NARS 현안보고서 제48호 2009. 12. 1

발간등록번호 31-9735032-000640-14

National Assembly Research Service

'7.7 DDoS 사고' 대응의 문제점과 재발방지 방안

국회입법조사처

현안보고서 Vol. 48

'7.7 DDoS 사고' 대응의 문제점과 재발방지 방안

배성훈 (문화방송통신팀 입법조사관)

2009. 12 . 1

국회입법조사처
National Assembly Research Service

요 약

분산서비스거부(Distributed Denial of Service : DDoS) 공격이란 해커가 감염시킨 개인용 컴퓨터(PC) 또는 서버로 공격을 하여 특정 시스템 자원을 고갈시킴으로서 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격방법이다.

2009년 7월 7일부터 만 3일 동안 좀비 PC 11만 5천여 대가 청와대 홈페이지를 포함, 국내·외 주요 홈페이지를 공격하여 접속 장애를 발생시켰다. 정확한 경제·사회적 피해현황은 조사되지 않았지만 최소 363억원에서 최대 544억원의 금전적 피해가 발생한 것으로 추정되며 피해기관의 신뢰도에도 악영향을 끼쳤을 것으로 판단된다.

이번 7.7 DDoS 공격은 치밀하게 계획된 공격방법으로 서버에는 처리 지연(혹은 불가능)을 초래하였으며, 치료되지 않은 일부 좀비 PC에서는 주요문서와 하드디스크를 손상시켰다. 또한, 지금까지 금품요구를 목적으로 이루어진 해킹과는 다르게 사회적 공공재를 겨냥한 테러의 성격을 띠고 있는 것이 특징이다.

금번 7.7 DDoS 공격에 제대로 대처하지 못한 원인으로는 정보보호 정책기능의 분산으로 인한 중앙통제기관의 부재, 사이버 공격의 지능화·조직화, 사이버 공격에 대한 훈련 및 국제 공조의 미흡, 인터넷 이용 증가에 따른 정보보호대상의 급증, 악성코드를 분석하기 위한 장비·전문인력의 부족, 사이버 위협에 대한 인터넷이용자의 대응미흡 등을 들 수 있다.

정부는 1996년부터 사이버 위협으로부터 안전한 인터넷 이용환경 조성을 위해 해킹바이러스대응고도화 사업을 수행하고 있다. 방송통신위원회의 2010년도 정보보호 강화 예산(안)은 2009년에 비해 88.5%가 증가한 769억원이다. 그 중 약 384억은 지능화·조직화하고 있는 DDoS 공격 등에 대비하기 위해 사이

버 검역체계, DDoS 긴급대피소 등을 구축·운영하고, VoIP[1]·IPTV·유무선환경의 융·복합서비스 등 새로운 서비스에 대한 정보보호 대책을 강화하는 데에 지원될 예정이다.

하지만 신규사업 및 대폭 증액된 사업의 경우 장비 및 시설투자의 중복이 발생할 소지가 있다. 따라서 한국인터넷진흥원(KISA)의 인터넷침해대응센터(KISC) 업무추진의 합리성을 제고하기 위한 정보화전략계획(ISP) 등에 이를 반영하여 구체적인 계획 수립 후 계획에 따라 수행하는 것이 바람직할 것이다.

결국 제2, 제3의 DDoS 공격이 발생하지 않기 하기 위해서는 다음과 같은 사항이 시급히 조치되어야 한다.

첫째, 정부 각 부처로 분산된 정보보호 기능을 효율적으로 조율할 수 있도록 사이버 위기관리를 위한 구심점이 필요하다.

둘째, 인터넷 침해사건의 대응을 위해 국내·외의 민관이 공조할 수 있는 실시간 공조체제가 필요하다. 해외 관련 유관기관[2]과 인터넷침해대응센터(KISC)간 긴밀한 국제공조협조와 국내 대형 인터넷서비스제공자(ISP), 포털, 백신서비스 업체, 전자상거래업체 등과 공조할 수 있는 협의체를 구성하고 실시간 정보수집 및 공유체제를 구축할 필요하다.

셋째, 이번 공격에서 나타난 법적 미비점을 보완할 수 있도록 정보보호에 관련된, 「(가칭)악성프로그램 확산 방지 등에 관한 법률(안)」등의 제정법령 정비를 긴급히 추진할 필요가 있다. 정부에서 제출한 「정보통신망 이용촉진 및 정보보호에 관한 법률」전부개정안을 보완할 경우 종합적 관리 측면에서 장점이 있을 수 있으나 「(가칭)악성프로그램 확산 방지 등에 관한 법률(안)」의 신규법률 제정을 통하여 규율대상을 명확히 하는 것이 국민들에게 법률규정에 대한 이해도와 법 집행시 예측가능성을 제고시킬 수 있다. 긴급조치 혹은

---

1) 인터넷전화(VoIP : Voice of Internet Protocol)

2) 주요국가의 인터넷침해대응센터(CERT)와 인터넷 서비스 제공자(ISP) 등

예방조치 등이 국가의 권력기관에 의하여 최근 이슈가 되고 있는 패킷감청 등의 오·남용으로 인해 통신의 자유, 표현의 자유, 재산권 행사의 자유, 소비자의 선택권 등 국민 사생활에 대한 기본권을 침해가[3] 없도록 「(가칭)악성프로그램 확산 방지 등에 관한 법률(안)」에 투명하게 절차적·제도적 안전장치를 마련할 필요가 있다.

넷째, 기업 및 개인의 정보보호 인식을 제고하고 투자를 확대방안을 모색할 필요가 있다. 우리나라 개인이 보유한 컴퓨터 1,900여만대 중 15.4%(293만여대) 이상의 개인용 컴퓨터가 백신소프트웨어 설치 및 업데이트 등 실행률이 저조하여 악성프로그램 감염에 노출되어 있다. 기업의 경우도 정보화 대비 정보보호 투자비율이 1% 미만인 기업이 2008년 기준 66.7%에 달하며, 사이버 침해사고 대응하기 위한 활동을 하지 않는다는 기업이 61.1%로 기업의 대응 역량도 미흡한 실정이다.

다섯째, 정보보호 수준제고를 위해 관련 조직을 확충하고 예산 투입을 지속적으로 확대할 필요가 있다. 정부 43개 중앙부처 중 자체 정보보안 전담부서를 운영중인 부처는 9개에 불과하며, 총 전담인력도 78.5명으로 부처당 1.45명에 불과하다. 특히 국무총리실, 감사원, 방송통신위원회 등 15개 부처는 1명 이하의 전담인력을 운영하고 있다. 또한 2009년 R&D예산(12.3조) 중 정보보안 예산은 0.22%(273억원)에 불과하다.

여섯째, 민간부문 사이버 침해 대응 전문조직의 육성이 필요하다. 최근 침해사고의 공격대상이 민·관 사이트를 구분하지 않고 있으며, 실무적인 복구 및 방어 노하우를 보유한 민간이 보다 적극적으로 대응 및 복구에 참여할 수 있도록 기존 협의기구들을 최대한 활용하여 실질적인 협의체가 구성·운영되도록 하는 것이 필요하다.

---

3) 동아일보, “[횡설수설/박성원]인터넷 감청”, 2009.11.18

차 례

표 차 례

그 림 차 례

Ⅰ. 7.7 DDoS 사건의 개요

1. 개요

가. DDoS(Distributed Denial of Service) 공격의 정의

□ '분산 서비스 거부' 공격 : 해커가 감염시킨 개인용 컴퓨터(PC) 또는 서버를 공격하여 특정 시스템의 자원을 고갈시킴으로써 시스템이 더 이상 정상적인 서비스를 할 수 없도록 만드는 공격 방법[4)]

○ 특정 컴퓨터 시스템을 공격하기 위해 해커가 서비스 거부(DoS) 공격을 위한 도구들을 여러 컴퓨터에 심어 분산시켜 놓고 공격 대상 컴퓨터 시스템이 처리할 수 없는 엄청난 물량의 패킷을 동시에 범람시켜 네트워크의 성능을 저하시키거나 시스템 마비를 유발하는 공격

- 즉, 대량의 트래픽을 유발해 네트워크를 마비시키는 수법으로, 정보탈취를 목적으로 하는 해킹과는 다름

□ DDoS 공격의 기원[5)]

○ DDoS 공격은 2000년 2월 아마존, 이베이, 야후 등 전자상거래 관련 사이트들이 사이버 공격을 받아 운영이 정지된 사건이 발생하면서 일반인들에게 알려지기 시작했음

○ 웜 바이러스 '코드레드'는 2001년 7월 윈도2000과 윈도NT 서버를 경유해 미국 백악관의 사이트를 DoS(Denial of Service)공격하는 방법으로 마비시켰음

- 코드레드 웜 바이러스는 발견된 지 보름 만에 전 세계적으로 30만대의 시스템을 감염시켰으며 원형과 변종 코드레드의 피해를 본 국내 시스템이 최소 3만여대에 이르렀음

---

4) TTA 정보통신용어사전(http://word.tta.or.kr/index.jsp), 2009.10.20

5) 네이버 백과사전(http://dic.naver.com) : 문화일보, "'7.7 DDoS 대란' 왜?", 2009.7.11.

○ 2003년 1월에는 슬래머웜에 감염된 다수의 서버가 KT 전화국 DNS 서버를 공격해 공격 2시간 만에 일부 전화국 접속 성공률을 10%로 하락시키고 하나로통신, 두루넷 등 다른 인터넷 서비스 공급자(ISP : Internet Service Provider)들과 SK텔레콤, KTF, LG텔레콤 등 무선인터넷 사업자들의 망에도 트래픽 증가를 유발시키는 사건이 발생했음

나. 7·7 DDoS 공격사건 개요

□ 2009년 7월 7일부터 7월 10일까지 만 3일 동안 진행된 DDoS 공격으로 국내·외의 주요 웹사이트에서 동시다발적으로 접속 장애 발생

○ 2009년 7월 10일 0시를 기준으로 악성코드에 감염된 PC에 대한 파일 파괴 및 부팅 에러를 일으켜 추가적 이용자 피해가 발생

□ 금번 '7·7 DDoS 사이버 테러'의 정확한 피해 액수는 조사되지 않았지만, 현대경제연구원에 의하면 최소 363억원에서 최대 544억원으로 추정됨[6)]

□ 피해기관의 중요자료 유출 등의 피해는 신고되지 않았으나, 피해기관은 신뢰도에 커다란 손실을 입은 것으로 파악됨

6) 현대경제연구원은 2008년 한국인터넷진흥원[(구) 한국정보보호진흥원]의 피해액 산정 방법인 시간당 GDP에 대해 인터넷이 기여하는 부분을 간접 추정하여 손실액을 산출하는 방법을 원용함. 이러한 피해액산정 산식은 개별업체, 기관의 정확한 피 해 파악을 근거로 산출하는 것은 아니며, 또한 획일적인 기준을 적용함에 따라 개별 업체의 특성이 제대로 반영되지 않기 때문에 산정된 피해액에 오차가 존재함에 유의할 필요가 있음.

2. 7·7 DDoS 사건일자별 진행현황[7)]

가. 상황발생시점 주요현황

□ 한국인터넷진흥원(KISA) 인터넷침해대응센터(KISC)에서 2009년 7월 7일 18시 44분경 DDoS 대응시스템을 통해 청와대, 국회 등의 홈페이지가 DDoS 공격을 받고 있음을 인지함

○ 19:00경 상기 정보를 관련기관(국가사이버안전센터 등)에 통보

□ 인지 후 초동 조치내용(7.7 19:00~7.8 02:40)

○ 19:05 방송통신위원회, KISA 관련부서 실무자들 비상대기

○ ~19:50 KISA, 공격 IP탐지 위치 확인

○ 19:50~01:00 공격 PC 이용자 동의하에 원격으로 이용자 PC 분석

○ 21:00 방송통신위원회 네트워크정책국, DDoS 공격 긴급대응반 구성·운영

○ 21:30 KISA 상황전파문 발송(8개 ISP 모니터링 강화 요청)

○ 21:35 KISA 1차 악성파일(샘플) 채취·분석

○ 00:00 'DDoS 공격으로 주요 홈페이지 접속장애' 보도자료 배포

○ 00:39 KISA, 1차 악성파일 내용 분석 결과 도출(공격대상 리스트 추출)

○ 01:30 KISA, 자체위기평가회의 개최 및 유관기관 경보발령 협의

○ 02:40 민간분야 대국민 '주의'경보 발령(4단계 중 2단계)

7) 방송통신위원회, 2009년 국정감사 제출자료, 2009.10.

나. 방송통신위원회의 주요 조치내용

□ 네트워크정책국장을 반장으로 한 비상대응반 구성・운영(7.7~)

○ DDoS 공격 대응을 위한 ISP 임원급 회의 소집(7.9. 09:00) 및 위원장 주재 ISP 등 사장단 긴급회의 소집(7.9. 14:30)

○ 범정부 차원의 사이버위기 대응을 위해 '사이버테러 관련 관계부처 차관회의'(7.9. 15:00), '국정과제 전략협의회'(7.9. 17:00), '국가정책조정회의'(7.10. 08:00) 및 '제4차 사이버안전전략회의'(7.10. 15:00)가 개최됨

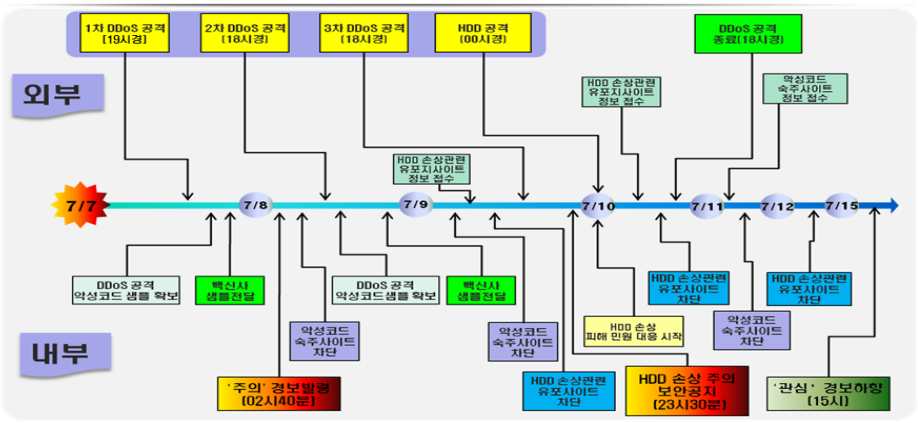
○ 악성코드를 유포하는 것으로 의심되는 숙주사이트 529건 차단(7.8~) 및 악성코드에 의한 PC 손상 가능성을 인지하여 적극 대응

- 3개 포털(네이버, 다음, 네이트) 뉴스란 긴급 게재 및 지상파 3사, YTN 긴급 자막방송 실시(7.9. 23:30) 등

○ DDoS 추가 공격 가능성이 낮아져 민간분야 사이버 경보단계 하향(주의→관심) 조정(7.15. 15:00) 후 '관심' 단계 유지

○ 국가사이버위기 종합대책 방향이 정립되고 DDoS 공격 징후가 없어 9월 17일 12:00시를 기해 사이버 경보단계 해제(관심→정상)

<그림 1> 7.7 DDoS 침해사고 대응 내역



자료 : 한국인터넷진흥원, 「DDoS 신규사업 예산내역 설명자료」, 2009.10.8.

