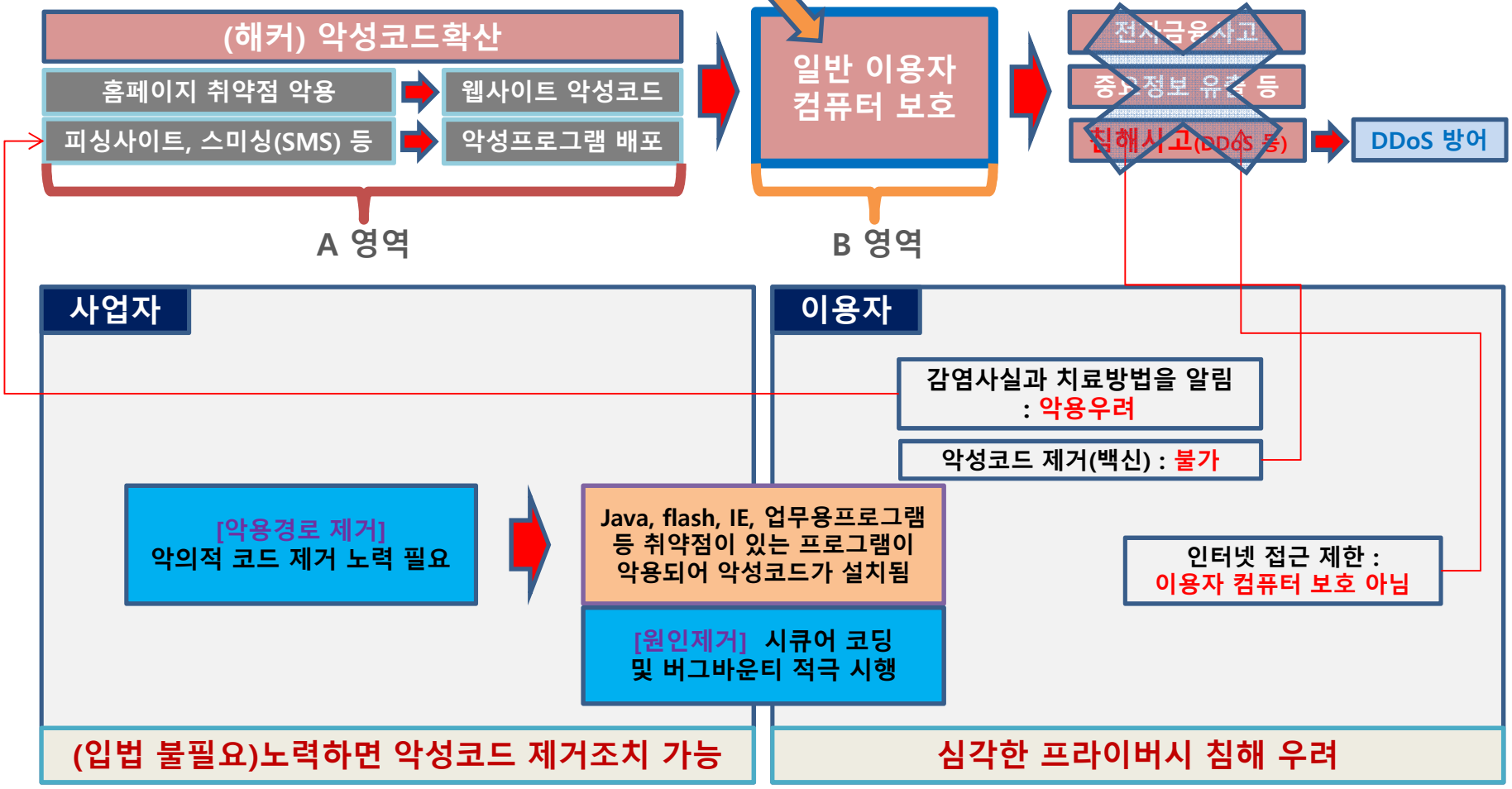
"악성프로그램 확산방지 등에 관한 법률안 " 필요여부 검토 (일명 좀비PC방지법)

