최근의 사이버테러에 대한 대응방안

정기석*

요 약

정보기술의 발전으로 인하여 도래한 정보사회는 국민생활에 질적인 향상을 가져다주었을 뿐만 아니라 사회적·경제적 생산성의 향상을 가져왔다. 그러나 이러한 순기능 이면에는 해킹·바이러스유포 등을 이용한 사이버테러와 같은 역기능 또한 심각하여 사회적으로 큰 문제가 되고 있다. 최근 들어 대규모 해킹사건이 자주 발생하고 있다. 인터넷업체의 대규모 개인정보가 유출되거나 금융전산망이 마비돼 고객들이 큰 피해를 입는 일이 발생하고 있다. 또 북한에 의한 해킹도 빈번하다. 북한에 의한 해킹은 우리 사회를 큰 혼란에 빠뜨릴 수 있으며 국가 안보에 위협을 가져오는 일이다. 따라서 본 논문에서는 국내 사이버테러 동향을 살펴보고 문제점을 분석하여 그 대응방안을 제시한다.

The countermeasure against recent cyber terrors

Jeong Gi Seog*

ABSTRACT

Information society which came due to advance of Information Technology improved the social and economical productivity as well as the quality of national life. But behind the right function the adverse effect as cyber terror is serious and become a big issue. Recently, hackings on a big scale occur frequently. The personal information stored in Internet company is leaked and customers are badly damaged by paralysis of banking system. Also hacking attacks by North Korea occur frequently. It causes confusion in our society and a threat to national security. In this paper, the trend of domestic cyber terror is observed and the countermeasure against cyber terror is proposed.

Key words : cyber terror, hacking, security, threat, personal information

접수일(2011년 12월 21일),수정일(1차:2012년 3월 11일)
게재확정일(2012년 3월 19일)

* 영동대학교 정보통신보안학과

1. 서 론

사이버테러에 대한 정의는 다양하지만 대체로 해킹, 컴퓨터바이러스 등 정보통신기술을 활용하여 네트워크나 컴퓨터시스템에 대한 공격을 가하여 사회혼란 및 국가안보를 위협하는 행위로 정의할 수 있다. 다시 말하면 사이버상에서 발생하는 범죄 중에서 사기, 명예훼손 등 일반사이버범죄와 구분하여 해킹이나 컴퓨터바이러스에 의한 공격을 통해 시스템장애를 일으키거나 정보를 삭제·유출하는 행위를 사이버테러라고 할 수 있다.

최근 들어 사이버테러에 의한 피해 규모가 확대되고 있다. 올해 들어서만도 3.4 디도스 공격, 현대캐피탈 사건, 농협 전산망 장애사건, 네이트·사이월드 사건(SK컴즈 사건) 등 대규모 해킹사건이 발생하였다. 현행법에서 사이버테러라는 용어는 사용되고 있지 않지만 그런 행위에 대해서 범죄행위로 규정하여 처벌을 하고 있다. 사이버테러의 범행 동기는 초기에는 자신의 해킹 실력을 과시하기 위함이었으나 최근의 경향은 금전적 이익을 얻기 위하여 하는 경우가 많다. 또 사회적 혼란을 노린 북한에 의하여 자행되는 경우도 증가하는 추세이다. 공격루트는 외국에서 국내로의 공격이 증가하고 있다. 중국을 통한 북한의 공격은 중국과의 외교문제로 비화될 소지도 있으며, 외국IP를 사용하는 공격은 당사국과의 수사공조 협정의 부재로 수사에 어려움을 겪을 수 있다. 또 이러한 외국IP에 의한 국내 공격은 국가안보와도 연계되는 것으로 국가차원의 대비가 필요하다. 정부는 3.4 디도스(DDos) 공격과 5월의 농협 전산망 장애사건 등을 계기로 2011년8월8일 '국가 사이버 안보 마스터플랜'을 발표하였다. 이 마스터플랜에서 지금까지 공공부문은 국정원에서, 민간부문은 방통위에서 총괄하던 우리 정부의 국가 사이버 안보 시스템을 국정원에서 컨트롤타워 역할을 하기로 하는 등 대비책을 마련하였다. 또한 정부는 사이버공간을 영토·영공·영해에 이어 국가가 수호해야할 제4의 영역으로 규정하고 사이버 안보 위협에 대한 예방,탐지,대응,제도,기반 등 5대 중점 전략과제를 추진키로 하였다[1]. 그러나 현재 국내의 정보보호 환경은 아주 열악한 상태이다. 정보보호 관련법의 난립, 기업의 정보보호에 대한 낮은 의식으로 인한 준비 부족, 인터넷업체의 과도한 개인정보 수집, 고속화된 정보통신망 등 해킹에 매우 취약한 형편이다.

