대 서버를 감염시켰다.(「1.25 인터넷 침해사고, 5년 후 지금」, 한국정보보호진흥원, 2008, 15면 참고).

20 윤해성, 「사이버 테러의 동향과 대응방안에 관한 연구」, 한국형사정책연구원, 2012.12., 244면.

21 동 규정에 따른 소프트웨어는 이용자가 사용할 수 있는 모든 소프트웨어가 대상이 되므로, 스마트폰에서 사용되는 소프트웨어(예를 들어, 앱스토어에 올라온 아이폰용 소프트웨어 등)도 모두 포함된다.



[그림 4] 소프트웨어 보안취약점 보완 프로세스

배포할 의무를 부과한다.[22]

(4) 웹사이트 정기점검 등(안 제10조)

개인정보 유출 등의 침해사고는 이용자가 단순히 악성프로그램이 은닉된 웹사이트를 방문하거나 악성코드가 포함된 게시물을 다운로드받는 등의 행위를 통해 발생하는 경우가 많음을 고려하여 웹사이트를 운영하는 사업자의 구체적인 침해 대응조치를 규정하고 있다. 이용자 접근성이 높은 포털이나 웹하드, P2P사이트 등의 게시판에 악성프로그램이 은닉되어 있는 경우, 해당 프로그램에 대한 삭제조치가 즉시 이루어지지 않으면 같은 경로를 통해 다수의 컴퓨터가 악성프로그램에 감염되어 DDoS공격이 일파만파로 확산될 수 있다. 현재로써는 웹사이트나 게시판에 은닉된 악성프로그램에 대하여 정부가 삭제명령을 할 수 있는 법적 근거가 미비한 실정이어서 악성프로그램 유포사이트가 탐지된 경우에 해당 웹사이트 운영자의

22 현행 「정보통신망법」 제48조의2(침해사고의대응 등)는 미래창조과학부가 취할 수 있는 침해사고 대응조치의 하나로 '소프트웨어사업자에 대한 침해사고 관련 소프트웨어의 보안취약점보안프로그램 제작·배포 요청' 및 '정보통신서비스 제공자에 대한 정보통신망 게재 요청'을 규정하고 있다. 하지만, 미래창조과학부가 해당 사업자에게 요청만 할 수 있을 뿐, 사업자가 협조하지 않을 경우 이에 대한 후속조치를 할 수 없어 소프트웨어가 보안취약점이 방치된 채 유포될 우려가 있다는 점에 한계가 있다.

연락처를 파악하여 전자메일을 통하여 1차 조치요청을 하고, 이행하지 않은 경우 전화로 2차 조치요청한 후 공문발송을 통해 3차 조치요청을 하고는 있다. 하지만 해당 요청에는 강제력이 없어 감염 웹사이트 운영자의 비협조로 보완조치가 이루어지지 않는 경우가 상당수인 실정이다.[23] 이에 대하여 안 제10조는 웹사이트 운영자에게 게시자료에 악성프로그램이 포함되어 있는지를 점검할 수 있는 기술적 장치를 마련하고 악성프로그램을 발견할 경우 신속한 삭제 등의 조치를 하도록 규정함으로써 인터넷 침해사고에 대한 이용자, 사업자의 적극적인 협력조치를 규정하고 있다.

4) 악성프로그램 확산방지를 위한 체계 구축

(1) 악성프로그램 확산방지 체계의 구축(안 제11조)

최근 공격적이고 조직적인 양상을 보이는 사이버 공격에 대하여 사이버방역시스템의 도입이 해법으로 제시되고 있다. 사이버방역시스템은 이용자가 인터넷을 이용하기 전 악성 봇 감염여부를 확인하고 감염PC의 경우에는 일정 사이트로 유도하여 치료한 후 인터넷을 이용하게 함으로써 좀비PC가 DDoS 공격에 이용되지 못하도록 하는 체계를 의미한다. 안 제11조는 이러한 인터넷방역사이트 구축 및 운영에 대한 법적 근거를 마련하고 있으며, 이는 일본에서 정부 주도로 운영되고 있는 안티 봇 시스템인 사이버클린시스템(일명 "CCC")[24]을 모델로 하고 있는 것으로 보인다. 일본의 사이버클린시스템은 통신 ISAC소속 70여개 ISP, JRCERT, 보안그룹 등이 참여하여 운영하고 있는 범정부적 봇 방지 조직으로써 사업자들이 정보 수집과 분석을 담당하고 정부는 감독기관으로서의 역할을 하고 있다. 물론, 일본의 선행사례가 있다고는 하지만 일본과 우리나라의 인터넷 이용환경은 차이가 있는 만큼 국가적 차원의 악성프로그램 대응 및 확산방지를 위한 인터넷방역사이트가 우리나라의 웹 이용환경에 적합한 방식으로 운영될 수 있도록 기술적 · 정책적 검토가 면밀히 이루어져야 할 것이다.

---

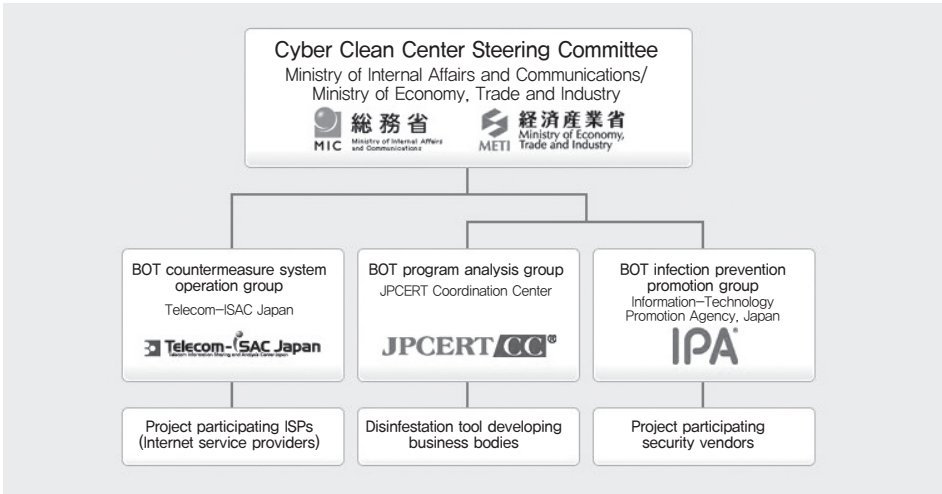
23 미래부에 따르면, 미조치업체인 100개 업체를 대상으로 거부 사유를 조사(통계기간 : 2010.6~2010.12)한 결과, 관련 근거 부족을 이유로 거부한 경우가 81%, 연락이 불가능한 경우가 11%, 조치능력이 부재한 경우가 8%로 나타났다.(제19대 국회 미래창조과학방송통신위원회 수석전문위원 검토보고서, 2013.6.3, 16면 참고).