목적 : 일반 이용자 컴퓨터를 보호할 수 있는 법체계 확립이 필요함
(현행 정보보호 법제는 네트워크(망) 또는 정보통신기반 보호를 중점으로 하고 있어, 이용자 컴퓨터의 보호 및 실효성 있는 침해사고 예방.대응에 한계가 있음)



(기술적 분석 결론) 일반 이용자 컴퓨터 보호를 위해, 프로그램의 취약점을 제거하고 (시큐어코딩, 버그바운티 등 시행), 취약점을 악용하는 전파경로 제거(웹사이트, 변조파일 등 조치) 하는 2가지 방안병행필요
(별도의 특별법이 없어도 기존 법 해석을 확대하여 시행/조치가 가능할 것임)

<2011.6.15, 국회 문방위 상임위장에서 열린 '악성프로그램확산방지 등에 관한 법률안'에 대한 공청회>

전문가 (찬성측)

권창범 변호사 주요 법률 내용 검토의견

1)이용자의 책무(안 제7조): 본 조항은 백신 설치 등 기본적인 보안수칙을 지키지 않아 악성프로그램에 감염된 컴퓨터가 소위 '좀비 PC'가 돼 DDoS공격에 악용되는 것을 방지하고자 하는 것으로 , 최근 사이버침해의 특징은 이용자를 공격 대상뿐 아니라 공격도구로도 사용하는 것이므로 이용자의 조치없는 침해사고 대응은 실효성을 거두기 어려우므로 반드시 필요한 내용임.

2)서비스제공자 등의 협력(안 제8조): 이용자의 백신 소프트웨어 설치 등 침해사고 예방 및대응에 대한 책무를 규정하면서 사업자에게 아무런 협력의무를 부과하지 않는 것은 법 체계에 맞지 않음. PC방, 도서관, 호텔 등 불특정 다수가 이용하는 컴퓨터의 경우 특정 개인이 사용하는 컴퓨터에 비해 관리가 소홀해 위험에 노출될 우려가 매우 높으므로 백신소프트웨어 설치 및 주기적 갱신 의무 부과는 타당함.

3)이용자 컴퓨터에 대한 접속요청(안 제12조): DDoS 등 침해사고는 인체나 동물에 발병하는 전염병과 마찬가지로 실제 감염된 컴퓨터를 확인하지 않고는 그 원인분석이 불가능해 적절한 대응이 곤란하므로, 침해사고 대응 및 원인조사를 위해 필요한 경우 이용자의 컴퓨터에 접근을 요청할 수 있는 법적 근거가 반드시 필요하며, 이 경우 접속업무 종사자의 목적외 열람 등을 금지함으로써 이용자의 사생활 및 통신비밀을 보장.

4)침해사고 대응 명령 등(안 제17조): 본 조항은 제정안의 핵심적인 규정으로 본 조항이 없을 경우 제정안의 제정이유 및 취지가 멸각될 수 있으나 동시에 접속경로 차단 및 접속 제한의 경우 국민의 통신기본권을 과도하게 제한한다는 비판이 있을 수 있음.

1) **이용자 직접 조치는 크게 의미가 없음 (상당수 백신이용중, 백신이 최신악성코드는 거의 탐지못함)**
2) **사업자의 의무는 맞는 이야기 이지만, 이용자 PC보호를 목적으로 하는 법안이므로... ...**
3) **현재 악성코드 유포지는 모두 파악되어있음, 즉 이용자PC를 조사할 필요는 없음**

