情 報 保 護 學 會 誌
第 12 券 第 6 號, 2002. 12

주요국 정보전 대응체계와 동향

이 철 원*, 장 병 화*, 이 철 수**

요 약

정보전의 개념이 도입된 90년대 중반이후 세계 각 국에서는 사이버 공간을 이용한 다양한 사이버 위협을 대처하기 위한 많은 노력을 기울이고 있다. 그러나, 9·11 테러를 겪으면서 미국을 비롯한 각 국에서는 사이버공간을 이용한 사이버테러 및 사이버전이 국가안위를 위태롭게 할 수 있다는 인식하에 기존 보안정책을 강화하거나 새로운 보안정책을 계획하거나 시행하고 있다. 본 논문에서는 미국, 일본 등을 중심으로 한 사이버 공간의 안전성 확보를 위한 최근의 노력을 소개하고자 하며, 우리나라의 사이버 공간 안전성 확보를 위한 참고자료로 활용되었으면 한다.

Ⅰ. 서 론

최근 십여 년 동안, 우리 나라는 커다란 변화를 경험하였다. 전자정부 구현 등 국가사회 전 부분에 걸친 정보 혁명으로 인하여 사이버공간은 우리 일상의 생활공간이 되었으며, 경제활동, 국가방위 및 일상 생활이 점점 더 사이버공간에 의존되어 가고 있다. 정보화가 추진되어감에 따라 이전과 다른 새로운 산업이 다양하게 창출되었으며, 국가의 부(富)를 증대시키는 새로운 방안으로 정보산업에 대한 인식이 전환되었다. 그러나, 컴퓨터관련 기술은 인류에게 창조에 대한 무한한 가능성을 제공하는 반면, 사이버공간을 이용한 초상권 침해 등과 같은 개인의 프라이버시 침해, 사회적 혼란을 야기하는 사이버테러 및 국가안위를 위태롭게 하는 사이버전에 이르기까지 개인의 프라이버시, 사회 안녕 및 국가의 안전에 대한 새로운 위협을 가중시키고 있다. 그럼에도 불구하고 많은 사람들은 정보기술(IT)이 과거의 인습에서 벗어나 새로운 번영의 시대를 건설할 수 있는 기회를 계속해서 열어줄 것이라고 믿고 있다. 그러나, 전술하다시피 이 새로운 시대를 열어가는 핵심시스템인 컴퓨터에는 많은 위협이 존재하고 있다. 전화를 하거나, 은행에서 돈을 송금하거나, 비행기를 탈 때에도 하나 이상의 정교한 컴퓨터 시스템이 운영하는 제어시스템에 의존하고 있다. 국가의 안전보장을 위한 국방시스템 또한 컴퓨터에 의해 제어되는 전력, 통신, 운송 등의 기반시설에 깊이 의존하고 있다. 컴퓨터에 의하여 제어되는 이 모든 시스템은 침입과 파괴에 취약하며, 핵심 경제분야와 정부기관 일부의 컴퓨터에 이러한 침입이 발생할 경우, 우리는 상상하기 어려운 피해를 입을 것이다.

국방, 통신, 금융, 운송, 전력, 정부서비스 등 국가사회를 운영하고 유지하기 위한 핵심시스템에 대한 물리적 및 사이버 위협은 실제로 존재하고 있으며, 향후 국가의 위기상황 또는 타국과의 분쟁 시 종래의 재래식 무기를 이용한 대규모 인명살상보다는 컴퓨터에 의해 통제되는 주요 기반구조를 대상으로 공격이 집중될 것으로 예상된다.

"핵심 기능의 어떠한 중단이나 조작은 단순하고, 드물며, 처리하기 쉽고, 지리적으로 고립되며, 미국의 복지에 미비하게 해를 입히는 것이어야 한다"라고 클린턴 대통령이 보안명령 63호(Presidential Decision Directive 63)에서 지적한 바와 같이, 미국을 비롯한 호주, 일본, 영국, 캐나다 등에서는 자국의 주요 기반구조를 보호하기 위한 노력을 범국가적 차원에서 추진하고 있다[1].

이러한 노력에도 불구하고, 지난 2001년 9월 11일 미국 뉴욕의 세계무역센터와 워싱턴 D.C.의 펜타곤에서 발생한 테러사태는 수 천명의 사망자가 발생하는, 진주만 사태 이후 미국에서 발생한 다시없

* 국가보안기술연구소 ({cheolee, bhchangx}@etri.re.kr)
** 한국정보통신대학원대학교 초빙교수(csl100@icu.ac.kr)

는 재앙의 하나로 기록되고 있다. 이번 사태는 미국의 정보력과 첨단기술에 대한 자신감을 일순간에 무력화시키는 계기가 되었으며, 미국 방위에 대한 경각심을 불러일으키는 일이었다. 9.11테러 1주일후 발생한 NIMDA 공격은 9.11테러와 같은 물리적 테러가 사이버 공간을 통해서도 발생할 수 있다는 사실을 증명시켜준 컴퓨터와 네트워크 기술에 의존적인 국가에게는 경종을 울려준 사건이었다.

