한국위기관리논집 제5권 제2호 2009. 119~135쪽

사이버테러 동향 및 대응방안

이철원*, 배병철
ETRI부설연구소

국가 인프라를 이용하여 상호 연동되는 에너지, 교통, 금융, 의료 등 국가 주요기반체계로까지 사이버 공격 위협이 현실화되는 시점에서 국가기반체계에 대한 사이버 위협을 경감하기 위한 법·제도적 대책 및 기술적 대응책을 마련하는 등 사이버테러 대응방안에 대한 보완이 필요하다. 본 논문에서는 사이버 테러의 특성 및 사례 분석을 통해 사이버 테러 대응체계 구축을 위한 방안을 설명한다.

주제어: 사이버 공격, 사이버 위협, 사이버 테러, 국가기반체계

Ⅰ. 들어가며

국외에서 발행되는 다양한 정보화 관련 지수를 고려할 때, 우리나라는 인터넷 강국의 면모를 계속 유지하고 있다. 우리나라는 UN의 전문기구인 국제전기통신연합(ITU: International Telecommunication Union)이 인프라 보급, 기회제공, 활용정도 등 3가지 요소를 종합·분석하여 정보통신 발전 정도를 평가하는 디지털 기회지수(DOI : Digital Opportunity Index)에서 2005년부터 3년 연속 1위를 차지하였다. 또한, 세계경제포럼(WEF, World, Economic Forum)에서 발표하는 네트워크 준비지수에서 지난해 9위를 차지 하였다. 2008년 7월 현재 국내 인터넷이용자는 3,619만 명(인터넷 이용률 76.5%), 초고속인터넷 가입자는 1,509만 가구로 전체가구 대비 초고속인터넷 보급률이 약 90%에 달하는 등 세계 최고 수준의 정보통신 인프라를 확충하고 본격적인 지식정보사회로 도약하고 있다.

인터넷뱅킹을 통한 조회, 자금이체 및 대출서비스 이용 건수는 하루 평균 2,243만 건으로 2008년을 기준하여 2007년에 비해 25.1% 증가하였다. 휴대전화와 PDA 등 이동통신기기를 이용한 모바일뱅킹은 2008년 일평균 106만 건으로 2007년에 비해 47.6%나 증가하였으나 인터넷뱅킹에서 차지하는 비중은 4.7%에 불과하였다. 금융서비스 전달채널별 업무 비중을 살펴보면 입금과 출금, 자금이체 등 입출금 거래를 기준으로 창구거래의 비중은 2008년 12월 기준으로 17.3%를 나타내 1년전 같은 시기에 비해 3.1% 하락하였다. 이에 반해 인터넷뱅킹을 포함한 비대면 거래의 비중은 79.6%에서 82.7%로 올라가 80% 선을 돌파하였다.

우리나라는 상기와 같은 정보통신 인프라를 이용하여 에너지, 통신, 교통, 금융, 의료, 수도 등 국가 기능유지에 필요한 기반체계를 발전시켜가고 있다. 기반체계를 운영·관리하는 설비가 인적 의존도가 큰 수동체계에서 IT를 접목한 자동화 체계로 급속히 전환되

* 교신저자

고 있으며, 기반체계 간 상호 의존도 증가로 인하여 기반체계 운영·관리에 적용하는 기술이 표준화·개방화 되고 있는 추세이다.

아이러니하게도 국내의 발전된 정보통신 인프라가 해킹과 바이러스 유포 등 사이버 공격을 위한 중간 경유지로 이용되고 있으며, 정보통신 인프라를 이용하여 상호 연동되는 에너지, 교통, 금융, 의료 등 국가 주요기반체계로까지 사이버 공격 위협이 현실화 되고 있는 실정이다. 2007년 러시아로부터 독립한 발트해 인터넷 강국인 에스토니아의 대통령궁, 의회, 각 부처, 집권당, 언론사, 은행의 전산망과 홈페이지 등이 국외로부터 사이버공격을 대대적으로 받은 사건이 발생하여, 사이버 위협이 국가 안보 및 국가경제에 심각한 영향을 끼친다는 사실이 입증되기도 하였다.

사이버 공격은 국가 기반체계뿐 아니라 개인의 일상생활에까지도 막대한 피해를 끼치고 있다. 악성댓글, 스팸메일, 개인정보 유출, 금전적 이득 취득을 목적으로 하는 피싱(Phishing)이나 파밍(Pharming)에 따른 개인적인 피해가 증가하고 있으며, 불건전 정보 유통, 개인 사생활 침해와 같은 부작용 등이 심각한 사회문제로 대두되고 있다. 심지어 국회에까지 보이스 피싱 사례가 발생하고, 사용자가 직접 제작한 콘텐츠인 UCC(User Created Contents)를 이용한 사생활 침해와 명예훼손, 음란물 노출, 정보보안 위협 등 UCC 역기능도 부상하고 있다.

또한, 2007년 와이브로 관련 핵심기술을 하드디스크나 이메일을 통하여 유출 하려던 시도가 적발되는 등 국가 경제에 지대한 영향을 미치는 산업기밀까지도 사이버 공격 대상이 되고 있다. 이와 같이, 에너지, 통신, 교통, 금융, 의료, 수도 등 국가 기반체계에 대한 사이버 공격은 개인의 사생활 침해와 인터넷 서비스 이용에 큰 피해를 끼칠 수 있다. 우리나라 주요 기반체계 및 핵심자산의 보호는 국가안보, 경제 활성화 및 개인의 일상생활 보장측면에서 매우 중요하다. 교통, 에너지, 수자원, 통신 등 국가적 필수 서비스를 제공하는 핵심자산에 대한 사이버 공격은 정부와 기업의 업무를 심각하게 훼손함은 물론 재앙적 결과를 초래할 수 있기 때문이다. 특히, 테러리스트에 의한 사이버공격은 국가 경제에 심각한 피해를 초래하기도 하며, 심지어 인명손실에까지 피해가 확산됨은 물론 사회 구성원의 사기저하 및 국가의 신뢰도 손상 등 유·무형의 막대한 피해를 동반한다. 사이버 공격은 재래적인 대량살상무기를 사용하는 전통적 테러보다 훨씬 심각한 물리적, 심리적, 경제적 및 국가안보 측면의 파급효과를 야기한다.

따라서, 국가기반체계에 가해지는 사이버 위협을 사전에 예방하고, 위협이 현실화 될 때 즉각적으로 탐지하고 대응하며 피해를 신속히 복구하고 공격 경위를 조사하여 재발을 방지함은 물론 법적 조치를 취하는 것이 매우 중요하다. 즉, 국가기반체계에 대한 사이버 위협을 경감하기 위한 법·제도적 대책 및 기술적 대응책을 마련하는 등 사이버테러 대응방안 보완이 절실히 필요한 시점이다.

II. 사회 전체가 직면하는 새로운 차원의 위협

IT의 사회기반화는 정보보호 측면에서 보면, 전혀 새로운 차원의 위험을 사회전체에 가져다주고 있다. IT 기술의 혁명이 생활 구석구석까지 급속하게 진행하기 시작한 가운데, 지금까지 경험하지 못했던 새로운 형태의 위험이나 범죄, 테러 등이 발생하고 있으며, 이러한 위험이 다른 위험으로 전이될 수 있다.

우선 개인정보의 침해가 점차 국가적인 수준의 위험으로 변모하고 있다는 것을 지적할 수 있다. 종래, 개인정보 침해는 절취한 개인정보를 이용하여 게임머니 획득, 개인정보 거래를 통한 금전적 이득 취득이 주류를 이루었다. 그러나, 최근 웹 포털, 게임사이트 등을 해킹하여 취득한 개인정보 특히 이메일 ID를 이용하여 국가 중요기관 종사자에게 악성코드가 첨부되

어 있는 메일을 전송하여 국가 중요기관의 기밀문서를 절취하는 등 국가적 위험으로 발전되고 있는 양상이 나타나고 있다. 대규모 개인정보 침해로 인해 사회 구성원의 심리적 불안이 유발되는 단순한 해킹에서 국가기밀이 누출되는 국가적 위험 사태로까지 확대될 수 있다. 개인정보 침해를 국가 위험관리와 분리해서 고려할 수 없는 이유가 바로 여기에 있다. 웜 바이러스 확산, 개인정보침해의 피해가 단순히 각각의 조직이나 개인의 업무·생활에 지장을 초래하는 것만이 아니라, 경제활동의 방해나 국민의 생명·재산에 관한 위험을 초래하는 상황이 되고 있다. 구체적으로는 다음과 같은 사례를 살펴볼 수 있다.

