국가 사이버 위기관리체계 강화 방안에 관한 연구

이재은*, 양기근**, 류상일***

충북대학교 행정학과*, 원광대학교 소방행정학과**, 동의대학교 소방안전학과***

이 연구에서는 국내·외 사이버 위기관리 체계 분석을 통해 변화하는 국내 실정에 적합한 국가 사이버 위기관리 체계 강화 방안을 모색하는데 목적이 있다. 이를 위해 미국, 영국, 독일, 일본의 사이버 위기관리체계에 대한 분석을 통해 법적 체계와 조직체계의 시사점을 도출하였다. 연구 결과, 한국의 사이버 위기관리체계 강화 방안을 다음과 같이 제시하였다. 첫째, 국가 사이버 위기관리는 개인, 조직, 기업, 공공기관, 정부기관 등이 각각의 수준에 맞는 사이버 위기관리 체계를 이루어야 한다. 둘째, 국가 사이버 위기의 개념을 국가위기 개념과 연계하여야 한다. 셋째, 국가 사이버 위기관리의 개념과 국가 위기관리 개념을 연계시키는 것이 필요하다. 넷째, 국가 사이버 위기관리 기관을 책임 정도에 따라 국가 사이버 위기관리 주관기관, 실무기관, 협력기관 등으로 체계화하여 관리하는 것이 필요하다. 다섯째, 국가 사이버 위기관리 법체계 정비가 필요하다. 여섯째, 국가 사이버 위기관리 조직체계를 강화하는 것이 필요하다. 일곱째, 국가 사이버 위기관리의 전문성을 확보해야 한다. 여덟째, 국가 사이버 위기 경보 체계 구축이 필요하다. 아홉째, 국가 사이버 위기관리 평가 체계를 구축하는 것이 요구된다. 열 번째, 국가 사이버 위기관리는 공공과 민간 분야에서의 전문인력 확보와 전문성 향상이 그 핵심요소로 제기된다. 열 한 번째, 국가는 국가 사이버 위기관리의 지속적인 발전을 이룩하기 위하여 학술적 발전에도 노력하여야 한다.

주제어: 국가 위기, 국가 사이버 위기, 사이버 테러, 국가 위기관리 체계

Ⅰ. 서론

최근 사이버 위기관리의 필요성이 증대되고 있다. 정보통신혁명에 의해 주도되어 변화되는 지식정보사회로의 사회변동 과정은 단순한 기술적 변화를 넘어서 사회구조, 경제생산구조, 인간의 상호작용 양식, 그리고 인간과 생태계 사이의 관계 등 인간생활의 전반적인 영역에서 막대한 변화를 가져왔기 때문이다. 이러한 맥락에서 볼 때 미래의 재난은 지금까지와는 전혀 다른 새로운 유형이 나타나거나 기존의 재난이 동시다발적으로 발생하여 새로운 모습으로 나타날 수 있다. 과거 농경사회나 전통적 산업사회에서의 1차 산업이나 2차 산업으로부터 IT에 기반한 지식정보사회로 진입하면 할수록 새로운 신산업의 등장이 가속적으로 이루어지고 있다. 우리 사회 또한 미래에는 과거에 예상하지 못했던 수많은 신종재난이 위험요소로서 나타날 것이다. 이는 IT부문의 발전을 통해 우리 사회가 직면한 많은 문제들을 해결할 수 있게 되었지만, 다른 한편에서는 전혀 새로운 성질의 문제들이 새로운 양태로 대두되면서 위기상황을 야기할 수 있는 것으로 이해된다.

이러한 위기 상황의 근본적인 원인은 새로운 문제를

기존의 관점과 경험으로 이해하고 해결하려고 하는데서 기인한 것으로 판단된다. 따라서 오늘 날의 IT에 기반한 지식정보사회에서 발생하는 각종 재난과 위험은 그 유형, 내용, 규모 등의 면에서 종전의 농경사회나 산업사회의 경우와는 매우 상이한 경향을 보이게 되어 이에 대한 예측 노력과 해결 노력이 절실하게 필요하다. 특히, 최근에는 컴퓨터 보급의 확대와 인터넷의 활성화로 인하여 사이버 위기가 급증하고 있다[1]. 사이버 위기는 오늘날 컴퓨터와 각종 전자기기에 의존하고 있는 현대 과학 사회에서 그 피해가 사이버에만 그치지 않고, 국민생활과 안보 및 정보통신, 금융, 원자력기기 등의 국가핵심기반에까지도 확대되고 있다.

국가위기관리체계는 과거에는 전통적 안보위기에 초점을 두었으나, 1990년대 중반 이후 각종 자연재난, 인적재난 및 사회재난의 발생으로 인해 재난위기로까지 점차 확대되었다. 또한, 9.11테러를 기점으로 하여 국가핵심기반 위기관리의 필요성이 부각되어, 오늘 날에는 국가핵심기반 위기도 국가위기관리체계 하에서의 관리 필요성이 크게 대두되었다.

국내·외 사이버 위기관리 현황을 보면, 한국의 경우, 2003년 발생한 1.25 인터넷 마비사고를 계기로 범 국가 차원의 사이버 안전체계 수립이 현안으로 대두되었다. 이에 사이버안전정책조정회의가 국가안전보장회의(NSC) 산하에 신설되었으며, 국가정보원은 2004년 2월 국가사이버안전센터(NCSC)를 개소하여 포괄적 국가 위기관리 개념 하에 사이버 안전분야를 국가위기관리 대상에 반영하여 중점 관리해 왔다. 이로써 정보통신부의 인터넷침해사고대응지원센터와 국방부의 국방정보전대응센터 등 민・관・군에서 추진해 온 사이버 안전 전문기구들이 생겨나게 되었다. 또한, 2004년 상반기의 주요 국가기관 해킹사건을 계기로 사이버공격에 의한 국가안보 위협 가능성이 현실로 나타남에 따라 국가적 차원의 일원화된 국가 사이버 안전체계 필요성이 제기되고 있다. 특히, 사이버 침해 사고가 발생하는 인터넷 공간은 민・관・군 영역이 구분되지 않기 때문에 각 분야별 정보공유 및 업무 협조 강화가 절실히 요구된다. 이에 2005년 1월 국가정보원을 국가 사이버안전 총괄기관으로 정하고 국방 및 민간분야와 사이버공격 관련 정보 공유 및 협력을 통해 국가사이버 안전관리업무 전체를 총괄하는 것으로 되어 있다. 그러나 현재 우리나라의 사이버 위기 대응기관으로는 국가정보원의 국가사이버안전센터, 국방부의 국방정보전대응센터, 정보통신부의 인터넷침해사고대응지원센터를 주축으로 대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 국가보안기술연구소, 정보공유분석센터(ISAC)등으로 다양하게 존재하고 있어 이들 간의 협력체계 강화가 절대적으로 요구된다.

이에 본 연구에서는 국내・외 사이버 위기관리 체계 분석을 통해 변화하는 국내 실정에 적합한 국가 사이버 위기관리 체계 강화 방안을 모색하는데 목적이 있다. 구체적으로 국가 위기관리 체계 하에서의 사이버 위기관리 개념 정립, 해외 위기관리체계 및 사이버 위기관리 시스템 분석, 우리나라 위기관리체계 및 사이버 위기 발생 현황 분석, 한국의 위기관리체계 발전을 위한 사이버 위기관리 강화 방안 제시가 연구의 세부 목적이다. 연구 방법으로는 국가 사이버 위기관리체계에 관한 선행연구 검토 및 사이버 위기 발생 현황 분석 등의 문헌분석 방법을 활용한다.

II. 국가 사이버 위기관리에 관한 이론적 논의

1. 국가 사이버 위기관리의 개념과 특징

사이버 위기란 사이버 세상에서 일어날 수 있는 모든 위협 요소를 총칭하는 것으로 이해할 수 있다. 사이버위기는 관점에 따라 다양하게 분류할 수 있다.

그 중에서 고의성을 기준으로 판단하면, '우연한 사고에 의한 위협'과 '악의적 위협'으로 분류가 가능하다. '우연한 사고에 의한 위협'은 사실 인간의 실수로 일어나는 일들이 대부분이다. 그러나 '악의적 위협'은 정보시스템

1) 최근 공공분야의 사이버 침해사고 발생 현황을 보면, 2003년도에 1,323건, 2004년 3,970건, 2005년 4,549건으로 계속적으로 증가하는 추세이다.

의 취약한 부분을 공격하여 시스템 내부에 침입하거나 시스템을 마비, 파괴하는 등의 사고를 유발하게 하는 것으로서 악의적 해킹, 오류 및 누락, 사기 및 절도, 악의적 컴퓨터 바이러스 유포, 산업스파이 활동 등의 다양한 형태로 나타날 수 있으므로 그 위협의 원인을 미리 파악할 필요가 있다. 또 다른 기준으로 행위 주체에 따라서 사이버침해 위협을 분류할 수 있다. 사이버침해는 그 행위 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분할 수 있다(박도권, 2007: 3).

<표 1> 수준별 사이버 침해 위협

구분	개인적 침해 위협	조직적 침해 위협	국가적 침해 위협
주체	• 해커 • 컴퓨터범죄자	• 산업스파이 • 테러리스트 • 조직화된 범죄집단	• 국가 정보기관 • 사이버 전사
목적	• 금전획득 • 영웅심 발휘 • 명성 획득	• 범죄조직의 이익달성 • 정치적 목적달성 • 사회 · 경제적 혼란야기	• 국가기능 마비 • 국가방위능력 마비
대상	• 민간시설망 • 공중통신망 • 개인용 컴퓨터	• 기업망 • 금융, 항공, 교통 등 정보통신망	• 국방 • 외교 • 공안망 등
공격방법	• 컴퓨터 바이러스 • 해킹, 메일폭탄, 홈페이지 변보, 패스워드 유출, 개인 신분 위장, 트로이목마 등 • 서비스거부 공격	• 개인적 공격방법 포함 • 유 • 무선 도청 • 정보통신망 스니퍼 • 통신망 교환시스템 동작 마비 공격	• 개인 • 조직적 공격 포함 • 첨단도청 및 암호 해독 • 전자공격 무기, 고에너지 전파무기, 전자기파 폭탄 등 • 기타, Chipping/ 초미세형로봇/ 전자적미생물

자료: 박도권(2007: 3).

한편, 국가사이버안전관리규정에서는 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 "사이버공격"이라고 규정하고, 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 "사이버안전"이라고 정의한다(국가사이버안전관리규정, 제2조). 이러한 사이버 위기는 전 세계에 그물망처럼 연계된 인터넷망을 통해 전개되며 소요시간도 그동안에 있었던 일반적인 위기와는 달리 수분이내에 끝나면서도 피해규모에서는 일반의 상상을 초월하고 심지어는 국가 안보에 심각한 위협으로 나타날 수 있다. 따라서 사이버위기는 그동안 우리 인류에 커다란 위협이 되어왔던 일반적인 위기와는 그 본질을 달리하는 것으로 볼 수 있다.

사이버 위기 또는 사이버 테러의 특징을 살펴보면 다음과 같다(조호대, 2006: 17-18). 첫째, 광역성 및 다양성이다. 일반적으로 사이버테러는 테러리스트가 목표로 정한 공격지점에 직접 접속하여 공격하는 것이 아니라 네트워크가 연결된 곳이라면 세계 어느 곳이든 공격을 감행할 수가 있다. 둘째, 최소의 인원으로 최대의 피해 가능성이다. 컴퓨터 네트워크를 이용하여 적의 정보통신망에 침투하기 위한 최소한의 기술만 있으면 사이버테러리즘은 가능하다. 물리적인 테러가 대규모 혹은 소규모라도 다수의 인원을 필요로 하는 것에 비해 목표 대상에 따라 필요 인원이 증가할 수는 있겠지만 사이버테러를 위한 인원은 다른 어떤 물리적인 테러를 수행하기 위한 인원에 비해 적다. 셋째, 증거의 은닉성과 비가시성이다.

2. 국가 사이버 위기관리에 대한 선행연구 검토

1) 국내 선행연구 검토

국내 사이버 위기에 관한 연구는 2000년 이후 주로 진행되어 왔다. 그러나 사이버 위기에 관하여 체계적인 유형 구분 등의 연구라기보다는 각 분야에서 제기되고 있는 사이버 연구가 대부분이다. 박도권(2007)은 사이버침해를 그 행위 주체에 따라 개인적 침해, 조직적 침해, 국가적 침해로 구분하고 있다(박도권, 2007: 3). 이를 기반으로 선행연구들을 개인 수준(강구형, 2008; 지무진, 2008; 박도권, 2007; 양은영, 2006; 이지혜, 2006; 고동우, 2004), 집단 및 조직 수준(김형준, 2007; 서성교, 2005; 배상균, 2005; 이동곤, 2004; 정일석, 2004), 국가 수준(김학권, 2008; 이성순; 2007; 이강무, 2006; 고준수, 2004)별로 정리할 수 있다.

그리고 사이버 위기에 관한 선행 연구를 사이버 위기의 유형별, 즉 사이버 범죄(문병학, 2004; 황영구, 2004; 한봉조, 2000; 조병인, 2001; 정완, 1999; 양근원, 2000; 강

동범, 1999; 조휘갑, 2001), 사이버 테러(김경섭, 2006; 양근원, 2003; 백광훈, 2001), 사이버전(남길현, 2004; 김성재, 2002) 등으로 구분할 수 있다. 이외에 국가사이버 안보체계 구축 전략(하옥현, 2005), 사이버공격에 대한 침해사고대응시스템의 자동화 모델 설계(최운호, 2005), 사이버전에 대비한 인력관리정책(신관근, 2004) 등의 선행연구가 있다.