다. 피해현황

□ 7.7 DDoS 사태 피해 집계 결과

○ 국내·외 사이트 피해 내역

- 1차 공격 피해 : 국내 12개 및 미국 14개 사이트에 접속장애 발생
- 2차 공격 피해 : 국내 15개 및 미국 1개 사이트에 접속장애 발생
- 3차 공격 피해 : 국내 7개 사이트에 접속장애 발생

<표 1> 국내 피해사이트 현황

구분	일자	피해사이트				소계
1차	7. 7 18:00 ~ 7. 8. 18:00	청와대 국방부	옥션 조선일보 네이버 (메일)		외교통상부, 국회 한나라당, 농협 신한은행 외환은행 네이버(블로그)	12
2차	7. 8 18:00 ~ 7. 9. 18:00	청와대 국방부	옥션 조선일보 네이버 (메일)	전자민원G4C 다음(메일) 파란(메일) 국민은행	기업은행 하나은행 우리은행 국가사이버안전센터 알툴즈 안철수연구소	15
3차	7. 9 18:00 ~ 7. 10. 18:00		옥션 조선일보 네이버 (메일)	전자민원G4C 다음(메일) 파란(메일) 국민은행		7

자료출처 : 방송통신위원회, 국회 국정감사 제출자료, 2009.10

□ PC손상 피해는 총 1,466건 접수

○ 7.10(금) 396건, 7.11(토) 209건, 7.12(일) 441건, 7.13(월) 337건, 7.14(화) 70건, 7.15(수) 13건

Ⅱ. 7.7 DDoS 공격의 특징과 발생원인

1. 7·7 DDoS 공격의 특징

가. 공격을 위한 치밀한 사전계획

□ 공격 스케줄링 및 업데이트 기능 탑재[8)]

○ 공격대상, 공격방법, 공격시간 등을 정해놓은 시나리오대로 공격

- 특정 사이트만을 공격목표로 함
- 시차를 두고 순차적으로 1차, 2차, 3차 공격을 하였음
- 공격 차수가 높아질수록 좀비PC 수가 줄어듦에 따라 공격대상 사이트 감소함
- 마지막 공격에서는 치료등으로 좀비PC의 수가 줄어들 것을 예상하고 공격 도중 컴퓨터 기억저장장치 파괴하라는 자폭명령이 내려짐

○ 외부에서 파일을 다운로드 할 수 있으며, 스케줄도 변경 할 수 있는 구조

○ 봇넷(BotNet)[9)]을 이용한 과거의 DDoS 공격과 달리 별도의 명령·제어 채널이 없음

8) 정순봉, 'DDoS 공격과 예방 및 치료방법(http://blog.naver.com/itexpert2007)', 2009.8.17

9) 악성S/W에 감염된 다수의 컴퓨터들이 네트워크로 연결되어 있는 형태의 좀비 PC 그룹

<표 2> 기존 DDoS 공격과 7.7 DDoS 공격 비교

구 분	기존 DDoS	7.7 DDoS
명령·제어 서버 존재여부	해커로부터 명령을 받는 명령·제어 서버 존재	악성코드를 업데이트하는 서버만 존재
공격 방법	명령·제어 서버를 통한 실시간 공격 제어	스케줄링을 통한 순차적 공격
방어 방법	명령·제어 서버 차단	공격PC의 악성코드 제거
공격 대상	홈페이지 1~2개	다수의 홈페이지에 동시 다발적 공격 수행
공격 목적	금전적 이득	미확인[10]
공격 주체	주로 중국 등에 위치한 해커 조직	미확인[11]

자료 : 방송통신위원회 제출자료, 2009.9

나. 특정 중요문서파일 손상기능

□ 하드웨어를 파괴하는 가능을 갖는 실행파일(PE: Portable Executable)이 7월 8일부터 다운로드 되어 동작됨

○ 해당 실행 파일은 이미지 파일(JPG)로 위장하여 다수의 IP로부터 다운로드 됨

○ DOC, PPT, KWP[12] 등 다수의 중요 문서를 손상시키는 기능도 확인됨[13]

10) 한국경제, '7.7 DDoS 공격의 배후는 북한...미군 지휘부 통신마비 겨냥', 2009.11.18, 미국 보안전문업체 맥아피 보고서에서 북한을 DDoS 공격의 배후로 단정하진 않았지만 가능성을 배제할 수 없다고 발표함

11) 연합뉴스, '美국방차관보 7월 디도스공격 진원 아직 확인중'. 2009.11.3.

12) 행정기관전산망에서 사용하는 '아래아 한글' 확장자

13) 아이뉴스24, "악성코드에서 정부용 확장자 발견 …사이버 전쟁 의혹 커져", 2009.7.10

다. DDoS 공격 목적의 변화

□ 금품 요구목적의 공격에서 사회적 공공재의 테러목적으로 변화

○ 과거에는 아이템 거래업체, 성인 화상채팅 사이트, 온라인 도박 사이트 등 공개적으로 수사를 의뢰하기 곤란한 업체를 대상으로 DDoS 공격을 가하고 금전을 요구하는 경우가 많았음

○ 그러나 7.7 DDoS 공격은 사회적 공공재를 겨냥한 테러성격을 띠고 있었으며, 공격 자체를 널리 알리려는 목적이 강한 것으로 판단됨

2. 7.7 DDoS 공격의 사회경제적 배경

가. 인터넷환경의 변화

□ 사이버 공격대상의 급증

○ 2003년 1월 25일 인터넷 침해사고 당시 보다 인터넷 및 전자상거래 사용이 폭증하는 등 인터넷 환경이 급속히 변화하면서 신규 악성코드 또한 급격히 증가하여 위험수준이 상승하고 있음

- 2009년은 2003년에 비하여 신규 악성코드가 약 80배 증가함(<표 3> 참조)
- IPTV, 모바일인터넷, 인터넷전화 등 새로운 인터넷 서비스의 활성화로 정보 보호 관리대상이 증가되고 있으며, 이에 따라 활성화 보호대상은 확대될 전망임

<표 3> 인터넷 환경의 변화

구 분		2003년(1.25)		2009년	증가율
인터넷 환경	인터넷사용량 증가	199Gbps	⇒	2,520Gbps	12.7배(1,166%)
	전자상거래	178조원	⇒	630조원	3.5배(254%)
	IP개수	3,098만개	⇒	7,224만개	2.3배(133%)
	신규 악성코드	20,547	⇒	1,656,227	80.6배(7,961%)

자료 : 방송통신위원회 제출자료, 2009.10

나. 사이버공격의 성격변화

□ 사이버 위협 패러다임의 변화

<표 4> 2005년 전후 사이버 위협 패러다임

구 분		2005년 이전	2005년 이후
인터넷 환경		개별망 기반의 국지적 서비스, 상호작용이 적은 정적인 웹1.0	방송통신 융합, 디지털 컨버전스, 상호작용이 많은 동적인 웹2.0
주요 사이버 위협 유형		해킹, 인터넷 웜, DoS(서비스거부)공격, 이메일 스팸	해킹, 스파이웨어, 봇넷, DDoS(분산서비스거부)공격, 휴대폰 스팸
공격 목적		호기심・자기과시, 서비스 가용성 침해	데이터 탈취를 통한 금전적 이득, 불법 유해정보 유포, 저작권 침해
주체별 보안 이슈	국가	기반시설, 국지적 네트워크 보안	All-IP 망 기반 범국가적 인프라 보호
	기업	웹사이트 변조, 서비스 장애	이용자정보 및 내부정보 유출
	개인	피해자	피해자인 동시에 가해자

자료 : 방송통신위원회, 내부자료, 2009.10

□ 인터넷 위협의 대형화 · 조직화

○ 단순해킹 → 개인정보 탈취 → 조직적・지능화된 공격(DDoS 등)으로 변화

- 자기과시 목적의 단순 해킹, 웜・바이러스 등은 감소추세이나, 국가기밀, 기업·개인의 금품탈취를 위한 영리목적성 공격은 증가하는 추세임
- 7.7 DDoS 침해사고처럼 사전에 치밀하게 기획되고, 웜, 바이러스, 해킹 등이 동시적으로 발생하는 복합화·지능화된 공격이 증가하는 추세임

○ 사이버공격에 의한 피해가 현실세계와 밀접하게 연계되고 있으며, 국가안보・경제안정 등을 위협할 수준으로 피해규모가 대형화하고 있음

- 최근 기업의 이미지 추락 및 경제적 손실, 개인의 프라이버시를 침해하는 대규모의 개인정보 유출사고가 빈번하게 발생함

※ 2008년 4월 옥션 개인정보(1,081만 명) 해킹, 2008년 9월 GS칼텍스 고객정보(1,100만 명) 유출 등 대규모 사이버 피해 사례 발생

3. 7.7 DDoS 공격에 대한 대응의 문제점

가. 사이버 공격에 대한 훈련 및 국제공조 미흡

□ 7.7 DDoS 공격징후에 대한 사전대비 부족

○ 방송통신위원회는 2008년 비상시를 대비하여 국내·외 유관기관과 침해사고 대응 모의훈련을 여러 차례 실시함[14)]

- 인터넷침해대응센터 자체 침해사고 대응능력 제고를 위한 모의 훈련(2008년 3월, 9월)
- 국내 주요 인터넷서비스제공업체(ISP), MSO(다수종합유선방송사업자 : Multiple System Operator) 사업자 간 침해사고 공동대응 모의훈련 실시(2008년 6월)
- 범국가적인 사이버 위협 대응 역량강화를 위한 '08년 을지연습 실시(2008년 8월)
- 국외 CERT[15)] 및 국내 주요 ISP와 국제 공동 모의 훈련실시(2008년 12월)

○ 사이버안전 민간분야 위기대응주관기관인 방송통신위원회와 공공분야 주관기관인 국가정보원이 공공·민간 공조 시스템 점검을 위해 2009년 6월 8일부터 12일까지 5일간 '사이버안전 민간분야 위기대응 통합연습'을 실시하였음

- 참여업체
  - 포털(네이버, 다음), ISP(KT, LG데이콤, SK브로드밴드, LG파워콤, 세종텔레콤, 온세텔레콤, 드림라인), IDC[16)](KIDC, KTIDC, 케이알라인), 이통사(SKT, LGT, KTF), 보안업체(안철수연구소, 하우리), 방송사(MBC, SBS, OBS) 등 20개

14) 한국정보보호진흥원, "해킹바이러스 대응체계 고도화 결과보고서", 2008.12.

15) 컴퓨터 비상 대응팀[CERT: Computer Emergency Response Team]

16) 인터넷 데이터 센터(IDC)는 전자 상거래를 행하는 기업으로부터 서버를 맡아서 그 기업의 인터넷 사업을 운용/대행하는 시설(word.tta.or.kr), 2009.11.4.

- 훈련내용

· 도상훈련 : DDoS 공격발생, 제로데이 악성코드 유포, 인터넷 트래픽 증가 등 가상 위협상황에 대한 실시기관 및 실무기관의 대응절차 연습

※ 위기대응 실무매뉴얼의 단계별(관심〈주의〈경계〈심각) 조치사항 훈련

· 실제훈련 : ISP, IDC 등 참여업체의 홈페이지를 대상으로 한 모의 침투훈련을 통해 정보유출 가능성 및 안전성 점검

- 훈련결과

· 도상훈련 : 가상위협상황에 대한 응대의 신속성은 전반적으로 우수하였음

· 실제훈련 : 일부업체의 홈페이지에서 보안 취약점이 발견되었으나 비교적 우수한 것으로 나타남

○ 방송통신위원회는 2008년 5회에 걸친 국내외 유관기관 침해사고 대응 모의훈련 및 7.7 DDoS 공격 한 달 전 사이버안전 민간분야 위기대응 훈련에서 전반적(비교적) 우수로 결과를 내렸으나[17], 봇 명령·제어서버 없는 유형으로 감행된 금번 7.7 DDoS 공격의 방어에서 등 문제점이 도출됨

□ 7.7 DDoS 공격의 국제공조체계의 미흡

○ 2009년 7월 5일 미국 컴퓨터침해사고대응팀으로부터 한국 인터넷침해대응센터는 미국 주요기관이 DDoS 공격받기 전에 공격정보의 통보를 받았으며, 7월 7일 우리나라 주요 사이트들이 공격받음에 따라 미국 관련기관에 DDoS 공격 로그를 요청하였음

○ 그러나 국가마다 침해사고 대응체계나 관련 법제도가 상이하여 국가간 신속한 정보공유 체계가 원활하지 않아[18] 인터넷 이상징후에 대한 정보수집이 지연되었으며, 이로 인해 침해사고에 대한 조기 대응에 차질을 가져옴[19]

17) 방송통신위원회, 2009 국정감사 제출자료, 2009.10.

18) KrCERT/CC의 요청을 받는 국외 CERT가 자국의 민간기관을 대상으로 공격로그 제출을 강제적으로 요구할 권한이 없으므로 앞으로 각국의 CERT 이외에도 Akamai 등의 국외 ISP 등과도 협력체계구축이 필요함

나. 사이버 정보보호 기능의 분산

□ 정부의 정보보호 총괄기능의 분산 및 민간부문 정책부서 축소

○ 2008년 정부 조직개편에 따라 정보보호 정책기획 기능이 방송통신위원회, 행정안전부, 지식경제부 등으로 분산됨에 따라 사건 발생 후 해당 사안을 주도적으로 관장하는 기관이 없었음

○ 또한, 전체 정보보호대상의 95%이상이 민간영역이라 할 때 이에 대한 정보보호는 법적근거, 전문인력, 첨단장비, 정교하고 세심한 정책과 제도수립 등이 필요함

- 정보보호 중요성이 증가함에 따라, 공공부문의 사이버위기 대응을 담당하고 있는 행정안전부, 국정원 등은 관련 조직이 지속 확대되고 있는 반면에, 민간부문의 사이버침해 위협수준이 더욱 높아지고, 피해규모가 커져가고 있음에도 불구하고, 민간부문 사이버위기 대응을 맡고 있는 방송통신위원회 정보보안 정책관련 조직은 (구)정보통신부 시절 국 규모에서 1개 팀 수준으로 축소됨

□ 민관협력 공조체제 한계 노출

○ 7.7 DDoS 사건과 같은 대규모 사이버 공격시 ISP, 보안업체 및 포털사이트 등 민간업체들과 인터넷침해대응센터(KISC) 사이의 유기적 협력이 부족하여[20], 정부의 긴급 상황대처에 한계를 노출함

- 2005년 6월부터 민간기업·기관에 소속된 침해사고대응팀(CERT)이 참여하는 협의체 조직인 CONCERT(Consortium of CERT : CONCERT)가 운영되고 있지만, 7.7 DDoS와 같은 비상상황에서 악성코드 수집·제거 및 시스템 복구 등 실질적인 대응에는 한계를 노출함

- 정부, 보안업체간 실시간 정보공유 및 언론대응 일원화가 미흡함

---

19) 이명수, 류찬호, "77 DDoS 침해사고 대응경과 및 범정부 차원의 대응방안", 한국인터넷진흥원(인터넷 & 시큐리티 이슈), 2009.9.