1) 컴퓨터 바이러스, 웜바이러스

컴퓨터 바이러스나 웜에 의한 피해가 사회적인 문제로 대두된 것은 오래지 않은 일이다. 2003년 1월에는 Slammer 웜이, 8월에는 Blaster 웜이 출현하여 짧은 기간에 전 세계의 네트워크를 마비시켰다. 이들은 소프트웨어의 취약성을 뚫고, 감염하는 것으로 취약성이 수정되지 않으면, 인터넷에 접속하고 있는 것만으로 피해를 입을 위험성이 있어, 우리나라에서는 Slammer 웜이 심각한 인터넷 접속장해를 초래했다. 또, Blaster 웜의 감염대상은 개인이 이용하는 운영체제(OS)를 탑재한 PC여서 우리나라에서도 개인사용자를 시작으로 큰 피해가 발생하였다.

2) 부정 접근

미국 카드결제처리회사의 시스템이 부정 침입되어 신용카드번호 약 800만매분이 도난당하는 등, 시스템에 대한 부정 접근에 의하여 기업의 고객 신용카드 번호나 고객사원의 명부 등이 유출되는 사건은 일일이 열거할 수 없을 정도이다. 국내에서도 인터넷 신용카드 결제 취약점을 악용해 수억원을 인출한 해킹 사건이 발생한 바 있다. 범인들은 대부분 카드 사용자가 일반 홈페이지와 쇼핑몰, 카드사의 접속 ID와 비밀번호가 동일한 것에 착안해 구글 등 검색엔진과 해킹도구를 이용해 인터넷 사용자의 접속정보 8만건을 수집했다. 이들은 이 정보를 이용해 쇼핑몰·카드사·결제대행회사(PG) 홈페이지에 접속해 부분적으로 남겨진 카드 정보를 조합, 카드번호를 완성했다. 범인들은 신용카드결제 체계의 취약점을 이용해 I사이트에서 타인의 아이템을 대신 구매해주고 현금화가 가능한 사이버머니를 충전받아 1억8000만원을 인출한 바 있다.

또한, 해커들이 온라인 소매상 등의 컴퓨터 서버에서 훔친 신용카드 번호가 러시아와 우크라이나 등 옛 소련 지역 거주자들이 만들어놓은 인터넷 암시장에서 활발하게 거래되고 있다고 미국의 유력 신문에서 보도된 사례도 있다. 이와 같이 정보시스템에 대한 부정 접근을 통하여 개인의 신용정보 유출을 통한 경제적 피해 유발, 기업의 산업기밀 유출 등 국가 경쟁력에도 악영향을 미치고 있다.

부정접근·부정조작에 의하여 단순한 Web 페이지의 변조 등과 같은 단순 위험사례를 벗어나, 실제로 피해규모가 심각한 사고나 사건도 발생하고 있다. 2003년 3월에는 인터넷 카페에 입력조작을 몰래 할 수 있는 키로거라는 소프트웨어를 설치하여, 입수한 패스워드 등을 근거로 1600만엔을 부정하게 이체하는 사건이 일본에서 발생한 바 있다. 또, 옥션 사이트 사용자 10인의 ID로부터 패스워드를 미루어 생각하여, 무단으로 사용·판매한 사건과 같이 인터넷 사용자의 패스워드 등이 도난당하여 악용되는 사건도 증가하고 있다. 개개의 기업이나 사용자의 피해를 넘어 경제거래시스템에 대한 신뢰의 문제로 발전하여 궁극적으로 국가경제에 커다란 악영향을 미칠 수 있다.

이러한 사례에서 알 수 있는 바와 같이 최근의 정보보안 관련 사고나 사건은 문제를 일으킨 당사자나 피해를 입은 당사자만의 문제에 그치지 않고, 주위의 거래상대, 친구, 불특정다수에 대한 피해, 경제시스템 자체에 대한 신뢰문제, 사회기반의 기능마비 등, 국가사회 전체에 영향을 미치는 문제로 확대해 나가는 경

향을 나타내고 있다.

또, 통신비용의 저가격화와 네트워크의 용량증대상 시접속화에 의한 이른바 '브로드 밴드화'가 IT 사용자 수나, 취급하는 데이터양을 급속하게 확대시키고 있는 것으로부터, 한 곳에서의 취약성에 기인하는 소규모 사고가 시스템네트워크 전체에 파급되어 대규모 피해로 이어질 가능성은 비약적으로 높아지고 있다.

SCADA(Supervisory Control And Data Acquisition) 시스템은 난방, 냉방 그리고 환기시스템, 에너지 발생 혹은 운반 설비들, 그리고 고속도로 혹은 철도 교통통제시스템 같은 일들을 제어하는 역할을 수행한다. SCADA 시스템은 우주왕복선 실험조차도 제어할 수 있다. 이런 시스템에 대한 성공적인 공격은 대규모 물리적 테러가 야기하는 피해효과를 훨씬 넘어서 재앙적 수준의 피해를 초래할 수 있다.

III. 사이버테러의 특성, 영향의 범위 및 현황파악

국가 기반체계에 가해지는 사이버테러의 특성, 영향의 범위 및 현황을 기술하기 전에 관리가 필요한 대상 영역에 대한 정의가 필요하다. 국가 기반체계란 에너지, 정보통신, 교통수송, 금융, 보건·의료, 원자력, 환경, 식용수 등 그 기능이 마비될 경우 인명과 재산 및 국가경제에 심각한 영향을 미칠 수 있는 물적·인적 체계를 말하며, 국가 기반시설이라 함은 국가 기반체계의 보호를 위하여 계속적으로 관리할 필요가 있다고 인정되는 시설 중 다른 기반시설이나 체계 등에 미치는 연쇄효과, 둘 이상의 중앙행정기관의 공동대응 필요성, 재난이 발생하는 경우 국가안전보장과 경제·사회에 미치는 피해규모 및 범위, 재난의 발생가능성 또는 그 복구의 용이성을 고려하여 지정된 시설을 말한다.

본고에서는 국가 기반체계 중 국가 안보 및 국가·공공기관이 운영·관리하는 기반시설에 대한 사이버테러 대응 체계는 국가 사이버안전관리체계 및 국가 위기관리지침에 의하여 이미 잘 정의되어 있으므로 이들 영역을 제외한 민간분야 국가 기반체계에 국한하여 사이버테러 대응 체계 구축 방안을 제시한다. 즉, 정보통신, 의료, 금융, 식용수, 전자적 대민서비스 등과 관련한 국가 기반체계에 국한한다.

국가 기반체계에 가해지는 사이버테러의 특성, 영향의 범위 및 위험 현황을 살펴보기 전에 국가 기반체계의 특성을 이해하는 것이 동 기반체계에 가해지는 사이버테러의 특성을 파악하기 용이하다.

1. 국내 경제와 국가안보는 국가 기반시설에 의해 크게 영향을 받는다. 국가 기반시설의 상호 연계 및 상호의존성을 이용하여 운송, 금융, 의료, 에너지 등 모든 영역의 기능과 서비스 실행이 가능하다.

2. 사이버테러리스트, 악의적 해커 등 다양한 형태의 위협원이 사이버 공격 수단을 이용하여 주요 기반시설을 공격할 수 있다. 사이버 주요기반시설은 서로 연결되어 있기 때문에 공격이 순식간에 타 기반시설로 파급되어 주요기반시설을 약화시킬 수 있다.

3. 혁신적인 기술과 네트워크 연결로 생산성과 효율성은 증가하지만, 사이버 보안 문제가 해결되지 않고 적절하게 통제되지 않는다면 국가적인 위험 또한 증가한다.

4. 국가 기반시설의 상호연결 및 상호의존적 성격 때문에 물리적 및 사이버 자산을 별도로 구분하여 보호하기에는 문제가 있다.

5. 사이버 보안은 기밀성, 무결성 및 가용성 확보를 위해 정보, 통신 시스템 및 시스템 내 보관된 정보의 손상, 불법적 접근 또는 해킹 방지를 포함한다. 또한 테러리스트의 공격이나 자연재해 발생 시의 정보와 통신 시스템 복구도 포함하고 있다.

상기 특성을 지닌 국가 기반체계에 대한 사이버테러의 특성은 사이버 공격 양상의 변화로부터 살펴볼 수 있다. 사이버 공격은 지적 호기심 충족 혹은 자기과시를 위한 영웅적 행태의 단순 해킹에서 경제적 이

익을 위한 의도적 해킹, 특정 국가를 대상으로 한 사이버 공격으로 발전하고 있다. 또한, 2004년 중국발 국가기관 해킹사고에서 알 수 있듯이 과거 불특정 다수에 대한 흥미 위주의 공격에서, 게임업체, 인터넷 포털 등 특정 조직이나 국가를 대상으로 개인정보, 국가기밀과 첨단 산업기밀을 탈취하는 등 조직적 형태로 발전하고 있다. 최근에 나타난 사이버테러의 특성은 다음과 같다.