이 중에서 사이버 테러와 사이버전에 관한 선행연구를 살펴보면 다음과 같다. 먼저, 사이버 테러에 관한 연구는 다음과 같다. 미국의 9.11 테러 이후 테러 문제에 대한 심각성의 인식은 사이버 위기관리 분야에서도 적잖은 연구를 짧은 기간 적지 않은 연구를 불러왔다. 특히, 테러에 대한 관심과 함께 우리나라는 사이버 테러 또는 사이버 경찰에 관한 연구로서 2000년 2월 국내 최초의 사이버테러형 웜바이러스 사건과 같은 해 경찰청 사이버테러대응센터 출범을 시작을 한 것으로 보여진다. 김경섭(2006)은 사이버테러리즘의 대응체계에 관한 연구에서 사이버테러의 사례를 분석하고 일본, 중국, 러시아 등 각국의 대응체계를 비교하고, 우리나라의 사이버대응체계를 분석하여 사이버 테러리즘 대응체계의 발전방향을 제시하였다. 양근원(2003)에서는 우리나라의 사이버테러에 대응하기 위해 법제화된 각종 법령들이 최근의 기술현상을 반영하지 못하는 등 실무현장에서 적지 않은 문제점을 가지고 있음을 지적하고 외국의 대응사례들과 비교 분석하여 우리나라의 법제도로 수용할 수 있는 방안을 제시하였다. 백종호(2002)는 주요 선진국과 우리나라의 사이버테러 대응 현황 및 문제점을 분석하고 이에 대해 사이버테러 대응 총괄체계 구축, 사이버테러 예방·대응활동 강화 방안 등을 제시하였다. 백광훈(2001)은 사이버테러리즘에 관한 연구를 통해 사이버테러리즘의 개념과 특징, 유형을 상세하게 소개하고, 사이버테러를 비롯한 사이버범죄에 대한 입법적 측면 이외의 대응방안과 입법적 대응방안을 각각 제시하였다. 특히, 백광훈(2001)은 사이버 테러의 개념을 명확하게 규정하고 그 특성과 유형을 체계적으로 정리하였다. 이윤근(2000)은 사이버테러리즘의 실태분석과 대응방안에서 21세기 정보화 사회의 가장 심각한 문제인 사이버테러리즘에 의한 피해실태와 주요 법령을 분석하고 나아가 국가 중요시설의 정보보호를 위한 미국과 일본, 중국 등 각국의 대응현황과 컴퓨터바이러스 해킹, 전자폭탄 등과 같은 주요 방법을 분석하고 대응전략으로 법·제도적인 측면과 운영적인 측면, 기술적 측면의 전략들을 제시하였다. 장석헌·최진태(1999)에서는 정보통신 수단을 이용한 사이버테러리즘의 위험에 대한 인식을 제고하고 사이버테러리즘의 공격에 노출된 분야와 사이버테러리즘의 심각성을 사전에 예상하여 그에 대한 전망과 대응방안을 제시하고 있다. 이를 위해 사이버테러리즘의 개념과 공격수단, 공격대상 등 사이버테러리즘의 본질을 검토하여 발생양상과 미국과 일본 등 국제사회의 동향을 분석한 후, 새로운 유형의 사이버테러리즘에 대한 대책을 제시하고 있다.

다음으로 국가 군사전략 차원에서 사이버전에 대한 연구이다. 남길현(2004)에서는 사이버테러전에 대비하여 국방정보보호 위협요소를 식별하고 이에 따른 장병 정보보호 필요성을 강조하면서 정보보호의식 확산교육의 목표, 기본방향, 교육방안을 제시하고 나아가 정보보호 교육방법의 발전방향을 제시하였다. 배성준(2004)은 사이버공격의 특징과 전망을 분석하여 사이버공격 대응현황 및 문제점을 도출하였으며, 이에 대한 대책으로 사전 예방적 차원의 노력, 정부·통신사업자·보안업체의 긴밀한 공동협력을 통한 새로운 개념의 방어체계 구축 방안을 고찰하였다. 김성재(2002)는 정보전 수행을 위한 한국군의 국방정보화 발전 방향에서 정보사회의 등장과 전쟁양상의 변화를 통해 국방정보화의 필요성을 인식하고 한국군의 국방정보화의 현 실태와 문제점을 분석한 후 국방정보화의 발전방향을 제시하였다. 원영제(2002)는 정보기술에 의한 전쟁 수행방식의 변화에서 정보전이 오늘날의 새로운 전장의 수행방식을 변화시켰다는 전제하에 정보전에 대한 이론과 분석 틀을 정립하여, 변화된 전쟁 수행방식으로서의 정보전 양상을 분석하고 있다. 남길현(2002)에서는 국방 사이버전 대응체계 구축방안에

서 국방정보화 중·장기 계획을 고찰하고 정보통신기반체계, 국방자원관리체계 등의 문제점과 국방전산망의 보안 위협 요소를 분석하고 보완 요구사항으로 정보보호 관리조직 및 인력 구성, 기술적 정보보호대책 등을 제시하였다. 이승구(2001)는 정보전 대비 국방부문 핵심정보자원 동원에 관한 연구에서 국가의 안보적인 측면에서의 정보전과 정보자원 동원현황을 분석하고 민간의 우수한 정보자원을 유사시 동원하여 전력화하는데 있어 필요한 제반 사항을 제시하였다. 특히, 정보전과 정보자원의 동원현황을 조사하였으며, 현재 국방부분에 필요한 지능형 정보기수로가 정보보호 보안관련 분야 등 핵심 정보기술을 분석한 후 국방정보화를 위한 민간 정보자원의 활용방안을 제시하고 있다. 김종탁 외(1999)에서는 사이버전에 대비하여 군 정보화 인력 및 보수교육 실태를 분석하여 전문인력 양성·활용 및 정보화 보수교육 방안을 제시하였다.

이처럼 사이버 위기에 관한 국내 선행연구는 각 학문 분야별로 연구가 진행되어왔다는 특징이 있다. 그리고 개인 수준에서는 개인정보 보호와 사이버 침해에 관한 연구가 주를 이루었고, 조직 수준의 연구는 사이버 범죄에 관한 연구가 주를 이루었으며, 국가 수준의 연구는 사이버 전쟁과 사이버 테러에 관한 연구가 상대적으로 많다는 것을 알 수 있다.

또한, 기존 논문의 연구 경향은 사이버 위기 연구의 짧은 역사로 인해 연구가 일정한 통계자료에 대한 재해석에 그치고 있으며 사이버 위기에 대한 대응책의 구체성이 부족하고, 현실적 어려움과 제도적 정책의 문제로 인해 종합적인 대응체제 구축에 한계가 나타나고 있다. 특히, 사이버 위기 유형별 연구를 실시함에 있어서 정책 개선방향의 제시는 통합적인 대응방안을 위주로 젊은 층 등 사이버 공간의 주 이용자에 대상을 두고 있어 사회 계층별에 따른 구체적이고 독립적인 대응체제의 부족함을 느낀다. 따라서 국내 선행연구 검토를 통하여 국가 사이버 위기관리에 관한 체계적인 연구가 필요하다는 것을 알 수 있다.

2) 해외 선행연구 검토

해외 사이버 위기관리 연구 경향을 살펴보면 다음과 같다. Alberts(2000)에서는 네트워크전의 중요한 개념과 특성을 정의하고 있으며, 이를 토대로 네트워크전에서의 수행 능력을 제고시키기 위한 방안들을 제시하였다. 즉 정보화시대에서의 안보 방안과 연합 환경 구축의 필요성을 나타내고 있다. 또한 교육과 훈련을 연계하는 통합과정과 적재적소에 자원을 배분하는 투자전략, 그리고 이들 모두를 포함하는 통합과정 등을 제시하고 있다. Molander(1996)에서는 사이버 스페이스의 급격한 변화에 대한 장래 미국의 안보전략과 정보조직을 위한 전략적 정보전의 특징과 중요성을 제시하였다. 주요내용으로는 전략정보전을 대비한 연방정부의 리더십 구축과 정부의 역할, 그리고 이를 통한 미국의 국가안보전략과 국가군사전략 등이 있다. Alberts(1996)에서는 정보기술의 도입과 유용성을 위한 전략들을 제시하였다. 주요내용은 정보기술의 발달은 군조직에 보다 완전하고 치밀한 정보를 제공하며 군조직의 변화를 초래한다고 분석하였다. 이에 정보기술의 시대에서 성공적인 군 조직 운용과 작전 수행을 위해서는 상황을 조화시키고 동시작전을 수행하는 방안을 제시하였다. Libicki(1995)에서는 정보전 유형을 지휘통제전, 정보기반전, 전자전, 심리전, 해킹전, 경제정보전, 사이버전의 7가지로 분류하고 있다. 다시 사이버전은 정보테러리즘 등으로 세분화하여, 이것이 새로운 유형인지 그리고 어느 정도 효과성이 있는지에 대해 조심스럽게 추정하고 있다.

III. 해외 주요국의 사이버 위기관리 체계 분석

1. 미국의 사이버 위기관리 체계

1) 사이버 위기관리 법체계 분석

2001년 9·11 테러는 미국의 안보체계를 개편하는 전기가 되었다. 미국은 2002년 2월 국토보안을 위한 국가안보전략(National Security Strategy of the United States of America)을 수립하여 국토안보법을 제정하고 테러 공

격으로부터 미 본토를 방어하기 위한 태세를 재정비하기 시작했다. 한편, 2006년 3월 16일 두 번째로 발표한 국가안보전략[2]에서도 안보원칙을 재천명하면서 테러예방과 차단을 주요 전략으로 채택하였다. 9·11 테러 이후 미국이 추진하고 있는 대테러 주요대책은 크게 4가지로 요약된다(박형근, 2007: 11-12).

첫째, 테러에 관한 포괄적 입법으로서 기존 대테러법을 강화한 애국법(USA PATRIOT Act 2001)[3]을 제정하여 사법집행기관 및 정보기관에 테러 차단 및 예방을 위한 강력한 수단을 제공하였으며, 2006년 5월 9일 한시법이던 애국법의 일부 조항들을 영구화 시킨 소위 애국법 II라고 불리는 「USA PATRIOT Improvement and Reauthorization Act of 2005(H.R. 3199)」 및 「USA PATRIOT Act Additional Reauthorizing Amendment Act of 2006(S. 2271)」을 통과시켜 수사와 관련한 권한 등을 강화하였다.[4] 둘째, 국토안보법을 제정[5]하여 국토안보부를 창설하고 이를 중심으로 국가 대테러시스템을 전면 개편하였다. 현재 국토안보부에는 약 18만명에 달하는 인력이 근무하고 있는데, 이는 펜타곤 다음가는 거대한 조직이다. 셋째, 정보기구 개혁 및 테러방지법 2004(The Intelligence Reform and Terrorism Prevention Act of 2004)을 제정하여 국가정보국장(Director of National Intelligence: DNI) 직을 신설하고 정보업무와 관련된 15개 기관의 정보프로그램을 감도하도록 하였으며, DNI 산하에 국가대테러센터(National Counterterrorism Center: NCTC)를 설치하였다. 넷째, 미국내 모든 법집행 기관간 정보공유를 의무화하여 효율성을 기하도록 하는 한편, 미국 출입국자에 대한 여권·비자 프로그램을 설치하고 항공기·선박에 대한 보안검색 시스템을 개선하도록 강제하고 있다.

2) 사이버 위기관리 조직체계 분석

(1) 미국의 정보보호 정책 추진체계와 국가기반보호계획(NIPP)

미국의 정보보호 정책의 효시는 1988년 DARPA의 주도로 CMU 내 침해사고대응팀조정센터(CERT/CC)가 설치된 것이라고 볼 수 있다. 그 후, 인터넷이 보급되면서 1996년 대통령 직속 주요기반보호위원회(President's Commission on Critical Infrastructure Protection: PCCIP)가 설치되었다. 또한 1988년에는 클린턴 대통령에 의해 연방수사국(Federal Bureau of Investigation: FBI)의 국가기반보호센터(National Infrastructure Protection Center: NIPC)나 상무부에 주요기반보증국(Critical Infrastructure Assurance Office: CIAO)이 설치되었다(민경식 외, 2006: 28-29). 그 후 부시 정권 초기 정보보호 정책은 9·11사태를 계기로 변화하게 되었다. 2001년 10월에는 백악관에 사이버보호실(Office of Cyber Security)과 대통령 직속 주요기반보호위원회(President's Critical Infrastructure Protection Board: PCIPB)가, 2002년 11월에는 국토안보부(Department of Homeland Security: DHS)가 설립되어 사이버보안에 대한 정책을 강화했다. 그리고 2008년 현재는 대통령 직속 국토안보회의(President's Homeland Security Advisory Council: PHSAC)가 대통령에게 국토안전보장에 관한 조언을 하고 있다.

또한 미국 정부는 정보보호 강화 추진을 위해 정보를 철저하게 공개 또는 공유하게 하고 신뢰성을 향상시키는 대책을 실시하고 있다. 2000년에는 정부정보보호개혁법(Government Information Security Reform Act: GISRA)이 제정되어, 각 정부기관은 예산 제정 절차의

---

2) 주요 내용 중에서도 '21세기 도전과 기회에 적응할 수 있는 미국 국가안보기구의 개혁'이 이 연구와 관련하여 의미있는 부분이다. 자세한 내용은 박형근(2007: 11)을 참조할 것.

3) 정식명칭은 'Uniting and Strengthening America by Providing Tools Required to Intercept and Obstruct Terrorism' 이다.

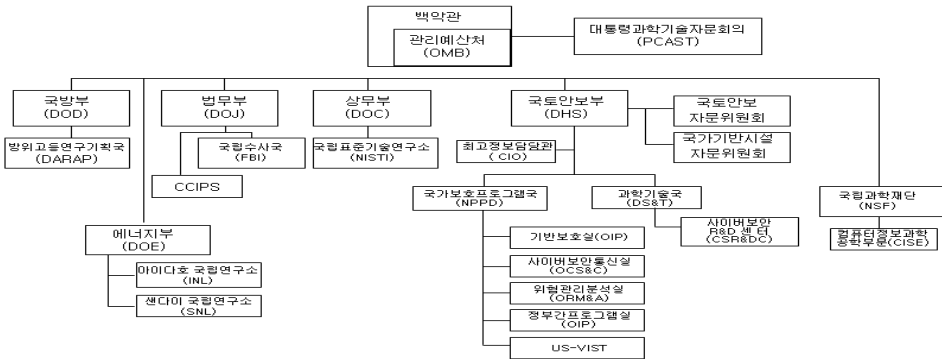
4) 2001년 제정한 PATRIOT ACT는 2005년 12월 30일 종료되는 16개조항의 한시적 규정에 대한 영구화 여부를 놓고 두 차례나 시한을 연장해가며 논란을 벌이다가 2006년 5월 9일 최종 개정되었다.