20) 지식경제부, 「국가 사이버테러 대응을 위한 정보보안 산업육성정책」, 2009.8

· 방송통신위원회, 국정원, 검찰, 경찰 등에서 제각각 정보보고 및 설명요구를 하는 등 침해대응 업체의 불필요한 업무증가함[21]

다. 장비노후화 및 악성코드 분석 전문인력 부족

□ 인터넷 침해 대응장비의 노후화

○ 인터넷침해대응센터(KISC)의 침해대응장비 및 시스템이 2003년 구축된 상태로 노후화됨은 물론, 최근의 네트워크 컨버전스 환경에 대비하기에는 한계가 있음

□ 사이버테러 대응을 위한 종합제어시스템 부재

○ 사이버 공격 상황에 대해 수동분석에 의존하여 즉시 대응에 한계점 노출됨[22]

- 7.7 DDoS 공격시 인터넷침해대응센터(KISC)의 역공학 도구 탐지, 분석도구 우회 기법이 적용된 다양한 유형의 공격에 대한 원인분석 지연으로 초동대응에 한계점 노출됨[23]
- 정상 서비스트래픽과 공격트래픽간 정확한 탐지 방법론 부족함

□ 공격대응을 위한 악성코드 분석 전문인력 부족함

○ 인터넷침해대응센터(KISC)의 조직, 인력이 '03년 수준에 머물러 있어 7.7 DDoS 침해사고에 보다 효과적으로 대응하기에는 한계 노출됨

- 특히, 7.7 DDoS 침해사고 당시 사고의 근원이 되는 악성코드 분석을 위한 전문인력이 3~4명에 불과함

※ 안철수 연구소의 경우 악성코드 분석인력이 20~30여명

---

21) 문화일보, '디도스 테러'싸운 민간연구소 "국정원.검.경.....보고하다 지쳐"_방송통신위원회도 매번 따로....공조 안돼 헛심만 써', 2009.7.13.

22) 지식경제부, 「국가 사이버테러 대응을 위한 정보보안 산업육성정책」, 2009.8.

23) 이명수, 류찬호, "77 DDoS 침해사고 대응경과 및 범정부 차원의 대응방안", 한국인터넷진흥원,「인터넷 & 시큐리티 이슈」, 2009.9.

라. 사이버 위협에 대한 인터넷 이용자의 대응 미흡

□ 컴퓨터 보유 및 백신 설치 현황[24)]

○ 컴퓨터 보유 현황

- 전체 가구(16,916,966가구)의 81.4%가 컴퓨터를 보유하고 있으며, 컴퓨터를 보유한 가구당 평균 컴퓨터 보유대수는 1.38대, 개인이 보유한 컴퓨터대수는 총 19,053,635대인 것으로 추정됨

<표 5> 가구 컴퓨터 보유 현황

	전체 가구*	컴퓨터 보유율	가구당 컴퓨터 보유대수	총 컴퓨터 보유대수
2008년	16,673,162	80.9%	1.36대	18,363,365대
2009년	16,916,966	81.4%	1.38대	19,053,635대

자료 : KISA, 「인터넷 이용 실태조사」, 2008.12 *통계청 장래추계가구 기준

<표 6> 컴퓨터 정보보호 프로그램 설치 현황

	바이러스 백신	악성코드차단 프로그램	유해정보차단 프로그램
2007년	90.0%	82.2%	51.4%
2008년	94.3%	90.6%	52.7%

자료 : KISA, 「개인 인터넷 이용자 정보보호 실태조사」, 2008.12

<표 7> 바이러스 백신 이용방법(바이러스 백신 이용자 기준) 현황

	실시간 바이러스 감시기능 설정	바이러스 예약검사 기능 이용	월1회 이상 바이러스 검사 실시
2007년	78.5%	-	77.1%
2008년	83.5%	57.4%	83.4%

자료 : KISA, 「개인 인터넷 이용자 정보보호 실태조사」, 2008.12

24) 한국정보보호진흥원, 「2008년 정보보호 실태조사」, 2008.12.

○ 컴퓨터 백신S/W 설치 및 업데이트 등 실행률이 저조하여, 전체 1,905만 여대 개인용 컴퓨터 중 15.4%(293만 여대) 이상이 악성코드 감염에 노출되어 있으며, 이는 금번 7.7 DDoS 공격에 동원된 11만5천 여대의 약 25배에 해당됨

- 인터넷에 연결된 것으로 추정되는 PC 중 94.3%인 최소 1,295만 여대(최대 1,793만 여대)에 백신프로그램이 설치되어 있으며, 그 중 16.6%인 최소 215만 여대(최대 298만 여대)는 월 1회 이상 바이러스 검사를 하지 않는 것으로 나타났음
- 백신 프로그램을 설치하지 않은 PC는 최소 78만 여대(최대 108만 여대)이고, 월 1회 이상 바이러스 검사를 하지 않는 PC는 최소 215만 여대(최대 293만 여대)로써 293만 여대 이상이 악성코드 감염위험에 노출되어 있음

□ 정보화 역기능과 사이버위협에 대한 개인의 적극적 대응 미흡

○ 이용자들은 정보보호의 중요성에는 공감하고 있으나, 정보보호 관련 최신 정보를 수집하거나 대책을 마련하는 이용자는 30.2%에[25] 불과함

○ 7.7 DDoS 발생 시 보안패치에 대한 국민들의 적극적 참여부족으로 대응에 한계

※ ISP가 감염 PC 이용자 8,600(1 · 2차 공격)명에게 무료백신 설치 안내를 하였으나 2,300명만 설치[26]한 것으로 나타남

□ 정부기관 및 공공기관의 백신서비스 이용현황[27]

○ 「웜/바이러스 백신S/W」 도입율[28]

- 행정기관 : 66.8%

---

25) KISA, 「개인 인터넷 이용자 정보보호 실태조사」, 2008.12

26) 한국경제, "'무사안일'이 파국 부른다", 2009.7.13.

27) 행정안전부, 「행정안전부 국무회의 보고자료」, 전자정부 민원서비스에 연결된 PC를 대상으로 전수 설문 조사한 결과, 2009.4.21

28) 2008년 행정기관「'08 전자정부 실태조사」, 공공기관「'08 공공부문 정보보호 설문조사」, 단, 행정기관은 전수조사, 공공기관은 302개 공공기관에 대해 표본 조사한 것임

- 공공기관 : 91.7%
- 중앙행정기관은 거의 백신S/W가 도입·설치되어 있지만, 일선 민원대상 PC는 백신S/W 도입이 저조한 실정임
- 민간은 94.3%의 컴퓨터에 백신프로그램이 설치되어 있는 것으로 나타남[29)]

○ 행정기관의 백신 보급률이 낮은 이유는 민간의 경우 개인용 PC를 위한 무료백신이 보급되고 있지만, 지방자치단체의 경우는 정보보안을 총괄하는 부처가 따로 존재하지 않음에 따라, 범정부적으로 백신서비스 설치를 관리·감독하는 기관이 없기 때문인 것으로 보임

- 현재 컴퓨터 백신S/W 구입·관리를 위한 별도의 예산은 없으며, 각 부처별로 간접비에서 개별적으로 편성하고 있는 실정임

마. 정보보호 인력 및 투자 부족

□ 정부의 43개 중앙부처 가운데 자체 정보보호 전담부서를 운영중인 부처는 9개에 불과함

○ 자체 정보보호 전담인력은 총 78.5명으로 부처당 평균 1.45명에 불과함

- 국무총리실(0.6명), 감사원(0.2명) 및 방송통신위원회(0.8명) 등 16개 기관이 1명 이하의 전담인력이 배치되어 있는 것으로 나타남

○ 정부 R&D 예산(12.3조) 중 정보보안 예산은 0.22%(273억원)에 불과함[30)]

29) 한국정보보호진흥원, 「개인 인터넷 이용자 정보보호 실태조사」, 2008.12.

29) 지식경제부, 「국가 사이버테러 대응을 위한 정보보안 산업육성정책」, 2009.8.

<표 8> 정부 부처별 정보보호 부서 및 인력현황

기관명	현 재		
	전담조직	정보보호인력	담당부서
합계(평균)		78.45명(평균1.45명)	
통일부	X	1	행정관리담당관
행정안전부	O	2	정보화담당관
외교통상부	O	3	외교정보보안팀
기획재정부	X	0.8	정보화담당관
노동부	X	0.75	정보화담당관
환경부	X	1.1	정보화담당관
농림수산식품부	X	0.65	정보화담당관
국토해양부	X	0.7	정보화통계담당관
문화체육관광부	X	1.5	정보화담당관
교육과학기술부	O	6	정보보호팀
법무부	X	0.8	정보화담당관
지식경제부	X	0.4	정보화담당관
보건복지가족부	X	2.75	정보화담당관
여성부	X	0.5	법무정보화담당관
국방부	O	9	정보화기획관
법제처	X	0.3	법제정보과
국가보훈처	X	1.1	정보화팀
국세청	O	6	전산정보관리관
기상청	X	1	정보통신기술과
농촌진흥청	X	1.6	지식정보화담당관실
대검찰청	X	2.5	정보통신과
문화재청	X	0.25	정보화기획팀
행정도시청	X	0.6	정보인프라과
방위사업청	X	3	전산정보관리소
병무청	X	2.3	정보기획과
산림청	X	0.7	정보통계담당관실
관세청	X	2	정보협력국
경찰청	O	10	정보통신담당관실
소방방재청	X	0.5	정보화담당관
식약청	X	0.2	정보화담당관
조달청	X	0.6	전자조달국
중소기업청	X	1.3	고객정보화담당관
통계청	O	3	통계정보국
특허청	O	2	정보기획국
해양경찰청	O	3	정보통신과
방송통신위원회	X	0.8	정보전략팀
감사원	X	0.2	지식관리담당관
국무총리실	X	0.6	인사과
민주평통	X	1	기획재정담당관
공정거래위	X	1.2	정보화담당관
금융위	X	0.3	규제개혁법무담당관
국가인권위	X	0.35	행정법무담당관
국민권익위	X	1.1	정보화담당관

자료 : 행정안전부 제출자료 2009.10(직무수행률을 기준으로 산정되었으며, 국방부, 경찰청은 기관의 특성상 타 기관과 조직 규모가 매우 상이하여 평균산정에서 제외)

□ 지식정보 보안산업의 인력수급 불균형[31]

○ 2007년 기준, 지식정보보안 분야 수요 인력은 31,705명이나 공급인력은 30,342명으로 인력부족 비율은 약 4.3%에 해당되며, 2013년에는 인력 부족 비율이 약 11.8%에 이를 것으로 전망됨

□ 기업 정보보호 활동과 투자도 낮은 수준임

○ 사이버 침해사고에 대응하기 위한 활동을 하지 않는다는 기업이 61.1%로, 기업의 대응역량도 미흡한 실정임

※ 7.7 DDoS 발생 당시 DDoS 보안장비를 갖추거나 여유 대역폭을 확보한 일부 기업을 제외한 대다수 기업들의 피해가 심했던 것으로 파악됨

○ 정보화 대비 정보보호 투자 비율이 1% 미만인 기업이 2008년 66.7%에 달하여 매우 취약하고(<표 9> 참조), 정보보호책임자(CSO)를 임명하고 있는 기업은 12.2%에 불과함

- 대부분의 기업이 해킹·DDoS 공격 등의 위협에 상시 노출되어 있지만, 보안 인식수준이 낮고 경영진의 관심이 미흡함

<표 9> 국내기업의 정보화 대비 정보보호 투자비율

연 도	정보보호 지출없음	1%미만	1%~ 3%미만	3%~ 5%미만	5%~ 7%미만	7%~ 10%미만	10%이상
2007	50.8	27.5	11.4	5.1	1.8	2.3	0.8
2008	44.5	22.2	15.3	8.2	3.4	6.0	0.3

자료 : 한국정보보호진흥원,「2008년 정보보호 실태조사」, 2008.12.

31) 지식경제부, 「지식정보 보안산업 진흥 종합계획」, 2008.12.

Ⅲ. 국내 · 외 사이버 보안 관련 법제

1. 주요국의 사이버 보안 관련 법제 현황

가. 미국

□ 관련 법률

○ 「컴퓨터보안법(Computer Security Act)」

- 미국국립표준기술연구소(NIST)를 중심으로 정부 컴퓨터의 보안관련 기준 프로그램을 제공하도록 하고 연방정부 컴퓨터 시스템의 운용에 관계되는 정부관계자 교육을 규정하고 있음

○ 「국토안보법(Homeland Security Act of 2002)」

- 포괄적인 테러로부터 미국의 전체 국가기반을 보호하기 위해서 제정된 법으로 총 17장으로 구성되어 있는데, 이중 특히 사이버보안과 관련하여 제2장의 정보 분석 및 기반시설보호에 관한 규정, 제10장의 정보보호에 관한 규정을 두고 있음
- 미 연방기관들이 분야별로 각각 분담하고 있는 국토안전보장업무를 총괄하는 국토안보부를 창설하고 정보기술을 유용하게 활용하여 사이버공격이나 물리적 공격으로부터 미국의 영토를 방위하기 위해 국가 정보통신 기반망을 비롯 주요기반보호를 국토안보의 핵심으로 인식하고 이를 위해 정보 분석 및 기반보호국을 설치함

○ 「애국법(USA Patriot Act)」

- 9.11 테러 직후 테러 위협에 대응하기 위한 수사력 강화와 국가 안보 확립을 목적으로 한 법률임
- 주요 내용을 살펴보면, 종래 법집행 기관의 용의자 관련 전화번호 기록권한을 인터넷이나 휴대전화를 포함한 전자통신으로 확대하고, DCS1000(이른바

Carnivore[32]) 등에 의한 IP주소 등을 기록함(다만, 통신내용은 기록하지 않음)

○ 「사이버보안강화법(Cyber Security Enhancement Act of 2002)」

- 2002년 하원에서 통과 후 상원에서 폐기되었으나, 「국토안보법」에 포함되어 통과됨
- 이 법 제2장 SEC. 225에는 사이버보안 강화법이 규정되어 있는데, 동(同)법에는 양형위원회 관련 내용, 긴급 공개 예외, 선의의 예외규정, 불법장치의 인터넷 광고, 강화된 벌칙, 프라이버시 보호 등이 규정되어 있음
- 특히 사이버 공격자가 고의 또는 부주의로 법률을 위반하여 심각한 신체적 상해를 유발하거나 시도하는 경우에 본 Title에서 정한 벌금이나 20년 이하의 징역 또는 이를 병과하고 공격자가 고의 또는 과실로 사망을 유발하거나 유발하고자 시도하는 경우에 유기 또는 무기징역에 벌금을 부과할 수 있도록 규정하여 신체의 상해나 생명의 위험과 관련된 컴퓨터 범죄의 처벌을 대폭 강화하고 있음

