情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

침해사고 국가 대응 체계 - National security system for countering information incidents

이 철 수*

요 약

사이버 공간이라는 새로운 국가 영역이 창조되었고, 그 영역에서의 각종활동이 국내는 물론 국제사회의 경쟁력에서 가장 중요한 국가 영역이 되고 있다. 반면에 사이버 공간에서의 침해사고 내지는 공격행위가 사이버 공간에서의 활동을 방해하고 사회의 혼란을 초래할 뿐 아니라 사이버 공간을 통해 국가 안보를 위협하는 테러, 정보전 양상이 뚜렷하게 증가하고 있다. 또 민주화와 인터넷의 개방 구조로 개인과 기업, 조직의 정보보호와 기밀 보호의 요구가 높아지고 있다. 이를 보호하고 국가 안보를 강화하는 사이버 공간의 안보체계를 제시한다.

Ⅰ. 서 론

침해사고, 사이버테러 등으로 불리는 사이버 공간상에서의 각종 사고는 국가의 경제, 국민 생활에 미치는 피해가 날로 심화되고 있을 뿐 아니라 직접적으로 또는 테러와 연계되어 국가의 안보를 위협하는 중요한 요인이 되었다. 미국을 비롯한 선진 각국은 사이버 공간의 형성과 더불어 전 세계적으로 확산되고 있는 테러에 대응하면서 국가의 안보체계를 강화하기 위한 노력을 하고 있다. 우리나라도 각종 침해사고에 대응하기 위한 국가안보의 강화 노력을 하여왔다. 현황을 살펴보고 보다 강력한 안보체제를 구축하기 위한 방안을 연구하여야 할 것이다.

Ⅱ. 본 론

1. 해외 각국의 사례

1.1 미국의 사례

미국은 9.11 테러를 당한 가장 큰 원인이 테러리스트들이 미국의 정보시스템과 정보를 이용하고 공유하여 테러를 계획하고 실행한데 비해 미국은 자국의 정보시스템을 활용하고 있는 테러리스트들의 정보를 공유하지 못하여 사전에 테러를 감지하고 예방하지 못하였다는 판단을 하였다. 이에 정보를 공유하기 위한 다양한 조치를 취하였다. 미국은 미국의 본토안보와 관련하여 100개의 정부기관에 임무가 분산되어있던 것을 본토안보부의 설립과 더불어 하나로 통합하고 사이버 공간에 대한 보안 부서를 본토안보부에 흡수하여 사이버안보와 지금까지 고려해온 본토안보를 하나로 묶어서 동시에 정책을 결정하고 시행하는 체제를 구축하였다. 2003년 2월에 국가 사이버 공간 방어 전략(National Strategy to Secure Cyberspace)을 수립 발표했다. 이 전략은 국민으로 하여금 자신이 소유, 운영, 통제하거나 이용하는 사이버 공간들을 안전하게 지키게 하는 것을 취지로 하고 있으며, 사이버 공간을 수호하는 일은 연방 정부, 주 정부와 지자체, 민간 부문, 그리고 국민 등 사회 전체의 유기적이고 집중적인 노력이 필요하다는 것을 강조하고 있다. 또 현안 문제로서 국가 사이버 공간 방어 대응 체계의 확립, 국가 사이버 위협 및 취약점 보완 프로그램 개발, 국가 사이버 공간 방어 인식과 교육 프로그램의 마련과 교육의 시행, 정부 사이버 공간의 방어, 국가안보와 국제 사이버 방어 협력 등을 들고 있다. 또한 미국은 사이버테러에 대한 국가조직과 정책을 테러 및 국가안보와 동일한 조직체계 하에서 수행하도록 하고 있으며, 정부내부와 지방 정부 그리고 의회 등과의 협력관계가 원활히 이루어지도록 최대의 노력을 다하고 있

* 경원 대학교 소프트웨어 대학원 (csl100@kyungwon.ac.kr)

다. 또한 침해사고에 대해서는 민간의 참여와 협조의 중요성을 인식하고 민관 협조체제를 구축하기 위한 신뢰확립, 교육훈련을 통한 인식 확산, 정부의 기술적인 지원, 등의 노력에 집중하고 있다.