5) http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm & http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf(검색일, 2008.8.28).

일환으로서 관리예산처(Office of Management and Budget: OMB)에 보호 대책의 상황을 보고하도록 하였다. 2002년에는 연방정보보호관리법(Federal Information Security Management Act of 2002: FISMA)이 제정되어, 현재 OMB와 NIST가 정보보호를 담당하고 있다.

국보안보부(DHS)는 국토안보 대통령령 7호(HSPD-7)를 근거로 국가기반구조와 주요자원(Critical Infrastructure/Key Resource: CI/KR)보호를 개선하기 위해 2006년 6월 국가기반보호계획(National Infrastructure Protection Plan: NIPP)을 발표하였다. 본 계획은 유비쿼터스 시대를 대비하기 위해 미국이 최근 발표한 핵심 정보보호전략이라고 볼 수 있다(민경식 외, 2006: 29-31). 이 계획은 전체 7개의 장으로 구성되어 있으며, 국가기반구조와 주요자원(CI/KR) 보호 프로그램을 구현하기 위한 보안 협력모델 수립, 장기적 위험 감소 프로그램 실행, 국가기반구조와 주요자원(CI/KR) 보호를 위한 자원의 효율적 사용 극대화를 목표로 하고 있다. 이를 위해 에너지, 물, 식량, 의료, 교통 및 IT 시스템과 같은 국가의 핵심자산 및 자원을 보호하기 위한 민간부문과의 협력관계를 규명하는 프레임워크(framework)를 포함한다.

국토안보부는 국가기반보호계획(NIPP)에서 기반구조부문조정위원회(Sector Coordinating Council: SCC) 및 정부부처조정위원회(Government Coordinating Council: GCC)를 운영하고, 핵심 기반구조의 소유자와 운영자에게 정보를 제공할 수 있는 프로토콜을 구현할 것을 밝히고 있다. 또한, 모든 17개 기반구조부문을 위한 국토안전보장정보네트워크(Homeland Security Information Network: HSIN)를 가동시키고, 국가기반보호계획(NIPP) 인식제고 계획도 수립하여 수행할 예정이다.



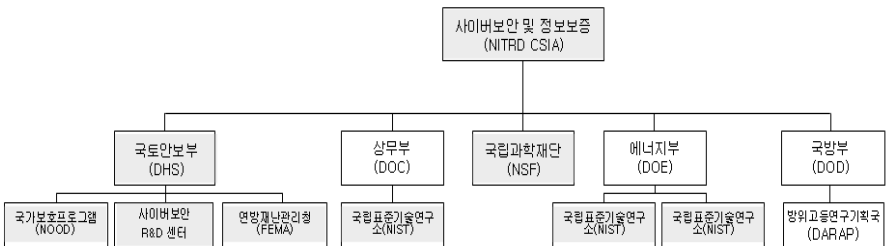
<그림 1> 미국의 정보보호 정책추진 체계

(2) 주요 정보보호 기관

미국은 정보보호 주무부처가 없는 대신 연방정부 수준에서 사이버보안 연구 개발 정책을 감독하고 조정한다(민경식 외, 2007: 47-49). 이 중 사이버보안 R&D 정책 조정의 핵심역할을 수행하는 곳은 2005년 8월에 설립된 '네트워킹 및 IT 연구개발(Networking and Information Technology Research and Development: NITRD)'의 사이버보안 및 정보보증(Interagency Working Group for Cyber Security and Information Assurance: CSIA) 부처간 실무그룹(IWG)이다. 위원들은 상무부(NIST 포함), 국방부(NSA, DARPA 포함), DHS, NSF, 에너지부, 법무부, 국무부, 교통부, 연방항공청, 재무부, NASA, 국립보건원 등이다(민경식 외, 2007: 47). CSIA IWG의 주요 기능은 부처간 프로그램의 기획 지원, 로드맵 설정 및 주기적 업데이트, 연방정부 정책 및 우선과제 수립을 위한

권고 마련, NITRD 프로그램의 예산증액을 위한 연간활동 요약 등으로, NITRD 소위원회와 인프라 소위원회에 보고한다. 그러나 직접 연구개발 과제를 수행하지는 않고 부처·기관의 연구개발 정책 및 프로젝트 조정만을 다룬다.

이렇게 연방정부 수준에서 조정된 연구 주제는 DHS, NIST, NSF, 에너지부, DARPA 등에 의해 수행된다. 주요 분야는 민간영역과 국방영역으로 구분할 수 있다. 육·해·공군연구소 등 국방부 연구조직도 사이버보안 프로그램을 갖추고 있지만, DARPA와 NSA를 중심으로 사이버보안 R&D 프로그램을 수행하고 있다. DARPA는 국방부의 중앙 R&D 조직으로 군사 목적의 혁신적이고 비용이 큰 연구를 지원하며 주로 3년에서 5년 이하의 단기적인 기밀 R&D 수행하고 있다. 그리고 NSA는 정보시스템 보안프로그램(Information Systems Security Program)과 통합 위조방지 프로그램(Consolidated Cryptologic Program)을 통해 사이버보안 연구자금을 지원하며 고속 암호화 및 특정 방어기능에 초점을 두고 있다(민경식 외, 2007: 48). 미국 사이버보안 연구의 주요 초점은 테러와의 전쟁을 위한 사이버공간 방어 연구라고 할 수 있다. 그러나 미국의 대부분 프로그램은 정부에 의한 연구개발이라도 정부기관이 독립적으로 수행하는 것이 아닌, 민간기업, 비영리연구소, 대학 부설연구소 등과 공동연구 및 위탁연구 형태로 추진되고 있다. 미국의 정보보호 연구개발의 체계를 나타내보면 다음 <그림 2>와 같다.



자료: 민경식 외(2007: 49) 수정.

<그림 2> 미국의 정보보호 연구개발 체계

국토안보부는 사이버보안과 안전한 차세대 정보통신 시반시설을 구축하기 위한 연구개발을 수행하고 있으며, 과학기술국(Directorate for Science and Technology)이 연구개발을 총괄 담당하고 있다. 정보보호 연구과제는 대부분 단기과제이며 연구개발의 일부는 NSF와 공동으로 실시하고 있다. DHS에서 진행하고 있는 사이버보안 관련 프로그램으로는 과학기술국 산하 사이버보안 R&D 센터(Cyber Security R&D Center) 운영이 대표적이다. 사이버보안 R&D센터는 2004년 3월 DHS에 의해 설립되어 미국의 사이버 인프라 보호를 위한 보안기술을 개발하고 있다. 즉 센터는 정보통신, 교통, 우편과 선박, 위기서비스, 그리고 국가유지를 포함하는 국가핵심기반에 대한 실질적인 보호를 확보하기 위한 DHS의 책임을 지원한다. 센터는 DHS 과학기술 안보프로그램 관리자(the DHS S&T Cyber Security Program Manager)의 감독하에 있는 독립적이며 비영리 연구기관인 'SRI International'에 의해 운영된다.

2. 영국의 사이버 위기관리 체계

1) 사이버 위기관리 법체계 분석[6]

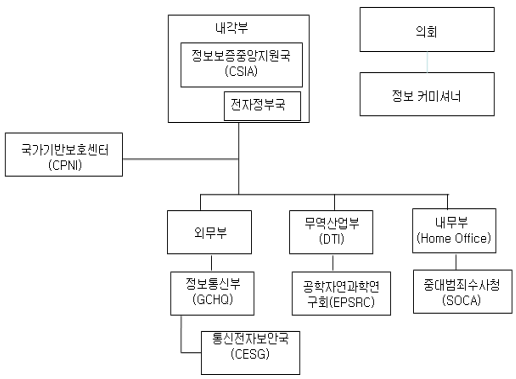
영국은 기존의 테러방지법이 전시에 준한 임시적 성격을 띤 법이었기 때문에 강력한 제재조치를 지니고 있었고, 이는 인권침해의 가능성이 높았다. 이러한 문제점을 해결하기 위하여 2000년 7월 20일 새로운 테러법(Terrorism Act 2000)을 제정하여 2001년 2월 19일부터 시행하고 있다. 이 법은 기존의 테러방지법이 북아일랜드 사태에 초점을 맞춘 임시법적 성격을 가진 것인데 비

6) 공성진(2007: 21)을 참조하였음을 밝힌다.

해 영구적인 성격의 법으로 대체하였다는데 의미가 있다. 이 법은 민사적 입증책임의 분배의 원칙에 따른 테러단체 통화의 압수와 금융기관에 대한 테러수사 목적의 예금계좌 확인 요구권을 신설하는 등 테러에 대한 수사권을 강화하고 처벌을 위한 절차상 특례를 인정하였다. 또한 범위를 넓혀 영국을 기반으로 자행되는 모든 국제테러활동에 대해 단속을 가능하도록 하였다. 이와 같이 영국은 북아일랜드 문제에 대응하기 위하여 테러대책을 수립하고 있었으나 9·11 테러가 발생하면서 이러한 수단 외에 테러를 방지하기 위한 강력한 법적인 대책을 수립하였다. 2001년 12월 14일 반테러리즘, 범죄 및 안전법(Anti-terrorism, Crime and Security Act)을 제정하여 테러범죄자에 대한 자산동결, 출입국관리, 병원체 및 독극물 통제, 통신자료 취득 등에 관한 기존의 규정을 개정하여 테러에 관한 수사권을 강화하고 있다.

2) 사이버 위기관리 조직체계 분석

영국의 사이버 위기관리(네트워크 및 정보보호)는 주로 내각부가 주된 책임을 지닌다(민경식 외, 2006: 79). 특히, 내각부의 정보보증중앙지원국(Central Sponsor for Information Assurance: CSIA)은 정보보호 관련 활동에 대해 정부 전체를 조정하는 역할을 하고 있다.



<그림 3> 영국의 주요 사이버위기관리 기관

(1) 국가기반보호센터(CPNI)[7]

영국은 국가기반시설보안조정센터(National Infrastructure Security Co-ordination Centre: NISCC)를 중심으로 사이버 테러 및 전자침해사고에 대비해 왔다. 즉 영국 내각장관(Home Secretary)은 정부부처·기관 및 민간 분야 조직을 대상으로 전자적 공격으로부터 국가핵심기반(Critical National Infrastructure)을 보호하기 위하여 1999년 12월 20일 NISCC를 창설하였다. NISCC는 주로 통신, 에너지, 금융, 교통, 중앙정부, 상하수도, 보건서비스, 비상사태 서비스 등 국가주요기반시설을 위한 주요 IT시스템 보호를 주요 업무로 하고 있었으며, 2007년 2월에는 국가기반시설보안조정센터(NISCC)와 MI5(the UK's Security Service) 그리고 국가보안자문센터(National Security Advice Centre: NSAC)를 통합하여 국가기반보호센터(Centre for the Protection of National Infrastructure: CPNI)를 신설하였다.

국가기반보호센터(CPNI)는 국가기반을 구성하는 업무와 조직에 통합된 보안자문을 제공하는 역할을 수행한다. 즉 보안자문을 통하여 CPNI는 테러리즘과 다른 위협(threats)에 대한 국가기반의 취약성(vulnerability)을 감소시킴으로써 국가안보를 보호한다. CPNI는 많은 정부부처와 기관으로부터 자원을 얻는 범 부처조직(interdepartmental organization)이다. CPNI는 MI5, 전자통신보안국(Communications Electronics Security Group: CESG), 그리고 국가기반에 대한 책임을 지고 있는 다른 정부부처들을 포함한다.

CPNI 자문은 국가핵심기반을 주요 목표로 하고 있다. 이러한 국가핵심기반의 주요 요소들은 국가가 필수적 서비스 전달을 유지하는데 핵심적이다. CPNI의 주요역할은 국가의 기본적인 서비스인 통신, 긴급서비스, 에너지, 재정, 식품, 정부, 보건, 운송 및 수자원을 더 안전하게 보호하기 위하여 테러리즘과 다른 위협으로부터 국가기반의 취약성을 저감하는 것이다. 또한 CPNI는 테러리스트와 다른 공격에 대한 취약성을 줄일 수 있는 어플리케이션(applications)를 개발하고 공격이 일어났을 때의 영향

7) http://www.cpni.gov.uk/(검색일, 2008. 11. 8)

을 줄일 수 있도록 하기 위하여 학술연구기관의 연구와 성과, 다른 정부기관, 연구소 및 민간부분으로부터 지원을 받는다.

(2) 영국 전자통신보안국[8][9]과 주요 조직

영국 전자통신보안국(Communication-Electronics Security Group: CESG)은 통신본부(Government Communication HeadQuarters: GCHQ)에 소속되어 있으며, 정보보증(Information Assurance: IA)을 담당한다. CESG는 정보공유를 안전하게 할 수 있는 환경을 만드는 것을 목적으로 하며 정부부처 및 공공기관 그리고 군을 대상으로 하지만 다양한 민간 회사들에게도 관련 서비스를 제공해준다. 특히, 전력·수도·보건 등 중요한 기반시설과 공공시설들이 주요 대상이 된다.[10] CESG는 통신과 전자 데이터의 보안을 위한 권고(Advice)와 지원을 제공함으로써 영국의 중요한 비밀들을 보호하는 것을 목적으로 한다. 이를 위해 정부와 중요한 다른 정보 소비자들에게 중요한 정보보호를 위한 정보보증 정책 및 관련 서비스를 다양한 방법으로 제공한다.