○ 「연방정보보안관리법(Federal Information Security Management Act of 2002:FISMA)」

- 「전자정부법(E-Government Act of 2002)」 제3편으로 제정되었으며, 연방의 주요 정보자원에 대한 보호 및 통제를 위해 포괄적인 프로그램을 제공하는 한편, 고도로 네트워크화된 국가기반 환경의 보호를 위해 민간인을 비롯해 국가안보 관련기관과 법집행기관 전체의 정보보호 노력을 조정함과 동시에 사이버위협에 대해 효과적으로 대응할 수 있도록 하기 위한 것

나. 일본

□ 관련 법률

○ 「전기통신사업법(電気通信事業法)」

32) 미국 연방수사국(FBI)이 사이버 범죄 예방을 위해 1999년 개발한 인터넷 전자우편(이메일) 감시 시스템

- 1984.12.25. 법률 제86호로 제정되어 2006.6.2일 법률 제50호로 개정되었는바, 이법은 전기통신사업의 공공성에 비추어 적정하고 합리적인 운영을 꾀함과 동시에 그 공정한 경쟁을 촉진하고 전기통신서비스의 원활한 제공을 확보하여 이용자의 이익을 보호하는 한편, 전기통신의 건전한 발달 및 국민편의를 도모하여 공공복리를 증진하는 것을 목적으로 하고 있음

○ 「고도 정보통신 네트워크 사회 형성 기본법(高度情報通信ネットワーク社会の形成に関する基本方針を定めた法律」

- 일명「IT기본법」이라고 하며 이법은 사이버안전 측면에서 최근 문제가 되고 있는 정보통신 네트워크 안전성 확보를 위하여 국민이 안심하고 네트워크를 이용하기 위한 네트워크 안전성 및 신뢰성 확보 등에 관한 조치가 선행되어야 함을 규정(제21조)
- '고도 정보통신네트워크 사회 추진전략 본부'로 하여금 정보통신 네트워크의 안전성 및 신뢰성 확보 시책에 대한 중점 계획을 작성토록 하는 등 우리나라의「정보화촉진기본법」과 유사함

□ 주요 정책

○ 2006년 2월 내각관방에서는 국가 전반의 정보보호 요구에 대응하기 위해 '제1차 정보보호 기본계획'을 수립하여 추진해 왔으며, 2009년 1월 현재 '제2차 정보보호 기본계획'을 마련하고 있음

- 정부・지방공공단체, 주요 인프라, 민간(개인 및 기업)을 대상으로 '정보보호 기본계획' 의 주요 대책을 2006년에서 2008년까지 3년간 추진했음
- 정부・지방공공단체, 주요 기반, 기업, 개인 영역으로 구분하여 'Secure Japan 200X'를 수립하고 실행성과를 평가함

○ 또한, 총무성에서는 u-Japan 정책을 통해 정보화 역기능에 관한 100대 과제를 정리한 'ICT 안심·안전 21 전략'을 추진 중에 있음

○ 경제산업성에서는 정보보호 위협에 대한 국제적 대응, 국제경쟁력 강화 기반 마련, 국내·외 다양화된 변화환경 대응을 위한 글로벌 정보보호전략을 추진 중에 있음

다. EU[33]

□ 유럽 연합(EU : European Union)은 25개 회원국으로 구성된 연합체로 정치적, 경제적, 안보적으로 공동정책을 취하고 있음

○ 2004년 제정된「EU 헌법(Constitution for Europe)」에 따르면 정보보안과 관련, 현재 6개 수준의 법적 규제가 있으나「EU 헌법」은 각 회원국들이 자국의 법체계를 수정하는 등 일정한 절차를 거쳐 승인되어야 하며 EU 25개 회원국 모두가 승인(혹은 국민투표)하지 않으면 그 효력을 발휘할 수가 없음

□ 관련 제도

○ 「프레임워크 지침(Directive 2002/21/EC)」

- 개인정보나 프라이버시를 안전하게 보호하고 통신네트워크의 안전성을 확보하는 것을 목적으로 함

○ 「안전한 인터넷 사회-대화, 협력 및 부권(Communication from the Commission, 2006.5.31)」

- "안전한 정보사회를 위한 전략(Strategy for a secure information society)"에 근거하여 정보시스템에 대한 공격증가, 모바일 기기의 사용증대 등에 따른 보안인식 제고를 위한 것임
- 주요 목표는 스팸, 스파이웨어 등 진화하는 위협에 대한 대처방안을 확보하고 법집행기관과의 협력을 강화, 신종 범죄에 대응하며 기반시설보호를 위한 프로그램을 제공하고 전자통신관련 법제도 재검토 등을 위한 것임

○ 「유럽 네트워크 및 정보보안 기구(ENISA: Europe Network and Information Security Agency) 설립에 관한 규칙(Regulation(EC) No 460/2004」

- ENISA의 설치를 규정하고 있는 법
- ENISA는 그리스 크레타 섬에 본부를 두고 있으며, EU 회원국에 '컴퓨터

33) 이연수, 이수연, 윤석구, 전재성, "주요국의 사이버안전관련 법•조직체계 비교 및 발전방안 연구", 국가정보연구, 제1권 2호, 2009.2.24

비상대응팀(CERT)'의 구축을 지원하며 이를 네트워크로 묶는 초국가적 시스템을 마련하고자 함[34]

- 이 규칙은 유럽집행위와 회원국을 대상으로 네트워크 및 정보보안에 대한 전문지식을 제공하고 EU 및 회원국의 네트워크 및 정보보안 활동을 지원하며 이해관계자들 간의 원활한 정보교환을 촉진하고 네트워크 및 정보보안 관련 기능을 조정하여 상호교류를 증대하기 위한 규정 등을 두고 있음

○ 「사이버범죄조약(Convention on Cyber Crime)」[35]

- 사이버범죄에 관한 가장 포괄적 문서이자 최초의 국제조약으로 각종 인터넷 범죄를 퇴치하기 위해 각 국가의 공조를 명기하고 있음
- 현재 총 43개국이 가입했으며, 2004년 7월 1일 발효되었으나 자국 내 의회의 비준을 받은 국가는 18개국 정도임

○ 「통신네트워크에 관한 데이터보존 지침」

- 테러리스트를 추적하기 위해 통신서비스 제공자가 통화 데이터를 6~24개월간 보존할 것을 의무화하도록 규정

라. 영국[36]

□ 관련 법률 및 지침

○ 「대테러범죄 및 안전보장법(Anti-terrorism, Crime and Security Act 2001)」

- 미국의 9.11테러 이후 테러 대응을 위해 필요한 여러 테러대책 관련 내용을 포함하고 있음

---

34) 세계일보, "유럽연합, 초국가적 대응체계 구축". 2009.7.21

35) 인터넷을 이용한 모든 범죄행위에 대하여 상세한 규정을 두고 이를 처벌하도록 한 최초의 국제조약으로, 일명'부다페스트조약'이라고도 함. 국제사회가 사이버범죄에 공동으로 대처하고 국가간 공조를 긴밀히 하기 위한 핫라인 설치 등이 명시되어 있음

36) 이연수, 이수연, 윤석구, 전재성, "주요국의 사이버안전관련 법•조직체계 비교 및 발전방안 연구", 국가정보연구, 제1권 2호, 2009.2.24.

- 정보보호 관련 주요 내용으로는 동법 제11편에 통신 데이터(전화, 인터넷 및 우편내용 등) 보전을 위한 권한 관계를 규정하고 있음
- 「정보보안관리에 대한 표준(BS 7799)」
- 1995년 정보자산을 체계적이고 표준적인 관리지침 및 방법에 따라 관리할 목적으로 영국 표준기관(BSI : British Standard Institution)이「정보보안관리에 대한 표준(BS 7799 ; British Standard for Information Security Management)」을 제정하였음
- 동(同)표준은 Part 1과 Part 2로 구성되어, Part 1은 조직에서 정보보호관리체계를 수립하기 위한 지침으로 활용할 목적으로 2000년 12월에 국제표준인 ISO/IEC 17799로 채택되었음
- Part 2는 정보보호관리체계의 규격(Specification)을 제시하는 인증심사시 활용되는 지침과 설명을 통해 정보보안 관리시스템의 모델을 지원해 주는 내용으로 2005. 10월에 역시 국제표준인 ISO/IEC 27001로 채택되었음

○ 정보보증중앙지원국에서는 2007년 국가정보보안정책(A National Information Assurance Strategy)을 발표하여, 기관의 효율적인 위협정보 관리를 위해 임원급의 책임과 의무를 강조하는 한편, 전문 기술인력 양성 및 홍보 정책을 추진

○ 내각부는 정부기관의 보안정책을 확산시키기 위한 '정보보호 기본정책 (HMG Security Policy Framework, 2008년 12월)' 등 정보보호 관련 정책을 발표

2. 우리나라의 사이버공격 관련 법·제도 현황

□ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정통망법") : 정보통신망의 안정성 확보를 위한 예방 및 대응조치 전반 규율

○ 정보통신망에 대한 침해행위 금지

○ 침해사고 대응을 위한 정보 수집, 예·경보 및 긴급조치의 발령

○ 침해사고 신고 및 원인의 분석

○ 정보보호 안전진단제도 및 정보보호관리체계 인증

□ 국가위기관리기본지침(대통령 훈령 제229호, 대통령실)

○ 국가 위기관리체계 구축 및 업무 수행의 기본지침

□ 국가사이버안전관리규정(대통령 훈령 제222호, 국정원)

○ 국가 사이버안전 조직체계 및 운영에 관한 사항

□ 사이버안전 (민간)분야 위기대응 실무매뉴얼(방송통신위원회)

○ 민간분야 위기상황 발생 시 방송통신위원회가 적용할 세부 대응절차 및 제반 조치사항 등을 규정

3. DDoS 공격 대응을 위한 관련법 제·개정 방안

가. 「(가칭)악성프로그램 확산 방지 등에 관한 법률(안)」(이하 "좀비PC법") 제정 추진[37]

□ 배 경

○ 7.7 DDoS 공격에서도 드러났듯이, 일반 이용자들의 PC가 자신도 모르게 악성코드에 감염되어 DDoS 등 사이버 공격을 받거나 공격기지로 악용되고 있음

○ DDoS 공격에 이용되는 좀비PC에 대한 조치를 취할 수 있는 법적근거가 명확하지 않아 피해가 확산된바 있음

○ 따라서 범정부적 종합대책수립과 침해사고대응에 적극적으로 대처하고, 악성 프로그램으로부터 이용자 PC 등 정보처리장치를 보호하기 위한 제도의 필요에 따라 방송통신위원회에서 「좀비PC법」을 준비하고 있음

37) 한국인터넷진흥원, 「(가칭)악성프로그램 확산 방지 등에 관한 법률(안)」제정을 위한 정책 토론회 발표자료, 2009.9.7.

□ 방송통신위원회 추진 법안의 주요내용

○ 침해사고 예방 및 대응을 위한 민관협력체계 마련

○ 컴퓨터 보안프로그램 개발 및 보급지원

○ 소프트웨어의 보안 취약점 보완

○ 악성프로그램 정기점검 의무화 및 삭제 명령

○ 좀비PC 등에 대한 인터넷서비스제공자(ISP)의 접속 제한 등

○ DNS sinkhole 적용

○ 침해사고 원인분석을 위한 이용자 컴퓨터 등 접속요청

○ 보안프로그램 긴급 배포

나. 「좀비 PC법」 제정과 「정통망 법」 전부개정(안)과 관련된 쟁점과 비교

□ 현재 「좀비 PC법」 단독 법안으로 발의하는 경우와 기존의 「정통망 법」 전부 개정안에 추가하는 방법을 둘러싸고 이견이 존재함

□ 「좀비 PC법」 제정의 경우

○ 장점

- 의무주체, 책임범위 등이 명확하여 법의 예측가능성 및 집행력이 높음
- 컴퓨터 이용자와 인터넷서비스제공자 등으로 적용범위를 명확하게 정의할 수 있음
- 기술개발 촉진·지원, 시범사업 실시 등 다양한 민관협력 시스템 및 촉진 정책 도입 가능함
- 유사용어의 사용에서 오는 입법기술상의 어려움 해소 가능 및 「정통망 법」의 정체성 유지 가능함

○ 단점

- 인터넷 침해사고 예방 및 대응에 관한 사항이 「정통망 법」, 「좀비 PC법」

등에 분산되어 침해사고 발생시 적용법규에 혼란을 초래할 수 있음

- 법제도 선진화를 위해 유사법령의 통폐합을 추진하고 있는 정책 추세에 반함
- 「정통망 법」을 개정하는 경우보다 관련 이해관계자들의 저항이 클 것으로 예상

□ 「정통망 법」 전부개정안에 추가하는 경우

○ 장점

- 인터넷 침해사고 예방 및 대응에 관한 사항을 하나의 법률에서 규율함으로서 종합적 관리 가능
- 현재 「정통망 법」 개정(안)이 이미 국회계류중인 바, 보다 빠른 입법도 가능
- 「정통망 법」의 일부 조문을 보완·개정하거나 신설하는 것이 입법경제상 효과적임

○ 단점

- 지금도 140여조에 이르는 전부개정 안에 새로운 내용까지 추가하면 법률이 방대하여 법률의 이해도가 떨어질 우려가 높음
- 현행 「정통망 법」은 '망'보호 중심으로 되어 있어 개인용PC가 감염된 좀비 PC를 이용한 침해행위에 대응할 수 있는 수단과 권한에 한계가 있음
- 추가할 수 있는 법조문에 한계가 있어 촉진규정은 빠지고 규제규정만 남게 될 우려가 있음

□ 「좀비 PC법」의 제정안과 「정통망 법」 전부개정안의 차이점 비교[38)]

주요 「좀비 PC법」 내용	「정통망 법」과의 차이점
1. 주요 용어의 정의 ① 컴퓨터 - 정보통신망에 접속이 가능한 정보통신처리 장치 중 개인용 컴퓨터단말기 등 대통령령이 정하는 장치	o 기존의 정보통신망은 "정보통신체제" 즉 네트워크를 중심으로 한 개념 - 「좀비PC법」에서는 개인의 PC나 스마트폰 등 "이용자의 단말기"가 대상