1) 단순 웜·바이러스는 감소, 금전적 목적의 악성코드 유포는 증가

2007년도에 한국정보보호진흥원에 접수된 웜·바이러스 신고건수는 5,996건으로 2006년(7,789건)에 비하여 23.0% 감소하였다. 감소한 원인에는 여러 가지 요인이 있겠으나 가장 직접적인 이유는 최근 들어 지적호기심, 컴퓨터 사용능력 과시를 목적으로 제작되어 네트워크를 통하여 급속히 전파하는 인터넷 웜이나 이메일 등으로 대량 전파되는 단순 웜·바이러스 제작 및 유포가 줄었기 때문이다. 반면 특정 온라인 게임의 계정, 개인정보를 탈취하는 등 금전적 이익을 목적으로 하는 악성코드 유포는 지속적으로 증가하는 추세다.

2) 국내 웹 사이트를 대상으로 한 분산서비스거부공격(DDoS) 증가

2007년도부터 해커가 국내 웹 사이트를 대상으로 메신저나 이메일, 전화를 통하여 금품을 요구하고, 이에 불응 시 DDoS 공격을 가하여 서비스를 마비시키는 금품요구 및 협박성 DDoS 공격이 증가하였으며 주요 특징은 다음과 같다.

- o 금품요구 및 협박성 분산서비스거부공격 증가
- o 공격대상 웹 사이트의 다양화
- o 공격 트래픽 규모의 증가
- o 공격에 악용되는 좀비 PC 감염 수단의 다양화

2009년 7월에는 국내 주요 포탈, 정부부처, 금융기관 등을 대상으로 DDoS 공격이 발생하여 일시적으로 정상적인 서비스 제공이 단절되는 사태를 초래하였다.

3) 웹 2.0 보안 고려 필요성 대두

웹 2.0 환경에서는 정보 소비의 주체로만 여겨졌던 이용자가 정보 생성의 참여자로, 적극적으로 의견을 제시하고 타인과 연계해 전문가 수준의 영향력을 갖게 된다. 이는 사용자의 정보 접근성과 편의성이 높아지고, 정보에 대해 능동적으로 이용하게 되었음을 의미한다. 또한 정보 자체 측면에서 볼 때 다양성과 품질이 향상되는 특성도 보이고 있다. 결국 인터넷 업계에서는 웹 2.0이 하나의 추세이자 새로운 비즈니스 모델로 자리잡아 가고 있다고 볼 수 있다.

하지만 웹 2.0 기술을 도입하고자 할 때 보안을 고려해야 하는데, 사용자의 참여가 높은 개방성의 특징을 갖는 환경이므로 기존 웹이 가지고 있는 취약점보다 더 많은 보안 취약점이 존재하게 된다. 또한 웹 2.0에서는 검증되지 않은 정보의 공개로 인하여 개인 프라이버시 침해의 문제가 발생될 수 있다. 얼마 전 웹 2.0 환경의 미국 MySpace에서 동영상 재생을 위해 사용하고 있는 Apple사의 Quick Time 동영상 파일에 악성 자바 스크립트를 삽입해 동영상을 재생하면 피싱 사이트로 연결되어 사용자의 계정 정보를 유출하려는 시도가 있었다. 따라서 웹 2.0 환경에서는 보안을 더욱 중요하게 고려하여야 하며 발생 가능한 보안 위협에 대하여 철저한 대응이 필요할 것이다.

4) 내부자 보안의 중요성 증대

최근에는 보안의 패러다임이 네트워크 보안에서 컨텐츠 보안으로 변화하고 있다. 기밀정보 유출에 따른 기업의 경제적 손실이 증가하고 있으며, 고객의 개인정보나 기업의 기밀정보 등이 이메일, 인스턴트 메시징 서비스, P2P 등을 통하여 무분별하게 유출될 수 있는 위험에 노출되어 있다. 실제로 미국 CSI/FBI 보고서에 따르면, 2002년 미국에서 발생한 정보유출 사

고 중에 약 80%가 내부자에 의한 것으로 파악되었다. 우리나라의 경우, 국가정보원 산업기밀보호센터에 따르면, 2003년도부터 2006년도까지 산업기밀 유출 적발사건이 92건에 이르며 총 피해예상 금액은 95조 9천억원에 달한다고 밝혔다. 이러한 정보유출의 문제가 산업기밀이나 행정 또는 군사에 관한 국가기밀정보를 대상으로 발생한다면 국가차원의 매우 중대한 피해가 아닐 수 없다. 그동안 보안이라 하면, 외부의 공격으로부터 내부의 자원을 안전하게 지키고자 하는 측면에 집중되어 왔다. 하지만 앞으로는 내부자로부터 내부자원을 안전하게 지키는 것도 보안의 영역에서 큰 비중을 차지하는 방향으로 그 패러다임이 변화하고 있다. 따라서 내부자 위협에 효과적으로 대응하기 위한 기술뿐만 아니라 관리 및 운영 측면에서의 접근도 동시에 이루어져야 할 것이다.

5) 응용프로그램을 겨냥한 보안 취약점 출현 증가

국내에서 가장 사용률이 높은 것으로 알려진 MS社의 윈도우 운영체제 및 관련 응용프로그램에 대한 보안업데이트 발표현황을 분석한 결과 Office 제품군에 대한 취약점 비율이 15%로 2006년도(15.6%)와 마찬가지로 응용프로그램 측면에서는 가장 많았으며, 인터넷 익스플로러 취약점은 12%로 2006년도(9.3%) 대비 약 3% 증가하는 결과를 보였다. 이처럼 최근에는 운영체제 자체 보다는 응용프로그램 취약점이 증가하고 있으며, 이에 따라 응용프로그램 취약점을 공격하는 사이버 공격도 지속적으로 증가할 것으로 보인다.

6) 중국발 악성코드 전파 및 해킹 증가

중국은 1990년대 중반부터 시스템 및 네트워크에 대한 연구를 통하여 중국 특유의 언더그라운드 해커 문화를 형성하였다. 1990년대 후반 중국 해커들의 기술은 외국에서 개발된 프로그램을 이용하는 수준이었지만 점차 해커들 스스로 트로이목마 프로그램이나 해킹 프로그램을 제작하기 시작하였으며, 최근에는 국내 국가·공공기관의 시스템을 해킹하여 주요 자료를 빼내가거나 웹서버 해킹을 통하여 우리나라 국민의 개인정보를 빼내가는 수준에 이르고 있다.

중국발 해킹은 우리나라뿐만 아니라 미국 등도 목표가 되고 있어 최근 미 육군에서는 주요 PC를 매킨토시로 교체하는 작업까지 수행하고 있는 상황이다. 그만큼 중국발 해킹은 전 세계적으로 큰 위협으로 자리 잡고 있다. 중국발 해킹에서 개인정보를 유출해가는 절차를 보면, 우선 접속자가 많은 유명사이트의 웹서버를 해킹하고, 악성코드를 은닉한 뒤, 보안이 취약한 PC를 이용하여 해당 웹사이트에 접속하는 인터넷 이용자의 PC를 악성코드에 감염시키고, 접속자 PC에 상주하여 주민등록번호, 각종 사이트 아이디 및 비밀번호를 추출하여 개인정보를 해커 컴퓨터로 이동시키는 방법을 이용하고 있다.

심지어는 중국 내에서 한국의 웹서버를 해킹하는 방법이나 한국인의 개인정보를 취득하는 해킹기법에 대한 자세한 설명과 도구가 담겨져 있는 잡지가 시중에 유통되고 있는 상황이다. 하지만 국가차원에서 중국발 해킹에 대한 근원지를 조사하는 과정에서 중국 내 IP가 근원지로 확인된 경우에도 중국과의 사법공조협정이 체결되지 않아 자세한 공격자 조사에 어려움을 격고 있다.

향후에도 이러한 중국발 해킹 및 악성코드의 전파는 계속적으로 증가할 것으로 예상된다.

7) 메모리 해킹수법 등 해킹 수법 고도화

메모리 해킹이란 램(RAM: Random Access Memory)이라고 불리는 주기억장치에 저장되는 데이터를 절취하거나 이를 조작하는 해킹 기법이다. 기존의 피싱과 파밍 등의 해킹 수법들이 메일이나 전화 등 외부수단을 이용해 사용자의 계좌와 비밀번호 등의 금융정보를 빼내는 것과 PC 해킹을 통해 백도어 프로그램을 설치한 뒤 전용 도구를 통해 메모리상의

데이터를 절취하고 변조한다는 점에서 차이가 있다. 이러한 메모리 해킹을 통한 인터넷뱅킹의 실질적인 피해는 아직 보고된 바 없지만 메모리 해킹 방식이 범죄에 악용될 경우 인터넷뱅킹 자체의 신뢰성과 안전성에 큰 위협이 된다는 점에서 최근 금융권과 당국의 주요 보안이슈로 떠오르고 있다.