NIMDA는 자동화된 사이버 공격으로서 컴퓨터 웜과 컴퓨터 바이러스를 혼합한 것이다. NIMDA는 엄청난 속도로 전세계로 전파되었으며, 침입한 컴퓨터 시스템을 여러 가지 방법으로 감염시켜 파일을 파괴하고자 하였다. 그것은 한 시간 내에 전국적으로 확산되어 몇 일간 지속되었으며, 86,000대의 컴퓨터를 공격하였다. NIMDA는 회사들이 온라인 접속을 하지 못하게 하고, 고객의 액세스를 차단하고, 어떤 회사들은 시스템을 전면적으로 재구축 하게 하는 등, 잘 보호되고 있었던 산업에 상당한 문제를 야기하였다. NIMDA 공격에 따른 실제 재정적 손실은 이러한 손실을 측정하는 일관된 방법이 없기 때문에 밝혀지지 않았다. 그러나, 업계 자료에 따르면 악의적인 코드로 인한 사이버 공격의 전체적인 재정적 영향은 2001년에만 130억 달러에 달할 것으로 추정된다[2].

NIMDA가 있기 두 달 전에는 Code Red라 불리는 사이버 공격으로 인해 불가 14시간 만에 150,000대의 컴퓨터 시스템이 감염되어 수십억 달러의 손실을 초래하였다. 그러한 공격은 사이버 공격의 정교함과 파괴력이 높아지고 있다는 것을 보여준다. 공격 빈도 역시 증대하였다. 카네기 멜론 대학교의 컴퓨터 긴급대응팀[CERT]의 조정 센터는 1998년에 3,700건의 공격을 보고하였으며, 현재 추세대로라면 2002년에는 110,000건이 될 것으로 예상하고 있다[3]. 국내의 경우 국가정보원이 발표한 바에 의하면, 2001년 국가·공공기관 해킹사고 발생건수는 507건으로 2000년대비 497%증가한 것으로 보고된 바 있다[4].

최근 발생한 일련의 사건을 통하여 미국, 일본 등 정보기술 강국에서는 자국의 사이버공간을 보호하기 위한 부단한 노력을 경주하고 있다. 본 논문에서는 사이버테러를 대응하기 위한 미국, 일본 등 주요국의 정책변화를 고찰하고자 한다. 최근 발표된 사이버공간 보안 국가전략, 미국 본토안보부 설립 배경 및 일본에서 2001년 10월 2일 발표한 「'사이버테러 특별행동계획'에 대한 후속조치」를 통한 행정부 및 전력·교통 등 중요 인프라의 사이버테러 대응 연락·협력체계 구축에 대하여 고찰한다. 특히 9.11 테러이후 변화된 미국의 사이버테러 대응 정책 변화를 집중 조명하고자 한다. 이를 통하여 국내 범 국가적 사이버테러 대응 정책 정립에 조그마한 도움을 주고자 한다.

II. 정보전의 개념 및 위협

1992년 미 국방부가 발표한 DoD Directive TS3600.1에서 정보전이란 용어를 처음 사용하면서 일반에 알려진 정보전은 현재 널리 사용되고 있는 용어이지만, 관점에 따라 정의가 약간씩 차이가 나며 또한 전쟁의 개념으로 군사적 차원과 민간차원에서 보는 시각에 따라 약간씩 다르다. Thomas Rona는 초기의 정보전의 개념을 "평시, 위기시, 경계시, 분쟁발생시, 전시, 전쟁 종료시, 복구시에 정보기술(수단)을 이용한 모든 전략/전술과 작전"이라고 포괄적으로 정의하였으며[5], Winn Schwartau는 정보전의 개념을 "컴퓨터 네트워크에 대한 공격"으로 협의로 정의하였다[6]. 또한 미 합참은 "정보우위를 달성하기 위하여 아군의 정보, 정보 프로세스, 정보시스템, 컴퓨터 네트워크를 보호하고, 적군의 정보, 정보 프로세스, 정보시스템, 컴퓨터 네트워크를 공격하는 일체의 행위"라 정의하였다[7].

모두가 새로운 사이버 위협에 대한 견해에는 일치하지만 Winn Schwartau는 정치·경제·사회적 차원에서 설명을 하고 있으며, Thomas Rona와 미 합참은 군사적 차원에서 정의를 내리고 있다. 엘빈 토플러는 그의 저서 War and Anti-War에서 "제 3의 물결 정보시대에서 전쟁은 대량파괴가 아닌 중요 데이터를 지우거나 손상시켜 적에게 피해를 가하는 정보전으로 변천하고 있으며, 정보전은 인명피해를 최소화시키면서 목적을 달성할 수 있다는 것이 특징이다[8]"라고 하였듯이 정보전은 과거의 전쟁개념과는 달리 물리적인 파괴가 아닌 국가의 신경조직인 정보통신망, 주요기반구조의 컴퓨터 등을 파괴 또는 무력화시켜 목적을 달성하는 새로운 개념의 전쟁으로 볼 수 있다.

이와 같은 정보전의 개념은 1996년 12월 미 국방차관 White가 미 국방부 지침 S-3600.1 정보작전(DoD Directive S-3600.1, Information Operations)에 서명함으로써, 기존의 정보전에 대한 미

국방부의 인식을 갱신하면서 변화를 갖게 된다[9].

정보작전은 국방부 단독으로 사이버공간을 통한 국가의 안전을 위협하는 사이버위협을 대처할 수 없음을 인식하고 국방부, 연방정부부처, 공공기관 및 산업체와의 협력체제를 강화시켜 주는 기틀을 제공하기 위한 것이다. 이와 같은 정책 변경의 내면에는 미국의 국가방위가 IT 기술을 기반으로 하는 국가의 주요 기반구조에 의존한다는 사실에 기인하며, 해킹, 사이버테러 등 주요 기반구조 침해위협을 방지하기 위해서는 주요 기반구조를 소유·운영 및 관리하는 국방부를 비롯한 연방정부, 공공기관 및 산업체의 보호노력을 통합하고 조정하는데 그 성공의 열쇠가 있다고 인식한 결과이다. 정보작전에서의 정보전은 전시 혹은 위기시에 적국에 대하여 특별한 목적을 달성하기 위하여 행하는 행위로 국한하였으며 평시 준비태세를 위하여 "정보보증"이라는 개념을 도입하고 연방부처 및 민간기관과의 상호 협력을 강조하였다. 우리나라에서는 아직도 정보전, 사이버전 및 사이버테러가 같이 혼용되고 있으므로 본 논문에서도 세가지 용어를 같은 의미로 혼용하겠다.