38) 이창범, 「좀비 PC 최소화를 위한 법/제도 제정 방향」, 2009.10.27

주요 「좀비 PC법」 내용	「정통망 법」과의 차이점
② 이용자 - 컴퓨터 등 정보처리장비를 이용·관리하는 개인, 법인, 단체	o 이 법의 이용자에는 망법과 달리 관리자가 포함됨 - 회사 등 법인 PC의 경우 PC관리자가 백신설치 등의 주체가 되어야 하기 때문임
③ 인터넷접속서비스 제공자 - 인터넷접속서비스를 제공하는 자	o 주요정보통신서비스 제공자는 전국적으로 정보통신망서비스를 제공하는 자인 바, 이동통신사 등 인터넷과 무관한 사업자도 포함되는 대신 SO/RO 사업자가 불포함 - 「좀비PC법」의 인터넷접속서비스 제공자에는 전국단위 인터넷망을 제공하는 사업자와 SO/RO사업자 모두 포함
2. 컴퓨터 보안프로그램의 보급 확산 및 시범 사업의 실시 - 컴퓨터 보안프로그램 보급확산을 위한 기술 등에 대한 시범사업 실시 - 백신소프트웨어의 성능점검 및 결과 공표 - 인터넷접속서비스 제공자, 포탈서비스 제공자 등의 이용자 백신설치 및 업데이트 지원 - PC방, 카페 등에서 다중이 이용하는 컴퓨터에 대한 백신설치 강화	o 기존 법제도에는 없는 새로운 규정으로 이용자 컴퓨터의 좀비 PC화를 근본적으로 예방하기 위한 조치
3. 소프트웨어의 보안취약점 보완 - SW 정기 보안패치 및 배포 - SW 보안취약점 점검 및 개선명령 등 조치 - 보안취약점 보완명령을 거부한 SW에 대한 제공 중지명령	o 「정통망법」은 침해사고 대응조치의 일환으로 소프트웨어 제작자에게 보안패치 제작·배포 등을 요청할 수 있도록 하고 있으나, - S/W제작자의 의무는 아닌 바, 제작자가 거부할 경우 강제할 방법이 없음

주요 「좀비 PC법」 내용	「정통망 법」과의 차이점
	o 「좀비PC법」에서는 침해사고 예방을 위해 침해사고 발생시는 물론 평상시에도 보안취약점 점검 및 보안패치 제작·배포요청을 할 수 있게 할 예정 - 또한, 공중의 이용에 제공되는 소프트웨어의 중대한 보안취약점이 발견된 경우에는 일정 기간을 정하여 개선을 명하고, - 미이행시 해당 소프트웨어의 제공중지를 명할 수 있도록 하여 보안취약점 개선요구의 집행력을 높이도록 함
4. 악성프로그램 삭제 명령	<신설> ※ 다만, 국회 계류중인 「정통망법」 전부개정안이 웹사이트 운영자 또는 관리자에게 악성프로그램 삭제 명령권을 규정 - “웹사이트”만을 악성프로그램 삭제의 대상으로 할 경우 파일 다운로드 등에 활용되는 FTP 등이 포함되지 못해 사각지대가 생김 - 「좀비PC법」에서는 “게시판” 운영자 및 관리자를 악성프로그램 삭제 명령의 대상으로 하고자 함 · “게시판”이라 함은 정보통신망을 이용하여 이용자가 자료를 게시할 수 있는 컴퓨터 프로그램이나 기술적 장치를 의미하며, Web외에 FTP, PC통신 등 네트워크를 이용한 모든 공간이 해당함
5. 좀비PC에 대한 ISP의 조치	o 현행 「정통망법」에서 좀비PC에 대

주요 「좀비 PC법」 내용	「정통망 법」과의 차이점
- 방송통신위원회의 인터넷접속서비스 제공자에 대한 좀비PC에 대한 통보 및 조치요구 - ISP의 좀비PC 이용자에 대한 통지 및 치료 안내 - 이용자의 ISP안내에 따른 좀비PC 치료 협조 - 방송통신위원회의 긴급 접속제한 명령	한 조치는 주요정보통신서비스 제공자가 이용약관에 따라 자율적으로 판단하여 해당 이용자의 접속을 제한하는 것이 전부임 ※ 「정통망법」 전부개정안에서도 ISP가 이용약관에 따라 보호조치 등을 요구할 수 있도록 규정할 뿐 정부의 권한은 없음 o 「좀비PC법」에서는 정부, 사업자, 이용자 모두가 역할을 수행하도록 설계 - 평상시의 경우에는 ①정부가 피해신고•DNS 씽크홀 등을 통해 좀비PC파악, ②정부가 ISP에 좀비PC 통보, ③ISP가 좀비PC의 이용자에게 통지 및 치료안내, ④이용자는 ISP의 안내에 따라 좀비PC치료를 진행 - 침해사고 발생시에는 ③에 따른 ISP의 통지에도 불구하고 치료를 거부한 이용자에 대한 인터넷 접속제한 조치를 할 수 있게 함 o 또한 이 법은 개별 이용자에게 통지를 할 수 없을 정도로 급박한 위기상황이 발생한 경우에는 방송통신위원회가 ISP에게 좀비PC에 대한 접속 제한 조치를 취하도록 명할 수 있게 하여 대규모 DDoS 공격시 신속한 대응이 가능해질 것으로 기대
6. 접속경로의 차단 및 DNS sinkhole 적용 - 인터넷접속서비스 제공자 및 집적정보통신시설 사업자에 대한 접속경로 차단명령	o 「정통망법」은 KISA가 침해사고 대응조치 중 하나로 주요정보통신서비스 제공자 및 집적정보통신시설 사업자(IDC)에 대한 접속경로 차단 요청을 할 수 있도록 규정

주요 「좀비 PC법」 내용	「정통망 법」과의 차이점
- 인터넷접속서비스 제공자에 대한 DNS sinkhole 적용 조치명령	o 「좀비PC법」에서는 접속경로 차단 조치를 주요 ISP와 IDC뿐만 아니라 SO/RO에게도 명령할 수 있게 하고, 명령 불이행시 과태료를 부과하도록 하여 집행력 강화 o 또한 「좀비PC법」은 접속경로 차단 조치 뿐만 아니라 DDoS 공격예방 수단인 DNS 씽크홀 조치명령을 도입함으로써 DDoS공격 등 침해사고에 대한 사후 대응보다 사전 예방 효과 극대화 추구
7. 침해사고 원인분석을 위한 이용자 컴퓨터 등 접속 요청	<신설> ※다만, 국회 계류중인 「정통망법」 전부개정안은 침해사고 대응을 위해 정보통신서비스 제공자에게 침해사고가 발생한 시스템에 대한 접근을 요청할 수 있도록 규정 -「좀비PC법」에서는 침해사고 원인분석, 악성코드 샘플채취 등을 위한 경우에 이용자의 컴퓨터에 접속을 요청할 수 있도록 하여, 이용자 컴퓨터가 주 타깃이 되는 악성 봇 감염에 의한 좀비PC문제 해결
8. 보안프로그램 긴급 배포	o 「좀비PC법」은 침해사고 발생시 대응에 필요한 이용자용 보안프로그램이 보급되어 있지 않은 경우 방송통신위원회가 용도제한용 보안프로그램(이른바 전용백신)을 배포할 수 있도록 함으로써 긴급사태의 경우에는 국가가 직접 이용자를 보호할 수 있는 수단 확보

자료 : 방송통신위원회, “DDoS 종합대책 세미나”(재구성), 2009.10.27

다. 바람직한 입법 방향

□ 정부에서 2008. 11월 국회에 제출한 「정통망 법」 전부개정안을 보완할 경우 종합적 관리 측면에서 장점이 있을 수 있으나 「좀비 PC법」의 신규법률 제정을 통하여 규율대상을 명확하여 국민들에게 법률규정에 대한 이해도와 법 집행시 예측가능성을 제고시킬 수 있음

○ 현행 「정통망 법」의 규율대상은 정보통신서비스 이용자에 한정되는 만큼 개인용 PC 등 단말 이용자를 위한 정책이 필요함

□ 「좀비 PC법」 제정을 위해서는 다음 사항을 고려하여야 함

○ 평시에 정부의 필요에 따라 포괄적인 강제규정을 두기보다는 규제적 요소를 명확히 규정하여 사업자, 이용자의 자율규제의 범위를 최대한 보장하는 것이 필요함

○ 긴급조치 혹은 예방조치 등이 국가의 권력기관에 의하여 최근 이슈가 되고 있는 패킷감청[39] 등의 오·남용으로 인해 통신의 자유, 표현의 자유, 재산권 행사의 자유, 소비자의 선택권 등 국민의 기본권에 침해가 없도록 「좀비 PC법」에 절차적·제도적 안전장치를 마련할 필요가 있음

○ 사이버 위기 시 대국민 재난방송 의무화, 무료 백신보급 업체에 대한 보상, 기술개발 등 정부지원의 내용을 포함시켜 촉진 법률로서의 면모도 갖출 필요가 있음

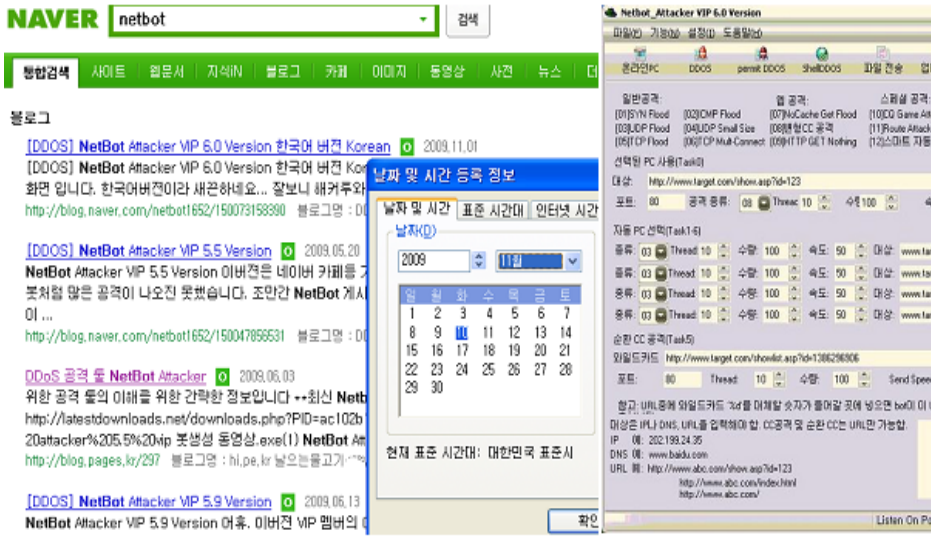
○ 최근 침해사고의 공격대상이 민·관 사이트를 구분하지 않고 있으며, 이번 7.7 DDoS사건에서 보듯이 실무적인 복구 및 방어 노하우를 보유한 민간이 활용하여 실질적인 협의체보다 적극적으로 대응 및 복구에 참여할 수 있도록 기존 협의기구들을 최대한 가 구성·운영되도록 하는 것이 필요함

39) 초고속 통신망에서 전송을 위해 잘게 쪼개진 데이터 조각(패킷)을 제3자가 중간에서 빼내 재구성하는 방식. 패킷 감청을 하면 특정인이 방문한 웹사이트와 검색 결과, 채팅 및 e메일 내용을 실시간으로 살펴볼 수 있음.

○ 최근 악성프로그램(또는 악성프로그램의 감염을 유인하는 전자적 정보)이 한글화 되어 정보통신망에 게시가 되고 있어 누구나 쉽게 접근이 가능함

- 정보통신서비스제공자는 자신이 운영·관리하는 정보통신망에 게시된 자료의 악성프로그램(또는 악성프로그램의 감염을 유인하는 전자적 정보)의 피해가 심각하여 이에 대한 긴급한 조치가 필요함

<그림 2> 악성프로그램의 검색 및 한글 악성프로그램



출처 : www.naver.com(검색 : 2009.11.10)

Ⅳ. 정부의 대응전략 검토

1.「해킹바이러스대응고도화」사업 검토[40]

가. 개요

□ 정부의 DDoS공격 대응을 위한 주요대책으로 「해킹바이러스대응고도화」 사업이 있음

○ 7.7 DDoS 공격이후 예산의 대폭적 증액이 이루어 졌으나, 예산부분의 타당성에 대한 충분한 검토가 이루어져야 할 것임

나. 사업목적

□ 상시적인 인터넷 이상징후 모니터링 등을 통한 인터넷침해사고 예방 및 분산서비스 거부공격의 위협에 대한 사전 대응체계구축 등 안전한 인터넷 이용환경 조성

□ VoIP・IPTV 등 융합서비스 기반 다양한 응용서비스의 안전성 확보를 통해 방송통신 서비스 신뢰성 확보 및 활성화 지원

다. 사업내용

□ 사업기간 : 1996년 ~ (계속)

□ 법적근거

○ 「정보통신망 이용촉진 및 정보보호 등에 관한법률」 제48조, 제48조의2, 제48조의3, 제48조의4, 제50조, 제50조의2 내지 제50조의8, 제52조, 제55조, 제56조

40) 방송통신위원회, 「2010년도 예산안 및 기금운용계획안 사업설명자료」, 2009.10.

□ 기타근거

○ 대통령 연두업무 보고시 정보보호기술훈련장 구축 추진보고('00.3)

○ 중장기 정보보호 로드맵('05. 5, 정보통신부)

○ 유비쿼터스 정보보호 기본전략('06. 12, 정보통신부)

○ 인터넷 정보보호 종합대책('08. 7, 방송통신위원회)

2.「해킹바이러스 대응 고도화」사업 예산(안)현황 및 검토

가. 2010년 예산(안) 현황

□ 방송통신위원회의 2010년도 정보보호 강화 예산은 769억원으로 2009년 예산(408억원)에 비해 88.5%가 증가하였으며, 그 중에서 DDoS 등 해킹바이러스 대응체계 고도화에 중점 투자하고 있음

□ 2009년 7월 7일 DDoS 사건이 발생된 이후 정부가 DDoS 대응 대책을 수립하면서 해킹바이러스대응체계고도화 사업에 2009년보다 276억 8,200만원이 증액된 384억 9,200만원을 2010년 예산에 편성

○ 지능화·조직화하고 있는 DDoS 공격 등에 대비하기 위해 사이버 검역체계, DDoS 긴급대피소 등을 구축·운영하고, VoIP·IPTV·유무선환경의 융·복합서비스 등 새로운 서비스에 대한 정보보호 대책 강화를 지원

□ 해킹바이러스 대응체계 고도화 주요사업

○ 인터넷침해대응센터 운영 및 Zero-Day 공격[41] 대응체계 구축

- 침해사고 이후의 대응활동보다 공격 빈도수 및 공격 규모 최소화를 위한 평시 예방 및 사전적 활동을 강화하여 사고 대응 중심에서 사전 예방

41) 보안 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이루어지는 보안 공격

중심의 보안체계 확립

- 국내에서 운용되는 전체 도메인에 대한 일일 해킹유무를 점검하여 악성코드 확산 방지 및 피해 예방활동 강화

○ 정보보호 예보체계 구축

- 인터넷 이용자들에게 손쉬운 정보보호 정보를 제공하여 이용자들의 보안의식 제고 및 국내 인터넷 환경의 안정성에 기여
- 주요 포털, 카페, 블로그 등과 연계가 가능한 도식화 아이콘 등을 이용하여 침해사고 실시간 속보 및 대처방안을 쉽게 전달할 수 있는 방안 마련