채점결과 : 25점 (1/4)

http://blog.dt.co.kr/blog/?mb_id=dubsrep&id=276

<2011.6.15, 국회 문방위 상임위장에서 열린 '악성프로그램확산방지 등에 관한 법률안'에 대한 공청회>

전문가 의견

염흥렬 교수 주요 검토 의견

1) 미래 사이버 보안 위협 환경 대비한 별도 법제정 필요: 3.4 DDoS 공격을 7.7 DDoS공격에 비해 성공적으로 막았으니 별도의 법제정까지는 필요없다는 의견도 있지만, 스마트폰에 대한 악성 앱이 급증함에 따라 좀비 스마트폰이 등장할 가능성이 높아지고 있음. 또 악성프로그램이 날로 지능화, 조직화 및 고도화 되고 있으며 국내 정보통신체계의 취약점을 이용한 악성 프로그램이 다수 출현하고 있음. 이 같은 현실을 고려하면, 확산 방지를 위한 기술적 관리적 대책의 고도화도 필요하지만, 기술, 관리적 대책이 실효적으로 작동하게 만드는 법제도적 기반 마련이 절실히 필요함. 또 **지금까지 법 근거 없이 수행되고 있는 기술적 대응을 법적 근거를 갖는 대응 체계로 전환해 미래 신규 보안 위협 환경에 대응할 필요**가 있음.

2) 인터넷접속서비스제공자의 역할 강화: 제17조 1항에서 방통위 명령에 의해 인터넷접속서비스사업자가 악성프로그램 유포 사이트와 명령 제어 서버에 대한 접속 경로를 차단 가능케 하고, 2항에서 개별 이용자에 대해 방통위가 일정 수준 이상의 침해사고 발생 시 악성프로그램에 감염된 해당 이용자에 대한 인터넷주소 차단 또는 이용자 정보통신망 접속 제한하며, 3~5항에서 정보통신망 차단 설비를 구축하고 있는 법인 및 단체 이용자에 대한 자체적인 차단 조치도 침해사고의 확산을 조기에 방지하기 위한 불가피한 측면이 있다고 판단됨. 이 과정에서 이러한 조치가 감염된 컴퓨터의 치료를 어렵게 하고 국가에 의한 지나친 규제가 된다는 의견도 있을 수 있으나, 이는 국가 위기 상황에서 정보통신망을 포함한 국가 기반의 붕괴를 막기 위한 최소 제한 조치로 판단되며, 침해사고 위기 상황이 종료되면 해당 이용자에 대한 정보통신망 차단 조치는 해제됨을 유의할 필요가 있음.

3) 악성프로그램 유포 사이트와 소프트웨어 제작자의 사전 예방 활동: 제9조 1항의 소프트웨어 사업자에 의한 소프트웨어 보안 취약성 점검 및 보안 패치 제작 및 배포, 제10조 1항의 웹 사이트 운영자에 의한 악성프로그램 정기 점검 및 발견 삭제 등 조치, 제10조 2항의 게시물에 포함돼 있는 악성프로그램 삭제 및 조치하도록 규정하고 있음. 다만, 이 과정에서 제기될 수 있는 국민 감시 우려의 경우, 소프트웨어에 의해 악성 프로그램 포함 여부를 판단하고, 현재 대부분의 PC사용자가 설치해 운영하고 있는 기존 백신 프로그램이 이용하고 있는 탐지 기술을 이용하며, 게시물이나 웹 사이트에 포함된 악성 프로그램 감염 여부 만을 살펴보고, 게시된 자료에 대한 삭제가 아니라 게시 자료에 포함돼 있는 악성프로그램만을 탐지해서 제거토록 규정하고 있어 일정 부분 해소될 수 있다고 판단됨.