따라서 본 논문에서는 최근 사이버테러의 동향을 살펴보고, 문제점을 분석하여 그 대응방안을 제시하고자 한다.

2. 사이버테러의 개념

사이버테러에 대한 개념 정의는 다양하다. 2005년 국가사이버안전매뉴얼에서는 '특정한 정치적·사회적 목적을 가진 개인·테러집단이나 적성국 등이 해킹·컴퓨터바이러스의 유포 등 전자적 공격을 통해 주요 정보기반시설을 오동작·파괴하거나 마비시킴으로써 사회혼란 및 국가안보를 위협하는 행위'로 정의하고 있다[2]. 또 다른 정의로는 '해킹·바이러스유포·웜바이러스유포·논리폭탄전송·대량정보전송 및 서비스거부공격·고출력전자총 등 통신망에서 사용하는 컴퓨터 시스템 운영방해 행위 내지 정보통신망 침해행위 또는 전자적 침해행위에 의하여 국가적·사회적으로 공포심 내지 불안감을 조성하는 행위'[3], '컴퓨터 통신망상에 구축되는 가상공간인 사이버 공간을 이용한 폭력행위를 가리키는 용어로, 컴퓨터 통신망을 이용하여 정부기관이나 민간기관의 정보시스템에 침입, 중대한 장애를 발생시키거나 파괴하는 등의 범죄행위'[4] 등이 있다.

이상의 정의를 살펴보면 공격수단은 해킹·바이러스 등으로 명시하거나 하지 않은 경우가 있고, 공격대상은 국가시설로 국한한 경우와 민간시설까지 포함하는 경우, 언급이 없는 경우가 있다. 또 공격효과로는 사회적 혼란이나 국가 안보 위협의 경우와 언급이 없는 경우가 있다. 공격수단은 해킹·바이러스를 명시 한 경우가 다수이고 효과면에서도 사회적 혼란이나 불안감 조성이 다수이다. 다만 민간기관의 정보시스템 포함여부가 문제가 되는데 현재 민간기관에서 보유하고 있는 개인정보가 수천만 건에 달하고 있어 유출시에 사회적 문제가 됨을 감안하면 민간기관도 포함해야 한다고 본다.

따라서 종합해 보면 사이버테러는 '해킹·컴퓨터바

이러스 등 정보통신기술을 활용하여 네트워크나 컴퓨터시스템에 대한 공격을 가하여 사회적인 혼란을 야기하고 국가안보를 위협하는 행위'로 정의할 수 있다.

그러나 사이버테러라는 용어자체는 우리나라 법령에 사용된 예가 없으며 국내법규로는 국가사이버안전관리규정(대통령훈령 제267호) 제2조에서 '사이버공격'이라는 용어를 사용하면서 '해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위'[5]라고 정의하고 있다.