8) ARP(Address Resolution Protocol) 스푸핑 기법을 이용한 악성코드 유포 증가

취약한 웹 서버를 사전에 해킹한 후 초기화면에 악성코드를 은닉하여 해당 사이트 방문자 PC를 악성코드에 감염시키는 침해사고 사례는 이미 이전에도 발생하였으나 최근에는 대상 웹 서버를 실제 해킹하지 않고도 정상적인 인터넷 사용자가 특정 웹 사이트로 접속하는 트래픽을 가로채어 변조함으로써 인터넷 이용자의 PC를 악성코드에 감염시키는 이른바 ARP 스푸핑을 이용한 악성코드 유포사례가 새롭게 출현하였다. 이러한 ARP 스푸핑 기법은 계속적 증가할 것으로 예측된다.

IV. 주요 사이버테러 사례

세계는 소련과 미국의 대결구도를 중심으로한 양극체제에서 사회주의권의 몰락 이후 미국이 주도하는 단극체제를 벗어나 군사력, 경제력, 에너지, 자원, 식량, 기술력 등을 바탕으로 한 다극화체제로 전환 중에 있으며, 다극화체제에서는 안정적인 에너지·자원의 확보 및 보호가 국가적인 주요 관심사로 부각되며 이 과정에서 국가간 우발사태가 발생될 수 있을 것으로 예상하고 있다[1].

국가간 혹은 정치·경제 세력간 우발사태는 사이버테러 형태로 표출될 수 있으며 정보기술을 바탕으로 한 경제·에너지·교통 기반시설이 전략적 공격 목표로 인식되고 있다. 특히, 물리적 전쟁수행 보다는 경제, 에너지, 교통 기반시설에 대한 사이버 공격 및 마비가 물리적 전쟁수행 보다 비용 및 파급효과 측면에서 더욱 효과적임에 따라 세계 각국은 사이버 역량 확보에 집중하고 있는 실정이다[2].

사이버테러는 다양한 사이버 공격 기법을 활용하여 사회기반시설 기능 마비, 주요정보 절취·변경·파괴, 국론분열 및 심리적 소요야기 등 전방위적으로 수행 가능하며, 공격 대상 '정찰', 공격 수행을 위한 '거점 확보', 주요 목표에 대한 '공격 수행' 단계로 구성되어 전쟁발발 여부에 관계없이 수행되고 있다.

국내외에서 발생한 주요 사이버테러에 대한 사례를 다음 <표 1>과 같이 살펴볼 수 있다.

1) 美 대통령과 정책입안자들에게 세계 경영과 외교정책에 관련된 정보를 제공하는 미국 국가정보위원회(NIC: National Intelligence Council)의 2008년 11월 20일 발간 보고서 '글로벌 트랜드 2025'中.

2) i) 미국, 영국, 중국, 독일 등 120여개 국가에서 사이버공격 도구를 개발 중, 2007년 사이버범죄 보고서, 美 McAfee社; ii) 북한은 한국과 미국에 대한 첩보수집과 사이버전 수행 전담부대인 '기술정찰조'를 확대 편성 시행 중, 매일경제, 20009년 5월 5일.

<표 1> 국내외 주요 사이버테러 사례

구분	사 례	내 용
국내 사례	군사자료 유출 시도 포착 (2008.01)	군 대상 해킹 코드 첨부 이메일 발송으로 군사자료 유출 시도
	개인정보 유출 (2008.02)	A社 회원 1081만명의 개인정보가 해킹사고로 유출
	대통령 방문일정 제하 이메일 해킹 (2008.03)	'이명박 방문일정'이라는 메일제목으로 악성파일이 첨부된 이메일을 공공기관에 발송 '대통령 출국일정'이라는 제목의 악성코드가 내포된 문서파일을 첨부
	청와대 해킹 (2008.04)	직원 PC의 웜·바이러스 감염으로 인한 해킹으로 '국가안전보장회의' 주요자료 제3국 유출
	예금 불법 인출 (2009.02)	H은행 인터넷 뱅킹 해킹사고로 고객 계좌에서 예금 불법 인출
	내부자료 유출 (2009.04)	A 정부부처 직원을 상대로 악성 이메일 배포 및 내부자료 유출
	7.7 DDoS 대란 (2009.07)	국내 주요 포탈, 정부부처, 금융기관 등을 대상으로 DDoS 공격이 발생하여 일시적으로 서비스 마비
해외 사례	일본, 자위대 이지스함 군사기밀 유출 (2007.04)	이지스함 레이더 정보, 탑재무기 성능 등에 관한 군사기밀의 중국유출 추정, 일본은 미국에 공식사과 및 재발방지 약속
	독일, 총리실 외무부 등 전산망 해킹 (2007.05)	독일 시사주간지 슈피겔이 중국 해커가 스파이 프로그램을 이용, 정부 주요 부처 컴퓨터에 침투했다며 중국군대 소속 해커에 의한 것으로 파악 보도
	러시아, 에스토니아 사이버테러 (2007.06)	에스토니아 수도 '탈린'에 있던 구 소련군 동상 철거되자, 러시아해커는 대통령궁, 정부부처, 금융기관 등을 대상으로 대규모 사이버테러를 감행, 2개월간 행정업무 마비 등 국가적 혼란 야기
	뉴질랜드, 정부 해킹 (2007.09)	뉴질랜드 정부 부처 웹사이트들이 공격을 당하고 정보자료들이 유출
	프랑스, 총리실 해킹 (2007.09)	프랑스 정부 전산망이 중국 해커에게 공격 당한 흔적을 확인
	중국-대만간 해커 전쟁 (2007.11)	중국 정보기관인 국가안전부가 대만 군사정보국 소속 첩보요원에 대해 공개 수배령 발령
	중국-대만간 해커 전쟁 (2007.11)	중국 정보기관인 국가안전부가 대만 군사정보국 소속 첩보요원에 대해 공개 수배령 발령
	그루지아-러시아 사이버전 (2008.08)	'남 오세티아'를 둘러싼 영토분쟁으로 무력충돌 발생시 그루지아 주요 정부 인터넷 사이트가 수차례 무차별 DDoS 공격을 당해 정부기관 사이트가 초토화됨
	미국, 국방부 전산망 해킹 (2008.11)	미 국방부 컴퓨터망이 대대적인 사이버공격 당함
	미국, 차세대 전투기 F-35 설계 해킹 (2009.04)	사이버스파이들이 미 국방부 연구개발망에 침투해 3000억달러의 개발비가 투입된 통합전투공격기 F-35의 설계와 전자시스템 관련 정보들을 대규모로 빼내감
	미국, 의료정보 해킹 (2009.05)	해커가 버지니아주 보건국 데이터베이스를 해킹, 8백만명 환자 의료정보에 대한 대가로 1,000만달러 금품 요구

V. 사이버테러 대응 체계

우리나라의 사이버테러에 대한 대응 체계는 정보통신기반보호체계, 사이버안전관리체계, 재난 및 안전관리체계 및 정보통신망 보호체계로 구분하여 고려할 수 있다. 어떤 면에서 보면 4가지 체계가 혼재하여 상당한 혼란을 유발할 것 같지만, 4가지 체계가 나름의 질서를 가지고 체계가 운영·유지되고 있다. 4가지 체계 모두 사이버테러를 예방하고 관리하기 위한 방안을 제시하고 있으며, 재난 및 안전관리기본법을 제외하고 나머지 체계도 사이버 재난관리 체계를 유지하고 있다. 그러나, 재난관리 측면보다는 사고 발생 후 사고수습에 중점을 두고 있다.

1. 사이버테러 예방 및 재난관리 현황분석

전술한 바와 같이 우리나라 사이버테러 대응 체계는 크게 4가지로 분류할 수 있다. 정보통신기반보호체계, 사이버안전관리체계 및 정보통신망 보호체계 및 재난 및 안전관리체계이다. 각각을 위하여 정부는 정보통신기반보호법, 사이버안전관리규정, 정보통신망 이용촉진 및 정보보호에 관한 법률, 재난 및 안전관리 기본법을 제정하여 시행중에 있다.