24 일본은 사이버클린센터(CCC, Cyber Clean Center)를 구축하여 악성봇에 감염된 사용자가 CCC 사이트를 방문하여 전용 백신을 다운로드 하고, 다운로드한 백신을 이용하여 악성봇을 치료하도록 하고 있다.(김영백, 염흥열, "DNS 싱크홀에 기반한 새로운 악성봇 치료 기법", 정보보호학회논문지, 2008.12, 108면 참고).

〈표 3〉 일본 사이버클린시스템(CCC)

1. 구성 및 운영

• 통신 ISAC소속 70여개 ISP, JRCERT, 보안그룹 등이 참여하여 운영하고 있는 범정부적 봇 방지 조직으로, 2006년 12월에 시작되어 현재까지 운영 중



2. 역할 및 절차

• 사업자 스스로 정보를 주고받으면서 인터넷 사업자 및 이용자 모두에게 이익이 되는 방향으로 공조
  – ISP로 이루어진 통신 ISAC이 하니팟을 운영하여 악성 봇 수집
  – JRCERT가 수집된 악성 봇을 분석하여 치료 프로그램을 만든 후, CCC사이트 및 ISP를 통해 봇 감염을 통지 받은 이용자에게 배포
  – JRCERT는 자신들이 분석한 악성 봇 정보를 보안업체 등이 소속된 IPA에 제공함으로써 이용자용 보안프로그램의 봇 치료능력을 업데이트 할 수 있도록 함
• CCC 홈페이지에서 제공하는 악성봇 감염여부 확인 및 치료 절차
  – 윈도우 업데이트, 웹 브라우저 보안설정과 같은 기본적인 사항부터 봇 제거용 전용 보안프로그램 제공, 백신 및 보안기기의 구매 권고까지 이용자 차원의 보안절차 전반에 대한 링크와 설명을 제공

(2) 이용자 컴퓨터에 대한 접속요청(안 제12조)

좀비PC를 발생시키는 악성 봇에 대한 적절한 대응방안 마련을 위해서는 감염 PC로부터의 악성 봇 샘플 채취가 선행되어야 한다. 현재 악성프로그램 샘플 추출 등 침해당한 시스템에 대한 접근이 필요한 경우 해당 컴퓨터 이용자의 사전 동의를 받고 있으나, 감염PC의 접근과 관련한 법적 근거 미비로 이용자의 동의를 구하는데 많은 시간이 소요되어 침해사고 전체에 대한 대응이 지체되고 있다. 이에 대하여 안 제12조는 침해사고 대응, 원인조사 등의 조치가 필요한 경우 정부가 이용자의 컴퓨터에 접근을 요청할 수 있는 법적 근거를 마련하고 있다.

이러한 접속요청권은 침해사고의 특성상 침해받거나 악성프로그램에 감염된 컴퓨터를 확

인하지 않고서는 원인분석이나 적절한 대응이 곤란하므로 침해사고 대응 및 원인조사를 위해 정부가 이용자의 컴퓨터에 접근을 요청할 수 있도록 하는 한편, 시스템 접근 남용 우려를 불식시키기 위해 명령권이 아닌, 요청권만을 부여하고 있는 것으로 보인다. 또한, 이용자의 동의에 의해서만 자료의 수집 및 조사를 실시할 수 있도록 하고 구체적인 조사 범위 등에 대하여는 대통령령으로 정하도록 하여 이용자에 대한 기본권 침해 논란을 최소화하고 있다.

〈표 4〉 접속요청권의 대상 및 범위 예시

1. 접속요청 대상 및 범위
• 웹서버와 같이 네트워크상에서 일반에 공개되어 있는 서버 중 해킹 피해를 입은 시스템 • 해킹피해를 입은 서버 중 악성봇의 C&C(악성 봇이 좀비PC를 감염시키고 명령을 내리는 데 이용되는 서버)로 악용되어 다른 시스템에 피해를 주는 서버 • 해커로부터 악성프로그램 유포 등에 악용되어 이용자 컴퓨터를 악성프로그램에 감염시키는 서버
2. 침해사고 원인조사 등을 위한 자료 수집 · 조사 범위
• 컴퓨터에 남겨진 공격자의 사용기록 정보, 공격 수행시 발생된 공격행위 기록 • 컴퓨터에서 수행되는 프로그램 정보, 해커의 악성프로그램에 대한 연결정보(링크) • 설치된 게시판 소프트웨어, 운영체제 및 패치의 수준 등 공격대상을 판단하기 위한 소프트웨어 정보 • 해커에게 악용된 것으로 확인되는 경우 해커의 행위를 채증하기 위한 네트워크 행위정보 • 컴퓨터에서 수행되는 악성프로그램에 의하여 발생하는 정보 • 악성코드에 감염된 시스템에서 인입되는 접속 정보(Command & Control 프로그램으로 접속하기 위한 프로토콜, 포트 등 정보) • 네트워크 정보 및 트래픽의 양 • 레지스트리 등 해커가 설치한 프로그램에 의한 시스템의 변경사항

침해사고의 특성 상, 사이버 공격은 정부와 민간 구분 없이 가해지고 있으므로 이에 대한 대응책 마련에 있어서 정부와 민간의 적극적인 협력을 바탕으로 대응책을 마련해야할 필요하다. 특히, 악성코드 샘플 수집은 대응 백신의 제작뿐만 아니라 정부가 해당 사이버 공격의 성격을 분석하고 대응책을 마련하는데 필수적이다. 다만, 안 제12조제2항에서 규정하는 '침해사고 발생 원인의 조사 및 분석을 위하여 필요한 자료'는 그 범위를 이용자가 예측하기 어려운 부분이 있는 만큼, 향후 시행령 제정 시 그 구체적인 범위를 명시함으로써 법률의 예측가능성을 높이고 정부가 수집하는 자료의 범위를 자의적으로 확대할 가능성을 제한할 필요는 있다고 본다.