한편, 사이버범죄의 정의를 살펴보면, 광의로는 '사이버공간에서 발생하는 범죄'[6], '인터넷 사이트와 그것들을 서로 연계시키는 컴퓨터 네트워크(즉, 인터넷)를 수단으로 하여 특정 네티즌이나 사이트 또는 네트워크 그 자체를 대상으로 하는 범죄'[7], '컴퓨터 시스템 또는 네트워크와 관련된 모든 위법행위. 여기에는 컴퓨터 시스템이나 네트워크를 사용해서 정보를 빼오거나, 다른 사람에게 제공하거나, 배포하는 행위가 포함된다.'[8] 등이 있고 협의로는 '컴퓨터 시스템의 보안과 컴퓨터시스템에서 처리하는 데이터를 대상으로 하는 컴퓨터 사용의 위법행위'[9], '개인 혹은 조직화된 단체가 사이버 공간에서 시간과 장소에 관계없이 개인과 단체들에 대하여 정치성을 내포하지 않고 경제적 이익과 관련된 행위 또는 반사회·문화적 행위를 범하는 경우'[9] 등이 있다.

종합해 보면 광의의 사이버범죄는 사이버상에서 발생하는 모든 범죄로, 협의의 사이버범죄는 사이버공간에서 일어나는 개인 또는 단체를 대상으로 해서 개인적 이익을 목적으로 하는 범죄로, 그리고 사이버테러는 해킹이나 악성프로그램을 이용한 공격으로 그 피해규모가 커서 사회적 혼란이나 국가안보에 위협이 되는 범죄로 규정할 수 있다.

3. 최근 사이버테러의 특징

2011년에는 3.4 디도스 공격, 현대캐피탈 사건, 농협 전산망 장애사건, SK컴즈 사건 등 대규모 해킹이 발생하였다. 이들 해킹의 특징은 첫째, 개인정보 피해규모가 확대되었다는 것이다. (그림 1)에서 보듯이 2006년 리니지명의도용에서는 피해규모가 120만 명이었으나 2011년 7월 SK컴즈 해킹에서는 3500만 명의 개인정보가 유출되었다[10]. 인터넷의 발달로 인터넷업체의 가입자수가 증가했기 때문이다.

자료: 방송통신위원회

(그림 1) 주요 개인정보 침해사고 추이

둘째, 외국서버를 통해 침투한다는 것이다.

2011년4월 발생한 현대캐피탈 사건은 필리핀서버를 통해서 현대캐피탈 서버에 접속하여 고객정보를 유출해 갔다. 해커가 외국서버를 통해서 국내해킹을 할 경우 범인추적이 쉽지 않다. 국내 공범은 검거됐지만 필리핀에 있는 해커는 아직 검거되지 않았다.

2011년7월 발생한 SK컴즈 사건은 중국IP로 해킹을 했다. 중국발 해킹에서 정보를 유출해가는 절차를 보면 국내의 한 서버를 악성코드로 감염시키고 특정PC를 지정하여 특정PC가 이 서버에 접속할 때 악성코드에 감염시키고 이 감염된 PC를 조종하여 SK컴즈 서버에 접속하여 고객정보를 빼내어 중국으로 전송하는 방법을 사용한다. 중국발 해킹의 경우 수사과정에서 중국IP로 밝혀져도 중국과의 사법공조협정이 체결되어 있지 않아 수사에 어려움을 겪는다. 2011년 6월부터는 보이스피싱과 사이버범죄 등 중국발 범죄 수사에 대해 미력이나마 공조하고 있다.

셋째, 북한에 의한 공격이다.

북한은 김일성대학과 김책공과대학 컴퓨터공학과에서 해커를 양성하고 있다. 3.4 디도스 공격의 경우 한국정부가 해킹사실을 얼마나 빨리 발견하고 복구할 수 있는지를 알기 위한 정치적인 동기에서 이루어졌다. 또 농협 전산망 장애사건은 우리사회의 혼란을

노린 북한 정찰총국의 소행으로 밝혀졌다.

북한은 1989년부터 사이버전 전담인력을 매년 100명이상 양성하고 있으며 미 국방부 자체 모의실험 결과 태평양 사령부 지휘통제소를 마비시키고 미 본토 전력망 피해를 유발시킬 정도의 사이버전 역량을 갖추고 있는 것으로 알려졌다[11].