4) 이용자 등 보안 지원 강화와 사회적 책임 강화: 제11조에서 규정한 각종 정보제공, 긴근 배포용 백신소프트웨어의 보급, 상당 및 운영 지원 등 인터넷방역사이트 구축 및 운영을 규정하고 있음. 다만 **제11조 인터넷방역사이트의 기능에 지원 대상으로써 이용자뿐만 아니라 민간 웹 사이트 제공자 등 응용서비스사업자 등도 포함해 침해사고 대응 능력이 부족한 민간 응용서비스사업자를 지원할 필요가 있음. 또 제12조 3항의 악성프로그램 확산 방지와 함께 침해사고 대응을 위한 기술 개발 등에 관한 협력 근거는 필요함. 다만 표준화된 방식을 이용한 정보공유가 중요한 만큼 기술 개발 협력뿐 아니라 정보 공유 표준 개발도 명시적으로 포함할 필요가 있음**. 또 제5조에서 '악성프로그램 대응 기술의 개발, 보급 등'도 '악성프로그램 대응 기술, 표준의 개발, 보급 등'으로 확대할 필요가 있음

1) **법제도 강화는 필요 (법률안 대폭 수정 필요)**
2) **악성코드 배포지나 유포지 차단(해당 악성코드나 악성파일)으로 충분히 소기의 목적 달성 가능**
3) **유포사이트, 소프트웨어 제작자의 사전 예방활동에 중심을 두고 실행되어야 함**
4) **민간 웹사이트제공자 등 지원, 정보공유 표준 개발 등 필요**

채점결과 : 80점 (4/4)

<2011.6.15, 국회 문방위 상임위장에서 열린 '악성프로그램확산방지 등에 관한 법률안'에 대한 공청회>

찬성측

조창섭 이글루시큐리티 상무 검토 의견

1)사용자의 기본권 침해: **백신프로그램의 설치, 이용을 규정**하고 있으나 이는 미이행에 대한 처벌규정도 없어 선언적 규정으로 악성프로그램을 예방하기 위한 홍보와 교육에 대한 효과를 높일 수 있는 필요한 조항으로 사용자는 필요에 따라 유, 무상의 프로그램을 설치하면 됨.

2)사업자의 부담증가와 정부의 시장 개입: 컴퓨터보안프로그램의 보급과 악성프로그램 치료지원에 대한 사업자의 과도한 비용 발생을 우려하나, 이는 강제 조항이 아닐뿐더러 현재도 사업자들이 수행하고 있어 추가적인 비용이 발생하는 것은 아님. 사업자들로 하여금 치료방법 안내와 지원을 체계화, 제도화해 정부와의 유기적인 협력을 구축하고자 하는 것, **정부의 차단명령권 또한 국가적인 위기 상황시에만 적용하는 것으로 국민적 혼란을 막기 위한 불가피한 제도로 생각됨**.인터넷 접속차단은 현행 정보통신망법에 ISP사업자의 이용약관에 규정돼 있으나 **정부의 명령권한이 없어 사업자가 손해배상 책임, 고객이탈 등의 이유로 접속제한에 소극적인 경우가 많아 실효적 대응이 안되므로 명령권을 도입하는 것이 타당함**.

3)공격받는자에 대한 대책 필요: 현재 제안법안에는 공격받는 자에 대한 대책이 빠져있음. 서비스를 제공하는 입장에서 가장 중요한 것은 가용성. 이는 공격을 받으면 신속히 복구하고 정상화하는 것을 의미하며, DDoS 공격의 특성상 공격이 시작되면 방어만으로 서비스를 정상화하는 데는 한계가 있음. 즉, 공격이 시작되고 수분, 수초 후에는 서비스를 중지할 수밖에 없음. 공격을 받는 쪽에서 방어하는 것은 네트워크 자원과 시스템 자원이 고갈되기 때문에 아무리 공격을 잘 막아도 결국 서비스를 할 수 없는 것. 그렇게 때문에 공격을 하고 있는 쪽의 치료 또는 네트워크를 단절하는 것이 가장 효과적이고 확실한 방법. 공격받는 자는 누가, 어떤 공격을 하는지 알 수 있음. 공격받는 자가 명확한 근거를 확보하고 ISP나 소관기관에 차단 요청을 할 수 있는 항목이 절대적으로 추가돼야함.