5) 악성프로그램 감염에 대한 대응조치 강화(안 제15조, 제16조, 제17조)[25]

(1) 감염 컴퓨터에 대한 조치(안 제15조)

이용자 컴퓨터가 악성프로그램에 감염된 경우에는 본인이 감염여부를 인지하기 전에 DDoS 공격에 이용되어 제3자의 재산권과 통신권을 침해하는 피해를 야기할 수 있으므로 정부와 사업자 및 이용자가 감염컴퓨터 치료를 위해 긴밀하게 협력하여 조치를 취할 수 있도록 하는 것이 중요하다. 제정안에서는 정부가 DNS 싱크홀[26]이나 피해 사이트의 침해사고 신고 등의 방법을 통해 알게 된 좀비PC 정보를 ISP에게 제공함으로써 ISP가 해당 이용자에게 통지할 수 있도록 규정한다(제1항 및 제2항). 이는 좀비PC의 IP(Internet Protocol)주소를 가지고 해당 이용자에게 연락할 수 있는 정보를 가진 주체는 ISP밖에 없음을 고려한 것으로 보인다. ISP는 이용자에게 감염사실 및 조치방법을 안내하여 이용자가 악성프로그램 치료 등의 조치를 취할 수 있도록 하여야 하며, 한국인터넷진흥원이 운영하는 인터넷방역사이트의 악성 봇 대응 시스템에 대한 링크를 제공하게 함으로써 사업자가 직접 좀비PC의 치료를 지원해야 하는 부담을 최소화할 수 있다. 이용자에 대한 통지 방법은 전화, 전자우편 외에 팝업 공지 등의 형태가 될 수 있으며 구체적인 내용은 대통령령으로 정하도록 하고 있다.

또한, 좀비PC가 다른 정보시스템 · 정보통신망에 위해를 가하거나 급박한 위험이 있는 경우 ISP가 이용약관에 따라 해당 이용자에 대한 인터넷접속 서비스의 제공을 제한 또는 중지할 수 있도록 하여(제3항),[27] 침해사고 피해확산을 방지하기 위한 대응조치를 규정한다. 이는 짧은 시간에 국가비상사태와 같은 국가존립을 해치는 정도의 사고를 야기하는 경우에만 취해지는 일시적인 차단 조치로 국민의 통신권을 보호하기 위한 최소한의 조치라고 할 수 있다.

---

25 제19대 국회 미래창조과학방송통신위원회 수석전문위원 검토보고서, 2013.6.3, 23-33면 참고.

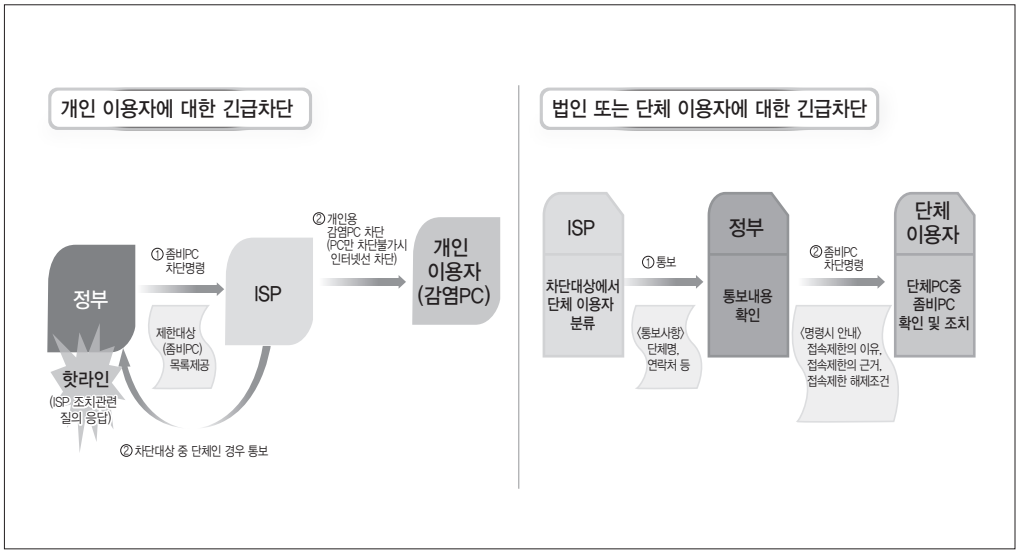
26 DNS 싱크홀(DNS sinkhole)은 좀비PC와 명령제어 서버(C&C서버)의 통신을 차단하여 해커의 명령 전달을 방지하고 관련 정보 등을 수집으로 DDoS 공격을 사전 예방하고 효과적으로 대응할 수 있는 기법으로, 일반 이용자가 보안에 대한 지식이 없더라도 감염PC가 사용하는 DNS서버를 운영하는 ISP에서 DNS 싱크홀을 적용 중 이라면 악성봇에 의한 악성행위를 차단 할 수 있는 효과가 있다.(최재영 외 2인, "DNS Response Policy Zone 을 이용한 DNS 싱크홀 운영 방안 연구", 한국정보처리학회, 2011.5, 1529면 참고).