넷째, 악성코드에 감염된PC(좀비PC)에 의한 공격이다. 3.4 디도스 공격의 경우는 여러 대의 PC를 악성코드에 감염시키고, 감염된PC들이 특정서버에 집중적으로 트래픽을 보내 과부하에 걸리게 하여 서버를 마비시키고 나중에는 감염된PC를 파괴하였다. 농협 전산망 장애사건과 SK컴즈 사건도 악성코드에 감염된 PC(좀비PC)에 의한 공격이었다. SK컴즈 사건의 경우 국내 한 소프트웨어 업체 서버의 자동 업데이트 파일이 악성코드에 감염되어서 파일을 업데이트하기 위해 그 서버에 접속한 PC를 감염시키고 이 감염된PC(좀비PC)가 SK컴즈 서버를 공격하였다.

<표 1> 최근 사이버테러 사례

사건	3.4 디도스	현대캐피탈	농협	SK컴즈
시기	2011.3	2011.4	2011.5	2011.7
공격자	북한	필리핀 서버(한국인)	북한 정찰총국	중국IP
피해	홈페이지 다운	175만명 고객정보 유출	서버파일 삭제	3500만 개인정보 유출
목적	정치적 동기(한국정부가 얼마나 빨리 발견하고 복구하는지 시험)	금전 요구	금전 요구는 없었고 사회혼란	금전 요구나 협박 없음
피해신고사례		2011.4.29까지 고객금전피해 신고 없음. 고객정보일부가 대부중개업자에게 팔려나감	개인피해 없음	개인피해 없음
공격 대상	한국정부,청와대,국정원,금융기관,인터넷기업			
공격방법	DDos	웹해킹	악성코드(좀비pc)	악성코드(좀비PC), 자동업데이트파일 이용
수사기관	경찰청 사이버테러대응센터	서울청 사이버범죄수사대	검찰	경찰청 사이버테러대응센터

4. 사이버테러 대비의 문제점

4.1 인터넷기업의 과도한 개인정보 수집

다수의 인터넷 기업이 서비스제공과 관계없이 상당수 국민의 주민등록번호, 휴대전화번호, 주소 등의 개인정보를 과도하게 수집·보관하고 있다. 2010년9월 기준 주요 인터넷 기업의 가입자수는 A포털 3284만 명, B게임 2375만 명, C쇼핑몰 2375만 명이다[10]. 이들 개인정보는 해킹에 의해 직접 전화사기, 메신저 피싱, 스팸 등 경제적 이득을 목적으로 사용되거나 해커가 다른 사람에게 판매하여 금전적 이득을 얻는데 사용될 수 있다. 인터넷 기업이 많은 개인정보를 보관하고 있는 한 해커들의 끊임없는 공격 대상이 될 것이다.

4.2 기업의 낮은 보안의식

한국인터넷진흥원(KISA)에 따르면[12] 2009년 국내기업 중 정보화투자 대비 정보보호 투자 비율이 1%미만인 기업이 17.9%이고, 정보보호에 전혀 투자하지 않는 기업이 전체의 63.5%에 달한다. 반면 미국 기업의 경우는 정보화투자 대비 정보보호 투자 비율이 10%가 일반적이다[13]. 또 정보보안 업무를 담당하는 전문 인력에 대한 필요와 인식이 낮다는 점도 문제다. 2009년 12월 기준 국내기업들 가운데 정보관리책인자(CIO)와 정보보호책임자(CISO)를 임명한 경우는 각각 18.7%, 14.5%에 불과하다. 미국 대기업, 정부기관의 70%이상이 CISO를 두고 있는 사실과 비

교하면 턱없이 부족한 실정이다. 정보보호 전담조직을 공식적으로 운영하고 있는 기업도 전체의 14.5% 수준으로 저조하다. 즉, 국내 기업의 80%이상이 정보보안관련 임원급책임자도, 전담조직도 갖추지 않고 있다.

국내 6500개 기업 중 정보보호정책을 수립한 기업은 전체의 25.8%에 불과하며 개인정보보호 전담조직을 운영하는 기업은 32.7%이다. 중견기업 중 정보보호투자를 늘린 비율은 39.1%로 대부분 예산을 동결하거나 줄이는 형편이다. 이는 기업들의 경우 해킹사태가 발생하더라도 법적 책임이 가볍기 때문에 보안에 투자할 유인동기가 적기 때문이다.