4)백신프로그램 설치, 이용과 협력요청에 대한 지원방안 필요: 이용자의 책무중 제7조 2항 백신소프트웨어의 설치, 이용에 관해 벌칙조항은 없다 할지라도 의무설치를 규정하고 있는바 이용자들의 사용도를 높이기 위해 정부의 지원방안이 마련돼야함. 사용자 입장에서 금액의 많고 적음을 떠나 매년 지불해야 하는 비용이 발생하는 것을 부담스러워하는 것이 사실이므로 사용료의 할인 등을 통해 누구나 사용하고자 하는 인식을 가질 수 있도록 방안 마련이 필요.

1) **프라이버시 침해가능성이 있음(최신 악성코드에 대한 즉시적 효과성도 없음)**
2) **망중립성이 회손될 수 있음**
3) **이용자 PC보호를 목적으로 만든 법안임, 필요한 내용이긴 하나 목적과 상관이 없음**
4) **핵심내용은 아님**

채점결과 : 15점 (1/4)

<2011.6.15, 국회 문방위 상임위장에서 열린 '악성프로그램확산방지 등에 관한 법률안'에 대한 공청회>

반대측

김기창 고려대 법학전문대학원 교수

1)보안취약점 있는 소프트웨어에 대한 배포 중지 명령권(제9조 3항): 무엇이 중대한 보안취약점 인지를 누가 어떻게 판단할 수 있는지. 만만한 국내 사업자만이 정부의 강제조치에 구속될 우려가 있음. 예를 들어, IE6는 이미 알려진 여러 보안취약점이 있지만, 한국 정부가 MS를 상대로 배포중지명령권을 발동 할 것인가. 전문업계가 해당 문제점이 중대한 보안취약점이라는 점에 대해 합의점을 형성할 수 있다면, 이 사실을 공지하고 대처방법을 안내하는 것이 적절하며, 그것만으로 충분히 효과를 거둘 수 있음. 무수한 프로그램의 보안취약점을 정부가 모두 탐지, 평가할 수 없으므로 이규정은 결국 자의적 법집행 시비를 불러일으킬 것.

2)결함있는 백신프로그램의 판매, 제공 금지 명령권(제13조 3항): 진단이나 치료를 제대로 못하는 백신프로그램은 판매, 배포를 못하도록 명령할 권한을 방통위에 부여하는 이 규정은 매우 이례적이고, 과도한 권한을 행정청에 부여하는 것임. 이른바 가짜 백신이 사회적 문제가 되는 것은 맞지만, 그런 행위는 상도덕이나 민형사상 사기사건으로 접근하는 것이 옳음. 방통위가 백신 프로그램 품질관리를 자처하고 나서서, 일정 수준에 미달하는 제품은 판매/제공을 금지하겠다는 것은 백신프로그램 개발, 판매 사업에 대한 사실상의 면허제도와 별다를 바가 없음. 이 규정은 시장 경제질서를 정면으로 부정하는 것임. 구체적으로 어느 수준에 못미치면 방통위가 백신업체에게 이러한 사형선고를 내릴 수 있는지는 기술적으로도 매우 큰 논란이 불가피함.

3)감염 사실 통지 제도(제15조 2,3항): 감염 컴퓨터를 운용하는 이용자에게 ISP가 전화, 전자우편 등 대통령령이 정하는 바에 따라 감염 사실을 알리고, 치료에 필요한 소프트웨어를 내려받을 수 있또록 링크 등을 제공하도록 하는 이 규정은 악성코드를 유포하려는 공격자에게 매우 유용한 기회를 제공해 주는 결과를 낳게됨. 전화를 이용한 피싱 기법으로 이용자에게 '당신의 컴퓨터가 감염됐으니 치료에 필요한 소프트웨어를 내려받으라'는 지시를 하고, 실제로는 악성 프로그램을 내려받도록 하는 행위, 이메일을 보내거나 화면에 팝업창을 띄워서 '귀하의 컴퓨터가 감염됐으니, 치료에 필요한 소프트웨어를 내려받으라'는 식의 공격방법이 발호하는데 최적화된 환경이 조성될 것임.