국립하이테크범죄국(National Hi-Teck Crime Unit: NHTCU)은 지난 2001년 4월 컴퓨터 범죄수사를 목적으로 창설되었으며, 영국에서 발생하거나 영국에 영향을 미치는 모든 인터넷 범죄 및 하이테크 범죄를 담당하며 CPNI·UNIRAS[11]뿐만 아니라 미국 NIPC(National Infrastructure Protection Center)와도 업무 공조를 하고 있다. 또한, 정부와 기업 간 협력관계를 증진시키기 위해 노력하고 있는데, 새로운 전자범죄에 대항하기 위해 기업의 기밀성 유지를 위한 강령(Confidentiality Charter) 등을 발표한 바 있다. 주요 임무는 심각하거나 조직화된 하이테크 범죄에 대항하기 위한 대응활동 지원, 국가기반시설에 대한 모든 심각한 위협에 대한 수사, 전략적인 위협성 평가업무 수행, 법 집행업무 지원 및 공동대응, 법 집행기관 및 사업자에 대한 조언 제공 등이다. NHTCU는 NCS(국립범죄수사대, National Crime Squad)로부터 지원받은 수사관, 포렌식 전문가, 컴퓨터 컨설턴트 등이 다수 소속되어 있으며, 하부조직은 크게 범죄수사부, 정보부, 전자증거부, 기술지원부의 네 부분으로 나뉘어져 있다. 범죄수사부는 조직화되거나 심각한 하이테크 범죄를 수사하고 법원 지원을 담당한다. 정보부는 영국의 모든 법 집행기관과 정보기관들을 위하여 전략적·전술적 정보를 제공한다. 전자증거부는 NHTCU에 의해 수행되는 하이테크 범죄수사를 위한 포렌식 기술을 지원한다. 그리고 기술지원부는 법원이나 정부를 위한 기술지원과 컨설턴트를 담당한다.

중대조직범죄수사청[12](SOCA: The Serious Organised Crime Agency)는 2006년 4월 1일 신설되었다. 주요 목적은 영국에 심각한 조직화된 범죄에 의해 가해지는 해(harm)를 줄이는 것이다. SOCA는 2005년 심각한 조직화된 범죄 및 경찰법(the Serious Organised Crime and Police Act 2005)에 근거하여 만들어 졌다. SOCA는 내무부(Home Office)에 의해 지원되지만 운영

8) 이하 내용은 국가사이버안전센터 홈페이지(www.ncsc.go.kr, 검색일, 2008. 8. 20)의 센터자료실-해외유관기관에 올라와 있는 해외 사이버테러 대응기관 소개 중 영국관련 내용(Monthly 사이버시큐리티, 41-48)을 참조하였음을 밝힌다.

9) 홈페이지는 www.cesg.gov.uk이다.

10) CESG는 그 기원을 따지면 80년 이상의 긴 역사를 가지고 있다. 1919년 GC&CS (Government Code and Cipher School)의 설립으로 시작하여, 1950년대 LCSA(London Communications Security Agency)로 발전하였고, 1965년 LCSA는 CESD(Communications-Electronics Security Department)로 조직이 확대되었고, 1969년 CESD는 GCHQ와 조직적으로 통합되어 CESG로 명칭이 변경되었다. 1978년 런던에 근거지를 두고 있었던 본부를 GCHQ가 위치한 Cheltenham으로 이전하였고, 1997년 이후 CESG는 비용회수(Cost-recovery) 원리에 의해 제공한 정보보안 보증 서비스 대부분에 대해서 과금정책을 적용하고 있다.

11) UNIRAS는 1992년 영국 전자통신보안국(CESG)의 주도로 영국 정부 컴퓨터 침해사고대응팀(UK Government CERT)으로 설립되었으며, NISCC 설립과 동시에 NISCC에 통합 운영되어 오다 2007년 2월 CPNI가 신설되면서 CPNI에 흡수되어 운영되고 있다. UNIRAS의 사고대응업무 대상기관은 원래 정부부처 및 기관이었으나 최근 보안 관련 민감한 업무를 다루는 정부 계약자 및 국가 주요기반시설 운영조직 등으로 크게 확대되었다.

12) http://www.soca.gov.uk/ (검색일, 2008. 11. 8). http://www.soca.gov.uk/downloads/annualPlan.pdf 참조.

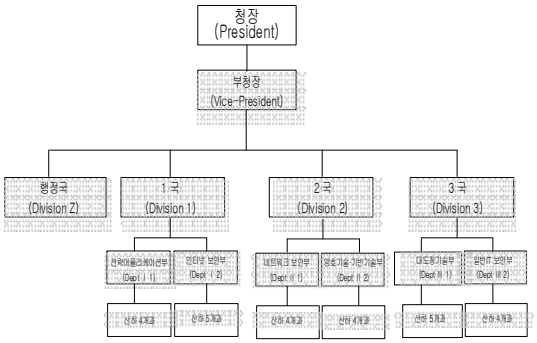
은 독립적인 비정부공공조직(Non-Departmental Public Body)으로 집행기관이다. SOCA는 SOCA가 법적 책임을 지고 내각장관(Home Secretary)에 의해 수립되는 전략적 우선순위를 충족시키도록 하는 책임을 지는 위원회에 의해 운영된다.

3. 독일의 사이버 위기관리 체계

1) 사이버 위기관리 법체계 분석[13]

독일은 유럽에서 가장 먼저 테러범죄자를 처벌하기 위한 법적 조치를 강구하여 실체법적 측면에서 테러범죄의 처벌범위를 확대하고 형량을 높이는 한편, 절차법상으로는 테러범죄자인 피의자 또는 피고인의 권리 및 수형자로서의 권리를 현저히 제한하는 규칙을 제정하였다. 1971년 테러가 형법에 규정되기 시작한 이래 본격적인 입법적 조치가 취해지기 시작한 것은 1976년 4월 22일의 제14차 형법개정이었다. 독일에서 테러와 관련하여 처벌되는 행위는 1976년 대테러법에 의하여 테러단체를 조직하는 행위가 처벌대상이 되었다. 이는 범죄단체조직에 대한 특별구성요건으로서의 성격을 지닌다. 이는 사전에 테러를 막는다는 전략에 기인한 것으로 독일의 테러전략의 중심적인 조항이다. 독일정부는 2001년 9·11 테러를 계기로 한층 강화된 테러대책을 수립하였는데, 그 주요내용은 테러 대책을 위한 재정확보, 법개정을 통한 효율적인 테러기관의 권한 강화, 신원확인, 주요시설의 보안강화 등이다. 이에 따라 국제테러대책법이 제정되어 2002년 1월 1일부터 발효되었다. 그 주요내용으로는 무엇보다 외국 테러단체에 대한 처벌의 확장이었다.

13) 공성진(2007: 28-33)을 참조하였음을 밝힌다.



자료: www.niscc.go.kr (검색일, 2008. 8. 20).

<그림 4> BSI의 조직도

2) 사이버 위기관리 조직체계 분석[14]

독일의 사이버테러 대응기관으로는 IT Security를 통해 정보통신기술의 신뢰를 조성하고, 정보화 사회의 기회를 완벽하게 이용하기 위해 1991년 설립된 연방보안기술청(Bundesamt fur Sicherheit in der Informationstechnik: BSI)[15]을 들 수 있다. BSI는 독일 연방정부가 1989년 6월 발표한 IT 정책의 일환으로 BSI 설립을 위한 법령이 제정(1990)되고, 1991년 1월 1일 설립되었다. 최근 정보보호 정책 중 주목해야 할 것은 "Bund Online 2005"라 불리는 전자정부 정책이다. 이 정책은 정부 서비스를 온라인으로 제공하기 위해 정보통신기술을 강화하는데 있다. 이 같은 목적으로 BSI는 공공서비스의 전자적 제공을 위한 정보보호의 모든 측면을 다룬 전자정부 매뉴얼을 개발해야 할 책임을 지는데, 안전한 인터넷 보호, 전자정부를 위한 네트워크 플랫폼, 암호화와 전자서명, 전자정부에 있어서의 인증과 같은 기술적 과제를 담당하고 있다(민경식 외, 2006: 80).

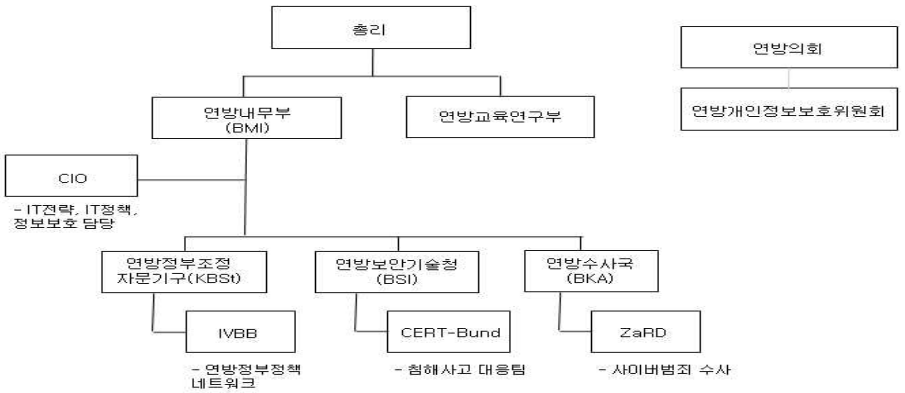
연방보안기술청(BSI)은 행정국과 1국, 2국, 3국의 4개 국으로 구성되어 있다. 1국에는 전략어플리케이션부와

14) 이 내용은 국가사이버안전센터 홈페이지(www.ncsc.go.kr, 검색일, 2008. 8. 20)의 센터자료실-해외유관기관에 올라와 있는 해외 사이버테러 대응기관 소개 중 독일관련 내용(Monthly 사이버 시큐리티, 59-64)을 재정리한 것이다.

15) BSI(Bundesamt fur Sicherheit in der Informationstechnik)는 영문으로'Federal Office for Security in the Information Technology'라는 뜻으로 독일 내무부 산하의 '연방보안기술청'이란 뜻이다.

인터넷 보안부가 있다. 2국에는 네트워크 보안부, 암호기술·기반기술부가 있다. 그리고 3국에는 대도청기술부와 일반 IT 보안부가 있다. 연방보안기술청(BSI)의 주요 기능으로는 정보보호업무를 주관하는 것이다. 구체적으로는 IT 기술사용에 따른 위험 조사 및 정보보호기술의 발전, IT system의 Security에 대한 평가 및 인증, 생산자, 유통업자, 소비자에 IT기술의 사용관련 조언, IT 기술의 발전 및 방향 분석, E-Government 지원, 독일 CERT, 국제 보안기준에 기초한 IT 시스템 인증, 컴퓨터 바이러스, 인터넷 보안, 주요 정보통신기반·IT 기반시설 보호, 수행 프로젝트: SINA, Sphninx, 전자서명, ElcrroDat 6-2, 보안교육 등을 수행하고 있다.

독일의 연방정부 기구 중 연방정부조정자문기구(The Federal Government Coordination and Advisory Agency for IT in the Federal Administration)도 정보보호 정책에 대한 기능을 하고 있다. 연방정부조정자문기구는 정부기관 전체를 조정하는 곳이지만 조직적으로는 연방내무부에 속해 있다. 연방정부조정자문기구는 연방기관에 IT전략과 솔루션의 설계 및 시행과 관련된 자문을 제공한다. 연방정부조정자문기구는 베를린과 본에 위치한 헌법기구 간의 보안통신을 제공하는 본-베를린 정보기술공동체(IVBB)의 운영도 담당하고 있다. 1999년에 설립된 IVBB는 현재 독일 연방기관들이 이 연방 네트워크에 접속할 수 있도록 해주는 연방행정정보망(IVBV)으로 확대하려 하고 있다고 한다(민경식 외, 2006: 81).



<그림 5> 독일의 주요 사이버 위기관리 기관

4. 일본의 사이버 위기관리 체계

1) 사이버 위기관리 법체계 분석

9·11 테러 이전에는 일본의 테러범죄에 관한 법적 규정은 없었다. 다만 실무상으로 "테러리즘이란 널리 공포 또는 불안을 느끼게 함으로써 그 목적을 달성하기 위하여 행하는 극좌 기타의 주장에 근거한 폭력주의적 파괴활동"이라고 정의하고 있었다(경찰청조직령, 제17조의 2). 또한 그러한 테러리즘이 외국인 또는 외국에 활동의 본거지가 있는 일본인에 의해서 행해지는 경우를 국제테러리즘이라고 규정하였다. 따라서 중핵파 등 일본 국내 극좌폭력집단이 외국에서 테러사건을 감행하여도 여기서 말하는 국제테러리즘의 범주에 속하지 않았다.

그러나 9·11 테러 이후 테러특별조치법을 제정하여 자위대의 활동 범위를 타국 영토까지 확대하고, 자위대의 전투 시 해외 파견을 처음으로 허용하는 등 적극적인 대응을 하고 있으며, 정부차원의 테러방지 대책이 추진되는 등 적극적인 움직임을 보이고 있다. 즉 2001년 11월 2일 미군 주도의 테러 보복공격을 자위대가 후방 지원하기 위한 '테러대책 특별조치법'을 제정하고, 일본 내 미군시설 등을 자위대가 경비할 수 있도록 한 '자위대법개정

안'과 의심 선박에 대한 선체 사격을 허용하는 '해상 보안청법 개정안'도 통과시켰다. 이 법의 제정과 관련하여 해외에 자위대를 파견하는 행위가 전쟁포기를 선언하고 있는 헌법 규정(일본 헌법, 제9조)에 위배되는 것이 아닌가 하는 점에 대하여 많은 논쟁이 있었다.

테러특별조치법은 2년간의 한시법으로 자위대의 활동 범위를 타국 영토까지 확대하고, 자위대의 전투 시 해외 파견을 처음으로 허용한 것이 특징이다. 또한 자위대법과 해상 보안청법을 개정하면서 주로 경찰관직무집행법의 범위 내에서 사용되던 자위대원과 해상보안청 직원의 무기사용 범위를 완화하였으며(특별조치법, 제12조), 자위대의 정보수집 권한 강화 및 주요시설 경호를 위한 출동권한 부여 등을 통하여 테러행위에 대한 신속하고 적극적인 대응이 가능하도록 제도 변화를 두었다. 아래의 내용은 일본의 정보화 및 사이버테러 대응관련 법규와 제도 및 기구의 연혁이다.