미국의 대응체계의 특징은 사이버안보와 국가안보, 테러와 사이버테러 등을 동일한 국가안보체계 하에서 수행한다는 것과 모든 국가조직의 역량을 통합으로 극대화하고 있고, 행정부와 법 집행 기구, 의회의 긴밀한 협조관계를 확립하고 있으며, 중앙정부와 지방 정부의 역할, 정부와 민간의 협력관계의 강화 등을 들 수 있다. 또 기능적으로는 정보의 공유와 사고보고 및 대응 조치활동 기능을 강화하여 정부나 기업은 물론 국민 개개인에게까지 역량이 미칠 수 있도록 하고 있다.

1.2 영국의 사례

영국은 사이버 공간의 발전과 확장에 대응하여 기존의 국가 안보조직을 강화하여 사이버 공간 안보 기능을 강화하고 있다. 즉 국가기반보호조정 센터(NISCC)와 국가침해사고대응 센터(UNIRAS)를 설립 운영하고 있다.

영국의 가장 두드러진 특징은 국가 주도의 침해사고 예방 및 대응 시스템이 미치지 않는 정보보호 사각지대를 보완하여 지속적인 정보보호를 추진하고, 관련 정보공유 및 대응을 하기 위해 WRAP(Warning, Advice & Reporting Point)를 설치하고 있다. WARP은 기관이나 단체가 아닌 IT정보보호에 관한 구성개념이다. 침해사고를 예방 및 대응하기 위해서는 위에서 설명한 NISCC나 UNIRAS와 같은 침해사고 대응 기관(CERT)과 연계해서 관련 경보나 대응 방안 등의 정보를 실시간으로 수신하는 방안이 가장 좋다. 하지만 해당 기관이 국내의 중, 소기업, 행정구의 전산 시스템 및 민간 개인 사용자 등에 대하여 모든 침해사고를 담당한다고 하면 해당 기관의 업무가 과도하게 걸려 정상적인 운영이 어려울 것이다. 또한 소규모 단체 역시 자신의 시스템을 보고하기 위해 모니터링하고 관리할 수 있는 설비와 인력을 갖추어야 하기에는 비용이 너무나 많이 든다. 이와 같이 CERT를 구성하기에는 작은 단체와 가정 사용자의 침해사고 예방 및 대응을 위한 작고도 효율적인 구성체가 WRAP이다. 침해공격이 점차 비대칭화하고 바이러스와 웜의 결합, 지능화 등으로 인해 가정의 시스템이 국가와 기업의 주요 정보시스템을 공격하는 거점으로 이용됨으로 가정의 침해사고 예방을 위한 대응책이 무엇 보다 시급하고 중요하게 되었다. 이를 해결할 수 있는 가장 효과적이고 경제적인 모델로서 WRAP는 유럽에 전파되고 있다.

1.3 호주의 사례

호주는 기존의 국가 보안 조직과 기능을 그대로 유지하고, 2002년에 대테러 위원회와 정보기반 보호 그룹을 신설하였다. 따라서 물리적인 테러와 사이버테러의 기능을 통합하여 관련 정책의 수립 시행을 하고 있다. 또 국가 보안 업무를 담당하고 있는 법무부 산하에 기반구조 자문 위원회를 두고 민간과 정부의 협력창구로 이용하고 있으며, 신뢰 정보네트워크(TISN)를 구성하였다.

신뢰정보 공유 네트워크는 2001년 11월에 기반구조 보호를 위해 정부와 민간의 task force형태로 구성되었고 2002년 3월에 민간, 연방정부기관, 주 및 지방 정부의 고위 대표자가 회의를 통하여 구축할 것을 결의하여 시작되었다. TISN은 주요기반 시설의 소유자나 운영자들에게 비즈니스 연속성, 중요한 경영 관련 정보와 정보시스템에 대한 공격, 취약점, 사이버 범죄, 태업이나 공격으로부터 주요 사이트의 보호, 수자원과 음식에 대한 원자력 및 화생방 위협, 해안과 해상 자산의 보호에 관한 정보를 공유하기 위하여 구성되었다. 신뢰정보네트워크의 특징은 정보를 공유하는 신뢰할 수 있는 채널을 확보한다는 것과 정보의 공유는 정부와 국가기관, 기업, 민간 등 사이버 안보와 관련된 모든 기관들의 신뢰를 바탕으로 하지 않으면 안 된다는 것이다. 신뢰 구축에 관한 노력은 많은 국가에서 나타나고 있는데 주로 정보와 민간의 협력체제 강화를 통하여 해결하려고 노력하고 있다. 그러나 호주의 경우 구체적으로 구축된 정보의 활용 방법, 보고 방법과 보고 정보의 공개여부 등을 개인이나 기관의 의사에 따라 추진하도록 하고 있다. 이는 CERT활동에도 커다란 영향을 주어 사고의 보고를 증대시켜 정확한 침해 현황을 파악할 수 있게 함으로써 최적의 신속한 대응을 가능하게 하고 있다.