4)감염 컴퓨터 이용자의 인터넷 접속 박탈(제15조 4항): 해당 PC, 단말기가 감염 컴퓨터라는 점이 확인되는 순간, DDoS 공격을 받고 있는 서버는 그 컴퓨터로부터 오는 트래픽을 즉시 차단할 수 있고, 실제로 DDoS 공격에 대한 대응은 이 방법을 기본적으로 채택하고 있으므로, 굳이 해당 이용자의 인터넷 접속자체를 박탈할 합리적 이유는 없음. 해당 컴퓨터 이용자에게 다른 서버에 대한 접속까지를 모두 차단할 경우, 인터넷전화, IPTV는 물론 장차 클라우드 기반의 컴퓨터 이용 패턴이 자리잡을 경우 당사자의 거의 모든 파일이나 정보에 대한 접근마저 차단당하는 포괄적인피해가 당사자에게 발생함. 이러한 피해는 기술적으로 정당화할 근거가 없음. 하나의 가구 구성원들이 다수의 단말기, PC를 사용하는 추세에 있고, 비록 특정 기기가 감염되더라도 다른 기기로 인터넷에 접속하는 것까지 봉쇄하는 것도 기술적으로 무모함.

채점결과 : 100점 (4/4)

<2011.6.15, 국회 문방위 상임위장에서 열린 '악성프로그램확산방지 등에 관한 법률안'에 대한 공청회>

반대측

이상직 KT 법무센터장

1)규제대상 관련(이용자의 컴퓨터): **본 법의 목적**은 이용자의 컴퓨터를 보호해 **침해사고를 방지**하는데 있는바, 컴퓨터의 정의는 본 법 자체에서 명확하게 정의할 필요 있음. 그럼에도 본 법 제2조 1호는 컴퓨터의 개념요소로 전자적 방법에 의한 정보전송 처리, 정보통신망에의 접속가능, 정보처리장치 중 개인용 컴퓨터단말기 등 대통령령으로 정하는 장치라고 규정함으로써 **하위 법령에 규제 대상인 컴퓨터의 종류와 범위를 위임함으로써 규제의 불확실성을 높이고 있음**. 따라서 규제 대상인 컴퓨터가 무엇인지 예측할 수 있도록 본 법에 명확하게 규정할 필요가 있음.

2)다른 법률과의 관계: 본 법은 컴퓨터의 보호 및 악성프로그램의 확산방지에 관해 다른 법률에 우선한다고 규정하고 있고, 부칙 제 3조에서 정보통신망법 제47조의3 2항 및 4항(정보통신망 일시 접속제한, 약관 규정사항)만을 삭제하고 있음. 그럼에도 불구하고, 정통망법 등과의 관계에서 정보통신망 침해행위의 금지(제48조), 침해사고의 대응(제48조의2), 침해사고의 신고(제48조의3), 침해사고의 원인분석(제48조의 4) 등과 관련해 어느 조항이 우선하는지 또는 보충적으로 적용되는지에 관해 명시적인 규정이 없음.

3)감염컴퓨터에 관한 조치: 인터넷접속서비스제공자는 방통위로부터 감염컴퓨터에 관한 정보를 제공받거나 피해를 입은 자의 요청이 있는 경우에 감염컴퓨터의 이용자에게 감염 사실 및 조치 방법을 알려야 할 의무가 있음. 그러나 피해를 입은 자의 요청이 있다는 이유만으로 그러한 요청을 뒷받침하는 근거가 있는지에 관한 확인없이 이용자에게 감염사실을 알리는 경우에 혼란이 야기될 수 있음. 따라서 **피해를 입은자의 요청이 있는 경우를 포함하고자 한다면 컴퓨터의 감염 등에 관한 구체적인 증거자료를 제시하는 경우로 제한할 필요**가 있음.