4.3 이용자 권리행사 부족

신규 악성코드 등 해킹 기술은 계속 발전하고 있어 해킹을 원천적으로 방지하는 것은 현실적으로 곤란하다. SK컴즈 사건의 경우, 관리자 PC에 설치된 신규 악성코드가 보안업체의 최신 백신에도 탐지되지 않아 고객정보가 유출되었다. 따라서 불필요한 계정 탈퇴, 패스워드 변경 등 이용자의 관리 노력이 중요하다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)에서 개인정보에 대한 열람권과 개인정보수집의 동의 철회권을 보장하고 있는 만큼 이용자는 개인정보를 열람해서 불필요한 정보는 삭제를 요구할 필요가 있다. 그러나 열람을 하거나 수집정보의 동의를 철회하는 방법을 수집방법보다 쉽게 해야 한다고 법에 명시하고 있음에도 불구하고 현실적으로 제약이 존재하는 것이 사실이다.

4.4 늑장신고 처벌 규정 미흡

업체에서 해킹사건 발생시 해킹사실이 외부에 알려지는 것을 꺼려해서 자체적인 해결을 시도하다 뒤늦게 신고하는 경우가 많다. 신고가 늦어질수록 사건해결에 어려움을 겪고 2차 피해의 가능성이 커질 수 밖에 없다.

현재 정보통신망법에 따르면 정보통신서비스 제공자는 개인정보 침해사고가 발생하면 즉시 방송통신위원회나 한국인터넷진흥원에 해당사실을 신고해야 한다. 하지만 벌칙조항이 마련되어 있지 않아 현재로서는 이를 지지키 않아도 규제할 방법이 없다. 정부는 2008년 해킹사실을 즉각 신고하지 않는 업체에게 과태료를 부과하는 내용의 정보통신망법 개정안을 발의했으나 아직까지 국회에 계류 중이다.

4.5 불법 소프트웨어 사용

소프트웨어가 기업용과 개인용(가정용)으로 구분되어 개인용은 무료로 배포(공개 소프트웨어)되고 기업용은 판매가 될 경우, 기업이나 영리기관에서는 공개용 소프트웨어를 사용할 수 없다. 만약 이를 위반하면 저작권법 위반이 된다. 최근 공개용 소프트웨어를 업데이트 하는 과정에서 악성코드에 감염되는 경우가 발생하고 있다. 따라서 기업에서는 기업용 제품을 구매해서 사용해야 법 위반도 하지 않고 악성코드 감염도 피할 수 있다.

SK컴즈 직원은 공개 소프트웨어를 사용해서 업데이트 하다 악성코드에 감되었고, 3.4 디도스 공격 때는 해커가 불법 파일공유사이트(P2P)를 통해 악성코드를 전파시켰다.

5. 사이버테러 대응방안

5.1.정보 유출 기업에 대한 처벌 강화

정보통신망법에서는 정보통신망에 무단침입한자는 3년 이하의 징역이나 3000만원 이하의 벌금이 부과되고 악성프로그램을 전달·유포한 경우에는 5년 이하의 징역 또는 5000만원 이하의 벌금이 부과된다. 그러나 정보통신서비스제공자 등이 보호조치를 위반했을 경우에는 2년 이하의 징역 또는 1000만원 이하의 벌금이 부과된다. 즉, 보호조치를 위반했을 때에 훨씬 낮은 벌칙이 부과된다. 앞에서도 언급한 바와 마찬가지로 해킹의 최근 경향은 북한이나 외국IP로 행해지는 경우가 많은데 외국IP의 경우 사실상 수사가 불가능하다. 또한 해커의 공격을 예측하여 미연에 방지하는 것 역시 어려운 일이다. 따라서 우리나라의 정보시스템 보안에 주안점을 둘 필요가 있다. 그러나 현재 우리나라의 정보보안 실태는 열악한 상태이다.