정보전은 정보 공간(Information Space) 혹은 사이버공간에서 일어나는 새로운 개념의 전쟁으로 다음과 같은 특징을 갖는다.

- ○ 범행의 광역화·익명성: 정보전 대상에 접근해야 할 필요가 없고 통신망(전화선)이 깔려 있는 곳이면 지구촌 어디에서나 공격이 가능하며 통신망 전체를 차단하지 않는 한 예방이 어렵고, 증거를 남기지 않아 공격자와 공격장소 추적이 곤란하다.
- ○ 사건예측 불가: 작고 은밀한 공간에서 컴퓨터 조작으로 공격이 가능할 뿐 아니라 신속한 처리속도로 삽시간에 범행이 가능하므로 공격받은 전산망이나 기간 시설이 완전 무력화되거나 정보유출·조작 등이 이루어진 후에야 공격받은 사실을 감지할 수 있다.
- ○ 피해 규모의 대형화: 최소의 노력과 금전적 투자로 테러효과를 극대화할 수 있는 수법으로 전력·통신·금융망 마비, 컴퓨터망 이용 상거래 중단, 철도·항공·군사장비 시스템 파괴, 군·경 비상연락망 교란 등 국가 안보를 위협할 수 있는 엄청난 피해와 혼란이 초래될 수 있다.
- ○ 미래형 첨단폭격: 정보전은 정보 시대의 산물로서 정보통신망의 급속한 발달과 비례하여 그 위협이 증대되고 있으며 21세기에는 컴퓨터 통신망(전산망)을 이용한 정보전 공격이 더욱 부각될 것으로 전망된다.

이러한 특징은 정보전을 수행하려는 조직, 국가들에게는 대단히 매력적으로 비칠 것이며, 특히 직접 기술을 습득하지 않아도 이 같은 지식에 뛰어난 해커를 고용하기만 해도 된다는 점에서 매력은 더욱 높다고 할 수 있다. 정보전의 이러한 특징을 이용해 주요기반구조를 공격할 수 있는 가상의 적들의 공격 형태는 다음과 같을 것이다.

- ○ 컴퓨터, 통신, 소프트웨어, 데이터, 케이블 또는 제어 절차와 같은 기반구조 구성요소에 대한 물리적(전자적 또는 기타의 방법을 사용한) 공격
- ○ 건물, 전력, 환경적 통제설비 등과 같은 주요 기반구조 지원설비에 대한 물리적 공격
- ○ 운영요원 또는 지원 요원에 대한 물리적 공격 또는 살상
- ○ 주요기반구조 구성요소에 대한 논리적(소프트웨어적) 공격
- ○ 컴퓨터로 통제되는 환경적 통제 설비에 대한 논리적 공격
- ○ 공격을 위장하기 위한 물리적 공격과 논리적 공격의 통합 공격
- ○ 데이터에 대한 논리적 공격(파괴 또는 혼란 유발)

최근 발표된 미국의 사이버공간 보안 국가전략 초안에서는 상기와 같은 사이버 공격 위협을 다음과 같이 극단적으로 예시하고 있으며, 이러한 시나리오가 악의적이든 우연이든 모두 발생하였다는 사실에 주목하고 있으며, 원격의 사이버공격에 의하여 이루어질 수 있다는 사실에 주목하고 있다[10].

"테러리스트 조직이 어느 날 아침, 오후 4시부터 6시간 동안 퍼시픽 노스웨스트의 전력 수급 망(electric grid)를 셧 다운 하겠다고 발표하고 실제로 그렇게 한다. 그 다음으로 이 집단은 자신들이 미국의 동부와 서부를 잇는 주 전기 통신 중계선 회로를 반나절 동안 무력화 하겠다고 발표하고, 그리고 이것을 저지하려는 우리의 노력에도 불구하고 그들은 실제로 그렇게 한다. 그 다음으로, 그들은 뉴욕 시를 지원하는 항공 관제 시스템을 다운시켜 모

든 항공 운항은 정지시키고 착륙하려는 비행기를 다른 데로 회항시키겠다고 위협한다. 그리고 실제로 그렇게 한다. 다른 위협들이 이어지고 성공적으로 실행됨으로써 우리의 주요 기반을 공격할 수 있는 적의 능력을 입증한다. 마지막으로 그들은, 자신들의 요구를 들어주지 않으면 수백만 건의 사기 거래에서 도용한 수십만 개의 아이디를 이용하여 전자상거래와 신용 카드 업무를 1주간 무력화 하겠다고 위협한다. 그로 인한 일반인의 공황과 혼란을 상상해 보라."

이러한 위협을 가하는 위협원은 스크립트 키디에서부터 단순히 자신의 파괴적인 기술력을 자랑하려는 해커, 악의있는 내부자, 사이버 공간을 이용하는 범죄조직 및 정보전 전사 등 매우 다양하다. 현재 우리도 모르는 사이 회사나 가정 내 컴퓨터 사용자가 사이버 공격으로 인해 피해와 손실을 겪고 있으며, 이로 인한 피해는 상당하며, 심지어는 파멸을 불러올 수도 있다. 이러한 피해가 국가적 차원에서 국가가 의존하는 네트워크와 시스템에도 발생할 수 있는 다음과 같은 요인이 존재한다.