채점결과 : 100점 (2/2)

<2011.6.15, 국회 문방위 상임위장에서 열린 '악성프로그램확산방지 등에 관한 법률안'에 대한 공청회>

반대측

최성진 인터넷기업협회 사무국장

1)이용자의 책무관련(제7조): 법안 7조에는 백신소프트웨어 설치, 이용 및 정기적 갱신, 소프트웨어 보안취약점보완프로그램의 확인 및 설치 등 이용자가 자신의 컴퓨터를 악성프로그램으로부터 안전하게 보호하기 위해 지켜야 할 책무를 규정하고 있는바, 네트워크에 접속하는 이용자 일반을 잠재적 위해 요소로 인식해 그들에 대한 국가의 일방적 계몽을 선언하고 있음. 악성프로그램 전파는 이용자가 선택적으로 사용하는 OS의 종류, 컴퓨터 활용 방식, 디바이스의 종류 등 다양한 변수가 존재. 이와 같은 다양한 변수 고려 없이, 이용자 일방을 타인의 컴퓨터에 위해를 가할 수 있는 잠재적 위협으로 간주하는 것은 국가가 국민을 계몽해야 한다는 전 근대적 사상에 기반하는 것으로 보일 우려가 있음.

2)소프트웨어 보안취약점 점검 등(제9조): 법안 9조에는 소프트웨어사업자가 소프트웨어의 보안 취약점을 점검하고 이를 보완할 수 있는 프로그램을 제작, 배포해야 하며 이를 보완할 수 있는 프로그램을 제작, 배포해야하며, 방통위는 중대한 보안 취약점이 있는 소프트웨어에 대해서 개선을 명하되 불응 시에는 제공의 중지 명령을 할 수 있도록 규정하고 있는바, 특정 SW에 보안 취약점이 존재한다는 기준이 명확하지 않음. OWASP 10대 취약점을 기존으로 삼을 것인지, 아니면 실제 아무런 위험이 발생하지 않았음에도 위험을 사전에 탐지해 이에 대한 기준을 마련할 것인지 불분명하게 명시하고 있음.

3)웹사이트의 정기점검 등(제10조): 10조에는 웹사이트 운영자에게 웹사이트 게시자료의 정기점검 및 악성프로그램 발견 시 삭제조치를 하도록 하고, 방통위는 악성프로그램이 숨겨진 게시판을 발견한 경우 해당 게시판의 운영자에게 삭제 명령 등 필요한 조치를 할 수 있도록 하고 있는 바, 비공개 카페 등 외부에서 접근이 용이하지 않은 방식으로 악성코드를 유포하는 경우, 근본적인 문제점에 대한 해소는 되지 않은 채 외부에 드러나는 현상에만 집중하는 문제점이 여전히 존재함. 방통위 등 국가 기관의 **일반적 업무협조로 이행 가능한내용을 굳이 법제화하는 것은 필요가 없어 보임**.

4)이용자 컴퓨터에 대한 접속 요청 등(제12조): 방통위를 가장한 제3자에 의한 피싱이 발생하는 경우, 법제도로 인한 새로운 유형의 피해가 발생할 우려가 있음. 이용자 컴퓨터에 대한 접근은 악성프로그램에 감염된 컴퓨터에 한정되고, 이용자 동의하에 이뤄진다 하더라도 많은 경우, 온라인 소외계층은 국가기관의 접속요청에 대한 이용자 동의의 의미를 잘 이해하지 못하고 수동적, 반사적으로 응할 수 있고 이로 인한 프라이버시 침해 문제도 존재할 것.

채점결과 : 100점 (4/4)