1) 정보통신기반보호체계

국방, 통신, 금융 등 주요 사회기반의 정보통신시스템에 대한 의존도가 심화되고 전 세계가 인터넷으로 연결됨에 따라 해킹, 컴퓨터 바이러스 유포 등 사이버 침해행위가 국가기반에 대한 새로운 위협요소로 대두되었다. 이에 대응하기 위해 국가차원의 대책 수립이 필요하게 되었고, 정부는 주요정보통신기반시설의 보호를 위하여 2001년 「정보통신기반보호법」을 제정하여 국가 사회적으로 중요한 정보통신기반시설을 중점관리대상으로 지정하고 지정된 기반시설의 관리기관으로 하여금 취약점 분석·평가를 수행하여 이를 토대로 효과적인 정보보호대책을 수립하여 이행하도록 하

였다.

정보통신기반시설이란 국가안전보장, 행정, 국방, 치안, 금융, 통신, 운송 및 에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 규정에 의한 정보통신망을 의미한다.

정보통신기반시설중 다음을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정하여 관리하고 있으며, 2007년 12월 기준 101개 시설이 지정되어 중앙행정기관으로부터 집중 관리되고 있다.

o 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

o 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도

o 다른 정보통신기반시설과의 상호연계성

o 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위

o 침해사고의 발생가능성 또는 그 복구의 용이성

주요 정보통신기반시설 보호를 위한 추진체계를 보다 자세히 살펴보면 다음과 같다. 주요정보통신기반시설에 대한 보호계획을 국가차원에서 효율적으로 조정하기 위해 국무총리실장을 위원장으로 하고 관계부처의 차관급 공무원을 위원으로 하는 정보통신기반보호위원회를 구성하여, 범정부적 차원에서 주요 정보통신기반시설 지정 및 보호계획을 심의·결정하도록 하였다. 동 위원회는 주요정보통신기반시설의 지정 및 취소, 주요 정보통신기반시설 보호계획의 조정, 주요 정보통신기반시설 보호와 관련된 제도의 개선 및 주요정책사항 및 보호계획의 추진실적 등을 심의하는 기능을 수행한다. 정보통신기반보호위원회의 효율적인 운영을 위하여 정보통신기반보호실무위원회가 설치되었으며, 공공분야와 민간분야 실무위원회를 분리운영토록 하였다. 동 실무위원회는 정보통신기반보호위원회에 제출된 안건과 정보통신기반보호위원회로부터 위임되거나, 정보통신기반보호위원회의 위원장으로부터 지시받은 사항을 검토·심의하여 정보통신기반보호위원회의 효율적인 운영을 보조하는 역할을 수행한다. 날로 더해가는 지능화된 사이버 침해 위협에 주요정보통신기반시설을 신속하고 효과적으로 보호하기 위하여 행정안전부장관과 국가정보원장이 주요정보통신기반시설로 지정할 필요가 있는 시설을 발굴하여 중앙행정기관에 기반시설로 지정토록 권고할 수 있는 근거를 마련하였다. 그리고 보호대책에 대한 사후관리체계 마련을 위하여, 행정안전부장관과 국가정보원장은 보호대책에 대한 이행여부를 확인할 수 있도록 하였다. 아울러, 보호지원을 요청할 수 있는 관리기관 및 지원사항의 범위를 확대하여, 전문기관 등에 기술적 지원을 요청할 수 있는 관리기관의 범위를 국가기관 또는 지방자치단체의 장인 관리기관에서 모든 관리기관으로 확대하였다. 이와 같은 개정을 통해 주요 정보통신기반시설 지정이 활성화되고, 공공 및 민간분야로 이원화된 정보통신기반보호실무위원회에 의해 좀 더 효율적인 주요정보통신기반시설의 관리가 이루어질 것으로 예상된다.

정보통신기반보호법은 사이버 재난관리 측면에서 대규모 사이버 침해사고가 발생했을 시, 침해사고대책본부를 설치·운영할 수 있도록 규정하고 있다. 침해사고대책본부는 주요정보통신기반시설에 대한 중대한 침해사고가 광범위하게 발생한 경우에 응급대책, 기술지원 및 피해복구 등을 수행하기 위하여 한시적으로 운영한다. 주요정보통신기반시설의 보호를 위한 지원기관으로 국가정보원, 행정안전부, 기무사는 주요 정보통신기반시설 보호대책의 수립 및 침해사고 예방·복구 등에 대한 기술적 지원을 수행하고 검찰과 경찰은 범죄수사 업무를 지원한다.

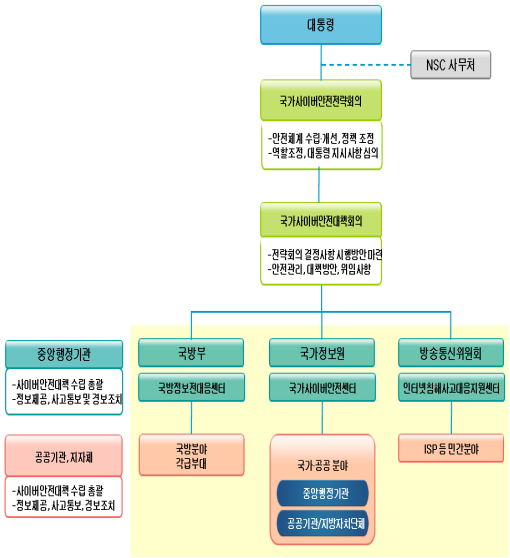
2) 국가 사이버안전관리체계

사이버안전이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기

밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다. 정부는 사이버안전 분야의 중요성이 높아짐에 따라 「국가사이버안전관리규정」을 제정하여 국가정보원이 국가 사이버안전과 관련된 정책 및 관리를 총괄·조정하도록 하는 등 범국가적 사이버안전 관리체계를 확립하였다. 국가 사이버안전에 관한 중요사항을 심의하기 위한 '국가사이버안전전략회의' 및 전략회의를 지원하기 위한 '국가사이버안전대책회의'를 설치하는 한편 행정안전부, 국가정보원, 국방부가 각기 민·관·군 영역에 대한 사이버 안전 업무를 담당하도록 하였다. 국가정보원은 국가사이버안전센터를 설치하여 국가차원에서 사이버공격에 대한 종합적이고 체계적인 대응을 수행하고, 국방부는 산하 국방정보전대응센터를 통해 국방 분야의 사이버안전 업무를 수행하며 행정안전부는 한국정보보호진흥원에 설치된 인터넷침해사고대응지원센터를 통해 민간분야의 사이버안전 업무를 수행한다.

사이버안전관리체계는 정보통신기반보호법과 충돌을 방지하기 위하여 동법에 의하여 지정된 주요정보통신기반시설을 제외한 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 적용된다. 사이버안전정책 및 관리는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정하도록 규정하였으며, 국가적으로 수립된 사이버안전대책의 수립, 시행 및 지도감독은 중앙행정기관의 장이 수행하도록 규정하였으며, 국정원장은 사이버안전대책의 이행여부 등 정보통신망에 대한 안전성을 확인하도록 명시하였다. 국가정보원장은 사이버 공격의 파급영향, 피해규모 등을 고려하여 "관심·주의·경계·심각" 등 수준별 경보를 발령할 수 있으며, 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우, 국가안전보장회의와 협의하여 "심각" 수준의 경보를 발령할 수 있도록 규정하고 있다. 단, 민간 분야에 대한 경보발령은 행정안전부가 책임지도록 명시하였다.

사이버 공격을 인지한 경우, 공공기관이나 지자체는 관계 중앙행정기관을 경유하여 국정원에 통보하도록 되어 있으며, 사이버 공격에 대처하기 위하여 국정원은 조치요령을 중앙행정기관에 통하여 통보하도록 규정되어 있다.



<그림 1> 국가 사이버안전관리체계

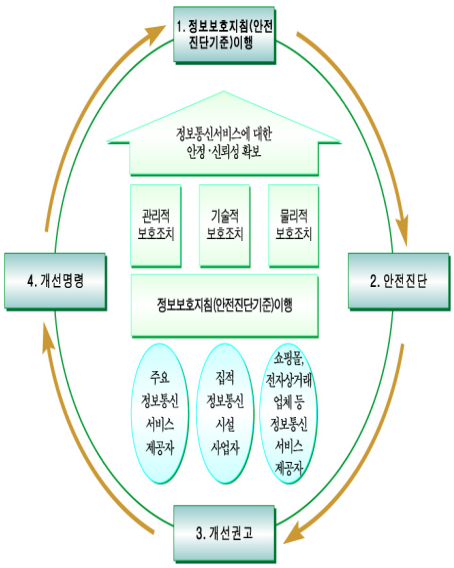
국가사이버안전관리규정은 사이버 재난관리 측면에서 사이버 공격이 발생하였을 경우, 경미사고는 중앙행정기관 또는 공공기관 자체조사 후 결과를 통보하는 형태이나, 심각한 사고일 경우, 관계 중앙행정기관의 장과 협의하여 범정부적 합동조사 및 복구지원팀을 구성·운영하도록 규정하고 있다.