- 잠재적인 적이 의도를 가지고 있다.
- 파괴적인 도구가 널리 이용 가능하다.
- 국가 시스템의 취약성이 많고 잘 알려져 있다.

이와 같은 사실은 국가가 주도하여 책임있게 위험을 관리하고 취약성을 악용하는 것으로 인하여 초래될 수 있는 피해를 최소화하기 위한 노력을 경주하여야 함을 의미한다.

Ⅲ. 미국의 정책동향 분석

사이버 공간에 존재하는 위협을 제거하기 위하여 세계 각 국의 많은 나라에서 막대한 예산과 인력을 투입하고 있다. 미국의 부시 대통령은 2001년 사이버 보안을 우선순위 쟁점으로 삼는 행정 명령을 발표하고, 연방 네트워크를 안전하게 지키기 위한 기금을 증액하였다. 또한 부시 대통령은 2002년에 연방 사이버 보안 기관들을 통합하고 강화하는 조치를 취한 바 있다. 본 장에서는 미국의 최근 정보전 대응정책 동향을 고찰하도록 하겠다.

1. 조직 정비 배경 및 현황

미국이 자국의 본토방위를 위한 독립된 기구를 대통령실에 두게 된 것은 우선 PDD 63에서 규정한 국가 조정자(National Coordinator)의 역할의 한계를 인식한 것이 그 원인이었다. 즉, PDD62에서 국가조정자는 NSC내에 임명한 테러 대응을 위한 연방 정부 활동 중심 기관이었으나, PDD62 그리고 PDD63에서 일반적인 권한과 책임이 기술된 것 이외에 대통령 명령이나 법으로 국가조정자의 권한과 책임에 대해 상세히 규정하지 않아 그 권한과 책임에 한계를 느끼게 되었다.

그 결과 중요한 조정 및 지휘 기능이 국가조정자에게 있는 것이 아니라 법무부, FBI, 연방긴급재난관리국((Federal Emergency Management Agency: FEMA), 및 OMB와 같은 다른 기관들이 담당하게 되었다. 또한 위협과 위험 평가, 국가 전략 개발, 연방정부와 주 정부와의 협력, 테러 및 사이버테러 대응 수행에 대한 감독 등의 기능들이 이들 기구에 남아있게 되었다.

따라서 조정 및 지휘 기능의 분산으로, 테러에 대한 총괄적 조정 및 지휘가 불가능하게 되었고, 연방차원의 테러 대책 및 대응을 위한 중심기관의 필요성에 따라 이를 구현하기 위한 여러 개선안들이 대두되었다.

이러한 제안들이 대두되는 가운데 9.11 테러사태가 발생하였으며, 이러한 테러에 대한 대책 및 대응 강화를 위하여 연방차원의 중심기관 설치의 필요성이 더욱 증가하였고, 이를 위한 각종 제안들을 고려하여 조직 정비를 단행하게 된 것이다.

9.11 이후 미국은 자국의 본토 방위를 위하여 기존의 조직체계에 변화를 주었다.

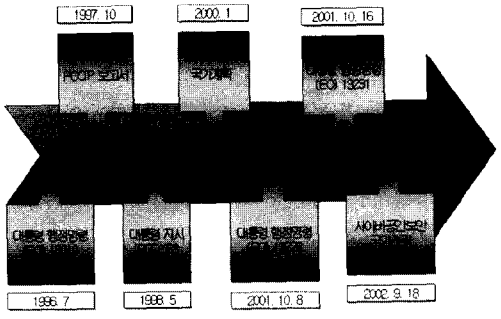
이를 위한 대표적인 것으로는 본토안보국(Office of Homeland Security: OHS), 대통령 사이버공간담당 특별 보좌관(Special Advisor to President for Cyberspace Security), 국가기반자문회의(National Infrastructure Advisory Council), 대통령주요기반보호협의회(President's Critical Infrastructure Protection Board: PCIPB) 및 최근 발표된 사이버공간보안 국가전략을 들 수 있다[10].

〔그림 1〕은 1996년부터 최근까지의 미국의 사이버테러 관련 주요 정책 변화를 나타내고 있다.

2. 본토안보국(Office of Homeland Security)

미국 연방정부가 본토안보국의 발족을 서두르게

된 이유는 앞서 간략히 살펴본 바와 같이 대테러 업무가 40개가 넘는 연방정부 기관에 분산돼 있는 현행 시스템으로는 핵·생물·화학무기의 동원 가능성까지 거론되는 갖가지 테러로부터 미국을 효과적으로 보호할 수 없었기 때문이다.



〔그림 1〕 미국의 사이버테러 관련 정책 변화

본토안보국과 같은 기관의 발족 필요성은 9월 11일 뉴욕 테러가 있기 전부터 논의된 것이나, 부시대통령은 9.11 테러사태 이후 약 10일 후인 9월 20일 본토안보국 신설계획을 발표하였다. 그리고 2001년 10월 8일 대통령 행정명령 13228을 공포하여 본토안보국을 대통령실내에 설치하였다[11].