또한 신뢰할 수 있는 채널의 확보를 위한 노력은 유럽을 중심으로 활발하게 진행되고 있다. 즉 보고 및 정보공유, 그리고 각종 조치사항의 전파를 위한 시스템을 공개소프트웨어를 중심으로 구축하여 공유하고, IODEF 등 보고의 방법을 표준화하는 노력이 진행되고 있다.

2. 침해사고 대응체계 수립 시 고려사항

외국의 사례에서 살펴본 것과 같이 침해사고에 대

응하기 위한 국가체계를 수립하기 위해서는 고려하여야 할 주요한 요소들이 있다.

2.1. 기존 안보기능과 사이버 안보기능의 통합

사이버 공간은 시공을 초월하고 국경이 존재하지 않는 공간이므로 누구에게나 열려있다. 따라서 한 국가의 안보에 관한 정보에서부터 기업의 기술정보, 개인의 사생활 정보에 이르기까지 각종 필요한 정보를 국가안보를 위협하는 집단이나 조직이 획득할 수 있다. 또 이러한 정보가 테러나 사이버테러 나아가서는 전쟁을 발발하기 위한 정보로 활용될 수 있기 때문에 사이버 공간의 침해 행위를 단순히 사이버 공간에서의 단편적인 활동으로 국한하여서는 안 되며 종합적인 국가안보의 차원에서 검토되어야 한다.

2.2. 민간과의 협력체계를 강화해야 한다.

각국의 사이버 공간에 대한 보안은 국가중요기반시설보호로부터 출발하고 있다. 이는 국가주요기반시설의 운영과 관리 통제가 정보통신기술에 의존하고 있기 때문이며, 정보통신망을 기반으로 이루어지기 때문이다. 이러한 정보통신망은 연계되고 상호운용성이 확보될 때에 효율성이 더 커지며 유용성이 높아지므로 오늘날에는 인터넷과 논리적, 물리적인 연결이 되어 민간기업 나아가서 민간의 개인 사용자까지도 접근이 가능하게 되었다. 이러한 현상은 사이버 공간의 안보의 영역을 민간 기업, 민간 개인 사용자에게까지 확대하지 않으면 국가주요기반시설을 보호할 수 없게 만들었다. 따라서 CERT의 활동 영역이 넓어졌고 가정의 사용자들로부터 사고보고를 받고 그들의 정보를 분석 공유하여 대응조치를 지원하지 하지 않으면 안 되게 되었다. 더구나 이러한 활동은 법, 제도로 강제함으로써 이루어 질 수 없는 사항이기에 WARP와 같은 개념이 도입되어 가장 가까이서 지원하고 도움을 주는 민간과의 협력 체제를 구축하지 않으면 안 되게 된 것이다.

2.3. 정보공유가 되어야 한다.

침해사고의 원인이 되는 내외부의 사고는 의도적 혹은 비의도적인 공격으로부터 발생한다. 공격은 시스템이 가지고 있는 취약점과 위협을 대상으로 하고 있으며 취약점은 시스템의 결합, 응용, 상호연결 등이 다양해지고 복잡해질수록 증가하고 있고, 증가하는 취약점만큼 해킹이나 바이러스 기술 또한 자동화, 지능화되고 있어 침해사고의 보고정보가 침해사고를 예방하고 치유하기 위해서 중요한 역할을 한다. 또 각종 취약점을 발견하고 이에 대한 보완 조치 프로그램이나 도구를 업체에서 만들어 배포하고 있다. 공격자가 테러를 지행하기 위해 접속한 시스템과 그들이 사용하거나 변조한 정보에 관한 정보도 테러 활동의 목적이나 증거를 확보하는데 필수적인 정보가 된다. 이와 같은 유형의 정보들은 공유되어 종합적으로 분석될 때에 가장 정확한 현상을 파악할 수 있게 되므로 정보의 공유는 사이버 안보의 필수적인 요소이다. 따라서 정보를 공유하기 위한 방법이 반드시 마련되어야 한다.

2.4. 신뢰관계가 수립되어야 한다.