3) 정보통신망 보호체계

우리나라 정보통신망 보호체계는 인터넷 서비스제공자 등 정보통신서비스 제공자의 정보통신망에 대한 사이버 공격을 예방하기 위하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정을 통해 도입된 정보보호 안전진단 제도가 대표적 사례이다. 정보보호 안전진단 제도는 방송통신위원회로부터 지정받은 안전진단 수행기관이 주요정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등 안전진단대

상자가 의무적으로 준수해야 할 정보보호조치 및 이행여부를 매년 확인하는 제도를 말한다.

동 제도를 통하여 안전진단대상 기관은 정보통신망 및 정보통신서비스에 대한 안전성 및 신뢰성을 확보할 수 있으며 서비스 이용자의 만족도를 제고할 수 있다.



<그림 2> 정보보호 안전진단 제도

정보보호관리체계(ISMS: Information Security Management System) 인증제도란 ISO9001(품질경영 시스템)과 같이 품질 보증을 위한 기업 내 일련의 활동에 대한 인증과 유사한 개념으로 정보보호를 위한 기업 내의 일련의 활동(정보보호관리체계)에 대해 객관적인 심사를 거쳐 인증을 취득하는 제도이다. 정보보호관리체계는 정보통신망의 안정성을 확보하고 조직의 정보자산을 보호하기 위해 기술, 관리, 물리적 정보보호대책을 구현하여 지속적으로 관리·운영하는 시스템으로 전사적으로 균형잡힌 정보보호활동을 할 수 있는 기틀을 재공해 준다. 특히, 핵심 산업기술과 고객의 개인정보(금융정보, 의료정보, 학사정보 등)를 취급하고 있는 기업에서는 정보보호관리체계 수립을 통하여 이러한 정보를 효과적으로 보호할 수 체계 마련이 가능하다.

우리나라는 2001년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 개정하여 정보보호관리체계 인증제도를 도입하였다. 도입배경중 중요한 요소는 국외 인증기관이 국내 주요기반시설을 대상으로 인증심사를 하여 발생할 수 있는 정보 유출을 방지하는 데 있다. 현재 정보보호관리체계 인증을 위한 세부 심사기준 및 업무지침 등이 마련되어 정보보호관리체계 인증제도를 본격 시행하고 있으며, 2008년 1월 현재 46건의 인증서가 발급되었다.

4) 재난 및 안전관리체계

우리나라 사이버 재난 및 안전관리체계는 "재난 및 안전관리기본법"에 잘 규정되어 있다. 동 법에서는 에너지, 정보·통신, 교통수송, 금융, 보건·의료, 원자력, 환경, 식용수 등 그 기능이 마비될 경우 인명과 재산 및 국가경제에 심각한 영향을 미칠 수 있는 물적·인적 체계를 국가기반체계로 정의하고 사이버 재난 및 안전관리의 대상으로 규정하였다. 여기서, 국가기반재난이란 국민의 생명·신체 및 재산과 국가에 피해를 주거나 줄 수 있는 것으로서 에너지·통신·교통·금융·의료·수도 등 국가기반체계의 마비와 전염병 확산 등으로 인한 피해를 의미한다(재난 및 안전관리기본법 제3조 제1호 다목).

한편, 국가기반시설이란 국가기반보호체계를 위해 계속적으로 관리할 필요가 있다고 인정되는 시설로 다음과 같은 요건을 만족하는 시설을 의미하며, 2008년 현재 8개분야 260여개 시설이 지정되어 있다.

o 다른 기반시설이나 체계 등에 미치는 연쇄효과

o 둘 이상의 중앙행정기관의 공동대응 필요성

o 재난이 발생하는 경우 국가안전보장과 경제·사회에 미치는 피해규모 및 범위

o 재난의 발생가능성 또는 그 복구의 용이성

국가 기반체계 사이버 위험관리 측면에서 재난 및

안전관리기본법의 가장 큰 의의는 국가기반체계의 마비 등을 자연·인적재난과 함께 "재난"의 범주에 포함하여 국가적으로 관리한다는 사실이다. 참고로 국가기반시설의 지정기준은 다음과 같다.

o 에너지 : 전력·석유·가스공급에 필요한 생산시설과 비축시설

o 정보통신 : 교환기 등 주요통신장비가 집중된 시설, 국가행정을 운영·관리하는데 필요한 기간망과 주요전산시스템

o 교통수송 : 인력수송과 물류기능을 담당하는 체계와 실제 운용하는데 필요한 교통·운송시설

o 금융 : 은행 및 증권사를 운영하는데 필요한 시설이나 체계

o 보건의료 : 응급의료서비스를 제공하는 시설과 이를 지원하는 혈액관리업무를 담당하는 시설

o 원자력 : 원자력시설의 안정적 운영에 필요한 주제어장치가 집중된 시설

o 환경 : 생활폐기물 처리를 위한 수집부터 소각·매립까지 계통상의 시설

o 식용수 : 식용수 공급을 위한 담수부터 정수까지 계통상의 시설

이와 같은, 국가 기반시설에 재난이 발생할 경우, 재난관리는 재난의 정도에 따라 다르다. 통상적 재난의 경우, 주무 중앙행정기관이 책임대응을 하며, 지역재난인 경우에는 해당 지방자치단체가 책임 대응을 한다. 그러나, 대규모 재난 발생 시 주무부처 장 및 지역대책본부장의 건의 또는 중앙본부장의 판단에 의해 중앙재난안전대책본부를 가동하여, 범 정부적 통합지원체계가 운영된다.

참고적으로, 대통령훈령 제124호로 공표된 국가위기관리기본지침에는 국민의 건강, 안전 및 경제적 안위를 확보하고 국가경제 및 정부의 핵심기능에 중대한 영향을 미칠 수 있는 인적, 물적, 기능 체계를 국가 핵심기반이라 정의하고 에너지, 식·용수, 의료·보건, 정보통신(사이버 포함), 금융, 수송, 원자력, 주요 산업단지, 정부 주요시설 등에 대한 위기관리대응 매뉴얼을 제작한 바 있다.

2. 문제점 분석

1) 사이버 테러 및 위기의 특성에 대한 고려가 미흡

최근의 사이버 공격 양상을 살펴보면 전통적인 물리적 위기와 사이버 위기가 분리되어 나타나지 않는다. 미국이 걸프전 당시 토마호크 미사일로 이라크를 공격하기에 앞서 이라크의 방공망을 사이버 무기를 이용하여 파괴한 작전은 두고두고 회자되고 있다. 물리적 공격의 위력을 배가하기 위하여 사이버공격이 선행되는 것은 국가 기반체계가 사이버 공간을 이용하여 상호의존하고 기반체계간 연계성이 높아질수록 자명한 일이다. 물리적 위기대응과 사이버 위기대응의 통합이 반드시 필요하다.

2) 다원화된 사이버테러 대응 및 위기관리 체계

앞서 현황분석에서 살펴본 바와 같이, 동일시설에 대하여 다른 이름으로 관리가 되는 다원화된 사이버테러 대응 및 위기관리 체계가 존재한다. 국가 기반시설(재난 및 안전관리기본법), 주요정보통신기반시설(정보통신기반보호법), 국가·공공기관 정보통신망(국가사이버안전관리규정), 정보통신사업자가 유지하는 정보통신망(정보통신망 이용촉진 및 정보보호 등에 관한 법률) 등 같은 시설이지만 다른 이름으로 각기 다른 기관에서 관리하고 있다. 관리하는 기관입장에서는 분명히 다른 시설이라고 강변할 수 있으나, 국가기반시설과 주요정보통신기반시설은 명백하게 같은 시설이고, 불행하게도 핵심설비인 정보통신망은 국가, 민간을 구분할 것 없이 상호 연계되고 있다. 따라서, 기반시설 및 정보통신망을 관리하는 기관은 중복성을 야기하여 피로도가 높아짐을 호소하고 있는 실정이다. 기반시설을 관리하는 중앙행정기관이 다르므로 실제 위기발생시 위기대처 지침이 없다면 동일명백하에 대

하여 부처별 위기대응지침을 준용하여야 하므로 위기대처에 혼선을 줄 우려가 있다. 유사하게, 사이버테러 및 위기관련 정보수집 및 상황파악에 혼선을 빚을 수도 있으며, 시설관리기관의 업무가 가중되는 것은 명확한 일이다. 아울러, 시설을 보호하기 위한 예산 및 인력의 낭비도 유발된다.