27 현행 「정보통신망법」 제47조의4(이용자의 정보보호)에서는 정보통신망에 중대한 침해사고가 발생하여 이용자의 정보통신망 등에 심각한 장애가 발생할 가능성이 있는 경우 이용약관으로 정하는 바에 따라 해당 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다고 규정하고 있으며, 「좀비PC법(안)」은 악성프로그램에 의한 DDoS 공격방법에 좀더 적합하게 대응하도록 이를 보다 명확화하여 규정하였다.

(2) 웹사이트의 접속경로 차단조치(안 제17조 제1항 및 제2항)

국가 시스템에 영향을 줄 정도로 심각한 침해사고가 발생한 경우에는 국가기반시설인 인터넷을 보호하기 위하여 정부가 ISP나 IDC에게 악성프로그램 유포에 이용되거나 이용될 가능성이 큰 웹사이트의 접속경로(도메인이름, 인터넷 프로토콜 주소 등) 차단 조치를 명할 수 있다. 현행 「정보통신망법」 제48조의2는 정부가 사업자에게 접속경로 차단을 요청할 수 있다고 규정하고 있다. 하지만 동 조항은 사업자에 대한 '요청'을 규정한 것으로 사업자가 협조하지 않을 경우 이에 대한 후속조치를 할 수 없어 공격이 해당 접속경로를 통해 확산되는 것을 효과적으로 차단할 수 없는 실정이다. 이에 대하여 안 제17조는 정부가 침해사고 확산에 이용되고 있거나 이용될 가능성이 큰 접속경로에 대하여 차단조치를 명령하고, 불응 시 제재조치를 취할 수 있도록 함으로써 제도적 실효성을 강화한다.

이에 따라, 국가 차원에서 중대하고 심각한 침해사고가 발생한 경우 정부는 ISP로 하여금 좀비PC 이용자 등의 인터넷 접속을 제한하거나 IP주소 차단 등의 조치를 취하도록 명령권을 부여할 수 있다. 인터넷 접속차단을 명할 수 있는 심각한 침해사고의 수준은 침해사고 일정 단계이상인 경우에만 가능하도록 엄격히 제한하고 있는 바, 이는 현재 국민의 생활에서 인터넷이 차지하는 영향력을 고려할 때 인터넷 접속차단은 심각한 부작용을 가져 올 수 있으므로 매우 제한적으로만 적용되도록 하려는 의도로 보인다.



[그림 5] 감염 컴퓨터에 대한 긴급차단 프로세스

이러한 정보통신망 접속 제한은 일시적 · 제한적으로 이루어져야 하므로 정부의 해제 명령이 있는 경우 ISP는 즉시 정보통신망 접속 제한을 해제하여야 하고, 정부는 조치에 대한 사유가 없어졌다고 인정할 때에는 지체 없이 조치의 해제를 명령해야 함을 규정한다. 이와 같이 중대한 침해사고 발생 시 정부가 ISP 등에게 접속차단 등의 긴급조치를 명할 수 있게 함으로써 사이버 침해의 피해 확산을 최소화하고 대응조치의 실효성을 보다 강화할 수 있을 것으로 기대된다.

2. 제18대 국회 제정안과의 차이점[28]

7 · 7 DDoS 대란 이후, 점차 지능화되어가는 침해사고에 실효적으로 대처하기 위하여 「좀비PC법(안)」이 제18대 국회에 발의되었으나,[29] 당시에는 정부의 권한이 지나치게 강하고 기본권 침해가 우려된다는 논란이 제기되면서 회기종료로 폐기되었다. 그러나 이후에도 조직적인 사이버 공격으로 해킹, 국가 전산망 마비, 개인정보 유출 등의 피해가 전국가적으로 지속 발생하면서 「좀비PC법(안)」의 제정 필요성에 대한 사회적 공감대가 형성되어 왔다. 이에 따라, 이용자 PC의 백신설치, 웹사이트 악성코드 정기점검, 감염PC 조치, 보안프로그램 긴급 배포 등 각종 사이버 공격에 대한 보안 강화를 골자로 하는 「좀비PC법(안)」이 제19대 국회에서 재발의 되었다.[30] 특히, 제18대 국회 제정안에서 그동안 문제로 지적되어 왔던 사생활 침해와 과도한 책임 부과에 대한 문제를 상당부분 보완하면서 개인 이용자에 대한 정보보안을 강화하고 정부의 자료조사권은 크게 축소한 것을 주목할 만하다.

1) 웹사이트 게시물 접속차단에 따른 조치결과 공개 의무 신설(안 제10조제3항)

제18대 국회 제정안의 경우 웹사이트 운영자가 자의적으로 게시물을 삭제할 우려가 있으며, 악성프로그램의 존재여부를 확인할 능력이 없는 게시판 운영자의 경우에는 정부의 삭제명령을 이행할 수밖에 없기 때문에(삭제명령 불이행 시 2천만 원 이하의 과태료 부과), 인터넷에 유통되는 정보에 대하여 정부의 규제권한이 과도하게 커질 우려가 있다는 지적이 있었

28 제19대 국회 미래창조과학방송통신위원회 수석전문위원 검토보고서, 2013.6.3, 18–19, 24–33면 참고.

29 「악성프로그램 확산방지 등에 관한 법률안」, 한선교 의원 대표발의('10.11.23).

30 한선교 의원 대표발의로 제19대 국회에 재발의('12.6.14)되어 미래창조과학부방소통신위원회에 회부된 후, 현재 국회(임시회) 제3차 법안심사소위에 상정('13.12.23)되어 계류 중에 있다.

다. 이러한 지적을 반영하여 제19대 국회 제정안에서는 웹사이트 운영자 및 게시판 운영자가 악성프로그램만 삭제하는 것이 곤란하여 게시 자료에 대한 접속을 차단하는 경우에는 이용자들이 알 수 있도록 조치결과를 '공개'하도록 하여 자의적 삭제 우려에 대한 문제를 보완하였다.