○ 융합서비스 정보보호 대응체계 구축

- VoIP 실태조사 대상 사업자를 점진적으로 확대하고 실태조사 결과를 바탕으로 법제도 개선 추진
- 융합서비스 침해사고 예방 및 신속한 대응을 위한 모니터링 체계 구축, 시범적용 후 단계적으로 사업자 확대
- 신규 IT서비스에서 발생 가능한 보안위협 분석 및 종합적 대응체계 수립을 통한 안정된 서비스 제공 기반 마련

○ 사이버 검역체계 시범도입

- 자신도 모르게 악성코드에 감염되어 DDoS 공격을 발생, PC내 자료유출 등 피해를 입고 있는 악성코드 감염PC 이용자에 한하여, 감염사실을 알려주고 치료할 수 있도록 하는 검역체계를 도입, 백신 및 보안 패치 생활화 유도 필요

<표 10> 해킹바이러스대응고도화 주요사업 예산비교표 (단위: 백만원, %)

사업명	2008년 결산	2009년 예산 (A)	2010년 예산안 (B)	증감 (B-A)	B/A
해킹바이러스대응체계고도화	10,194	10,810	38,492	27,682	256.1
ㅇ 인터넷침해대응센터운영	5,090	5,210	6,954	1,744	33.47
■24시간종합상황실상시운영	1,550	1,670	1,583	△87	△5.2
■인터넷 침해사고 예방/분석 및 대응기술 강화	1,265	1,345	1,388	43	3.2

사업명	2008년 결산	2009년 예산 (A)	2010년 예산안 (B)	증감 (B-A)	B/A
■국내 해킹피해 예방 및 대응활동	718	738	721	△17	△2.3
■국내외 침해사고 공동협력체계 및 이용자보호 강화	1,237	1,337	1,262	△75	△5.6
■방송통신위원회산하 정보보호강화	320	120	-	△120	순감
■인터넷침해대응센터 조직 강화	-	-	2,000	2,000	순증
○ Zero-Day 대응체계 구축	2,000	2,900	23,040	20,140	694.5
■DDoS 대응체계 운영	2,000	2,000	3,335	1,335	66.8
■공격근원지 예방을 위한 웹 보안수준 강화	-	900	98	△802	△89.1
■DDoS 긴급대피소 구축	-	-	4,012	4,012	순증
■악성도메인 대응체계 구축	-	-	195	195	순증
■신규보안 위협에 대한 탐지 및 대응 시스템 구축	-	-	5,600	5,600	순증
■인터넷침해대응센터 노후장비 교체	-	-	4,400	4,400	순증
■現 악성코드 탐지 및 점검 대상 웹사이트 전면 확대	-	-	1,000	1,000	순증
■kr DNS 전용 DDoS 대응장비 등 구축	-	-	4,000	4,000	순증
■유관기관간 실시간 정보공유·전파를 위한 포털 시스템 구축	-	-	400	400	순증
○ 공공기관 정보보호 지원	500	100	-	△100	순감
○ 웹사이트 보안수준 확인시스템 구축운영	500	700	503	△197	△28.1
■웹 사이트 보안수준 확인시스템 운영 및 안정화	500	600	122	△478	△79.7
■웹 사이트 보안수준 확인시스템 고도화	-	0	331	331	순증
■웹 사이트 보안수준 확인시스템 이용 확산		100	50	△50	△50
○정보보호기술 온라인학습장	300	300	258	△42	△14
○악성코드 분석 및 종합관리 체계 강화	-	600	464	△136	△22.7
○정보보호 예보체계 구축	-	500	1,491	991	198.2
○융합서비스 정보보호 대응 체계 구축	-	500	1,782	1,282	256.4
■VoIP 서비스 보안대책 마련	-	300	391	91	30.3

사업명	2008년 결산	2009년 예산 (A)	2010년 예산안 (B)	증감 (B-A)	B/A
■IPTV 침해사고 대응체계 구축	-	100	247	147	147.0
■모바일 악성코드 분석 및 무선랜 등 보안대책 마련	-	100	544	444	444.0
■신규 IT 서비스 보안시스템 대응체계 구축	-	-	600	600	순증
○인터넷에 접속하는 PC에 대한「사이버 검역체계」시범도입	-	-	4,000	4,000	순증
■PC감염 알림 및 전용백신 보급체계구축	-	-	4,000	4,000	순증

자료 : 방송통신위원회, 「세입세출예산안 및 기금운용계획안 설명자료」, 2009.10.

나. 주요사업의 검토

□ 2010년도 예산증액 현황

○ 2009년 6월 당초 정부는 2010년 해킹바이러스체계고도화 사업의 예산을 97억 1,400만원으로 편성하였으나, 2009년 7월 7일 DDoS 사태가 발생된 이후 DDoS 대응 대책을 수립하면서 2009년 10월, 당초 편성안보다 287억7800만원(296.3%↑)이 증액된 384억 9200만원으로 확정되어 국회에 제출되었음

- 증액된 예산을 보면, 2010년 계획에도 없었던 신규 사업비로 180억원과 기존사업에서의 107억 7,800만원의 증액이 있었음
- 이는 인터넷 침해사고의 예방 및 대응을 위해 모니터링하고 조치해야하는 대상 네트워크가 인터넷침해대응센터가 구축되던 2003년에 비하여 10배 이상 성장하였기 때문임
- 정보보호의 대상 역시 기존의 네트워크 레벨에서 인터넷 이용자 및 서비스 레벨까지 확대되었기 때문임

<표 11> 2010년 예산편성안(6월 기준) 대비 예산이 증액 또는 신설된 사업

기 능	'10예산 편성안(A) (6월 기준)	'10예산 확정안(B) (10월 기준)	증 감	
			(B-A)	%
□ 해킹바이러스대응체계고도화	9,714	38,492	28,778	296.3
ㅇ 인터넷침해대응센터운영	5,070	6,954	1,884	37.2
- 인터넷침해대응센터 조직 강화	0	2,000	2,000	순증
ㅇ Zero-Day 대응체계 구축	2,190	23,040	20,850	952.1
- DDoS 대응체계 운영	378	3,335	2,957	782.3
- DDoS 긴급대피소 구축	1,512	4,012	2,500	165.3
- 신규보안 위협에 대한 탐지 및 대응 시스템 구축	0	5,600	5,600	순증
- 인터넷침해대응센터 노후장비 교체	0	4,400	4,400	순증
- 現 악성코드 탐지 및 점검 대상 웹사이트 전면 확대	0	1,000	1,000	순증
- kr DNS 전용 DDoS 대응장비 등 구축	0	4,000	4,000	순증
- 유관기관간 실시간 정보공유·전파를 위한 포털 시스템 구축	0	400	400	순증
ㅇ정보보호 예보체계 구축	400	1,491	1,091	272.8
ㅇ융합서비스 정보보호 대응 체계 구축	800	1,782	982	122.8
- VoIP 서비스 보안대책 마련	400	391	△9	△2.3
- IPTV 침해사고 대응체계 구축	150	247	147	98
- 모바일 악성코드 분석 및 대응환경 개선	250	444	194	77.6
- 신규 IT서비스 보안시스템 대응체계 구축	0	600	600	순증
ㅇ인터넷에 접속하는 PC에 대한 사이버 검역 체계 시범도입	0	4,000	4,000	순증
- PC감염 알림 및 전용백신 보급체계 구축	0	4,000	4,000	순증

자료 : 「2010년 세입세출예산안 및 기금운용계획안 설명자료」6월 예산편성안과 10월 예산 확정안 자료를 이용하여 주요예산의 재구성, 2009.10.

○ 2010년도 해킹바이러스체계고도화 사업예산 384억 9,200만원은 2005년부터 2009년까지 총 5년 동안의 해킹바이스체계고도화 사업예산 362.5억[42]보다 많은 금액임

<표 12> 해킹바이러스체계고도화 사업의 예산반영 추이

'05년	'06년	'07년	'08년	'09년	계
51.5억	59.5억	59.5억	83.9억	108.1억	362.5억

자료 : 방송통신위원회, 「2010년 세입세출예산안 및 기금운용계획안 설명자료」, 2009. 10.

□ 주요사업의 예산검토

○ 해킹바이러스체계 고도화 사업중에서 신규사업 및 대폭 증액된 사업의 경우, 장비 및 시설투자의 중복이 발생할 소지가 있으므로 인터넷침해대응센터(KISC)에서 업무추진의 합리성을 제고하기 위한 정보화전략계획(ISP) 등에 반영하여 세밀하고 구체적인 계획수립 후 계획에 따라 수행하는 것이 바람직함

○ 2009년에 설치된 DDoS 대응시스템의 탐지와 차단 성능은 10Gbps급으로 설정되었으나 확장성에 대한 고려가 필요함

- 인터넷망 연동구간(IX)에 DDoS 대응시스템을 설치하는 DDoS 대응체계 운영사업의 경우 2010년에 예산이 782.3% 증액됨

※ 2009년에 4개 인터넷 망 연동구간(IX)에 신규로 설치하였고 2010년에 7개를 신규로 설치할 계획임

- 인터넷 망 연동구간(IX)에 10G급 장비를 신설하는 방식으로 탐지범위를 확대하고 있으나, 향후 추가적인 회선증설 및 대역폭의 증가가 예상되는 바, 설치할 DDoS 대응시스템의 선정기준으로 out of path 방식[43] 등 10G 이상의 회선에 대해서도 탐지가 가능하도록 확장성을 고려한 사업계획수립이 필요함

42) 방송통신위원회, 2010년 예산안 및 기금운용계획안 사업별설명자료, 2009.07.

43) In line 방식의 반대 개념으로 용량이상의 트래픽을 샘플링하여 모니터링하는 방식

○ DDoS 긴급대피소 운영사업이 민간 영역을 침해할 가능성이 발생하지 않도록 지원대상의 명확한 기준이 필요

- DDoS 긴급대피소 운영사업은 피해를 입은 기업이 DDoS 공격 트래픽을 일시적으로 DDoS 긴급대피소를 거치도록 하여 DDoS 피해기업의 피해를 최소화하고자 하는 사업으로 2010년에 40억 1,200만원의 예산이 편성되었음
- 그런데 DDoS 긴급 대피소 운영사업은 일부 민간기업이 제공하고 있는 서비스로 관련 시장 활성화에 역행할 수 있음
- 현재 DDoS 긴급 대피소 사업과 유사한 서비스를 KT 등 민간 IDC에서 상용으로 제공 중이며, 따라서 민간 IDC가 제공하고 있는 서비스를 공공에서 무료로 제공함에 따라 관련 시장을 축소·폐지하는 결과를 초래하지 않도록 사업지원대상 기준을 명확하게 설정하여야 함

○ DNS 싱크홀 적용과 관련하여 현재 DNS 싱크홀 우회 등의 신규 위협 발생에 대한 대비책도 마련하여야 할 것임

- 해커가 명령·제어서버를 P2P나 일반 홈페이지를 이용할 경우에는 명령·제어서버의 파악 또는 접속차단이 어려움
- 악성코드 분석도구를 우회하는 지능형 봇의 지속적인 증가에 대한 대비도 필요함

○ 해킹바이러스 대응체계 고도화 사업으로의 예산편중으로 인한 정보보호대응능력 강화사업의 예산이 전년대비 21.3%가 감액되어 34억 7,000만원의 예산안이 편성되었음

- 기업 및 주요 정보통신기반시설 등의 정보보호 수준을 향상시키기 위한 정보보호 대응능력 강화사업 등 사전 예방능력 강화 분야의 예산증액의 검토가 필요함

<표 13> 정보보호대응능력 강화사업 2010년 예산안 현황 (단위:백만원)

기 능 별	'08 예산	'09예산 (A)	'10예산안 (B)	증감 (B-A)	%
□ 정보보호대응능력 강화	2,430	2,060 (4,410)	3,470	1,410	68.4
·정보보호안전진단 지원	700	700	580	△120	△17.1
·정보보호관리체계(ISMS) 인증	310	610	650	40	6.6
·정보보호컨설팅전문업체지정지원	100	-	-	-	-
·영세 IT서비스 기업 안전성 점검 지원	1,000	600	388	△212	△35.3
·소규모 방송통신사업자 정보보호 강화	320	-	-	-	-
·집적정보통신시설 안전성 강화	-	150	-	△150	순감
·정보보호 체계정비 및 수준제고	(890)	(860)	651	△209	△24.3
·네트워크 인프라 정보보호	(894)	(800)	530	△270	△33.7
·암호이용활성화	(250)	(500)	494	△6	△8.3
·정보통신기반보호 지원	(740)	(190)	177	△13	△6.8

주 : ( )안의 사업은 2009년까지는 정보보호 인프라 강화사업으로 편성되었다가 2010년부터 정보보호 대응능력 강화사업으로 통합 편성됨

자료 : 방송통신위원회, 「2010년 세입세출예산안 및 기금운용계획안 설명자료」, 2009. 10.