3) 부처 이기주의

무엇보다 우리나라 사이버테러 대응 및 위기관리 체계의 가장 큰 문제점은 부처 이기주의에 의한 중복이다. 우리나라 정부조직법에는 각 부처의 역할이 명확히 명시되어 있다. 그럼에도 불구하고 중앙행정부처별로 부처간 타협, 언론 플레이 등을 등에 업고 무분별하게 사이버 보안 관련 법률을 양산해 왔다. 따라서, 동일시설에 대한 중복규제 등의 문제가 발생하고, 교묘한 선긋기를 통하여 중복체계의 충돌을 피해온 것이 사실이다. 사이버테러 대응 및 위기관리 기능이 국가정보원 및 행정안전부 등 여러 부처로 분산되어 있어 효율적이며 총괄적으로 운영되지 못하고 있다.

사이버테러 대응 및 위기관리 체계의 효율적인 운영을 위해서는 총괄기관을 지정하여 각 중앙행정기관에 소관 기반시설의 사이버테러 대응 및 위기관리 책임을 부여하고 그 이행결과에 대하여 사후 점검하는 형태로 운영하는 것이 바람직하다. 사이버테러 대응 및 위기관리는 어느 한 부처의 독단으로는 절대 수행될 수 없으며, 국가 기반시설을 운영·관리하는 중앙행정기관의 절대적 협조가 필요하기 때문이다.

4) 강력한 정보공유 체계 부재

사이버테러로 인한 위기 상황을 전파하고 효율적으로 대응하기 위하여 반드시 필요한 것이 정보의 공유이다. 그러나, 현재의 정보공유는 지극히 형식적이다. 사이버 공격을 분석할 수 있는 자료를 주고받기 보다는 지극히 형식적인 정보공유가 이루어지고 있다. 사이버테러 사태 판단 및 사이버공격의 징후를 포착하기 위해 사전에 사이버공격 정보를 탐자·전파할 수 있는 체계를 구축하고 그 정보를 사이버테러 대응 및 위기관리 총괄기관에게 제공하여야 한다. 또한 총괄기관에 과도한 정보가 집중되거나 불필요한 정보가 공유 및 유출되지 않을 수 있도록 수집 정보의 종류 및 정보처리 과정 등을 명확히 규정하여야 하며, 국회 등에게 정보공유를 위한 정보 수집 및 활용실태를 보고하여 그 정당성을 검토 받아야 한다.

5) 사이버 위기사태 해결을 위한 물자/인원 동원 방안 부재

사이버 위기사태 해결을 위해서는 관계기관의 사이버 위기대응 정책과 함께 이를 실현할 수 있는 물자 및 인원에 대한 동원을 통해 물리적 대응방안 실시가 필요한 경우가 다수 발생할 것으로 예상된다. 『재난 및 안전관리기본법』에서는 재난 대응을 위해 필요한 물자·자재의 비축, 재난사태 선포시 인력·장비 및 물자의 동원명령 발령을 규정하고 있으나, 사이버 위기에 관해서는 명확한 규정이 존재하지 않는다. 사이버 위기사태 해결을 위해 필요한 물자 및 인원을 동원할 수 있는 근거 마련이 필요하다.

6) 사이버 위기사태 해결을 위한 훈련계획의 부재

실질적 사이버 위기사태 해결을 위해서는 조직의 위기대응 계획 수립과 함께 이의 훈련을 통해 위기대응 방법을 체득하여야 하나, 『재난 및 안전관리기본법』의 경우 재난예방을 위한 재난대비훈련만을 명시하고 있다.

7) 위기대응 계획의 이행여부 점검방안 부재

정부는 국가안전보장회의 사무처 주관으로 각 분야별로 사이버 위기가 발생했을 시, 관계자가 따라 할 수 있는 위기대응 지침을 마련하고 이에 기반하여 각 기관의 위기대응 계획을 수립하나, 지침과 계획의 주

요내용의 이행을 점검할 수 있는 체제를 마련하지 못해 실질적으로 영향력을 갖는 지침이나 계획이 아닌 문서상의 지침이나 계획으로만 존재하게 될 가능성이 있다. 따라서, 각 부처가 수립한 위기대응 계획의 이행여부를 정기적으로 점검하여 계획이 계획으로만 그치지 않도록 하는 것이 바람직하다.

8) 사이버 위기 대처 관련 과학기술 진흥방안 부재

『재난 및 안전관리기본법』에 안전관리에 필요한 과학기술의 진흥, 안전관련산업의 육성 및 지원 등에 대해 규정하고 있으나, 제로데이 공격 일반화, 복합공격 등이 등장함에 따라, 이를 이용한 적성국의 사이버 위기 유발 가능성이 매우 높으므로 평시 사이버공격 무력화 기술 등 사이버 위기관련 연구 개발에 대한 투자가 필요하다. 또한 사이버위기사태 대응 기술 개발 전문기관을 선정·육성하여 관련 전문가 및 기술을 양성하여야 한다.

9) 사이버 위기관리 적용대상 측면의 문제점

우리나라는 현재 국가기반시설, 주요정보통신기반시설로 일부 시설만을 지정하고 있으나, 정보통신망의 연계, 융합 등을 고려 일부 시설이 아닌 기반체계별 접근이 필요하다. 정보통신망의 연계, 기간시설의 상호 의존성으로 인하여 지정되지 않은 시설에 대한 사이버 공격을 통하여 지정된 주요 기반시설에 대한 공격이 가능하고 지정되지 않은 기반시설의 피해는 지정된 시설까지 피해를 미치기 때문이다. 다만, 분야별로 핵심자산을 식별하고, 핵심자산이 필요로 하는 정보보호 특성을 구현하여 위기시 핵심자산에 대한 대응방법에 초점을 맞출 필요가 있다.

VI. 사이버테러 대응 체계 구축을 위한 제언

1) 국가사이버위기관리법 제정

산재해 있는 사이버테러 대응 및 위기관리 관련 법제를 정비하여 국가차원의 사이버 위기를 예방하고 위기발생시 일원화된 종합적인 사이버테러 대응 및 위기관리 체계를 구축하기 위해 조속히 국가사이버위기관리법을 제정할 필요가 있다.

2) 일원화된 사이버 사이버테러 대응 체계 구축

사이버테러로 인한 위험을 저감을 위하여 시급히 필요한 것은 일원화된 사이버테러 대응 체계를 구축하는 것이다. 행정안전부 등 여러 부처로 분산되어 있는 사이버테러 대응 체계를 일원화하는 것이 무엇보다 시급하다. 일원화하는 방법에는 두 가지를 고려할 수 있다.

첫째, 행정부처를 통제할 수 있는 부처에 사이버테러 대응체계를 총괄하도록 기능을 부여하는 것이다. 국가정보원에 총괄기능을 부여하여 각 중앙행정기관 및 하위기관에 대한 사이버테러 대응 및 위기관리 기능을 부여하는 것이다.

o 국가정보원 : 사이버테러 대응 총괄

o 행정안전부 : 개인정보보호를 포함한 전자정부 분야 사이버테러 대응 담당

o 방송통신위원회 : 방송 및 통신분야 사이버테러 대응 담당

o 금융위원회 : 금융 및 증권분야 사이버테러 대응 담당

o 국토해양부 : 수송(교통), 수자원 및 댐 분야 사이버테러 대응 담당

o 보건복지가족부 : 의료체계 사이버테러 대응 담당

둘째, 여러 가지 법률에 산재되어 있는 사이버테러 대응관련 법제를 통합한다. 이미 정보보호 관련 법제의 통합은 많이 거론되고 있으나, 부처 이기주의식 통합을 벗어나지 못하고 있는 상태이다. 과감하게 부처 이기주의를 청산하고 정부조직법상 기능에 맞게 사이

버테러 대응 기능을 단일화할 필요가 있다. 이미 신정부 출범시 정보보호 관련기능을 통합하려 했으나, 여러 가지 이유로 여러 부처로 그 기능이 분산되어 통합의 시너지를 내지 못하고 있다. 따라서, 사이버테러 대응 관련 법제를 통합하여야 한다.

두 가지 방안 모두 현재 여러 법률에 중복되는 요소는 반드시 제거하여야 한다.