본토안보국은 대통령 본토안보 담당 보좌관을 국장으로 하는 대테러 업무 총괄 기구이다. 본토안보국의 주 임무는 테러리스트의 위협과 공격으로부터 미국의 안전을 보장하기 위한 총괄적인 국가 전략을 수립하고 집행을 조정하는 것이다. 테러리스트의 위협과 공격은 물리적 공격 뿐만 아니라 사이버 공격도 포함된다. 본토안보국은 미국내의 테러리스트 위협 및 공격에 대한 탐지, 준비, 방어, 예방, 대응 및 복구 등 각 행정부처의 노력을 총괄적으로 조정하는 기능을 수행한다.

그러나 이러한 본토안보국의 활동에 관하여 문제점이 제기되고 있다. 즉, 본토안보국은 관련 각 부처 조정 권한만 있을 뿐, 지휘·명령할 권한 없고 본토안보 관련 프로그램에 대한 예산 검토권이 본토안보국에 부여되어 있으나, 부처의 테러 대응 예산에 대하여 변경하거나 거부할 권한 등, 부처의 예산 통제에 대한 실질적인 권한은 없다. 이러한 문제점 제기는 결국 2002년 6월 부시대통령에 의한 본토안보부 설립 계기를 마련해 주었다.

3. 본토안보회의(Homeland Security Council)

본토안보에 대한 대통령 명령 제1호에 의해 2001년 10월 29일 그 조직과 운용이 발표된 본토안보회의는 테러범의 위협과 공격으로부터 미국을 수호하고, 잠재적인 테러 공격을 감소시키고, 공격 발생시 피해를 최소화하기 위해 연방, 주, 지방 부처에 대한 총괄적 조정 강화 필요성에 따라 설립되었다.

이는 對테러와 관련하여 종전 국가안전보장회의(NSC)가 담당하던 미국내 테러의 위협이나 공격과 관련된 정책 운영에 관한 책임이 본토안보회의로 이관된 것을 의미한다.

본토안보회의는 보안에 대한 모든 정책의 효율적 개발과 실행을 촉진하고 관련된 정부 부처의 활동에 대한 조정을 담당한다.

그리고 본토안보회의에 본토안보회의 고위급위원회(Homeland Security Council Principals Committee: HSC/PC)를 설치하였는데, 재무·국방·법무·보건인적서비스·교통 장관과 관리예산국장·CIA 국장·FBI 국장·연방 재난관리 국장 등이 상임위원이 되고, 본토안보국장 겸 본토안보담당 대통령보좌관이 그 의장을 맡고 있다. 또한 대통령안보담당특별보좌관은 본토안보회의 고위급위원회의 모든 회의에 참여한다.

본토안보회의 내에 본토안보에 대한 정책 문제를 고려하고 실무협의회의 활동을 감독하기 위해 차관급협의회를 설치하였다. 이 차관급협의회는 본토안보회의 고위급 위원회를 구성하는 각 부서의 차관급 관리들이 참여하며, 사이버공간보안담당 대통령특별보좌관, 테러퇴치를 위한 대통령국가보안부보좌관(the Deputy National Security Advisor for Combating Terrorism) 등이 업무관련 참여위원으로 동 회의에 참여한다.

또한 연방정부 부처들의 조국보안 정책 개발 및 실행을 조정하고, 동 정책에 대해 주 정부 및 지방정부와 조정하며 본토안보회의의 정책 조정을 위한 실무위원회로서 대통령의 정책 결정을 위한 대안 제시를 위해 본토안보회의 정책조정위원회(Homeland Security Council Policy Coordination Committees: HSC/PCCs)를 11개 두고 있다.

각 위원회의 구성 및 임무에 관해서는 참고문헌[12]를 참조하기 바란다.

4. 사이버공간 안보담당 대통령 특별 보좌관

미국 정부는 사이버테러에 대비하여 주요기반시설을 소유하고 운용하고 있는 민간부분과의 협력 강화를 위해 사이버공간 안보담당 대통령특별보좌관을 임명하고 '사이버테러 및 정보보안 관련 업무'를 담당하고 '테러대응 업무'를 종전 국가안전보장회의(NSC)의 '대테러리즘 담당 국가조정관'이 수행토록 임무를 분리하였다. 이는 사이버공간의 보안이 중요하게 대두되는 시점에서 시의적절한 것으로 평가받고 있으며, 동 대통령특별보좌관은 정보시스템 보안을 위한 각 부처 및 연방 정부, 지방 정부의 활동을 총괄 조정하고, 침해사고 발생시 그 복구를 총괄하며 주요정보통신시설을 운용하고 있는 민간 분야와의 업무를 조정하고 협의하는 역할을 담당하고 있다[10].

동 보좌관으로 임명된 Richard Clarke는 임명된 후 GOVNET라는 인터넷과 독립된 네트워크를 조성하여 정부를 위한 새로운 안전한 통신망으로 구축할 것을 발표한 바 있다.

5. 대통령 주요기반보호 협의회

2001년 10월 16일에 발표된 대통령 행정명령 13231에서는 미국의 국가 주요 기반구조 보호를 위한 최고 정책기관으로 대통령 직속 주요기반보호협의회(President's Critical Infrastructure Protection Board: PCIPB:)를 설립을 명하였고, 이 협의회의 설립을 통해 주요기반보호 정책을 보다 강화하고 효과적으로 집행할 수 있는 국가 조직체계를 정비하는 것을 그 내용으로 하고 있다[13].

협의회는 국무장관, 재무장관, 국방장관, 법무장관 등 주요부처 장관과 CIA국장, 합참의장, OMB 국장, 과학기술정책국장, 국가경제위원회 의장, 대통령안보담당보좌관, 본토안보 담당 대통령 보좌관 등 최고위급 행정부 관리로 구성되었다. 또한 원할한 업무수행을 위하여 상무부의 CIAO 국장, NCS (National Communications Systems)의 매니저, NSA의 정보보증담당 부장, CIA 커뮤니티 관리 담당 부국장, FBI의 NIPC 부국장 등으로 조정위원회를 구성하였다.