〈표 5〉 제정(안) 제10조

제18대 국회 제정안	제19대 국회 제정안
제10조(웹사이트의 정기점검 등) ① 웹사이트를 운영하는 자로서 대통령령으로 정하는 자(이하 "웹사이트 운영자"라 한다)는 자신이 운영하는 웹사이트에 게시된 자료에 악성프로그램등이 포함되어 있는지를 정기적으로 점검하는 기술적 조치를 하여야 하며, 게시된 자료에 악성프로그램등이 포함된 사실을 발견한 경우에는 즉시 해당 악성프로그램등을 삭제하는 등 필요한 조치를 하여야 한다.	**제10조(웹사이트의 정기점검 등)** ① (제18대제정안과 같음)
② 방송통신위원회(미래창조과학부)는 악성프로그램등이 포함된 게시판(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제9호의 게시판을 말한다. 이하 같다)을 발견한 경우 해당 게시판의 운영자에게 악성프로그램등의 삭제 등 필요한 조치를 명할 수 있다.	② (제18대 제정안과 같음)
	③ 웹사이트 운영자와 게시판 운영자가 제1항 및 제2항에 따른 조치를 함에 있어 해당 악성프로그램등만을 삭제하는 것이 곤란하여 게시된 자료에 대한 접속을 차단하는 경우에는 그 사실을 이용자가 알 수 있도록 1개월 이상 공개하여야 한다.

2) 감염 컴퓨터에 대한 조치 구체화(안 제15조제1항 및 제3항)

제19대 국회 제정안은 이전 제18대 국회 제정안이 정부가 ISP에게 '감염 컴퓨터에 관한 정보'를 제공할 수 있다고만 규정하고 있어 어떤 유형의 정보가 제공되는지 불명확하다는 지적을 반영하여, 미래창조과학부가 ISP에 제공하는 정보의 범위를 '감염 컴퓨터의 IP주소 등 대통령령으로 정하는 정보'로 규정하여 정보의 유형에 대한 예측가능성을 높이면서도 IP주소 외에 다른 정보는 대통령령으로 정하도록 함으로써 법 집행의 탄력성도 일부 인정하고 있다.

또한, ISP의 이용약관에 따른 서비스 제공 중지 조치와 관련하여, 이전 제정안은 '감염 컴퓨터 이용자의 인터넷접속서비스 제공 제한 · 중지조치'로 규정하여 이용자의 기본권을 필요 최소한도로 제한하는 규제인지에 대한 논란[31]이 있음을 고려하여 ISP가 감염 컴퓨터 이용자

31 감염 컴퓨터 이용자의 인터넷접속서비스 제공을 제한 또는 중지할 경우, 컴퓨터를 치료하기 위한 백신프로그램의 다운로드 등이 불가능해지고, 결합상품 이용자의 경우에는 통신회사에 따라 전화나 TV까지도 모두 정지될 수도 있어, 초고속인터넷과 인터넷전화, IPTV를 함께 제공하는 결합상품을 하나의 IP주소를 사용하여 서비스하는 사업자의 서비스를 이용하는

의 인터넷접속서비스의 제공 제한 · 중지조치를 하더라도 '일시적으로만' 할 수 있도록 하였으며, 감염 컴퓨터의 인터넷접속차단에 대한 이용자의 예측가능성을 제고하기 위하여 ISP가 감염 컴퓨터의 이용자에게 통지하여야 할 사항에 '인터넷접속서비스의 제한 기간, 부당한 제한에 대한 이용자의 이의제기 절차' 등을 명시하여 인터넷 접속차단으로 인한 피해를 최소화할 수 있도록 규정하였다는 점이 주목할 만하다.

〈표 6〉 제정(안) 제15조

제18대 국회 제정안	제19대 국회 제정안
제15조(감염 컴퓨터에 대한 조치 등) ① 방송통신위원회(미래창조과학부)는 악성프로그램의 확산방지를 위하여 침해사고의 신고 또는 제14조에 따른 인터넷주소의 변경 조치 등의 방법으로 수집한 감염 컴퓨터에 관한 정보를 인터넷접속서비스 제공자에게 제공할 수 있다.	**제15조(감염 컴퓨터에 대한 조치 등)** ① 감염 컴퓨터의 이용자는 악성프로그램 확산방지를 위하여 미래창조과학부에 신고할 수 있으며, 미래창조과학부는 이용자의 신고 또는 제14조에 따른 인터넷주소의 변경 조치 등의 방법으로 수집한 감염 컴퓨터에 관한 인터넷 프로토콜 주소 등 대통령령으로 정하는 정보를 인터넷접속서비스 제공자에게 제공할 수 있다.

3) 접속제한 등의 조치에 따른 고지 의무 신설(안 제17조제2항)

제18대 국회 제정안 제17조제2항은 '일반 이용자를 대상으로 정보통신망 접속제한 등'을 규정하였으나, 정부가 개인의 인터넷주소를 차단하고 정보통신망으로의 접속을 제한하는 것이 이용자의 기본권을 침해할 수 있다는 비판이 지속제기 되었다. 이에 대하여 제19대 국회 제정안은 미래창조과학부가 정보통신망으로의 접속 제한 등의 조치를 할 때에 이용자에게 해당 사실을 고지하도록 의무를 부과함으로써 조치로 인한 부작용이 최소화될 수 있도록 지적사항을 일부 보완하였다.