3) 사이버테러 정보 수집·전파체계 구축

사이버테러 위험은 위험이 발현되는 속도가 빠를 수도 늦을 수도 있다. 1.25 인터넷 대란의 주범인 슬래머웜의 경우, 불과 10분 만에 전세계로 확산되었고 최근 많이 나타나고 있는 IRC 봇 공격은 탐지되지 않는다면 수개월 혹은 수년 동안에 걸쳐 사이버 공격을 하며 중요문서 등을 유출한다. 따라서 사이버 위험의 경우 위험요소를 수집하고 징후를 탐지하며, 징후가 발현되었을 시 즉각적인 대응이 무엇보다 중요하다. 현재 국가정보원, 지식경제부, 교육과학기술부, 국토해양부, 행정안전부 등이 사이버테러 정보 수집·전파체계를 구축·운영하고 있으나, 국가정보원을 제외하고는 그 수준이 낮은 상황이다. 사이버테러 정보 수집·전파체계를 고도화함과 동시에 저변을 확대하는 것이 중요하다. 기반체계를 관리·운영하는 기관은 반드시 사이버테러 정보 수집·전파체계를 구축하여야 한다. 이와 더불어, 국가적 차원에서 사이버테러 정보를 탐지하고 대응하기 위해서는 기반체계에 대한 사이버테러 정보 수집·전파체계 간의 공조가 필수적이며, 정보공유도 필수적 요구사항이다.

사이버테러 정보 수집·전파체계는 계층구조를 갖도록 설계하여 최상위 계층에서는 국가차원의 사이버 위기 징후 탐지 및 대응이 가능하도록 하여야 한다. 또한, 사이버테러 정보 수집·전파체계에는 단계별 위기 경보와 발령체계 유지가 필요하다.

4) 사이버 위기관리를 위한 구체적 국가계획 수립 시행 및 평가체계 구축

사이버 위기를 관리하기 위하여 기반체계 각 분야별로 사이버 위기 예방, 탐지, 대응, 복구 사이클을 갖는 분야별 보호계획을 수립하여야 한다. 분야별 보호계획의 실행력을 담보하기 위하여 보호계획 이행에 대한 평가체계를 구축하여 평가결과를 성과평가에 반드시 반영하여야 한다. 또한 예산과 연계하여 평가결과가 좋지 않은 기관은 정보화 예산보다 정보보호 예산을 더 배정하도록 행정지도를 하여야 한다. 계획의 수립, 실천, 평가, 평가결과 반영의 사이클이 제대로 운영되어야 사이버 위기관리 능력이 향상 될 것이다. 국정원은 보호계획 수립지침을 작성하여 배포하고, 각 기관이 작성한 보호계획을 종합·조정하여 국가차원의 보호계획을 수립하여야 한다.

5) 위험관리 기반 국가 기반시설 보호 프로그램

기반시설을 보호하기 위한 보호 노력은 투자대비 효과를 고려하여야 한다. 이를 위하여 반드시 위험관리에 기반한 기반시설 보호 노력을 진행하여야 한다. 불행하게도 우리나라는 아직도 기반시설 보호를 위한 위험분석 방법론을 가지고 있지 못한 실정이다. 보안목표 설정, 핵심자산 식별, 위험평가, 보호 우선순위 결정, 보호 프로그램 실행, 효과 측정의 루프를 가진 위험분석 방법을 시급히 개발하여 적용하여야 한다.

6) 민·관 협력모델 설정

국가 기반시설의 많은 부분을 이미 민간이 소유하고 있거나 민간에 이양될 계획이다. 따라서, 기반시설 소유주가 민간인 경우 민간과 협력체계 구축이 무엇보다 중요하다. 법률에 의하여 민간 기반시설 소유주를 규제하여도 좋지만 가장 좋은 방법은 기반시설 보호를 위한 모범사례를 정부에서 개발하고 이를 민간이 따르도록 유도하는 것이다. 이를 위하여 분야별 민관 기반시설 보호협의체 결성이 필요하다. 동 협의체를 통하여 민간과 정책 협의, 보호대책 구현 방안 논

의, 정부의 기반시설 보호정책 홍보 등이 자연스럽게 수반되어 정부의 보호 프로그램 구현 모범사례 등이 민간으로 자연스럽게 이관되어 국가 전체의 기반시설 보호수준 제고가 가능해진다.

7) 교육, 훈련 및 예행연습 실시

국가 기반시설 보호를 위하여 무엇보다 중요한 것은 교육, 훈련 및 사이버테러에 대처하기 위한 예행연습이다. 기반구조 보호를 담당하는 구성원의 수준이 다양할 경우, 보호 프로그램의 수준을 정하기가 매우 어려울 것이다. 실질적인 교육과 실전같은 훈련은 이와 같은 불안감을 해소하는데 매우 도움이 된다. 기반시설 보호 담당자, 운영자, 관리자를 대상으로 초급, 중급, 고급 등 다양한 교육 코스와 훈련 코스를 개발하여 활용하여야 한다. 또한 을지훈련, 미국의 사이버스톰(Cyber Storm)과 같이 전 부처와 기반시설 관리기관이 참여하는 위기대응 연습을 매년 실시하여 사이버 위험이 발현되었을 시 신속하게 대처할 수 있는 능력을 배양하여야 하며, 국정원 등 관계기관에서는 사이버테러 및 위기 대응 예행연습 프로그램을 지속적으로 개발하여야 한다.

8) 사이버테러 대응 연구개발

사이버 위험을 관리하기 위한 위험분석 도구 개발이 가장 시급하며, 이와 관련하여 식별한 핵심자산을 보관하기 위한 국가적 DB를 구축하고 비인가자의 접근을 제어하는 접근통제 기술 및 DB 데이터를 보호하기 위한 암호화 기술 개발이 필요하다. 핵심자산의 상호의존도 및 연계성을 파악하기 위한 시뮬레이션 기술개발이 필요하며, 사이버테러 정보 수집·전파체계 기능 고도화를 위하여, 고속 분석 및 상황판단 기술, Secure 정보공유 기술, 사이버위기 예측모델 개발 등이 필요하다. 사이버테러 대응을 위한 가장 난이도가 높은 기술로 사이버 위험 감내 기술이 있으며, 자주적 사이버테러 및 위기 대응기술 확보를 위하여 네트워크 분리 및 재구성 기술, 침입감내 네트워크 기술 개발이 필요하다.

최근 들어 사이버 공격의 대상이 되고 있으며, 그 피해의 확산 규모가 어마어마한 제어시스템에 대한 보안기술개발도 시급한 연구개발 과제이다.

8) 국제공조

국가 기반시설은 국내뿐 아니라 국외와도 연계된다. 또한 국내의 기반시설에 대한 외국으로부터의 사이버 공격에 대한 대응은 국내 독자적이 아닌 외국과 협력하여 수행되어야 하며, 치외법권 지역에서 발현된 사이버 공격에 대한 처벌 역시 외국과 긴밀한 공조가 필요하다. 이미 여러 분야에서 상당한 수준까지 공조가 이루어지고 있어, 현재의 공조체계를 잘 발전시켜 나가면 될 것으로 판단된다. 그러나 아쉬운 것은 사이버 공격 대응 연구분야에 대한 국제공조체계가 미흡한 점이다. 사이버테러 및 위기 대응분야에서 첨단기술을 보유하고 있는 미국 등 주요국의 연구소 및 학계와 과감한 공동연구를 수행할 때라 판단된다.

<참고문헌>

▷ 곽정호. 2005. 방송의 보편적 서비스제도 도입방안 분석. 정보통신정책. 17(1): 1-37.
▷ 국가사이버안전관리규정[2008. 8. 18. 대통령훈령 제222호].
▷ 국가정보원·방송통신위원회·행정안전부·지식경제부. 2009. 2009 국가정보보호백서.
▷ 이재은. 2004. 재난관리와 국가핵심기반 보호체계 구축방안. 한국정책논집. 4: 77-90.
▷ 재난 및 안전관리기본법[2006. 2. 21. 법률 제7849호].
▷ 정보통신기반보호법[2008. 6. 22. 법률 제8852호].
▷ 정보통신망이용촉진및정보보호등에관한법률[2008. 6. 13. 법률 제9119호].
▷ 정보통신부. 2007. 한국, 디지털기회지수(DOI) 3년 연속 세계 1위. RAD19-0705437 보도자료. 2007. 5. 17.
▷ 한국정보사회진흥원. 2009. 2009 WEF 네트워크 준비지수 발표 결과.
▷ 한국정보화진흥원. 2009. 2009 국가정보화백서.

李哲源: 아주대학교에서 정보보호 전공으로 공학박사를 취득하고,

한국전자통신연구원 선임연구원과 한국정보보호진흥원 과제책임자를 거쳐 현재 ETRI 부설연구소 본부장으로 재직중이다 (cheolee@ensec.re.kr).

裵秉哲: 충남대학교 대학원에서 박사과정을 수료(컴퓨터 통신 및 보안 전공)하고, 국방정보체계연구소 연구원과 국방과학연구소 연구원을 역임하였다. 현재는 ETRI 부설연구소 과제책임자로 재직중이다 (bcbae@ensec.re.kr).

접수번호: #091130-02
접수일자: 2009. 11. 30.
심사완료: 2008. 12. 23.