<표 2> 일본의 정보화 및 사이버테러 대응관련 법규·제도·기구 연혁

년도	일본의 정보화 및 사이버테러 대응관련 법규 · 제도 · 기구 연혁
1985. 1	「시스템감사기준」 공표(1996.1 개정)
1994. 8	「고도정보통신사회추진본부」 내각 설치
1995. 7	「컴퓨터바이러스대책기준」 고시(통산성)
1996. 8	「컴퓨터부정엑세스대책기준」 고시(통산성)
1999. 8	「부정엑세스행위의금지등에관한법률」 제정(우정성산성·경찰청)
1999. 11	「소프트웨어관리가이드라인」 공표
2000. 2	내각관방 산하 내각위기관리감실에 「정보시큐리티대책추진실」 설치
2000. 5	「전자서명및인증업무에관한법률」 제정(우정성·통산성·법무성)
2000. 7	「정보통신기술(IT) 전략본부」 설치
2000. 11	「IT 기본전략」 결정
2000. 12	「중요인프라의 사이버테러 대책에 관한 특별행동계획」 발표 → 내각관방장관(정보시큐리티대책추진실) 중심 자율적인 민관 대책유도
2001. 1	「고도정보통신네트워크사회형성기본법」 제정 →「e-Japan 전략」 수립 : 향후 5년내 세계 최첨단 IT 강대국실현 목표
2001. 3	「e-Japan 중점계획」 발표
2001. 6	「e-Japan 2002프로그램」 발표
2001. 11	「e-Japan 중점계획」, 「 e-Japan 2002 프로그램」의 가속·조기집행 발표
2002. 4	「정보시큐리티대책추진실」에 NIRT(National Incident Response Team) 설치
2002. 6	「e-Japan 중점계획 2002」 발표
2002. 8	「주민기본대장네트워크」 가동(전국민에게 11자리 주민코드 부여)
2002. 11	전기통신의 적정이용을 위한 규칙정비(제15차 IT전략본부회의)
2003. 5	초고도 정보통신네트워크사회 구축을 위한 7개 중점분야 결정(IT전략본부) → 의료, 식생활, 생활, 중소기업금융, 지식개발, 취업·노동, 행정서비스
2003. 7	「e-Japan 전략II」 발표('전자정부 구축계획-2003'동시발표)
2003. 8	「e-Japan 중점계획-2003」 발표
2004. 2	「e-Japan 전략II」 가속화계획 발표 → 2006년까지 정보보안, 행정, 국민생활 등 사회 전반적인 분야에서 IT 전자화의 집중추진

자료: www.niscc.go.kr(검색일, 2008. 8. 20).

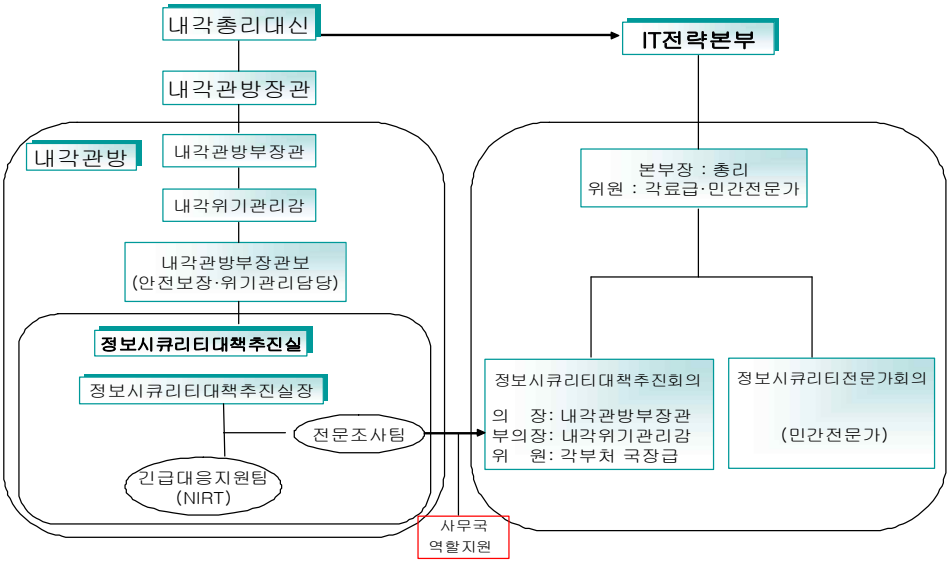
2) 사이버 위기관리 조직체계 분석[16]

일본의 사이버테러 대응 조직은 내각관방 정보시큐리티대책추진실, 내각 고도정보통신네트워크사회추진 전략본부(일명 IT전략본부), 경찰청, 총무성, 경제산업성 및 일본컴퓨터긴급대응센터(JPCERT/CC) 등 민간기관으로 구성되어 있다.

(1) 내각관방 정보시큐리티대책추진실

정보시큐리티대책추진실은 인터넷의 급속한 이용확대 등 국민생활의 IT발전에 따른 부정엑세스(해킹), 컴퓨터 웜바이러스 확산 등에 대처하기 위해 2000년 2월 내각관방장관 산하에 설치되었다. 주요 역할은 각 정부부처와의 협력을 도모하고 민관 전문가로 구성된 비상근 팀의 조언을 받아 전자정부의 정보보호 확보 및 중요인프라 사이버테러 대책 등 민·관의 정보보호 확보를 위한 정책추진을 총괄·전담하고 있다.

16) 이하 내용은 국가사이버안전센터 홈페이지(www.ncsc.go.kr, 검색일, 2008. 8. 20)의 센터자료실-해외유관기관에 올라와 있는 해외 사이버테러 대응기관 소개 중 영국관련 내용(Monthly 사이버 시큐러티, 66-72)을 참조하였음을 밝힌다.



자료: www.nisсc.go.kr (검색일, 2008. 8. 20).

<그림 6> 일본정부의 정보시큐리티 정책·조직체계 조직도

또한, 내각총리대신 산하 '내각 고도정보통신네트워크사회추진 전략본부(IT전략본부)'에 설치된 정보시큐리티대책추진회의와 민간전문가로 구성된 정보시큐리티전문조사회의 사무국을 담당하면서 각 부처 업무조정을 하고 있다.

(2) 내각 고도정보통신네트워크사회추진 전략본부(IT전략본부)

정보통신 기술의 활용에 따라 세계적인 규모로 진행중인 급격하고도 대폭적인 사회경제구조의 변화에 신속정확하게 대응할 필요성을 고려, 고도정보통신네트워크사회의 형성에 관한 시책을 신속하고도 중점적으로 추진하기 위해 2001년 1월 내각에 설립되었다.

전략본부는 고도정보통신네트워크사회 형성에 관한 중점계획을 작성, 그 시행을 추진하며, 그 외 고도정보통신네트워크사회의 형성에 관한 중요시책을 심의하고 이를 위해 사안별 민·관 전문가를 소집, '전문조사회'를 운영한다. '시큐리티대책추진회의'는 내각관방 부장관을 의장, 내각위기관리감을 부의장으로 하여 정부부처 국장급으로 구성되며, 정보보호 대책추진을 전담하고 있으며, '정보시큐리티전문조사회'는 민간전문가들로 구성되어 민관분야의 정보보호 대책 추진에 관한 사항의 조사, 검토를 전담하고 있다. '각부처 정보화총괄책임자(CIO)연락회의'는 2003.7월 「전자정부구축계획(案)」과 관련 공공 앙케이트 조사를 실시한 바 있으며, 'IT 전략의 향후 바람직한 방향에 관한 전문조사회'를 수시 운영하고 '평가전문조사회'는 「e-Japan전략II」에 관한 정부의 추진상황 평가 등을 수행한다.

(3) 경찰청 사이버포스센터(Cyber Force Center)

하이테크범죄·사이버테러를 예방하고 피해확대를 방지하기 위해 2001년 경찰청 정보통신국 사이버테러대책기술실에 설치되었으며 범죄수사 등의 지원을 위해 동경에 센터를 두고 오사카·나고야·히로시마·후쿠오카·센다이·삿포로·사이타마·타카마츠 등 전국 8개 관할 경찰국내에도 설치되었다.

전국 경찰기관에 설치되어 있는 인터넷 접속점의 IDS를 24시간 감시하여 관련정보를 수집·분석하는 관제장비인'검지(檢知)네트워크시스템'을 운영하여 사이버테러 조기탐지 및 긴급대응 업무와 함께 관련분야 연구개발과

전문인력에 대한 교육훈련을 실시하고 있다.

또한, 긴급출동차량에는 현장 활동에 필요한 각종 분석컴퓨터, 백업장치, 과학수사장비, 자가발전기 등을 구비하여 활동하고 있다.

(4) 총무성

총무성 정보통신정책국 정보유통진흥과는 '국민을 위한 정보시큐리티사이트'[17]를 개설하고 일반 국민이 안심하고 인터넷을 사용할 수 있도록 정보보호 필요성, 기초지식, 용어설명, 실제 일어날 수 있는 사고·사례를 소개하고, 이용 대상별 정보보호대책을 구분하여 최종사용자(학생·일반이용자), 홈페이지개발자(인터넷서비스제공업체, 사설서버이용자), 기업·조직 업무이용자(직원·정보관리담당자) 등을 대상으로 상세한 보안대책을 제시하고 있다.

또한, 정보시큐리티 홈페이지[18]를 개설하여 정부정책과 관련된 정보시큐리티 예산, 중요공지사항, 정책보고서 등을 홈페이지에 게시하고 중요한 취약점·보안권고사항의 경우 내각관방·경찰청·총무성·경제산업성이 보도자료 형식으로 공동발표하고 있다.

(5) 경제산업성

경제산업성은 '정보시큐리티에 관한 정책, 긴급정보사이트'[19]를 운영 중인데, 일본 정부의 각종 IT정책은 물론 정보보호통합전략 등을 한곳에 모아 놓은 종합포탈사이트로 정보보호 각 부문별 상세자료를 수록하고 있다. 그리고 전자서명과 정보보호 평가·인증, 암호기술평가, 정보보호감사제도, 사업소인증제도 등을 비롯한 관련법규, 가이드라인 등과 함께 각종 정보보호 기구·협(의)회·센터 등을 링크로 제공하고 있다.

Ⅳ. 한국의 사이버 위기관리체계 분석

17) http://www.soumu.go.jp/joho_tsusin/security/index.htm

18) http://www.soumu.go.jp/joho_tsusin/security/security.html

19) http://www.meti.go.jp/policy/netsecurity/index.html

1. 국가사이버 위기관리 법체계

한국의 사이버 위기관리에 관한 법체계는 국가사이버안전관리규정(대통령훈령, 제222호), 정보통신기반보호법(법률, 제8852호), 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률, 제8867호), 산업기술의 유출방지 및 보호에 관한 법률(법률, 제8900호), 소프트웨어산업진흥법(법률, 제8852호) 등이 있다. 이와 같이 국가사이버 위기에 대한 체계적인 법정비가 되어 있지 않고, 공공분야, 국가핵심기반보호 분야, 정보통신망 분야, 산업기술정보 분야, 민간 소프트웨어산업정보 분야 등의 분야별로 산재하고 있어 이에 대한 법체계 정비가 시급하다.

1) 국가사이버안전관리규정

국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호하기 위하여 국가사이버안전관리규정을 두고 있다(국가사이버안전관리규정, 제1조). 이러한 국가사이버안전관리규정에서는 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 "사이버공격"이라고 규정하고 있고, 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 "사이버안전"으로 규정하고 있다(국가사이버안전관리규정, 제2조).

그러나, 이 훈령에서는 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망에 대하여만 적용하고, 「정보통신기반보호법」 제8조의 규정에 의하여 지정된 주요정보통신기반시설에 대하여는 적용하지 아니하고 있다(국가사이버안전관리규정, 제3조).

이 훈령에 따라 우선, 중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임이 있으며 이를 위하여 사이버안전업무를 전담하는 전문인력을 확보하

는 등 필요한 조치를 강구하여야 하고, 다음으로, 관계 중앙행정기관의 장은 소관 공공기관 및 지방자치단체의 장으로 하여금 전문인력의 확보 등 필요한 조치를 강구하도록 하고 있다(국가사이버안전관리규정, 제4조). 또한, 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정하도록 규정하고 있다(국가사이버안전관리규정, 제5조). 기타 이 훈령에서는 국가사이버 안전의 효율화를 위하여 국가사이버안전대책회의와 국가사이버안전센터를 두도록 규정하고, 또한 사이버안전대책의 수립 및 시행과 사이버공격과 관련한 정보의 협력 및 경보 발령, 사고통보 및 복구, 사고조사 및 처리 등의 규정을 두고 있다. 이밖에도 전문기관간 협력, 연구개발, 인력양성 및 교육홍보, 예산, 안전성 확인에 관한 특례 등을 규정하고 있다.

2) 정보통신기반 보호법

전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 이 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하기 위하여 정보통신기반 보호법을 두고 있다(정보통신기반 보호법, 제1조). 이 법에서는 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 정보통신망을 "정보통신기반시설"로 지칭하고, 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 "전자적 침해행위"라 규정하고 있다. 또한, 전자적 침해행위로 인하여 발생한 사태를 "침해사고"로 규정하고 있다(정보통신기반 보호법, 제2조).

그리고, 이 법에서는 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 두도록 규정하고 있고, 기타 주요정보통신기반시설보호대책의 수립, 이행, 시설보호 계획수립, 주요정보통신기반시설의 지정, 보호지침, 침해사고 통지, 침해행위 금지, 복구조치, 정보공유 및 분석센터 구축, 정보보호컨설팅 전문업체의 지정, 관련기관에의 지원, 민간협력 등의 사항을 규정하고 있다.

3) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함으로써 국민생활의 향상과 공공복리의 증진에 이바지하기 위하여 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 두고 있다(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제1조).