〈표 7〉 제정(안) 제17조제2항

제18대 국회 제정안	제19대 국회 제정안
제17조(침해사고 대응 명령 등) ② 방송통신위원회(미래창조과학부)는 정보통신망의 안정적 운영을 중대하게 방해하거나 심각한 장애를 초래할 위험이 있는 경우로서 대통령령으로 정하는 수준 이상의 침해사고가 발생한 때에는 인터넷접속서비스 제공자에게 이용자에 대하여 다음 각 호의 조치를 하도록 명할 수 있다. 1. 인터넷주소의 차단 2. 정보통신망으로의 접속 제한 3. 그 밖의 대통령령으로 정하는 조치	**제17조(침해사고 대응 명령 등)** ② 미래창조과학부는 정보통신망의 안정적 운영을 중대하게 방해하거나 심각한 장애를 초래할 위험이 있는 경우로서 대통령령으로 정하는 수준 이상의 침해사고가 발생한 때에는 인터넷접속서비스 제공자에게 이용자에 대하여 다음 각 호의 조치를 하도록 명할 수 있다. 이 경우 해당 이용자에게 조치의 이유 및 근거, 조치의 해제조건 등을 알려야 한다. 1. 인터넷주소의 차단 2. 정보통신망으로의 접속 제한 3. 그 밖의 대통령령으로 정하는 조치

경우, 인터넷접속서비스 제공을 중지하면 위의 3개의 서비스가 모두 중단되는 부작용이 있을 수 있다.

4) 기타(안 제2조, 제7조, 제19조 등)

제19대 국회 제정안은 자료제출의 요구에 있어서 제18대 국회 제정안이 정부의 자료제출 요구 권한을 '이 법에 위반되는' 사항을 발견하거나 신고 또는 민원이 접수된 경우를 포괄하고 있어 이용자의 책무(안 제7조) 등 일반국민에 대한 정부의 과도한 권한을 인정한다는 비판을 수용하여 '제8조부터 제17조까지의 규정을 위반'한 경우 등으로 자료제출 요구권에 대한 근거조항을 제한하였다. 또한, 자료제출에 응하지 않은 당사자의 사업장에 출입하여 검사하도록 한 규제를 완화하여 일정한 물리적 장소에서 컴퓨터를 갖추고 다중이 정보통신망에 접속하여 서비스를 이용할 수 있도록 하는 자(안 제8조제3항)에 대하여만 관계 자료 등을 검사할 수 있도록 하여 기본권 침해에 대한 우려를 크게 해소하려 했다는 점에 특징이 있다.

Ⅳ. 향후 과제

현재 국회에 계류 중인 「좀비PC법(안)」이 국회를 통과하여 시행되면 사이버 공격에 대한 정부와 사업자, 이용자 간의 민관 협력적 대응 체계를 구축하고 보다 실효성 있는 긴급조치를 시행할 수 있을 것으로 기대 된다. 특히, 정부의 좀비PC 차단 명령, 특정 기능의 보안프로그램 긴급배포 등을 통해 신속하게 피해확산을 최소화할 수 있으며, ISP, 포털 등과의 주기적인 위기대응방법 훈련과 인터넷방역사이트 구축 등을 통해 단순히 침해에 '대응'하는 것 뿐 아니라, 좀비PC 치료 및 감염 '예방' 체계를 확보하는 데 많은 기여를 할 것으로 생각된다. 현재 국회에 계류 중인 좀비PC 제정안은 제18대 국회 제정안에서 지적되어온 사항을 상당부분 보완했음에도 불구하고 개인의 기본권 침해와 정부에 대한 과도한 권한 부여의 문제로 인해 국회통과에 난항을 겪을 가능성이 크다. 따라서 「좀비PC법(안)」의 원활한 법 시행과 제도 정착을 위해서는 몇 가지 추가적인 법적 쟁점에 대한 검토가 필요한 바, 이하에서는 「좀비PC법(안)」에 대하여 제기될 수 있는 논란과 이에 대한 향후 과제를 살펴보기로 한다.

1. 입법 시 고려사항

1) 이용자 기본권의 침해가능성 검토

「좀비PC법(안)」 제정과정에서 가장 논란이 되었던 것은 컴퓨터보안프로그램 설치 및 좀비

PC 치료를 위한 IP제공, 이용자 컴퓨터에 대한 접근요청 등이 이용자의 사생활을 침해하고, 나아가 패킷감청 등을 허용하는 것이 아니냐는 것이었다.[32]

그러나 「좀비PC법(안)」은 이용자 동의 없는 이용자 컴퓨터에 대한 조사나 컴퓨터보안프로그램의 강제 설치 등 이용자의 기본권 침해가능성이 있는 수단은 규정하고 있지 않음을 주목할 필요가 있다. 보안프로그램 설치 여부를 원격으로 모니터링하는 것은 현행 「정보통신망법」 제48조에서 금지하는 해킹에 해당하여 법적으로 허용되지 않으며, 이 법 위반에 대한 조사권의 대상도 개인이용자가 아닌 사업자에 한정되어 있다. 또한, 감염PC에 대한 접속요청은 백신제작 및 DDoS공격 원인분석과 대응책 마련에 필수인 악성코드 샘플 등을 수집하기 위한 것으로 취득한 정보를 목적 외로 사용하는 경우에는 벌금 등의 제재조치를 부과하고 있다(안 제23조).

다만, 접속요청권의 주체는 미래창조과학부로 규정한 반면, 접속주체에 대해서는 명확한 규정을 하고 있지 않으므로 접속주체와 요청주체가 동일하다면 자구 수정으로 그 취지를 명확히 하고, 접속주체가 미래창조과학부 산하기관이라면 이를 명확히 규정하는 개선은 검토할 필요가 있다. 아울러, 이용자의 동의 절차를 단순한 '동의'라고만 규정하는 경우 소유자나 이용자에게 사실상 동의절차가 무의미하게 작용할 가능성이 있으므로 '서면에 의한 동의' 정도로 강화하여[33] 기본권 침해 가능성을 최소화하는 방안을 고려할 필요가 있다고 본다.

2) 홈페이지에 은닉된 악성프로그램 삭제조치의 위법성 여부 검토

홈페이지를 통해 유포되고 있는 악성프로그램에 대한 정기점검 및 삭제조치를 규정한 안 제10조가 이용자들의 인터넷 활동을 검사하고, 반정부적 표현물을 배제하기 위한 용도로 악용되는 등 정부의 규제권한이 과도하게 커질 우려가 있다는 지적[34]이 제기된 바 있었다.