이는 경영진의 인식부족과 가벼운 처벌 때문이다. 최근 정보유출 규모가 확대되고 있는 만큼 수천만 명의 개인정보를 보관하는 업체는 철저한 보호조치를 해야 할 법적·도덕적 의무가 있다할 것이다. 따라서 정보통신망법의 보호조치 위반시 현재보다 더 무거운 형량으로 법개정을 할 필요가 있다.

5.2 개인정보 수집 제한 대상의 확대

최근 정보유출 규모가 확대되고 있는 이유 중 하나는 업체가 많은 정보를 보유하고 있기 때문이다. 해킹의 목적이 과거 자신의 과시에서 현재는 금전적 이득으로 변함에 따라 저장되어 있는 많은 정보는 해커들에게는 유혹이 아닐 수 없다.

개인 정보 중 주민등록번호에 대한 보호 조치는 법적으로 강화되고 있다. 정보통신망법에서 일일 평균 이용자수가 일정 기준에 해당하는 정보통신서비스 제공자는 회원가입시 주민등록번호 이외의 방법으로 가입할 수 있도록 해야 한다고 명시하고 있고, 지난 9월30일부터 시행된 개인정보보호법에서는 일일평균 이용자수가 1만명 이상인 개인정보처리자는 회원가입시 주민등록번호 이외의 방법으로 가입할 수 있도록 해야 한다고 명시하고 있다. 지난 8월8일 방송통신위원회가 발표한 '인터넷상 개인정보보호 강화 방안'에 따르면 현재는 이용자의 동의가 있으면 누구나 주민등록번호를 수집할 수 있지만 내년부터는 본인확인 차원에서 1회성으로 주민등록번호를 물을 수 있으나 저장해서 보관할 수는 없도록 했다.

그러나 주민등록번호 이외의 개인정보에 대한 수집 제한 조치는 마련되어 있지 않다. 수집제한 대상을 확대하여 수집하지 않도록 하는 법제화가 필요하다.

5.3 국가보안체계 정비

최근 들어 3.4 디도스 공격, 농협 전산망 장애사건 등 북한에 의한 해킹이 자주 발생하고 중국 등 외국 발IP를 사용하는 해킹이 빈번하므로 이를 국가안보차원에서 국가보안체계를 정비할 필요가 있다.

일부 탈북자의 증언에 의하면 북한 정찰총국 산하에 최소 1000명에서 최대 3000명에 달하는 사이버공격 조직이 있고 북한은 물론 중국 전역에서 활동하는 것으로 알려져 있다. 또한 이 정찰총국은 천암함 폭침, 연평도 포격은 물론 농협 전산망 장애사건 등 각종 사이버테러도 주도한 것으로 알려져 있다. 북한의 사이버전 능력은 미국 중앙정보국에 필적한다는 분석도 있다[14].

우리나라 정부의 보안 감시 체계는 공공·민간·국방부문을 국정원·방통위·국방부에서 각각 총괄하고 있다. 그러나 세 부분으로 나뉘어 있어 부처간 협력에 어려움이 많아 통합의 필요성이 대두되고 있었다. 최근 들어 일련의 대형 해킹사건이 발생하자 정부는 지난8월8일 '국가 사이버 안보 마스터플랜'을 발표했다. 이 마스터플랜은 공공·민간부문은 위기상황이 발생할 경우 국정원이 컨트롤타워 역할을 하도록 하고 있다. 이는 북한의 사이버공격이 가속화되고 있는 시점에서 대북 정보를 총괄하는 국정원에서 사이버보안의 책임을 총괄하는 것은 국가 안보 차원에서 국정원에 합당한 힘을 실은 것으로 볼 수 있다. 다만, 국가적인 사이버감시체계가 발전하면 할수록 개인정보보호나 프라이버시 문제 등이 불거질 가능성이 큰 만큼 여기에 대한 대비도 철저히 해야 할 것이다.