- 이 과정에서 영세 IT서비스기업의 정보보호 대응능력을 사전에 강화하기 위한 예산들이 감액 조정되었음

  · 영세 IT서비스 기업의 안전성을 점검 지원하는 사업의 2010년 예산이 2009년에 비하여 35.3% 감액되었음

  · 집적정보통신시설의 관리적, 기술적, 물리적 보호조치에 대한 이행점검으로 안정된 서비스 제공과 신뢰할 수 있는 이용환경을 조성하고 사업자의 보안의식 고취하기 위한 집적보통신시설의 안전성 강화사업은 2010년에 관련 예산 1억 5,000만원이 전액 삭감됨

  · 중장기 정보보호 정책 수립, 정보보호 실태조사, 정보화 역기능 관련 경제적 효과 연구 등 안전한 방송통신 환경조성을 위한 기반이 되는 정보보호 체계정비 및 수준제고 사업은 24.3% 감액되었음

· 방송·통신 분야 네트워크인프라 서비스에 대한 사전적 정보보호 위협 분석과 대책검토 등 예방수단을 마련하여 네트워크인프라 서비스의 안정성 강화하고자 하는 네트워크 인프라 정보보호 사업은 33.7% 삭감됨

- 이와 같이 사전적 정보보호 대응능력을 강화하기 위한 예산을 감액하고 침해사고 발생시 대응 예산을 증액하는 식으로 예산을 배분하는 것은 예산의 효율성 측면에서 재고해 보아야 할 것 필요가 있음

· 7.7 DDoS 공격을 당한 정부가 200억원 긴급 예산을 편성해 DDoS 보안 시스템을 갖추는 것과는 정반대로 영세 IT기업과 중소기업의 정보보호 사업의 삭감은 재고해 보아야 할 필요가 있음

Ⅴ. 사이버 침해사고의 재발방지 방안

□ IT가 발전하고, 인터넷망이 고도화됨에 따라 해킹위험성이 급증하고 있으나, 우리나라의 정보보호 대응시스템은 여러 문제점을 노정하고 있었으며, 이 점에서 7.7 DDoS 대란 사태는 예견되었다고 할 수 있음

○ 2008년 정부 조직개편에 따라 정보보호 정책기능이 여러 부처로 분산되어 보안정책 수립, 부처간 역할 조율 등 사이버 위기관리를 위한 구심점이 없었음

○ 방송통신위원회는 2008년에만 5회에 걸친 침해사고 대응 모의훈련과 2009년에도 7.7 DDoS 공격을 전후하여 여러 번의 대응훈련을 하였음에도 불구하고 새로운 유형의 DDoS 공격[44]에 대하여 제대로 대응하지 못하는 문제점을 노출하였음

○ 민간협력 및 국제간 공조체제 미흡으로 사전정보 수집이 원활하게 이루어지지 못하는 등 조기 침해사고 방지에 한계점이 드러남

- DDoS 공격징후에 대한 사전대비 역량 부족함
- 사이버공격 대응을 위한 종합제어시스템 부재함
- 정부, ISP, 보안업체 및 포털 등 민간업체들과 실시간 정보공유 및 언론대응 일원화 미흡함

○ 국가와 민간기업 모두 정보보호를 위한 인력배치 및 예산투자에 소극적이었음

- 43개 정부 중앙부처 중 국무총리실, 감사원 및 방송통신위원회 등 16개 기관이 정보보호 전담부서 및 전담인원이 전무하거나 미흡한 실정임
- 2008 정보보호 실태조사에 의하면 사이버 침해사고에 대응하기 위한 활동을 하지 않는다는 기업이 61.1%이고 정보화 대비 정보보호 투자 비율이 1% 미만인 기업은 66.7%이며, 그리고 정보보호책임자(CISO)를 임명하고 있는 기업은 12.2%에 불과함

44) 기존의 디도스 공격처럼 지령 서버를 차단하는 것으로 문제를 해결할 수 없는 새로운 진화된 변종공격 방식

○ 전체 1,905만여대의 개인 컴퓨터 중 15.4%(293만여대)이상이 악성코드 감염의 위험에 처해 있으며, 최근에는 한국어 DDoS 공격툴이 나오는 등 대규모 DDoS 사이버공격은 언제든 재발할 수 있는 상태라 할 수 있음

□ 제 2의 7.7 DDoS 사태를 방지하기 위해서는 다음과 같은 사항이 조치되어야 함

○ 유사시 긴급 침해사고 사안에 대한 대응능력 향상을 위하여 정부 각 부처로 분산된 정보보호 기능의 효율적인 부처 간 조율 등 사이버 위기관리를 위한 구심점이 필요함[45)]

○ 전체 정보보호대상 영역의 95%이상이 민간영역으로 민간부문의 정보보호를 위해서는 법적근거, 전문인력과 첨단장비를 갖추도록 하며 정교하고 세심한 정책과 제도의 마련 등이 필요함

- 민간부문 사이버위기 대응을 맡고 있는 방송통신위원회 정보보안 정책관련 조직을 1개 팀 수준에서 국 규모로 확대하여 사이버 위기관리 능력을 강화하여야할 필요가 있음

○ 실시간 사이버 공조체제 활성화 필요함

- 관련 유관기관과 인터넷침해사고대응센터와 공조할 수 있는 협의체를 구성하고 침해사고에 관한 실시간 정보수집 및 공유체계 확립 필요함
- 최근 침해사고의 공격대상이 민·관 사이트를 구분하지 않고 있으므로 민간이 보다 적극적으로 대응 및 복구에 참여할 수 있도록 기존 협의기구들을 최대한 활용하여 실질적인 협의체가 구성·운영될 필요가 있음
- 미국, EU, 중국 등 해외 주요국과 사이버 위기대응에 필요한 정보공유 및 협력 등 공조활동의 강화가 필요함

○ DDoS 공격등 사이버 침해사고 대응을 위한 정보보호 관련 법령 정비를 시급히 추진이 필요함

45) 이명수, 류찬호, “77DDoS 침해사고 대응경과 및 범정부 차원의 대응방안”, 한국인터넷진흥원,「인터넷 & 시큐리티 이슈」, 2009.9

- DDoS 공격등 사이버 침해사고 대응을 위한 법령 정비에 있어서 정부의 필요에 따라 포괄적인 강제규정을 두기보다는 규제적 요소를 명확히 규정하여 사업자, 이용자의 자율규제의 범위를 최대한 보장하는 것이 필요함
- 긴급조치 혹은 예방조치 등이 국가권력기관에 의하여 최근 이슈가 되고 있는 인터넷 패킷감청 등의 오·남용으로 인해 통신의 자유, 표현의 자유, 재산권 행사의 자유, 소비자의 선택권 등 국민의 기본권에 침해가 없도록 관련 법령 제·개정에 있어서 절차적·제도적 안전장치를 마련할 필요가 있음
- 신규 법률의 내용에 있어 사이버 위기 시 대국민 재난방송 의무화, 무료 백신보급 업체에 대한 보상, 기술개발 등 정부지원의 내용을 포함시켜 촉진 법률로서의 면모를 갖출 필요가 있음

○ 7.7 DDoS와 유사한 침해사고에 대한 사전예방 및 침해사고 발생 시 신속한 대응을 위해서는 전문인력 및 분석기술의 고도화가 필요함

- 정부는 인터넷을 통해 유포되는 악성코드를 수집하여 분석한 후 침해사고 발생 전에 백신개발에 활용하는 등 사전예방 및 침해사고 발생 시 신속한 분석을 위해서 전문인력 확보가 필요함
- 또한, 악성코드에 대한 신속하고 정확한 분석을 위해 가상화기반의 다양한 악성코드 분석기술 및 분석도구 우회기능이 있는 악성코드에 대한 고도화된 분석기술을 확보할 필요가 있음

○ 민간부문 사이버 침해 대응 전문조직의 육성이 필요함

- 최근 침해사고의 공격대상이 민·관 사이트를 구분하지 않고 있으며, 실무적인 복구 및 방어 노하우를 보유한 민간이 보다 적극적으로 대응 및 복구에 참여할 수 있도록 기존 협의기구들을 최대한 활용하여 실질적인 협의체가 구성·운영되도록 하는 것이 필요함

참 고 문 헌

이명수・류찬호, “7.7 DDoS 침해사고 대응경과 및 범정부 차원의 대응방안”, 한국인터넷진흥원, 「인터넷 & 시큐리티 이슈」, 2009.9.

이연수・이수연・윤석구・전재성, “주요국의 사이버안전관련 법・조직체계 비교 및 발전방안 연구”, 국가정보연구, 제1권 2호, 2009.2.24.

원유재, “봇넷 대응기술 동향”, 한국정보보호진흥원(KISA), 2008.8.

KISA, 「개인 인터넷 이용자 정보보호 실태조사」, 2008.12.

KISA, 「인터넷 이용 실태조사」, 2008.12.

행정안전부, 「행정안전부 국무회의 보고자료」, 2009.4.21.

지식경제부, 「지식정보보안산업 진흥 종합계획」, 2008.12

국가정보원, 「2008 국가정보보호 백서」, 2008.

한국정보보호진흥원,「2008년 정보보호 실태조사」, 2008.12.

지식경제부, 「국가 사이버테러 대응을 위한 정보보안 산업육성정책」, 2009.

방송통신위원회,「악성프로그램 확산 방지 등에 관한 법률」제정을 위한 정책토론회 발표자료”, 2009.9.9.

방송통신위원회, 「2010년도 예산안 및 기금운용계획안 사업설명자료」, 2009.7.

문화일보, 「7.7 DDoS 대란’ 왜?」, 2009.7.1.

아이뉴스24, “악성코드에서 정부용 확장자 발견 …사이버 전쟁 의혹 커져”, 2009.7.10.

전자신문, “이번 DDoS 공격의 특징”, 2009.7.9.

문화일보, ‘디도스 테러’싸운 민간연구소 “국정원.검.경.....보고하다 지쳐”_방송통신위원회도 매번 따로....공조 안돼 헛심만 써’, 2009.7.13.

한겨레, “악성코드 잽싸게 진압한 누리꾼들_내 PC는 내가 지킨다.”, 2009.7.13.

전자신문, “러・그루지아 ‘총성없는 전쟁’ 계속”, 2008.8.18.

정순봉, “DDoS 공격과 예방 및 치료방법”, 2009.8.17, <http://blog.naver.com/itexpert2007>

한국정보보호진흥원, 「2008 해킹바이러스 대응체계 고도화 결과보고서」, 2008.12.

동아일보, [횡설수설/박성원]인터넷 감청, 2009.11.18

[부록 1] 「(가칭)악성프로그램 확산 방지 등에 관한 법률(안)」에 담을 주요내용과 현행법의 관련 조항 비교

준비 중인 법률에 담을 주요 내용	현행법 관련조문
1. 주요 용어의 정의 ① 이용자 – 컴퓨터 등 정보처리장비를 이용·관리하는 개인, 법인, 단체	□ 정보통신망이용촉진및정보보호등에관한법 제2조제1항제4호 4. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
② 백신 소프트웨어 – 컴퓨터 바이러스 등 악성프로그램을 찾아내어 기능을 정지시키거나 제거하는 컴퓨터 프로그램	□ 정보통신망이용촉진및정보보호등에관한법 : 백신 소프트웨어 용어사용 제28조 (개인정보의 보호조치) ① 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
2. 침해사고 예방 및 대응을 위한 민관협력체계 마련 – 침해사고 예방조치 및 지원 – 침해사고 상황전파 및 대응훈련	□ 정보통신망이용촉진및정보보호등에관한법률 제48조의2(침해사고의 대응 등) ① 방송통신위원회는 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다. 1. 침해사고에 관한 정보의 수집·전파 2. 침해사고의 예보·경보 3. 침해사고에 대한 긴급조치 4. 그 밖에 대통령령으로 정하는 침해사고 대응조치 □ 정보통신망이용촉진및정보보호등에관한법 전부개정안 제51조(침해사고의 대응 등) ① 방송통신위원회는 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 진흥원이 수행하도록 할 수 있다.

준비 중인 법률에 담을 주요 내용	현행법 관련조문
	1. 침해사고에 관한 정보의 수집·전파 2. 침해사고의 예보·경보 3. 침해사고에 대한 긴급조치 4. 그 밖에 대통령령으로 정하는 침해사고 대응조치
3. 컴퓨터 보안프로그램의 개발 및 보급 지원 – 컴퓨터 보안프로그램 개발 및 보급지원 – 시범사업 실시 및 지원	□ 정보통신망이용촉진및정보보호등에관한법 제6조 (기술개발의 추진 등) ① 지식경제부장관은 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 대통령령으로 정하는 바에 따라 관련 연구기관으로 하여금 연구개발·기술협력·기술이전 또는 기술지도 등의 사업을 하게 할 수 있다. ② 정부는 제1항에 따라 연구개발 등의 사업을 하는 연구기관에는 그 사업에 드는 비용의 전부 또는 일부를 지원할 수 있다. ③ 제2항에 따른 비용의 지급 및 관리 등에 필요한 사항은 대통령령으로 정한다.
4. 컴퓨터 보안프로그램 보급 확산 – 우수 보안프로그램 추천·장려제도 – 보안프로그램 설치·이용 및 최신업데이트 – 정보통신서비스 제공자의 이용자 지원	<관련 조문 없음>
5. 소프트웨어의 보안취약점 보완 – SW 정기 보안패치 – SW 보안취약점 점검 등 조치 – 보안취약점 보완명령을 거부한 SW에 대한 제공 중지명령	□ 정보통신망이용촉진및정보보호등에관한법 및 동법 시행령 제48조의2(침해사고의 대응 등) ① 방송통신위원회는 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다. 1. 침해사고에 관한 정보의 수집 · 전파 2. 침해사고의 예보 · 경보 3. 침해사고에 대한 긴급조치

준비 중인 법률에 담을 주요 내용	현행법 관련조문
	4. 그 밖에 대통령령으로 정하는 침해사고 대응조치 시행령 제56조(침해사고 대응조치) 법 제48조의2제1항제4호에서 "그 밖에 대통령령으로 정한 침해사고 대응조치"란 다음 각 호의 조치를 말한다.<개정 2009.1.28> 2. 「소프트웨어산업 진흥법」 제2조제4호에 따른 소프트웨어사업자 중 침해사고와 관련이 있는 소프트웨어를 제작 또는 배포한 자에 대한 해당 소프트웨어의 보안상 취약점을 수정·보완한 프로그램(이하 "보안취약점보완프로그램"이라 한다)의 제작·배포 요청 및 정보통신서비스 제공자에 대한 보안취약점보완프로그램의 정보통신망 게재 요청 법 제47조의3(이용자의 정보보호) ③ 「소프트웨어산업 진흥법」 제2조에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 한국인터넷진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알려야 한다.
6. 악성프로그램 정기점검 의무와 및 삭제 명령	□ 정보통신망이용촉진및정보보호등에관한법 전부개정안 제2조(정의) 9. "게시판"이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램이나 기술적 장치를 말한다. 제47조(악성프로그램 등의 삭제요청) ① 방

준비 중인 법률에 담을 주요 내용	현행법 관련조문
	송통신위원회는 악성프로그램 또는 악성 프로그램의 감염을 유인하는 전자적 정보가 숨겨져 있는 웹사이트를 발견한 경우 그 운영자 등에게 해당 프로그램 또는 정보의 삭제를 요청할 수 있다. ② 제1항의 경우 웹사이트 운영자 등은 특별한 사유가 없는 한 이에 따라야 한다.
7. 좀비PC등에 대한 ISP의 접속제한 등 – 좀비PC에 대한 ISP의 조치 – 방송통신위원회의 긴급 접속제한명령	□ 정보통신망이용촉진및정보보호등에관한법 제47조의3(이용자의 정보보호) ② 주요정보통신서비스 제공자는 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. ④ 제2항에 따른 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 대통령령으로 정한다. □ 정보통신망이용촉진및정보보호등에관한법 전부개정안 제48조(이용자에 대한 보호조치) ① 정보통신서비스 제공자는 자신의 서비스를 이용하는 이용자의 정보통신망에 장애가 발생할 가능성이 있는 경우에는 이용약관으로 정하는 바에 따라 그 이용자에게 보호수단을 제공하고 이를 실행하도록 요구할 수 있다. ②「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자로서 전국적으로 정보통신망서비스를 제공하는 자(이하

준비 중인 법률에 담을 주요 내용	현행법 관련조문
	"주요정보통신서비스 제공자" 라 한다)는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보통신망에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다. ③ (생략) ④ 제2항에 따른 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 대통령령으로 정한다.
8. DNS sinkhole 적용	<관련 조문 없음>
9. 침해사고 원인분석을 위한 이용자 컴퓨터 등 접속 요청	□ 정보통신망이용촉진및정보보호등에관한법 전부개정안 제46조(취약점 점검 지원 등) ② 방송통신위원회는 침해사고가 발생한 정보통신망에 대한 취약점 점검, 기술 지원 등의 조치를 위하여 긴급히 필요한 경우 이에 대한 접속을 해당 정보통신서비스 제공자에게 요청할 수 있다. ③ 제1항 및 제2항에 따라 취약점 점검, 기술 지원 등을 하는 자는 해당 정보통신망에 의해 처리되는 정보를 취약점 점검, 기술지원 등의 목적 외로 열람하여서는 아니 된다.
10. 보안프로그램 긴급 배포	<관련 조문 없음>
11. 손해배상책임의 감경	<관련 조문 없음>
12. 보안프로그램의 목적 외 이용금지	<관련 조문 없음>