하지만 악성프로그램 정기점검은 보안프로그램에 의해서 수행되며 사람이 하는 것이 아니기 때문에 악성코드 감염 여부만을 알 수 있을 뿐, 게시물의 내용에 대해서는 알 수 없다. 또한, 악성코드 감염이 확인된 게시물에 대하여는 해당 악성프로그램만 삭제하는 것이 원칙이며, 게시물 자체를 삭제하는 것은 아니다. 게시된 자료와 악성프로그램이 분리될 수 없어 부

32 전자신문, "좀비PC 방지법, 6월 공청회 통해 통과될까?', 2011.4.21.

33 김중권외 8인, "정보통신망법 개정 연구", 방송통신위원회 연구결과보고서, 2012.12, 120-121면.

34 한겨레, "당·정 좀비피시법 제정 목청, 안보 명분 무차별 규제 우려", 2011.3.11.

득이하게 게시된 자료에 대한 접속을 차단해야 하는 경우에는 이용자들이 조치 결과를 알 수 있도록 1개월 이상 공개하도록 규정하고 있으므로 이러한 조치로 인해 이용자의 기본권이 과도하게 침해된다고 단정하기는 어려울 것으로 보인다. 또한, 현재에도 대형 포털 등의 경우에는 정기적인 점검활동을 하고 있으나 중소 웹사이트 운영자들의 경우 자율적인 실시를 기대하기 곤란한 만큼, 동 규정을 통해 삭제조치를 규정하여 해당 게시판 이용자의 정보보호를 강화하는 방안을 마련할 수 있을 것으로 판단된다. P2P, 웹하드 등이 악성프로그램 유포의 주요 거점으로 확인되고 있는 상황에서 악성프로그램에 감염된 웹사이트의 경우 보안 프로그램 설치, 정기점검 등의 기술적 조치 등의 보완조치가 이루어지지 않으면 같은 경로를 통해 악성프로그램에 재감염 될 수 있으므로 신속한 삭제 조치가 필요하다고 하겠다.

3) 인터넷 접속경로 차단명령의 위법성 여부 검토

DDoS와 같은 공격은 매우 빠른 속도로 확산되므로 신속히 감염원을 차단하는 것이 필수적이다. 하지만 이에 대하여 정부의 접속경로에 대한 차단 조치 명령 권한을 부여하는 것은 지나친 규제가 될 수 있다는 우려가 시민단체를 중심으로 제기되어 왔다.[35]

그러나, 「좀비PC법(안)」은 근본적으로 개인의 인터넷 사용을 제한하기 위한 것이 아니라 개인 PC를 범죄에 악용하려는 자들로부터 국민의 재산권과 통신권을 보호하기 위한 것이라는 입법 취지를 고려할 필요가 있다. 접속경로 차단 등의 조치는 좀비PC에 대한 차단이 아니라 이용자에게 감염사실을 알리고 치료를 지원하는 것이 우선적인 목적이다. 즉, 이용자에 대한 차단이 아닌 접속경로에 대한 차단이며, 일정 수준 이상의 침해사고 발생 시에만 인터넷 접속을 차단한다는 점에서 과잉금지 원칙에도 반한다고 단정하기도 어렵다.

또한, 이미 현행 「정보통신망법」 제47조의4[36] 및 ISP사업자의 인터넷 서비스 이용약관에도 차단 요청에 대한 사항이 규정되어 있다. 물론, 「정보통신망법」의 경우 정보통신서비스 제공자가 자율적으로 시행하도록 하고 있어 정부가 차단을 명령할 권한은 없다. 하지만 이로

35 녹색소비자연대는 인터넷 접속경로 차단조치에 대하여 개인의 권리를 국가안보의 이름으로 제한하는 권위주의적 발상이라고 비판하면서 개인PC의 안전상태 점검과 분석·조사, 인터넷 접속제한은 도둑맞을 위험이 크다고 해서 국가가 계약한 사설 경비회사가 모든 국민의 생활터전인 주거공간에 언제든 침입하도록 하는 법을 만들고, 개인이 '동의'했다고 사람을 죽인다고 면죄돼 처벌을 받지 않은 것과 같다는 우려를 제기한 바 있다(미디어오늘, "소위 좀비PC법에 대하여", 2009.10.28. 참고).

36 「정보통신망법」 제47조의4(이용자의 정보보호) 제2항은 주요정보통신서비스 제공자는 중대한 침해사고 발생 시 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 미 이행시 정보통신망으로의 접속을 일시적 제한 가능하다고 규정한다.

인해 사업자들은 가입자 이탈, 민원 발생 등을 우려하여 차단을 꺼려하기 때문에 침해사고가 발생하는 경우 적기에 신속하게 대응하지 못하고 대응 절차가 지연되는 문제가 야기되고 있다. 이러한 측면에서 악성코드 감염을 차단하는 가장 유효한 수단인 접속경로 차단에 대한 법적 근거를 마련할 필요성이 인정된다고 본다. 다만, 인터넷 접속 제한 또는 차단 조치는 침해사고 경보단계 중 경계수준 이상 시에만 제한적으로 가능하도록 시행령 제정 시 이를 명확하게 규정하는 방안을 검토하는 것이 바람직할 것으로 보인다.

2. 국회 미 통과 시 고려사항

미래창조과학부는 2013년도 핵심 추진과제로 '사이버안보 강화'를 선정하고,[37] 그 일환으로 「좀비PC법(안)」의 제정을 추진하기 위하여 사생활 침해 등 우려되는 부분들을 최소화 할 수 있도록 협의하여 국회 통과를 추진할 것임을 밝힌 바 있다.[38] 하지만, 현재까지도 「좀비PC법(안)」에 대하여는 많은 찬반 논란이 존재하고 있다. 새로운 보안 위협에 법적 근거가 있는 대응체계를 마련해야 한다는 찬성의 의견도 있지만, 앞서 살펴본 바와 같이 법안이 악성코드 감염을 방지, 억제하는데 도움이 되기보다는 공권력에 의한 사생활 침해 우려가 크다는 야권의 반대의견도 지속 제기되고 있다.[39] 법안을 발의한 여당과 야당의 의견이 첨예하게 대립하고 있는 만큼 협의에 다소 어려움이 있을 것으로 전망된다.