최근 계속되고 있는 북한의 사이버공격은 정부기관이나 금융·의료 등 국가적 주요기관에 대한 사이버테러를 자행하여 국가를 혼란에 빠뜨리기 위한 사전작업으로 평가된다. 북한에 의한 해킹은 그 의도와 방법을 파악하여 재발 방지에 최선을 다 해야 할 것이다.

5.4 업체 보안 전담 조직 구성

국내 정보보호전담조직을 운영하는 업체가 15.4%로 아주 미흡한 상태이다. 보안전담조직은 최고경영자(CEO) 직속으로 정보보호책임자(CISO)를 두어야 한다. 정보보호 전담부서는 정보보호에 관한 전사적인 문제에 대한 주관부서이며 기관 전체의 정보보호를 확보할 실무적인 책임을 진다. 정보보호부서장은 CISO(정보보호담당 임원)에게 보고하며 CISO는 정보보호부서의 경영자로서의 역할과 다른 부서의 정보보호에 대한 방향제시를 수행하고 또한 CEO에게 정보보호 상태를 직접 보고할 의무를 가진다.

지난 8월8일 발표된 '인터넷상 개인정보보호 강화 방안'에서도 일정규모 이상의 기업에 CISO 지정을 제도화하는 방안이 제시되었다.

방송통신위원회는 해킹 등 보안사고가 발생할 경우 경영자의 책임을 명확히 하기로 했다. 지금까지는 CEO차원에서 책임지는 경우는 드물었다. 정보통신망법을 개정해 보안사고 발생기업 CEO의 처벌을 강화하는 방안도 검토 중이다[15]. 정보보호 전담조직을 구성해서 책임자의 책임 하에 운영되면 정보보호는 한층 강화될 것이고, 또 CEO에 책임을 부과함으로써 정보보호에 대한 경영자의 인식을 제고할 수 있을 것이다.

5.5 국제협력 강화

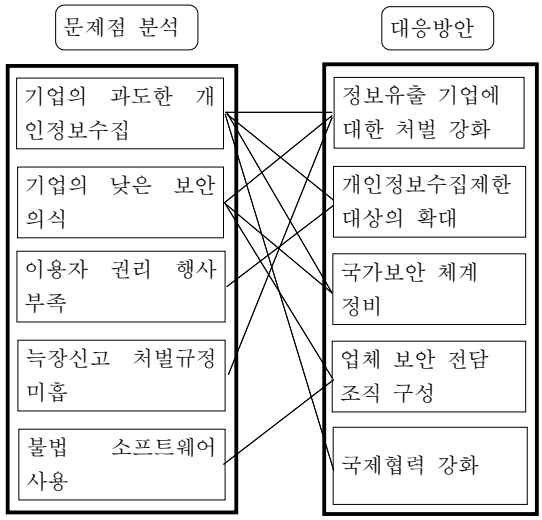
최근의 사이버공격 형태는 국가간 연계되고 있는 것이 특징이다. 해커들은 역추적을 피하기 위하여 여러 기관 또는 해외를 경유하여 공격을 감행하고 있다. 따라서 기관간 국가간 공조대응의 필요성은 그 어느 때보다도 절실해지고 있다.

최근의 사이버공격 형태는 외국IP를 사용하는 특징이 있다. 북한이 중국IP를 사용하는 공격, 중국인의 국내공격이나 현대캐피털 사건과 같이 한국인이 필리핀 현지서버를 통해 국내 서버를 공격하는 경우 등이 있다. 북한이 중국IP를 사용하는 공격의 경우 중국과의 외교문제가 발생할 수 있으며, 중국인의 공격의 경우는 중국당국의 수사협조가 소극적일 수 있다. 현대캐피탈 사건과 같이 필리핀에서 한국인에 의한 공격의 경우엔 필리핀당국과 수사공조를 통해서 사건을 해결하여야 한다. 따라서 인터폴 사이버범죄관련기구, 국제컴퓨터침해사고 대응협의회(FIRST), FBI 컴퓨터범죄회의 등과의 긴밀한 협조가 요구된다.