동 위원회(PCIPB)는 다음과 같은 정보시스템 보호와 관련된 연방정부의 노력 및 계획을 인지하고 조정할 예정이다.

- 민간분야의 주요기반, 연방 및 지방정부의 주요기반과의 협력과 보호, 그리고 기업 및 학교 조직에 대한 지원
- 연방정부의 부처 및 기관의 주요기반보호
- 관련 국가 안보 프로그램

대통령 주요기반보호협의회의 주요임무는 다음과 같다.

- 민간분야 및 주 정부 및 지방 정부와의 협력 강화
- 정보공유
- 침해사고 조정 및 위기 대응
- 행정부 정보보호 전문가들의 채용 및 교육
- 연구개발
- 사이버범죄 수사 및 사이버 범죄 대처 프로그램의 강화
- 국제적 정보기반보호를 위한 협력
- 입법
- 본토안보국과의 협력

6. 국가주요기반자문회의

국가주요기반자문회의(National Infrastructure Advisory Council)는 국가 주요기반보호 업무를 위하여 대통령을 자문하는 민간 중심의 자문기구로써, 대통령 행정명령 13231에 의하여 설치되었다[13].

NIAC의 위원은 민간부문, 학계, 연방 정부와 지방 정부 출신 및 금융, 교통, 에너지, 긴급 정부서비스 등 주요기반 보호와 관련된 기업 대표자중에서 선정한다. 동 자문회의의 가장 큰 기능은 주요기반보호를 위한 정부·공공 부문과 민간부문의 협력을 강화하고 이에 대한 정책적 자문을 수행하는 것이다.

7. 본토안보부

본토안보부는 다음과 같은 필요성에 의하여 '02년 6월 부시대통령에 의해 설립이 제안되었다[14].

- 미국 본토 방어를 본연의 임무로 하는 단일 부서
- 국경, 교통 분야, 공항/항구 및 주요 기반의 안전을 보호
- 다양한 정보원으로부터 본토안보관련 첩보 분석 및 종합

- ○ 주, 지방 정부, 민간 기업 및 국민과 위협과 대비에 대한 정보 교류, 조정
- ○ 생화학 테러 및 대량살상 무기로부터 미 국민 보호를 위한 정부의 활동 조정
- ○ 연방 재난 대응 활동(federal emergency response activities) 관리

이와 같은 필요에 의하여 설립된 본토안보부의 임무는 첫째, 미국에 대한 테러리스트의 공격 예방, 둘째, 테러 방지를 위한 미국의 취약점 최소화 그리고 테러 공격 후 피해최소화와 복구이며, 이 임무를 수행하기 위하여 연방·주·지방정부, 민간 및 모든 미국시민들을 동원할 수 있다. 본토안보부는 테러로부터 미국 본토를 보호하기 위한 단일의 내각수준 조직으로 되게 하며, 명백하고 효과적인 역할을 하는 다음 네 개의 국으로 구성되게 된다.

- ○ 국경 및 교통 보안
- ○ 재난대처 준비 및 대응
- ○ 화학, 생물학, 방사선, 핵 대응
- ○ 정보분석 및 기반 보호

새로운 부의 설립후에도 법무부와 FBI는 테러공격대비관련 법 집행기관 역할, 국방부는 테러 등 심각한 재해의 경우 중요 원조 역할, 교통부는 고속도로 및 철로 안전·항공교통 통제의 역할, CIA는 외국 첩보사항의 정보 수집과 분석 등 기존 기관의 본토안보를 위한 역할을 계속적으로 수행하게 된다.

8. 사이버공간보안 국가전략

대통령 주요기반보호위원회는 '02년 9월 미국 국민의 삶에 매우 중요한 미국의 기반을 보호하기 위한 사이버공간보안 국가전략을 발표하였다. 동 전략에는 국가 전략의 5 가지 단계인 홈 사용자, 대기업, 기간 부문, 국가, 국제적인 공동체를 대상으로 정부 및 비정부 실체들이 사이버 보안을 촉진하기 위하여 취할 수 있는 구체적인 조치, 사이버 보안을 위한 기존의 노력 및 지속적인 분석, 토론과 논의가 필요한 쟁점을 소개하였다. 본 논문에서는 국가가 시행하여야하는 대표적인 구체적 조치만을 소개하며 구체적인 사항은 참고문헌[2]를 참조하기 바란다.

- ○ 보다 안전한 IT 제품 조달을 강화하기 위한 NIAP(국가정보보증프로그램)의 포괄적인 검토
- ○ 전자 정부의 보안 도구와 서비스를 확대
- ○ 전자 인증 사업의 일관성과 상호 운용성 도모
- ○ 위협 관리 도구의 적극적 배치
- ○ 서비스 중단 동안 운용의 연속성을 위한 다양한 대안 평가
- ○ 안전한 망 프로토콜 채택을 주도
- ○ 시나리오 기반의 보안 및 비상 태세 연습의 비용 효율성 검토
- ○ 경계 경로 프로토콜(BGP), 인터넷 프로토콜(IP), 도메인 네임 시스템(DNS) 등에 대한 보안을 개선
- ○ 안전한 라우터 기술 및 관리의 채택을 개선
- ○ 감시제어데이터수집시스템(SCADA) 보안 증진
- ○ 학계, 업계, 정부간에 R&D의 해당 범위, 식별 및 조정에 대한 기존 메커니즘의 검토
- ○ 보안성이 내재된 무선 LAN용 고도 표준 및 프로토콜의 지속적인 개발 등