이 법에서는 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등에 의하여 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태를 "침해사고"로 규정하고(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제2조),정보통신서비스를 제공함으로써 이용자의 권익보호와 정보이용능력의 향상에 이바지하고, 이용자는 건전한 정보사회가 정착되도록 노력하여야 하며, 정부는 정보통신서비스 제공자단체 또는 이용자단체의 개인정보보호 및 정보통신망에서의 청소년보호 등을 위한 활동을 지원할 수 있도록 규정하고 있다(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제3조).

또한 행정안전부장관, 지식경제부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자의 개인정보의 보호 등을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하도록 규정하고 있다(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 제4조).

4) 산업기술의 유출방지 및 보호에 관한 법률

산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지하기 위하여, 산업기술의

유출방지 및 보호에 관한 법률이 있다(산업기술의 유출방지 및 보호에 관한 법률, 제1조).

이 법률에서는 국내외 시장에서 차지하는 기술적·경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 산업기술을 "국가핵심기술"이라 지칭하고(산업기술의 유출방지 및 보호에 관한 법률, 제2조), 국가는 산업기술의 유출방지와 보호에 필요한 종합적인 시책을 수립·추진하여야 하고, 국가·기업·연구기관 및 대학 등 산업기술의 개발·보급 및 활용에 관련된 모든 기관은 이 법의 적용에 있어 산업기술의 연구개발자 등 관련 종사자들이 부당한 처우와 선의의 피해를 받지 아니하도록 하고, 산업기술 및 지식의 확산과 활용이 제약되지 아니하도록 노력하여야 하며, 모든 국민은 산업기술의 유출방지에 대한 관심과 인식을 높이고, 각자의 직업윤리의식을 배양하기 위하여 노력하여야 한다고 규정하고 있다(산업기술의 유출방지 및 보호에 관한 법률, 제3조).

5) 소프트웨어산업진흥법

소프트웨어산업의 진흥에 필요한 사항을 정하여 소프트웨어산업 발전의 기반을 조성하고 소프트웨어산업의 경쟁력을 강화함으로써 국민생활의 향상과 국민경제의 건전한 발전에 이바지하기 위해서, 소프트웨어산업 진흥법을 두고 있다(소프트웨어산업 진흥법, 제1조).

이 법에서는 컴퓨터·통신·자동화 등의 장비와 그 주변장치에 대하여 명령·제어·입력·처리·저장·출력·상호작용이 가능하도록 하게 하는 지시·명령(음성이나 영상정보 등을 포함한다)의 집합과 이를 작성하기 위하여 사용된 기술서 기타 관련 자료를 "소프트웨어"라 지칭하고(소프트웨어산업 진흥법, 제2조), 국가와 지방자치단체는 소프트웨어산업의 진흥을 위하여 필요한 각종 시책을 수립·시행하여야 한다고 규정하고 있다(소프트웨어산업 진흥법, 제3조). 또한, 지식경제부장관은 소프트웨어산업의 진흥을 위하여 중·장기적인 기본계획을 수립하도록 규정하고 있다(소프트웨어산업 진흥법, 제4조).

2. 국가사이버 위기관리 조직체계

1) 국가사이버안전전략회의 및 국가사이버안전대책회의

국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의를 두고, 전략회의의 의장은 국가정보원장이 맡는다. 위원으로는 교육과학기술부차관·외교통상부차관·법무부차관·국방부차관·행정안전부차관·지식경제부차관·보건복지가족부차관·국토해양부차관·대통령실 외교안보수석비서관·방송통신위원회 상임위원·금융위원회 부위원장 및 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원으로 하고, 전략회의는 ① 국가사이버안전체계의 수립 및 개선에 관한 사항, ② 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항, ③ 국가사이버안전 관련 대통령 지시사항에 대한 조치방안, ④ 그 밖에 전략회의 의장이 부의하는 사항 등을 심의한다(국가사이버안전관리규정, 제6조). 또한, 전략회의의 효율적인 운영을 위하여 전략회의에 국가사이버안전대책회의를 두도록 규정하고 있다. 대책회의의 의장은 국가정보원의 사이버안전업무를 담당하는 차장이 되며, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 한다. 대책회의는 ① 국가사이버안전 관리 및 대책방안, ② 전략회의의 결정사항에 대한 시행방안, ③ 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항, ④ 그 밖에 대책회의의 의장이 부의하는 사항 등을 심의한다(국가사이버안전관리규정, 제7조).

2) 국가사이버안전센터

사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터를 두고, 사이버안전센터는 ① 국가사이버안전정책의 수립, ② 전략회의 및 대책회의의 운영에 대한 지원, ③ 사이버위협 관련 정보의 수집·분석·전파, ④ 국가정보통신망의 안전성 확인, ⑤ 국가사이버안전매뉴얼의 작

성·배표, ⑥ 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, ⑦ 외국과의 사이버위협 관련 정보의 협력 등의 업무를 담당하고 있으며, 국가정보원장은 사이버안전센터의 업무 수행과 관련하여 필요하다고 인정하는 경우에는 관계 중앙행정기관의 장에게 소속 공무원 및 전문요원의 파견을 요청할 수 있도록 규정하고 있다(사이버안전관리규정, 제8조).

3) 정보통신기반보호위원회

주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회를 두고 있다. 위원회는 ① 주요정보통신기반시설 보호정책의 조정에 관한 사항, ② 주요정보통신기반시설에 관한 보호계획의 종합·조정에 관한 사항, ③ 주요정보통신기반시설에 관한 보호계획의 추진 실적에 관한 사항, ④ 주요정보통신기반시설 보호와 관련된 제도의 개선에 관한 사항 등을 심의하도록 규정하고 있다(정보통신기반 보호법, 제3조, 제4조).

4) 개인정보분쟁조정위원회

개인정보에 관한 분쟁을 조정하기 위하여 개인정보분쟁조정위원회를 두고 있다. 분쟁조정위원회의 업무를 지원하기 위하여 한국정보보호진흥원 내에 사무국을 두고, 분쟁의 조정업무를 효율적으로 수행하기 위하여 분쟁조정위원회에 5인 이하의 위원으로 구성되는 조정부를 두되, 그 중 1인은 변호사의 자격이 있는 자로 규정하고 있다. 조정부의 구성 및 운영에 관하여 필요한 사항은 행정안전부령으로 정하고 있다(정보통신망 이용촉진 및 정보호보 등에 관한 법률, 제33조)

5) 산업기술보호위원회

산업기술의 유출방지 및 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 산업기술보호위원회를 두고 있다. 위원장은 국무총리가 되고, 위원은 ① 관계중앙행정기관의 장으로서 대통령령으로 정하는 자, ② 산업기술의 유출방지업무를 수행하는 정보수사기관의 장, ③ 산업기술의 유출방지 및 보호에 관한 학식과 경험이 풍부한 자로서 위원장이 위촉하는 자 등을 위원으로 두고, 간사위원은 지식경제부장관이 된다. 지식경제부장관은 산업기술의 유출을 방지하고 산업기술을 보호하기 위하여 필요한 방법·절차 등에 관한 지침을 관계중앙행정기관의 장과 협의한 후 위원회의 심의를 거쳐 제정하고 이를 대상기관이 활용할 수 있도록 규정하고 있다(산업기술의 유출방지 및 보호에 관한 법률, 제7조, 제8조).

6) 소프트웨어사업분쟁조정위원회

소프트웨어사업에 관한 분쟁을 조정하기 위하여 지식경제부장관 소속하에 소프트웨어사업분쟁조정위원회를 두고 있다. 위원회는 당사자의 일방 또는 쌍방의 신청에 의하여 분쟁을 심사·조정한다. 다만, 국가를당사자로하는계약에관한법률의 해석과 관련되는 사항, 하도급거래공정화에관한법률의 적용을 받는 사항 및 약관의규제에관한법률의 적용을 받는 사항을 제외하고 있다. 위원회는 ① 발주자와 수급인간의 소프트웨어사업에 관한 분쟁, ② 공동도급형태로 소프트웨어사업에 참여한 수급인간의 책임에 관한 분쟁 및 수급인과 하수급인간의 소프트웨어사업의 하도급에 관한 분쟁, ③ 수급인과 제3자간의 소프트웨어사업상의 책임에 관한 분쟁, ④ 소프트웨어사업 계약의 당사자와 보증인간의 보증책임에 관한 분쟁, ⑤ 그 밖에 소프트웨어사업에 관계한 자간의 책임에 관한 분쟁 등을 조정하고 있다(소프트웨어산업 진흥법, 제37).

3. 한국 국가사이버 위기관리 법 및 조직 체계의 문제점

한국의 국가사이버 위기관리 법체계와 조직체계를 요약해 보면, 다음 <표 3>과 같다. <표 3>에서 보는 바와 같이 현재, 한국의 사이버 위기관리에 관한 법체계는 국가사이버안전관리규정(대통령훈령, 제222호), 정보통신기반보호법(법률, 제8852호), 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률, 제8867호), 산업기술의 유

출방지 및 보호에 관한 법률(법률, 제8900호), 소프트웨어산업진흥법(법률, 제8852호) 등이 있다. 즉 국가사이버 위기에 대한 체계적인 법정비가 되어 있지 않고, 공공 분야, 국가핵심기반보호 분야, 정보통신망 분야, 산업기술정보 분야, 민간 소프트웨어산업정보 분야 등의 분야별로 산재하고 있어 이에 대한 법체계 정비가 시급한 실정이다. 그리고, 각 개별법에 의해서 국가사이버안전대책회의, 국가사이버안전센터, 정보통신기반보호위원회, 개인정보분쟁조정위원회, 산업기술보호위원회, 소프트웨어사업분쟁조정위원회 등 분야별 국가사이버 위기관리 조직체계를 편제하고 있어 이에 대한 정비도 필요하다.

기존에는 정부 차원의 인터넷 침해대응체계 등이 부실하였던 것이 사실이다. 즉 사이버 침해 대응 기능이 국정원, 국방부, 정통부로 분산되어 있었고, 침해 대비 범정부 차원의 위기관리 대응 매뉴얼이 미비하였고, 보안 프로그램 및 전문 인력과 장비 등이 취약하였다. 이러한 문제를 해결하기 위하여 2008년 8월 18일, 「국가사이버안전관리규정」(대통령 훈령)을 마련하여, 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관 간 협력을 강화하고, 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호하기 위하여 국가사이버안전전략회의, 국가사이버안전대책회의를 두고, 아울러 국정원에 국가사이버안전센터를 마련할 수 있도록 관련 법령을 정비하였다.

<표 3> 국가사이버 위기관리 법 및 조직 체계

구 분	사이버 위기 보호대상	조직체계	기능 및 업무	다른 법률과의 관계 특징
국가사이버안전관리규정	· 국가안보 위협하는 사이버공격 · 국가정보통신망 보호	· 국가사이버안전전략회의 및 국가사이버안전대책회의	· 국가사이버안전에 관한 중요사항 심의	· 정보통신기반보호법에 의해 지정된 주요정보통신기반시설에 대하여는 적용하지 않음
		· 국가사이버안전센터	· 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응	
정보통신기반 보호법	· 전자적 침해행위 · 주요정보통신기반시설 보호	· 정보통신기반보호위원회	· 주요정보통신기반시설의 보호 사항 심의	· 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 근거하여 정보통신망 용어 지칭
정보통신망 이용촉진 및 정보보호 등에 관한 법률	· 개인정보 보호 · 침해사고 대응 · 정보통신망 보호	· 개인정보분쟁조정위원회	· 개인정보 보호 및 침해에 관한 분쟁 조정	· 전기통신기본법 및 전기통신사업법에 근거를 두고 정보통신만 용어 지칭 · 통신과금서비스에 관하여 전자금융거래법과 경합
산업기술의 유출방지 및 보호에 관한 법률	· 산업기술의 부정한 유출방지 · 산업기술 보호 · 국가핵심기술 및 국가연구개발사업 보호	· 산업기술보호위원회	· 산업기술의 유출방지 및 보호에 관한 사항 심의	· 과학기술기본법의 규정에 근거하여 국가연구개발사업 용어규정 · 산업기술유출에 관한 분쟁조정에 민사조정법 규정 준용
		· 산업기술분쟁조정위원회	· 산업기술에 대한 분쟁조정	
소프트웨어산업 진흥법	· 소프트웨어산업 진흥 및 보호	· 소프트웨어사업분쟁조정위원회	· 소프트웨어사업의 분쟁을 조정	· 정보시스템의 효율적 도입 및 운영에 관한 법률의 규정에 의해 소프트웨어산업 용어 지칭

그러나 위의 법체계 및 조직체계의 분석에서도 알 수 있듯이 국가사이버안전관리규정은 훈령의 성격이기 때문에 관련 정보통신기반보호법(법률, 제8852호), 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률, 제8867호), 산업기술의 유출방지 및 보호에 관한 법률(법률, 제8900호), 소프트웨어산업진흥법(법률, 제8852호) 등과 상충되고, 각 개별 법령의 사이버 위기 보호대상이 제 각각 다르며, 각 개별법 하의 조직체계 및 기능과 업무가 중복되는 등의 문제점이 있다.

따라서 이러한 문제점을 해결하기 위해서는 첫째, 국

가사이버안전관리규정이 법률로서의 효력을 지닐 수 있도록, (가칭)국가사이버위기관리법 마련이 필요하다. 그래야만 국가 사이버 위기라는 포괄적 개념속에서 사이버 위기관리를 효과적으로 대응할 수 있고, 다른 유사법률과의 관계도 명확히 할 수 있기 때문이다. 둘째, 국가사이버위기관리법이 마련되면, 각 개별법에 산재되어 있는 국가안보를 위협하는 사이버 공격, 국가정보통신망보호, 전자적 침해행위, 주요정보통신망보호, 개인정보 보호, 산업기술 및 정보 보호, 소프트웨어 보호 등의 기능을 재조정 할 수 있는 근거가 마련되어, 현재와 같이 기능중복으로 인한 비효율을 없앨 수 있다. 셋째, 사이버 강국에 걸 맞는 사이버 안전 관리체계의 구축을 위해서도 (가칭)국가사이버위기관리법의 마련이 필수적이다. 즉 국가 사이버 위기관리 의사결정기구, 전담 및 총괄 조직, 위기관리 매뉴얼, 인적 및 물적 자원의 확보 등이 가능해 지고, 사이버 안전관리 기관별 임무와 역할 정립을 위해서는 통합법 마련이 필요하다. 넷째, 관련 유관기관 및 민간기관과의 정보 공유, 합동 훈련 등 긴밀한 공조체계 구축 및 가동이 가능해지기 위해서라고 사이버 안전 총괄 및 분야별 전담기구 설치와 시급하다. 그러기 위해서는 사이버 위기관리에 관해 산재해 있는 법률을 통합할 (가칭)국가사이버위기관리법의 마련이 필요하다.