자료출처 : 방송통신위원회, 내부자료, 2009.10

[부록 2] 국내·외 DDoS 공격 현황

1. 해외 주요국가에서의 DDoS 공격관련 현황

□ 초창기 사이버 테러는 주로 호기심이나 금전적 이익을 위해 벌어졌으나, 점차 정치적 의도에서 자행되는 사례가 증가하고 있고, 특정 국가의 암묵적인 지원하에 국가간 사이버 전쟁으로 확대되는 경우도 빈번해지고 있음

□ 워싱턴포스트에 따르면 지난해 미국 정부 컴퓨터망에 대한 해킹 등 사이버 공격은 5,488건으로 2007년에 비해 40%나 증가했음

○ 2009년 4월에는 펜타곤 보안시스템의 보안망이 뚫려 3,000억 달러짜리 차세대 전투기 'F35' 개발 정보가 정체불명의 해커에게 유출되는 사건도 발생했음

○ 7.7 DDoS 공격때도 미국 백악관과 재무부, 연방무역위원회 등이 피해를 입었음

□ 해커부대를 전략적으로 육성하고 있는 국가도 늘고 있음

○ 중국은 2003년부터 베이징 광저우 등지에 2,000여명의 해커로 구성된 '전자전 부대'를 창설해 운영하고 있음

- 중국에선 '홍커(레드 해커)'로 불리는 100만여 명의 민간 해커들이 활동하고 있는 것으로 알려짐
- 홍커들은 2001년 5월 DDoS공격으로 백악관 홈페이지를 마비시킨 바 있으며, 2004년에는 국내의 한국국방연구소, 원자력연구소, 외교부, 언론사 등 10여개 사이트를 공격하였음

○ 러시아도 옛 소련 국가보안위원회(KGB)의 후신인 연방보안국(FSB)에 사이버전 전담 부서를 두고 사이버 무기 개발과 전문가 양성에 힘을 쏟고 있음

- 2009년 1월 러시아 해커들은 키르기즈스탄의 2개 ISP들에 DDoS 공격을 가해 인터넷망을 마비시킴
- 2008년 8월 러시아 해커들은 그루지야의 주요 정부 사이트, e-mail, 통신 서

비스를 대상으로 공격하여 대통령 홈페이지를 비롯해 20여개 금융, 방송 사이트를 다운시킴[46]

<표 14> 세계주요국의 사이버 테러 현황

발생 시점	피 해 내 용
'09. 1.	■ 러시아 해커 키르기즈스탄 공격 - 러시아 사이버의용군이 키르기즈스탄의 대형 ISP에 대하여 DDoS공격으로 인터넷이 마비
'08.12.	■ 반크 홈페이지 공격 - 일본 네티즌의 공격으로 반크사이트에 대한 해외 접속 불가
'08. 8.	■ 러시아-그루지아 사이버전쟁 - 영토분쟁으로 무력충돌이 확산되고 있는 가운데 러시아 해커들에 의해 그루지아 국방부, 외교부 등 주요 사이트가 공격을 받음
'07. 4.	■ 러시아 해커 에스토니아 공격 - 에스토니아 수도 '탈린'에 있던 舊소련군 동상이 철거되자, 러시아 해커에 의해 대통령궁, 정부부처, 정당, 금융기관 등 대상 대규모 사이버테러 감행으로 행정업무 마비 등 국가적 혼란 야기
'07. 2.	■ 루트 DNS DDoS 공격 - 13개 루트 DNS 중 6개를 대상으로 하는 DDoS 발생

자료 : 방송통신위원회 내부자료, 2009.10.

2. 우리나라 DDoS 공격 현황

□ 국내 웹 사이트에 대한 DDoS 공격은 2006년 11월에 최초 접수된 이래 2009년 8월까지 한국인터넷진흥원에서 136건의 DDoS 공격 신고를 접수하였음

○ 년도별 DDoS공격 신고 현황[47]

46) 전자신문, '러·그루지아 총성없는 전쟁 계속', 2008.8.18.

47) DDoS 통계는 KISA에서 2006년 11월 최초 신고 접수받은 시점부터 대응한 건수임 (금번 7.7 DDoS건은 제외한 수치임)

<표 15> DDoS공격 신고 현황

구 분	2006년	2007년	2008년	2009.10	계
금품요구	1	12	27	13	53
기 타	3	35	26	21	85
계	4	47	53	34	138

자료 : 방송통신위원회 내부자료, 2009.10.

- 2009년 10월까지 DDoS 신고건수 중에서 금품요구 DDoS공격이 전체 중 38.4%(53건)로 나타났으며, 2009년 10월까지 신고된 34건 중 13건(38.2%)임

○ 업종별 DDoS 피해기관 현황

- DDoS 업종별 피해현황을 보면 기업이 22.1%(30건)로 제일 높으며, 그 다음이 게임아이템거래 사이트 14.0%(19건), 인터넷 쇼핑몰 12.5%(17건) 순으로 나타났으며, 상위 3업종이 전체 발생건수의 절반에 가까운 49%(66건)를 차지함

<표 16> 업종별 피해기관 현황

구 분	2006	2007	2008	2009.8	계	백분율
게임아이템 거래사이트	0	13	5	1	19	14.0%
금융	0	1	2	0	3	2.2%
기업	1	9	11	9	30	22.1%
기타	0	5	5	1	11	8.1%
기타/국외	2	3	0	1	6	4.4%
비영리	0	0	2	1	3	2.2%
성인	1	1	1	0	3	2.2%
쇼핑몰	0	2	13	2	17	12.5%
언론	0	1	0	1	2	1.5%
온라인 게임	0	0	3	0	3	2.2%
온라인 교육	0	1	2	5	8	5.9%
온라인 서점	0	0	0	1	1	0.7%
웹하드	0	2	5	0	7	5.1%
인터넷 방송	0	1	0	1	2	1.5%
정부/공공	0	0	0	1	1	0.7%
커뮤니티	0	1	2	4	7	5.1%
포털	0	1	2	3	6	4.4%
호스팅 업체	0	6	0	1	7	5.1%
계	4	47	53	32	136	

자료 : 방송통신위원회 내부자료, 2009.10(재구성)

□ 최근 해킹, 개인정보 탈취 및 시스템 파괴 등으로 국한되었던 인터넷 침해사고가 기업대상 금품요구 및 사회불안 조장 등 대단위 피해양상으로 발전하고 있음[48)]

<표 17> 최근 3년간 국내 주요 DDoS 침해사고 사례

발생시점	피 해 내 용
'09. 3.	■ 커뮤니티 포탈 DDoS 피해
'09. 2.	■ IT 보안업체 위장 DDoS 공격 검거(협박성) - 보안전문가들이 보안업체를 설립한 후 해당 사 서비스를 이용하도록 하기 위해 bot을 이용하여 DDoS 공격
'08. 7.	■ 포탈 카페에 대한 DDoS 공격(보복성) - 카페 강제 탈퇴당한 10대가 중국사이트에서 DDoS 공격 프로그램을 구입하여 보복
'08. 6.	■ 정당 홈페이지 DDoS공격 - 해당 홈페이지 접속장애 발생
'08. 3.	■ 증권사 사이트 DDoS공격(협박성) - 중국 해커의 협박성(2억) DDoS 공격으로 사이트 장애 발생
'08. 2.	■ 게임사 DDoS 공격 - 동남아 해커들에 의한 DDoS 공격으로 게임사이트 일시적 폐쇄
'07.10.	■ 아이템 거래사이트 대상 DDoS 공격(협박성) - 아이템 거래 3개 사이트 홈페이지 접속장애 발생

자료 : 방송통신위원회 내부자료, 2009.10.

48) 이명수, 류찬호, “77DDoS 침해사고 대응경과 및 범정부 차원의 대응방안”, 한국「인터넷 & 시큐리티 이슈」, 한국인터넷진흥원, 2009.9.

현안보고서 발간 일람

호 수	제 목	발간일	집필진
제1호	태안기름누출사건에 따른 국가 위기대응태세점검 및 향후대책	2007.12.18	김종연 최준영
제2호	국제지명표준화 관점에서 바라본 독도표기문제 및 대응방안	2008. 7.31	김종연 최준영
제3호	인터넷 실명제 쟁점	2008. 8.28	김여라
제4호	한·미 방위비 분담의 현황과 쟁점	2008. 8.28	김영일 신종호
제5호	국민연금과 직영연금 간 가입기간 연계제도	2008.10. 6	원시연
제6호	2008 미국 대선의 주요 이슈와 우리나라에 대한 시사점	2008.10. 8	김준 외 7인
제7호	미국의 대북제재현황과 테러지원국 지정 해제의 영향	2008.10.15	이승현
제8호	지방행정체제 개편의 쟁점과 입법부의 과제	2008.10.31	하혜영 외 6인
제9호	오바마시대 개막의 의의와 시사점	2008.11. 6	김준 외 7인
제10호	자전거 이용 활성화를 위한 관련 법률 검토 및 쟁점 분석	2008.12. 8	박준환
제11호	군경력 가산점제 재도입 논의의 쟁점	2008.12.10	조규범
제12호	쇠고기 수입위생조건 국회심의규정의 검토 및 개정방향	2008.12.11	정민정 김남영
제13호	사이버공간에서의 이용자 보호와 인터넷서비스제공자의 역할	2008.12.11	이유주
제14호	인터넷 전화와 번호이동제도의 현황과 발전방향	2008.12.11	박 철
제15호	선진국형 식품안전관리체계 마련 방안	2008.12.12	김 준 배민식
제16호	공무원연금제도 개혁논의와 주요 쟁점	2008.12.22	원시연
제17호	주식 공매도 현황 및 개선방안	2008.12.29	박충렬

호 수	제 목	발간일	집필진
제18호	기초보장 급여체계의 개선 : 개별급여 방식을 중심으로	2008.12.30	유해미
제19호	국가대표선수 은퇴 후 진로 강화를 위한 지원체계의 현황 및 발전방향	2009. 1. 7	김신애
제20호	국회 및 주요국 의회의 질서유지제도	2009. 2. 6	전진영
제21호	선상투표제도 도입관련 쟁점 및 시사점	2009. 2.20	김종갑 외 3인
제22호	강제철거에서의 주거권 보호를 위한 입법적 개선방향	2009. 2.23	조규범
제23호	신·재생에너지 의무할당제 도입관련 쟁점분석	2009. 4. 1	유재국
제24호	「교통사고처리특례법」일부 위헌 판결에 따른 영향분석 및 후속조치 검토	2009. 4. 1	박준환
제25호	정치자금 소액기부의 현황과 활성화 방안	2009. 4.14	조만수
제26호	헌법재판소 변형결정의 기속력에 관한 입법개선방향	2009. 4.16	김선화
제27호	대량살상무기확산방지구상(PSI)의 현황과 쟁점	2009. 5.11	정민정
제28호	영리병원 도입 논의 및 정책과제	2009. 5.15	이만우
제29호	일자리 나누기 정책의 개선과제	2009. 6. 2	정종선
제30호	LED 조명산업의 현황과 지원정책의 개선방향	2009. 6.30	유재국 이상은
제31호	금융채무불이행자 현황 및 지원정책의 개선방향	2009. 7. 9	임동춘 주규준
제32호	존엄사 입법화의 쟁점과 과제	2009. 8.13	이만우 조규범
제33호	온라인상 불법저작물 대책 및 개선방향	2009. 8.21	나채식
제34호	전화금융사기(보이스피싱) 대응책의 현황 및 개선방안	2009. 8.21	이유주
제35호	일본의 정권교체 그 의미와 시사점	2009. 9. 3	이현출

호 수	제 목	발간일	집필진
제36호	북한 황강댐 방류에 대한 국제법적 고찰	2009. 9.22	정민정 김상욱
제37호	미국하원의 발언관련 규범	2009. 9.28	전진영
제38호	법률명 약칭 법제화 방안	2009. 9.28	김남영
제39호	저출산 대응 주요정책의 현황 및 과제	2009.10.15	유해미
제40호	신종플루의 대유행(Pandemic) 및 정책대응	2009.10.16	이만우 허종호
제41호	대규모 소매점에 대한 규제: 쟁점과 대안	2009.10.20	박충렬 정민정
제42호	석면 관련 법제의 개선방안: 현황, 문제점, 해외 사례를 중심으로	2009.10.21	김 준 최준영
제43호	희유(稀有)금속자원 재활용의 문제점과 개선방안	2009.10.27	김경민 신가은
제44호	입학사정관제의 바람직한 운영을 위한 제언 - 미국입학사정관제의 시사점 -	2009.11.10	정환규
제45호	국회 인사청문제도의 현황과 개선방안	2009.11.12	전진영 김선화 이현출
제46호	고령사회 대비 노인요양시설확충사업의 방향성 검토	2009.11.20	원시연
제47호	방송광고판매 경쟁체제 도입과 쟁점	2009.11.27	김여라

현안보고서 제48호

발 간 일 2009년 12월 1일
발 행 임종훈
편 집 사회문화조사실 문화방송통신팀
기획관리관 기획협력팀
발 행 처 **국회입법조사처**
서울특별시 영등포구 의사당로 1
TEL 02·788·4524
인 쇄 경성문화사 (TEL 02·786·2999)

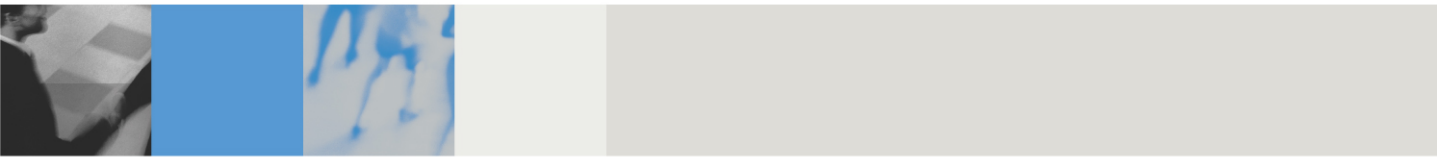
1. 본 책자의 무단 복제 및 전재는 삼가주시기 바랍니다.
2. 내용에 관한 자세한 사항은 집필자에게 문의하여 주시기 바랍니다.
3. 전문(全文)은 국회입법조사처 홈페이지(http://www.nars.go.kr) 자료마당에 게시되어 있습니다.

ISSN 2005-3215
발간등록번호 31-9735032-000640-14

ⓒ 국회입법조사처, 2009

현안보고서 제48호

'7.7 DDoS 사고' 대응의 문제점과 재발방지 방안



NARS National Assembly Research Service
(우)150-703 서울시 영등포구 의사당로 1 (국회입법조사처) tel.02)788-4510(代)
www.nars.go.kr
ISSN 2005-3215