Ⅳ. 일본의 정책동향 분석

9.11테러 이전 일본은 내각관방에 정보보안대책실을 설치하고, 이를 통한 종적인 국가적 정보보안대책을 추진하였다. 9.11테러 발생이후, 총리가 주재하는 긴급 관계성청회의를 거쳐 과거 폭탄 등을 위주로 한 물리적 테러의 개념에서 한층 그 폭을 넓혀 생화학·핵에 대한 대응책 마련과 고도 정보화시대에 접어들면서 새로이 등장한 사이버테러 대책 강화 등을 중점추진사항으로 의결하였다. 이는 사이버테러를 대테러대책의 하나로 분류함으로써 기존의 대테러대책에서 진일보한 자세를 보여주고 있다. 다음은 각 부처별 주요 추진사항이다.

- ○ 정보의 일원적 집약과 신속한 분석대응
  - Intelligence Community 정보통신 네트워크 구축 (내각관방)
  - 정보수집기능강화 (내각관방)
- ○ 중요시설 동향파악 강화
  - 경찰·해상보안청·자위대의 경비능력·즉각대응체제 강화
  - 원자력 발전소 등의 방호조치 강화
- ○ 사이버테러 대책강화
  - 사이버테러대책의 보완·강화 (경찰청)
  - 사이버 공격에 대한 대처수단 등 연구 (방위청)

- 사이버테러 방지를 위한 고성능 네트워크 보안 시스템 정비 (총무성)
- 부정액세스·컴퓨터바이러스 등에 관한 정보제공 등 강화 (경제산업성)

○ 하이재킹 등 방지대책 강화
- 통관·세관검사 기능 강화 (재무성)
- 공항 등의 보안·경비 태세 강화를 위한 보안검사장 등 정비 (국토교통성)
- 기내 보안대책 강화

한편, 일본 정부가 911테러이후 추진하고 있는 사이버테러 대책의 구체적 조치로서, 2001년 10월 2일 「'사이버테러 특별행동계획'에 대한 후속조치」[15]를 통한 행정부 및 전력·교통 등 중요 인프라의 사이버테러 대응 연락·협력체계 구축 및 보호대상 정보시스템 지정 들 수 있으며, 구체적 내용은 〔표 1〕과 같다.

특히, 「'사이버테러 특별행동계획'에 대한 후속조치」에서는 내각관방을 중심으로 긴급상황 발생시 정보연락이 필요한 경우로서 ▸예고, 조직적인 예비행위 등의 예후, ▸중요시스템의 경미한 장애, ▸중요시스템의 중대한 장애, ▸사이버공격의 확인이라는 상황을 설정하고 각 사안별 연락체계를 정하였으며, 자세한 사항은 참고문헌[10]을 참조하기 바란다.

또한 중요인프라 사업자가 관계중앙행정기관에 연락을 취해야할 경우 중, '사이버공격의 탐지'에 관하여 연락대상이 되는 사이버공격의 징후와 연락의 대상이 되지 않는 것을 구분하고 있으며 연락대상이 되는 대표적인 경우는 다음과 같다.

○ 중요시스템에의 영향이 상당정도 예상되는 공격을 탐지
- 외부로부터 침입할 수 없는 내부네트워크의 중요시스템에 부정액세스 시도가 있었을 경우
- 중요시스템에 장애를 일으킬 우려가 있는 컴퓨터 바이러스가 발견된 경우
- 공격 패턴이나 과거의 사례로 비추어보아, 중요시스템에 중대한 영향을 미칠 우려가 있을 것으로 예상되는 공격이 있었을 경우

○ 중요시스템에 대하여 특정 그룹 등이 명백한 의도와 목적을 가지고 공격한 것을 탐지한 경우

한편, 전자정부 및 민간 중요인프라에 대한 사이버테러 대책을 원활히 수행하기 위하여 2002년 4월 1일 내각관방 정보보안대책추진실에 국가긴급대응팀(NIRT, National Incident Response Team)[12]이 설치되었다.

〔표 1〕 보호대상이 되는 각 중요인프라의 중요시스템

분야	사이버공격에 의한 위협·위험성	대상 시스템
정보통신	· 전기통신서비스 정지 · 전기통신업무에 관한 통신비밀유출 · 방송프로그램제작·긴급재해대응 등 정보발신기능의 장애	· 전기통신사업용 설비 · 통신관리업무 시스템 · 방송업무용 시스템군
정보서비스	· 정보시스템 공통의 취약점에 의한 광범위한 장애 등	
금융	· 자금이체, 융자업무 등의 업무정지 등	· 자금증권계 시스템 · 국제계 시스템 · 대외접속계 시스템 · 결제 시스템
항공	· 운항 지연, 결항 · 항공기의 안전운항에 대한 지장 등	· 운항계 시스템 · 예약·탑승 시스템 · 정비 시스템 · 화물 시스템 · 항공관할 시스템 · 기상정보 시스템
철도	· 열차운행 지연, 운휴 · 열차의 안전운행에 대한 지장 등	· 열차운행관리 시스템 · 전력관리시스템 · 좌석예약시스템
전력	· 전력공급 정지 · 전력플랜트의 안전운용에 대한 지장 등	· 제어시스템 · 운전감시 시스템
가스	· 가스의 공급정지 · 가스플랜트의 안전운용에 대한 지장 등	· 플랜트제어시스템 · 원격감시·제어 시스템

인원구성은 정부 및 민간의 전문가 15인으로 구성되어있으며, 통신총합연구소의 오오노 히로유키박사가 총괄지휘를 담당하고 있다. NIRT는 각 정부부처 정보보안 상담대응, 사이버테러 관련정보의 수집·분석, 사이버테러 피해확산 방지 및 복구에 대한 기술적 지원 등의 임무를 수행하고 있다.