V. 국가 사이버 위기관리체계 강화 방안

이상의 논의를 기반으로 우리나라 국가 사이버 위기관리 체계의 강화 방안을 다음과 같이 제시할 수 있다. 첫째, 국가 사이버 위기관리는 개인, 조직, 기업, 공공기관, 정부기관 등이 각각의 수준에 맞는 사이버 위기관리 체계를 이룰 때 비로소 국가 사이버 위기관리가 가능하다는 점을 전제로 한다. 국가 사이버 위기관리의 가장 기본적 이념은 국가를 구성하는 최소 단위인 국민의 사이버 상의 안전 확보뿐만 아니라 국가 사회적으로 중요한 기능, 시스템, 시설 등을 보호하기 위하여 사이버 위기를 관리하는데 있다. 또한, 국가 사이버 위기관리는 개인을 포함하는 개별 국가 구성요소의 안전뿐만 아니라 국가사회 전반에 대한 위협을 가져오는 사이버 위기 상황의 예방과 대비, 대응, 복구를 통해 국가사회의 사이버 기능과 시스템, 시설이 보호될 수 있도록 해야 한다.

둘째, 국가 사이버 위기에 대한 개념 정의가 국가 위기와 연계되는 것이 필요하다. 이러한 맥락에서 국가 사이버 위기는 "정보통신 기술을 통해 국민의 생명과 재산 및 건강, 국가의 주권과 영토, 그리고 국가를 구성하는 정치・경제・사회・문화 체계 등 국가의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태"로 정의할 수 있다. 이러한 국가 사이버 위기의 정의는 다음의 내용을 포함한다. 우선, 국가 사이버 위기의 정의에는 컴퓨터나 인터넷, 모바일 통신, 무선 망 등의 포괄적 의미의 정보통신 기술을 활용하는 것들이 모두 포함된다. 둘째, 국가 사이버 위기에는 정보통신 기술을 활용하여 국민생활안전에 대한 위협, 국가의 주권 및 영토 등 전통적 안보에 대한 위협, 국가 핵심기반에 대한 위협 등을 모두 포함한다. 셋째, 국가 핵심기반, 즉 금융・교통・전력・정보통신・에너지・원자력・댐・주요산업단지・공중보건 마비의 경우에는 정보통신 기술을 활용함으로써 온라인 및 오프라인 상에서의 시스템, 시설, 기능의 마비를 가져올 수 있는 상황을 모두 포함한다. 넷째, 이외에도 현재의 과학 기술이나 인지 능력의 한계로 말미암아 사이버 위기로 인식하지 못하지만 향후 국민의 생명과 재산을 위협하거나 국가의 안전을 정보통신 기술을 이용하여 위협할 수 있는 신종 사이버 위기를 고려해야 한다.

셋째, 국가 사이버 위기관리의 과정 및 활동 요소들이 국가위기관리와 연계되는 것이 필요하다. 국가 사이버 위기관리는 국가 사이버 위기를 효과적으로 예방・대비하고 대응・복구하기 위하여 국가가 자원을 기획・조직・조정・통제하는 과정으로서 다음과 같은 단계 및 활동으로 구성되어 있다. 우선, 예방 단계는 국가 사이버 위기 요인을 사전에 제거하거나 감소시킴으로써 국가 사이버 위기의 발생을 억제하거나 방지하기 위한 활동 과정을 말한다. 대비 단계는 국가 사이버 위기 상황 하에서

수행해야 할 제반 사항을 사전에 계획・준비하고 교육・훈련을 실시하여 국가 사이버 위기에 대한 대응 능력을 높임으로써 국가 사이버 위기 발생에 즉각적으로 대응할 수 있는 태세를 강화시켜나가는 활동 과정을 말한다. 그리고 대응 단계는 국가 사이버 위기가 발생한 경우 국가의 자원과 역량을 효율적으로 활용하고 신속하게 대처함으로써 사이버 위기로 인한 직・간접적 피해를 최소화하고 2차적인 국가위기 및 국가 사이버 위기의 발생 가능성을 감소시키는 활동 과정을 말한다. 마지막으로, 복구 단계는 국가 사이버 위기로 인해 발생한 피해를 국가 사이버 위기 발생 이전의 상태로 개량 복구함으로써 재발하지 않도록 하기 위한 활동 과정이다.

넷째, 국가 사이버 위기관리 기관을 책임 정도에 따라 구분하는 것이 필요하다. 국가 사이버 위기관리 기관은 해당 국가 사이버 위기관리에 대하여 책임을 지는 공공 및 민간 조직을 의미하는 것으로 정의할 수 있다. 이러한 차원에서 국가 사이버 위기관리의 주관기관은 해당 국가 사이버 위기관리 정책에 대하여 관리 책임을 지는 공공 및 민간 조직을 말한다. 다음으로, 국가 사이버 위기관리 실무기관이란 해당 국가 사이버 위기의 대상이 되는 기능・시설, 시스템을 직접 운영하거나 관리하는 공공 및 민간 조직을 말한다. 셋째, 국가 사이버 위기관리 협력기관이란 해당 국가 사이버 위기 유형의 위기관리에 있어서 주관기관과 실무기관의 활동을 지원하고 협조하는 공공 및 민간 조직을 의미하는 것으로 구분하는 것이 가능하다.

다섯째, 국가 사이버 위기관리 법체계 정비가 필요하다. 현재 우리나라는 국가 사이버 위기관리에 관한 개별 법률들이 산재되어 체계화되어 있지 못하며 법률 간의 협력이나 연계가 미흡한 실정이다. 따라서 전통적 안보 차원, 국가 핵심기반 차원, 국민생활 안전 차원 등에서의 국가 사이버 위기를 포괄할 수 있는 기준이 되는 법률의 제정을 통하여 국가 사이버 위기관리와 관련된 법률을 체계화하는 것이 요구된다. 이와 함께 지금까지는 각 기관 간 역할이나 국가 차원의 대응체계를 고려하지 않고 소관부처 중심으로 업무수행이 이루어져 정보공유와 업무 협조에 있어서도 소극적일 수밖에 없었고, 사이버 테러리즘으로 인한 침해사고와 관련한 민간기업의 정보제공, 정보보호안전진단 등 침해사고 최소화 방안이 미흡하였다. 이러한 문제점들을 개선하고 실질적인 대응업무를 마련하고 정착시키기 위해서는 관련 법제도의 개선이 필요하다. 그리고 현재까지 사이버 위기관리를 위한 국내의 독립적인 법률의 부재로 인하여 국가 핵심기반 시설이나 시스템에 대한 국내외의 사이버 공격을 예방하고 대비하며 실제로 사이버 위기가 발생하는 경우 공격에 대응하는 시스템이 미흡한 상태이다. 특히, 민간 기업 및 개인에 대한 사이버 위기는 물론 국가 사회적으로 중요한 기능을 수행하는 핵심기반 마비와 관련된 사이버 위기관리를 위한 체계 구축이 필요로 된다.

여섯째, 국가 사이버 위기관리 조직체계를 구축하는 것이 필요하다. 즉 국가 사이버 위기관리 기능을 원활하게 수행하기 위해서 국가사회 전반의 국가 사이버 위기관리의 기준과 새로운 모범을 제시하는 한편, 각 부처 및 국가사회의 구성요소들에 대해 국가 사이버 위기관리 정책을 집행할 수 있는 조직 체계 구축이 필요하다. 예를 들면, 국가 사이버 위기관리에 관한 주요 정책의 심의 및 기획・조정, 통합된 국가 사이버 위기관리의 기능을 수행하기 위하여 현행 '국가사이버안전센터'의 기능을 확대 강화하는 것이 필요하다. 특히, 국가 사이버 위기와 관련된 정보의 종합적 수집, 분석, 처리의 종합적 기능을 수행하고 각 정부 및 공공 기관을 통할하며 민간부문과의 협조체계를 구축하는 것이 요구된다.

일곱째, 국가 사이버 위기관리의 전문성을 확보해야 한다. 국가 사이버 위기에 효율적으로 대응하기 위해서는 사이버 상에서의 정보통신 기술을 활용할 수 있는 전문적이고 기술적인 지식과 응용 능력을 지녀야 할 뿐만 아니라 사이버 범죄 및 테러리즘이라고 하는 보안 분야의 전문적인 이해도 지녀야 한다. 각 기관별 사이버 위기 대응 센터 및 사이버 범죄 수사기관의 전문 인력은 공공분야, 민간분야, 그리고 국방 분야 모두 부족한 실정이다.

따라서 국가 핵심기반과 관련된 국가기간전산망을 사이버 상에서 안전하게 운영하기 위해서는 보안시설과 장비에 대한 지속적인 투자와 함께 관련 인력에 대한 지속적인 교육과 훈련, 연습을 실시해야 하는 한편, 전문성을 확보하기 위한 노력을 기울여야 한다. 즉 전문적인 교육·훈련·연습을 통해 빠른 기술적인 변화를 보충하도록 해야 하며, 시스템을 운영하는 직원의 전문성을 최대한 보완해 주는 것이 필요하다.

여덟째, 국가 사이버 위기 경보 체계 구축이 필요하다. 과거에는 국가 사이버 위기가 발생한 후 효과적인 위기관리를 위해 사후 위기관리에 중점을 두는 경향이 있었으나 최근에는 위기 징후를 사전에 탐지하여 사이버 위기 발생을 사전에 방지하는 사전 조기 경보·사전 위기관리의 운용이 중요시되고 있다. 각종 국가 사이버 위기로 인하여 국민과 국가의 안전에 피해가 예상되는 경우, 국가 사이버 위기관리 관련 기관들로 하여금 필요한 조치를 취하게 하기 위하여 국가 사이버 위기 경보를 발령하는 것이 필요하다. 즉 국가사이버안전센터는 국가 사이버 위기 발생의 징후가 식별되거나 발생이 우려되는 경우에 국가 사이버 위기관리 기관들이 사전에 필요한 조치를 취할 수 있도록 국가 사이버 위기경보를 발령해야 한다. 따라서 국가사이버안전센터는 국가 사이버 위기 경보의 발령에 따른 국가 사이버 위기관리 기관별 조치 사항의 이행 실태를 점검하고, 필요하다고 인정하는 경우에는 국가 사이버 위기관리 기관의 관계 직원의 출동 또는 물자 및 지정된 장비·인력의 동원 등 필요한 조치를 취할 수 있어야 한다.

아홉째, 국가 사이버 위기관리 평가 체계를 구축하는 것이 요구된다. 국가 사이버 위기관리의 효과성 확보를 위해서는 국가 사이버 위기관리 기관의 정책 및 활동에 관한 평가를 하는 것이 필요하다. 이러한 사이버 위기관리 평가의 기본 내용은 다음과 같다. 첫째, 국가 사이버 위기를 예방하기 위한 정책의 수립·집행 및 조치 사항, 둘째, 국가 사이버 위기의 발생에 따른 대응 조치와 이에 필요한 대비 활동, 셋째, 국가 사이버 위기 발생으로 인한 피해 복구 및 안정화 대책, 넷째, 국가 사이버 위기 유형별 관리 정책 및 관리 체계, 규정 등이다.

열 번째, 국가 사이버 위기관리는 공공과 민간 분야에서의 전문 인력 확보와 전문성 향상이 요구된다. 전통적 안보 영역은 물론 국민생활안전 영역과 국가 핵심기반 영역의 사이버 위기를 관리하는 데 필요한 전문 인력을 양성하기 위하여 노력하는 것이 요구된다. 이러한 전문 인력을 양성하는 방법으로 국가가 직접 국가 사이버 위기관리 전문 기관을 운영하는 방안과 각 지역별 여건과 학문적 심화를 위하여 관련 대학이나 연구소 또는 정부가 인정하는 기관을 교육기관으로 지정하거나 협약을 통하여 전문 인력의 양성 기관으로서 기능하게 할 수 있다. 이는 오늘 날 끝없이 변화하고 있는 국가 사이버 위기 환경 변화로 인해 각종 다양한 사이버 위기에 대응할 수 있는 종합적 대처 능력을 지닌 사이버 위기관리 전문 인력을 양성·개발하고 사이버 위기관리 전문 인력의 활동 여건을 개선하기 위해서도 필요하다.

열한 번째, 국가는 국가 사이버 위기관리의 지속적인 발전을 이룩하기 위하여 학술적 발전에도 노력하여야 한다. 이러한 노력을 통해 예방 효과를 높이고 대형 사이버 위기 발생 시의 혼란과 무질서를 조금이라도 줄이는 것이 국가 사이버 위기관리의 접근 방식이다. 학술적이며 과학적으로 사전적 위험관리를 하기 위해서는 다음과 같은 사항이 반드시 필요하며 충분한 자료의 확보가 먼저 이루어져야 한다. 첫째, 자료 수집 영역의 확대. 둘째, 지속적으로 자료를 수집하고 관리하여 활용할 수 있는 데이터베이스의 구축, 셋째, 자료 수집, 위험요인 및 자료 분석, 관련 정보의 전파이다. 국가는 국가 사이버 위기에 대한 정확한 원인의 진단과 분석, 교훈의 도출 등을 위하여 국가 사이버 위기 발생 시에 관련된 다양한 학문 분야별 전문가들을 공동으로 파견하여 각종 국가 사이버 위기 사례에 대한 전문가들의 연구와 분석, 관련 자료의 수집·정리·보관이 함께 이루어지도록 노력하여야 한다. 국가 사이버 위기 유형중 빈번하게 발생하는 국가 사이버 위기의 원인 분석 및 개선방안, 관련된 자료의 종합

DB 구축, 기술 지원 등의 사업을 추진하기 위하여 국가보안기술연구소 및 민간 연구소 등의 활용이 요구된다. 국가의 사회기반시설이 제 기능을 발휘하면서 사회적 경제활동이 활발하게 이루어지기 위해서는 사이버 위기의 발생 메카니즘을 연구하여 위기의 발생 위치와 규모를 예측하고 사회 전체 시설의 위험성을 최소화하는 기법을 개발하고 연구하는 것이 필요하다.