제18대 국회에 제출된 법안 역시 국회 소위심사예정이었으나 여야 의견 차이로 미결되어 폐기되었던 것을 고려해볼 때, 국회 미 통과에 따른 제정안의 향후 개선방안도 검토해볼 필요가 있다. 제정안이 국회에 통과되지 못한다하더라도, 지속적으로 발생하는 사이버 공격에 대한 일반 이용자에 대한 보호 및 정부 유관기관과의 체계적 협조 등을 규율하는 법체계 구축은 필요하기 때문이다. 따라서 별도의 법제정이 어려울 경우 「정보통신망법」 개정을 통해 악성코드 감염 PC에 대한 접속요청권을 신설하거나, 접속경로 차단 요건 등을 강화하여 침해확산 방지를 위한 접속경로 차단명령을 규정하는 등의 개정[40]을 고려해볼 필요가 있다. 물

37 미래창조과학부, "2013년도 업무보고-과학기술과 ICT를 통한 창조경제와 국민행복 실현",2013.4.18.

38 이데일리, "[미래부 업무보고] 좀비PC 동의없이 접속차단법 재추진", 2013.4.18.

39 디지털타임스, "좀비PC법 인터넷접속 차단 찬반 팽팽", 2011.6.15.

40 「정보통신망법」 제48조(정보통신망 침해행위 등의 금지 등), 제48조의2(침해사고의 대응 등) 등 관련 규정을 개정하여 대응조치 주체를 구체화하고 법문의 의미를 명확히 하여 규율체계를 재정비하는 방향이 바람직할 것으로 보인다.

론 이 경우에도 시민단체, 인터넷 협회, ISP 및 소프트웨어 업체 등 다양한 민간사업자 등 관련 각계의 의견 수렴 등 충분한 논의가 선행되어야 할 것임은 물론이다.

Ⅴ. 결론

사이버 공격은 더 이상 단순 해킹 공격에 국한되지 않는다. 실제로 최근 악성 애플리케이션의 급증으로 좀비 스마트폰 등 신규 악성프로그램 등이 등장하고 있으며, 국내 정보통신체계의 취약점을 이용한 악성프로그램은 기존 DDoS 방어대책을 우회하는 진화된 공격 양상을 보이고 있어 단순한 악성코드 탐지 및 치료만으로는 사전 방어가 어려운 측면이 있다. 그런 점에서 악성코드 확산 방지를 위한 효율적인 기술·관리적 대책 마련이 실로 중요하지 않을 수 없다.

이에 대하여 「좀비PC법(안)」은 정보보호 생활화를 위하여 정부와 사업자, 이용자가 책임과 의무를 분담하고 악성코드 감염 등 급증하는 침해사고로부터 일반 이용자를 보호하여 국민의 재산권 보호 등 안전한 인터넷 이용환경을 조성하고자 함을 목적으로 한다. 현행 「정보통신망법」 등 기존 법체계만으로는 법적 규율 대상의 한계와 인터넷서비스제공자의 소극적인 대처 등으로 효율적인 대응에 곤란을 겪고 있음을 고려해볼 때, 신규 입법을 통해 국내 사이버 보안체계의 한계를 보완하고 정보보호 체계를 강화할 필요성이 인정된다.

그러나 앞서 살펴본 바와 같이, 「좀비PC법(안)」에 대하여 개인의 기본권 침해와 국가 공권력 개입 등 민감한 문제가 지속적으로 제기되고 있는 만큼, 국회 입법 추진을 위해서는 관련 사업자와 시민단체 등 각계의 의견 수렴을 통해 보다 제정 필요성에 대하여 보다 심도 있는 논의가 병행되어야 할 것으로 본다. 이러한 과정을 통해 변화하는 IT 환경과 사이버 공격기술 진화에 부응할 수 있는 법제를 재정비하고 사이버 보안체계를 보다 효율화할 수 있을 것이다.

참고문헌

권양섭 (2014). “사이버 범죄 처벌규정의 문제점과 대응방안”. 「법학연구」, 제53집. 한국법학회.

김범수 외 13인 (2011). “스마트 시대 정보보호 전략과 법제도”, 「한국학술정보」.

김영백 · 염흥열 (2008). “DNS 싱크홀에 기반한 새로운 악성봇 치료 기법”, 「정보보호학회논문지」.

김중권 · 오병철 · 최경진 외 5인 (2012). “정보통신망법 개정 연구”, 「방송통신위원회 연구결과보고서」.

미래창조과학부 (2013). “2013년도 업무보고–과학기술과 ICT를 통한 창조경제와 국민행복 실현”.

박재용 (2012), “정보보안 전문인력 양성을 위한 교육과정 분석”, 「경영정보연구」, 제31권 제1호.

신영웅 · 전상훈 · 임채호 · 김명철 (2013). “국가 사이버보안 피해금액 분석과 대안–3.20 사이버 침해사건을 중심으로”, 「국가정보연구」, 제6권 1호.

염용진 · 배병철 (2006). 「악성 프로그램의 진화」, 정보통신산업진흥원.

염흥열 (2011). “3.4. DDoS 공격과 7.7. DDoS 공격은 어떻게 다르나”, 방송통신위원회 웹진

윤해성 (2012). 「사이버 테러의 동향과 대응방안에 관한 연구」, 한국형사정책연구원.

정 완 (2013). “한 · 미 사이버보안 법제 동향에 관한 고찰”, 「경희법학」, 제48권 제3호.

최상용 (2014). “인터넷을 통해 유포되는 악성 프로그램 대응전략”, 「전자공학회지」.

최재영 · 오상석 · 민성기 (2011). “DNS Response Policy Zone 을 이용한 DNS 싱크홀 운영 방안 연구”, 「한국정보처리학회」.

한국인터넷진흥원 (2013), 「2013 정보보호실태조사 (개인편)」.