V. 결 론

본 논문에서는 9.11 테러 이후 미국, 일본을 중

심으로 한 각국의 정보전 대응동향을 고찰하였다. 각 국은 테러의 성격을 재래식 테러로부터 새로운 성격의 테러(super terrorism)로 규정하고 이에 대한 대응 또한 범죄행위의 방지나 처리라는 국내 치안적 차원에서 다루어지는 것이 아니라 전쟁행위에 맞서는 국방차원에서의 자위적 방어(self-defense)로 규정하고 있음을 알 수 있다.

이렇듯 해킹대응에서 시작된 각 국의 사이버 공간 위협 방지 대책이 사이버테러, 사이버전으로 전이될 것으로 전망된다.

이러한 상황에서 정보 인프라 구축이 발전되어 있는 우리나라의 경우에도 사이버 테러, 사이버전에 대비한 종합적인 대책을 강구할 필요성이 절실히 요구되고 있다.

이러한 인식을 바탕으로 국가정보원, 국방부, 정보통신부 등 관련 부처간 협의 및 조정을 통하여 범국가적인 사이버테러 대응 국가계획 수립이 필요하다고 판단되며, 국가보안기술연구소, 한국정보보호진흥원 등 관련 연구기관, 정보보호산업체 및 학계의 노력이 조화되는 사이버테러, 사이버전 대응기술 연구가 활발히 추진되어야 할 것으로 판단된다.

참 고 문 헌

[1] http://www.ciao.gov/Protecting America's Critical Infrastructures, 1998. 5.

[2] 국가보안기술연구소, 사이버공간보안 국가전략, 2002. 10.

[3] http://www.cert.org/stats/cert_stats.html

[4] http://www.nis.go.kr

[5] Martin Libicki, What is Information Warfare?, August 1995

[6] Winn Schwartau, Information Warfare Chaos on the electronic superhighway, (Thunders Mouth Press 1996)

[7] The Chairman of the Joint Chiefs of Staff Instruction 3210.1, 1996

[8] Toffler Alvin and Heidi, War and Anti War - making sense of todays global chaos, (Warner books, 1993)

[9] DoD, DoD Directive s-3600.1 Information Operations(IO), 9 Dec. 1996

[10] 김현수외, 9.11테러이후 미국·일본의 대응동향, 국가보안기수연구소 내부 TM, 2002. 6.

[11] Executive Order 13228 of October 8, 2001. - Establishing the Office of Homeland Security and the Homeland Security Council.

[12] Homeland Security Presidential Directive-1,http://www.whitehouse.gov/news/releases/2001/10/20011029-16.html, October 29, 2001

[13] Executive Order 13231 of October 16, 2001. - Critical Infrastructure Protection in the Information Age.

[14] http://www.whitehouse.gov/homeland

[15] http://www.kantei.go.jp/jp/it/security/tyousakai/dai1/susumekata.html.

〈著 者 紹 介〉

이 철 원 (Cheolwon Lee)

1987년 : 충남대학교 수학과(이학사)

1989년 : 중앙대학교 전자계산학과(이학석사)

2001년 : 아주대학교 컴퓨터공학과 박사과정 수료

1989년~1996년 : 한국전자통신연구원 선임연구원

1996년~2000년 : 한국정보보호센터 선임연구원/통신모델링 과제책임자

2000년~현재 : ETRI부설 국가보안기술연구소 팀장, 책임연구원

관심분야 : 컴퓨터 및 네트워크 보안, 정보통신기반보호, 정보보호시스템 평가기준

장 병 화 (Byunghwa Chang)

1975년 : 연세대학교 전기공학과(공학사)

1979년 : 한국과학기술원 전기전자공학과(공학석사)

1988년 : 한국과학기술원 전기전자공학과(공학박사)

1974년~1982년 : 한국과학기술연구소 전자공학연구부 선임연구원

1982년~2000년 : 국방과학연구소 부장, 책임연구원

2000년~현재 : ETRI부설 국가보안기술연구소 부

장, 책임연구원
관심분야 : 통신 보안, 정보전, 정보보호시스템 평가기준

이 철 수(Cheolsoo Lee)
명예회원

1968년 : 육군사관학교(이학사)
1972년 : 서울대학교 수학과(이학사)
1977년 : 한국과학기술원 전산학과(이학석사)
1980년 : 한국과학기술원 전산학과(이학박사)
1980년~1981년 : 육군본부 전산위원
1981년~1982년 : 서울지하철공사 연구위원
1982년~1993년 : (주) 데이콤 올림픽사업단장, 행정전산사업본부장, 종합연구소장
1993년~1998년 : 한국전산원 원장
1998년~2000년 : 한국정보보호센터 원장
2000년~현재 : 한국정보통신대학원대학교 초빙교수
1996년~현재 : 서울지방법원 조정위원
1999년~2000년 : 대검찰청 컴퓨터수사자문위원회 자문위원
1996년~2001년 : CALS/EC협회/기술협회 감사
1995년~2000년 : 인터넷협회 감사
2002년~현재 : 국방부 정보화추진자문위원
2002년~현재 : 프로그램 심의 조정위원회 위원
관심분야 : 컴퓨터 및 네트워크 보안, 정보전