5.6 개인정보의 암호화 강화

정보를 암호화하면 설령 유출되어도 해독(복호)을 하지 못하면 의미 없는 정보가 될 것이므로 정보보호를 할 수 있다. 그럼에도 불구하고 국내에서는 특정 정보에만 국한되어 암호화가 되고 있다. SK컴즈 사건에서도 드러났듯이 암호화된 개인정보는 주민등록번호와 비밀번호 뿐이었다.

정보통신망법 시행령에서 개인정보 중 비밀번호, 바이오정보, 주민등록번호, 계좌정보 등 금융정보는 암호화하도록 규정하고 있다. 내년부터는 주민등록번호는 저장·보관이 금지되므로 암호화에서 제외될 것이다. 업체가 저장하고 있는 개인정보 중 암호화 대상을 확대할 필요가 있다.



(그림 2) 대응방안의 체계도

6. 결 론

최근 들어 해킹사건은 그 피해 규모가 확대되고 있고 외국IP를 사용하여 국내로 침투하고 있으며 북한에 의한 공격이 증가하고 있는 특징을 보이고 있다. 인터넷업체들이 필요이상의 정보를 수집하여 많은 정보를 보유하고 있는 것이 경제적 이득을 노리는 해커들의 표적이 되고 있고, 우리사회의 혼란을 노리는 북한에 의한 공격은 더 큰 혼란을 획책하는 사전 탐지의 성격을 띠고 있는 것으로 보여져 대응책 마련이 시급한 실정이다.

이에 대응하기 위하여 인터넷업체들이 수집하고 있는 정보를 최소화하고 저장하는 정보의 암호화를 의무화하는 법개정이 필요하고 북한의 사이버테러에 신속하고 철저하게 대응할 수 있는 국가 사이버 안보

체계를 구축할 필요가 있다. 또한 외국과의 사이버테러 대응을 위한 국가간 공조시스템을 구축할 필요가 있다.

참고문헌

[1] 방송통신위원회,“정부, ‘국가 사이버안보 마스터플랜’ 수립”, 2011.8.

[2] 국가정보원, “국가사이버안전매뉴얼”, 국가사이버안전센터, 2005.10.

[3] 백광훈, “사이버테러리즘에 관한 연구”, 한국형사정책연구원, 2001,

[4] TTA, ‘정보통신용어사전’, 한국정보통신기술협회

[5] 대통령훈령 제267호, ‘국가사이버안전관리규정 제2조’, 2010.

[6] 사법연수원편집부, ‘신종범죄론’, 사법연수원, 2008.

[7] 이민식, “사이버공간에서의 범죄피해”, 한국형사정책연구원, 2000.

[8] Debra Littlejohn Shinder, Ed Tittel 공저; 강유역, ‘사이버범죄 소탕작전 컴퓨터 포렌식 핸드북’, 에이콘출판사, 2003.

[9] 이태윤, ‘새로운 전쟁, 21세기 국제 테러리즘:미 9.11테러와 대테러 전쟁의 실체’, 모시는 사람들, 2004.

[10] 방송통신위원회, “인터넷상 개인정보보호 강화방안”, 2011.

[11] 문종식,이임영, “사이버테러동향과 대응방안”, “정보보호학회지”, 제20권, 제4호, pp.21-27. 2010.

[12] 방송통신위원회, “2010년 정보보호 실태조사(기업편)”, 한국인터넷진흥원, 2011.

[13] 양철민, “IT보안을 다시 본다:날뛰는 해커 고개 숙인 보안업체”, 서울경제신문, 2011.8.

[14] 진영태,이유라 , “북 해커 온라인 게임 털어 외화벌이”, 서울경제신문, 2011.8.

[15] 유주희,이유라, “정부, ‘사이버안보 마스터플랜’ 발표”, 서울경제신문, 2011.8.

[저 자 소 개]

정 기 석 (Gi-seog Jeong)

1983년 2월 고려대학교 전자공학과 학사
1988년 8월 고려대학교 전자공학과 석사
1992년 8월 고려대학교 전자공학과 박사
현재 영동대학교 정보통신보안학과 교수

email : gsjeong@yd.ac.kr