Ⅵ. 결론

이 연구는 국내・외 사이버 위기관리 체계 분석을 통한 변화하는 국내 실정에 적합한 새로운 사이버 위기관리 체계 강화 방안을 모색하는데 목적을 두었다. 최근 미국, 독일, 프랑스 등은 사이버 전담 조직을 두고, 일본과 영국의 경우에는 우리나라와 같이 부문별로 기관이 존재하고는 있으나 이를 조정하기 위한 센터 내지 위원회가 존재하고 있어 각 대응기관 간 협력체계가 강화되어 있다. 미국, 영국, 독일, 그리고 일본 등의 경우 이미 국가 사이버 위기관리 체계에 대한 정립을 끝낸 수준으로 인력 및 기술개발 보완 등의 활용 및 안정화 단계에 진입했다고 볼 수 있다. 그러나 IT 선진국인 우리나라의 경우 IT산업 발전 속도는 이들 선진국을 능가하고 있으나, 국가 사이버 위기관리 체계는 이제 갓 체계 정립 단계에 있다고 볼 수 있다.

특히, 최근의 사이버 침해 형태는 단순 자기과시에서 벗어나 금전적인 이득추구로 본격화 되고 있으며 정보유출을 목적으로 한 악성코드가 크게 증가하고 있고, 피싱 등 여러 사회공학적 방법과 유기적으로 결합한 사이버 공격 수법이 나날이 증가되고 있다. 또한, 다양해진 공격 수법은 과거 웜 바이러스 등의 악성코드에 집중된 경향에서 벗어나 봇넷 구성, 방문자가 많은 홈페이지 해킹, 백신 등 정보보호제품의 취약점 공격 등으로 진보되고 있다. 이처럼, 향후 국가 사이버 위기는 고도화, 다양화, 은밀화를 지향 할 것으로 예상할 수 있으며, 그 피해는 전산망 장애에 국한되지 않고, 기관, 기업의 중요자료 및 개인 정보 유출로 이어질 것으로 예측된다. 따라서 우리나라도 국가 사이버 위기관리 체계를 강화할 필요성이 더욱 제기된다.

이러한 관점에서 본 연구에서는 다음과 같은 정책적 시사점을 제시하였다. 첫째, 국가 사이버 위기관리는 개인, 조직, 기업, 공공기관, 정부기관 등이 각각의 수준에 맞는 사이버 위기관리 체계를 이룰 때에 비로소 국가 사이버 위기관리가 가능하다는 점을 전제로 해야 한다. 둘째, 국가 사이버 위기의 개념을 국가위기 개념과 연계하여 “정보통신 기술을 통해 국민의 생명과 재산 및 건강, 국가의 주권과 영토, 그리고 국가를 구성하는 정치・경제・사회・문화 체계 등 국가의 핵심요소나 가치에 중대한 위해가 가해질 가능성이 있거나 가해지고 있는 상태”로 정의하는 것이 필요하다. 셋째, 국가 사이버 위기관리는 국가 사이버 위기를 효과적으로 예방・대비하고 대응・복구하기 위하여 국가가 자원을 기획・조직・조정・통제하는 과정으로 정의하고 관리체계를 갖추는 것이 필요하다. 넷째, 국가 사이버 위기관리 기관을 책임 정도에 따라 국가 사이버 위기관리 주관기관, 실무기관, 협력기관 등으로 체계화하여 관리하는 것이 필요하다. 다섯째, 국가 사이버 위기관리 법체계 정비가 필요하다. 특히, 민간 기업 및 개인에 대한 사이버 위기는 물론 국가사회적으로 중요한 기능을 수행하는 핵심기반 마비와 관련된 사이버 위기관리를 위한 체계 구축이 필요로 된다. 여섯째, 국가 사이버 위기관리의 기능 수행을 위해서는 국가사회 전반의 국가 사이버 위기관리의 기준과 새로운 모범을 제시하는 한편, 각 부처 및 국가사회의 구성요소들에 대해 국가 사이버 위기관리 정책을 집행할 수 있는 국가 사이버 위기관리 조직체계를 강화하는 것이 필요하다. 일곱째, 국가 사이버 위기관리의 전문성을 확보해야 한다. 이를 위해 보안시설과 장비에 대한 지속적인 투자와 함께 관련 인력에 대한 지속적인 교육과 훈련, 연습 등을 실시하는 한편, 전문성을 확보하기 위한 노력을 기울여야 한다. 여덟째, 국가 사이버 위기 경보 체계 구축이 필요하다. 위기 징후를 사전에 탐지하여 사이버 위기 발생을 사전에 방지하는 사전 조기 경보・사전 위기관리의

운용이 필요하다. 아홉째, 국가 사이버 위기관리 평가 체계를 구축하는 것이 요구된다. 국가 사이버 위기관리의 효과성 확보를 위해서는 국가 사이버 위기관리 기관의 정책 및 활동에 관한 평가를 하는 것이 필요하다. 열 번째, 국가 사이버 위기관리는 공공과 민간 분야에서의 전문 인력 확보와 전문성 향상이 요구된다. 열한 번째, 국가는 국가 사이버 위기관리의 지속적인 발전을 이룩하기 위하여 학술적 발전에도 노력하여야 한다.

<참고문헌>

▷ 강구형. 2008. 전자정부하에서 각 행정기관 홈페이지의 개인정보 노출 방지에 대한 연구. 한남대 경영산업대학원.

▷ 강동범. 1999. 컴퓨터犯罪처벌규정에 대한 비교법적 고찰. 법률행정논집 7: 1-37. 서울시립대학교법률행정연구소.

▷ 고동우. 2004. 사이버범죄 예방을 위한 인터넷 사용 실태 조사 연구: 경기도 소재 고등학교 학생을 중심으로. 안양대학교 경영행정대학원.

▷ 고준수. 2004. 9.11테러이후 국가정보체계의 발전방안 : 주요선진국의 정보체계 비교를 중심으로. 고려대학교 정책대학원.

▷ 공성진. 2007. 테러와의 전행, 어떻게 수행할 것인가. 2007년 국정감사 정책자료집 시리즈-1.

▷ 김경섭. 2006. 사이버 테러리즘의 대응체계에 관한 연구. 한남대 사회문화대학원.

▷ 김성재. 2002. 정보전 수행을 위한 한국군의 국방정보화 발전 방향. 한남대 경영대학원.

▷ 김학권. 2008. 군 사이버전 수행을 위한 사이버전사 양성방안. 경희대학교 경영대학원.

▷ 김형준. 2007. 금융범죄 예방을 위한 금융감독체계의 개선. 국민대학교 법무대학원.

▷ 남길현. 2004. 군 정보보호의식 확산을 위한 장병 교육방안 연구. 교수논총 제37집: 115-146 국방대학교.

▷ 문병학. 2004. 사이버 범죄 실태와 경찰수사에 대한 연구. 부산대 행정대학원.

▷ 민경식 외. 2006. 주요국 정보보호 동향조사 2007-유비쿼터스 시대의 정보보호 정책을 중심으로. NIA I -RER-06052. 서울: 한국정보보호진흥원.

▷ 민경식 외. 2007. 주요국 정보보호 연구개발 동향조사 2007-연구개발 정책의 흐름을 중심으로. NIA I -RER-07043. 서울: 한국정보보호진흥원.

▷ 박도권. 2007. 사이버침해 위협에 관한 연구. 한양대 공학대학원. 석사.

▷ 박윤해. 2005. 컴퓨터범죄에 관한 연구. 숭실대 대학원. 박사.

▷ 박형근. 2007. 각국의 테러대응체계와 운용에 관한 연구. 경기대학교 정치전문대학원 석사학위 논문.

▷ 배상균. 2005. 사이버범죄에 있어서 ISP의 형사책임에 관한 연구. 광운대학교.

▷ 백광훈. 2001. 사이버 스토킹과 그 처벌법규 및 문제점. Security World 50: 69-73. 시큐리티정보.

▷ 서성교. 2005. 사이버 범죄의 대응방안에 대한 연구. 서남대학교 경영·행정대학원.

▷ 신관근. 2004. 사이버전을 대비한 인력관리정책에 관한 연구. 경원대 대학원.

▷ 양근원. 2000. 사이버범죄의 특징과 수사방향. 수사연구 200: 16-25.

▷ 양근원. 2003. 사이버테러의 실태와 법적 대응에 관한 연구. 경희대 국제법무대학원.

▷ 양은영. 2006. 사이버공간에서의 명예훼손에 관한 법적 고찰: 정보통신망이용촉진및정보보호등에관한법률 제61조를 중심으로. 단국대학교.

▷ 이강무. 2006. 테러 위협이 한국 안보에 미치는 영향. 경남대학교 행정대학원.

▷ 이동곤. 2004. 사이버테러 범죄에 관한 연구. 영산대학교 법무대학원.

▷ 이성순. 2007. 뉴테러리즘이 경제·사회에 미치는 영향 및 대비방안. 경원대 경영대학원. 석사학위 논문.

▷ 이지혜. 2006. 청소년 사이버범죄 분석을 통한 고등학교 법교육 개선방안: 부산지역을 중심으로. 동아대학교.

▷ 정 완. 1999. 컴퓨터범죄 대응에 관한 국제동향. 수사연구 185: 26-32.

▷ 정일석. 2004. 사이버 위기관리 방안에 관한 연구. 용인대 체육과학대학원. 석사.

▷ 조병인. 2001. 사이버범죄의 규제에 관한 제언. 수사연구 211: 136-141.

▷ 조호대. 2006. 사이버 테러 대응 방안에 관한 연구. 한국위기관리논집. 2(1): 14-29.

▷ 조휘갑. 2001. 정보보호 환경과 정책 방향. 한국통신학회지 18: .69-75. 한국통신학회.

▷ 지무진. 2008. 전자상거래에 있어서의 소비자보호에 관한 연구. 경남대학교 대학원.

▷ 최운호. 2005. 대규모 사이버공격에 대한 침해사고대응시스템 자동화 모델 설계. 한세대 대학원.

▷ 하옥현. 2005. 국가 사이버안보체계 구축 전략. 고려대 정보보호대학원.

▷ 한봉조. 2000. 사이버범죄수사에 대한 국제적 협력문제. 형사정책연구 42: 45-63. 한국형사정책연구원

▷ 황영구. 2004. 사이버범죄에 대한 대응시스템과 그 발전방안에 관한 연구. 계명대 대학원.

▷ Albert, David. 2000. *Network Centric Warfare, Developing and Leveraging Information Superiority, CAISR Cooperative Research Program*. Washington, D. C. : Department of Defense.

▷ Albert, David. 1996. T*he Unintended Consequences of Information Age Technologies*. Washington, D. C. : National Defense University.

▷ Libicki, Martin. 1995. *What is Information Warfare?*.

Washington, D. C. : National Defense University.
▷ Molander, Roger. 1996. *Strategic Information Warfare*. National Defense Research Institute.

李在恩: 연세대학교에서 행정학 박사학위를 취득하고(논문: 한국의 위기관리정책에 관한 연구: 집행구조의 다조직적 관계 분석을 중심으로. 2000), 현재 충북대학교 행정학과 부교수로 재직중이다. 주요 관심분야는 위기관리, 조직이론, 정책집행 등이며, 재난관리론(공저, 2006) 등의 저서와 "지방정부 재난관리 기관의 반응 분석(2008)", "Securing the National Security and Reinforcing the Cyber Crisis Management System in Asia(2008)", "근거이론적 접근을 통해 본 이재민의 반응분석(2008)" 등이 있다(jeunlee@chungbuk.ac.kr).

梁奇根: 경희대학교에서 행정학 박사학위를 취득하고(논문: 위기관리 조직학습체제에 관한 연구: 한국과 미국의 위기관리 사례 비교분석을 중심으로, 2004), 한국행정연구원 정책평가센터 초청연구원과 경남발전연구원 부연구위원을 거쳐 현재 원광대학교 소방행정학부 전임강사로 재직 중이다. 한국행정학회 일반상임이사(2007)를 역임하였으며, 주요 관심분야는 재난관리, 지방행정, 조직론 등이다. 주요 저서 및 논문으로는 인간관계의 이해(2007, 공저), 재난관리론(2006, 공저), 현대사회와 행정(2004, 공저), "지속가능한 재난관리를 위한 지역자율방재조직의 활동프로그램과 활용방안 연구(2008)", "지방정부의 위기관리 조직학습화 방안(2007)", "한국과 일본 기계산업의 전략적 협력방안(2007)", "지방행정서비스에 대한 주민만족도 실증분석(2007)", "한국의 재해의연금 모금 및 배분체계 개선방향에 관한 연구(2006)", "지방정부간 공유재 갈등 사례(2006)" 등이 있다(withgg@wku.ac.kr).

柳賞溢: 충북대학교에서 행정학 박사학위를 취득하고(논문: 한국의 지방자치단체 재난대응체계, 2007), 충북대 국가위기관리연구소와 충남발전연구원을 거쳐 현재 대불대학교 소방행정학과에 재직 중이다. 위기관리, 소방행정, 네트워크이론이 주요 관심분야이며, 주요 논문으로는 "행정학에서 재난관리분야의 학문적 연구경향(2007)", "네트워크 관점에서 지방정부 재난대응과정 분석: 미국의 허리케인과 한국의 태풍 대응사례를 중심으로(2007)", "지방자치단체의 재난대응 네트워크 분석(2008)"등이 있다(ryusi@mail.daebul.ac.kr).

접수번호: #081112-01
접수일자: 2008. 11. 12.
심사완료: 2008. 12. 19.