침해사고를 당하였다는 자체가 조직의 이미지나 명예를 실추시키는 결과를 가져온다고 생각하는 조직이 많다. 또 정보의 제공이나 사고보고는 개인이나 조직의 상황을 타인에게 알리는 결과를 가져온다. 따라서 의도적으로 사고를 은폐하는 경우가 많다. 특히 시스템에 미치는 영향이 경미하거나 내부자에 의해서 발생된 사고의 경우 이를 은폐하여 다른 시스템을 공격하는 숙주로서의 역할을 수행하게 된다. 따라서 정보 공유나 침해사고의 보고는 신뢰관계의 수립이 되어 당사자의 의지가 존중되고 그에 따라 정보가 완전히 보호될 수 있도록 하여야 한다. 또 보고 내용이 전송될 때 전송로 상에서 변조되거나 유출되지 않도록 신뢰네트워크를 통하여 정보가 전송될 수 있도록 인증기반구조를 갖추어야 한다.

2.5. 경보시스템이 필요하다.

최근 바이러스나 웜 등은 전 세계적으로 국가, 시스템의 종류, 응용의 종류, 시간에 관계없이 창궐하고 있으며 분산서비스 거부 공격도 같은 현상을 나타내고 있다. 또 이들은 발생과 동시에 빠른 속도로 전파되어 불과 수분 이내에 전 세계로 전파되는 현상이 나타나고 있다. 이러한 현상을 예방 차단하고 전파를 막기 위해서는 그림 1과 같은 침해사고 대응 생명주기에 따른 활동이 전개될 수 있도록 표준운영절차(sop)가 제정, 시행되고 경보체계가 확립되어 조기에 대응조치를 취할 수 있는 도구나 기술적, 물리적인 방법을 제공하여야 한다.

2.6 국제협력을 위한 관계정립이 필요하다

침해사고의 결과는 우리나라에서 나타나지만 공격의 원천은 반드시 국내에서 존재하지 않는다. 외국의

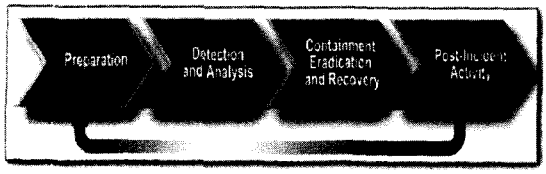

그림 1. 침해사고대응 생명주기

개인이나 집단 혹은 국가단체로부터의 공격이 더 많은 혼란을 초래하거나 경제적으로 치명적일 수 있으며 나아가서 정보전의 경우에는 다수의 대량 공격행위가 국외로부터 이루어 질 것이다. 이러한 공격은 공격 이전의 탐지 활동이 있게 된다. 이러한 증후를 파악하기 위해서, 또 예방을 위한 예경보를 하기 위해서 침해사고 대응 기관간의 국제적인 협조와 정보의 공유가 필수적이다.

3. 우리나라의 대응 현황

우리나라는 사이버 공간에 대한 침해사고 대응을 위한 체계는 "정보통신 기반 보호법"과 대통령 훈령으로 제정된 "국가사이버안전관리 규정"에 근거를 두고 있다.

전자는 국가의 주요정보통신기시설을 보호하기 위한 것으로 국무총리를 위원장으로 하고 중요정보통신기반시설 소관부처인 중앙정부기관의 장을 포함하여 대통령이 지정하는 25인 이내의 위원으로 구성된 정보통신기반보호위원회와 실무위원회를 두고 있다. 또한 주요 정보통신기반시설로서 73개 기관의89개 시설을 지정하고 그를 보호하기 위한 취약점 평가 및 대응계획의 수립과 시행, 침해사고 보고, 대응 조치로서 예경보의 발령과 긴급 대책반의 설치운영, 복구와 정상화 조치 등을 포함하고 있다. 또 정보통신부는 정보보호정책개발 및 정보보호지원업무를 지원하고, 국가정보원은 국가공공기관에 대한 보호지원업무를 지원하도록 하고 검찰청과 경찰청은 인터넷범죄 수사 정보보호 지원을 하도록 정하고 있다. 그 외에도 민간 정보보호 전문 업체를 지정하여 취약점 평가 및 복구 지원을 받도록 하고 있다. 정보공유를 위해 정보공유 분석 및 공유센터의 설립 근거와 침해사고 대응센터와 국가기관간의 정보공유 근거를 마련하고 있다. 침해사고에 대응하기 위한 기술의 개발과 인력 양성을 하한 근거를 마련하고 있다.

반면에 "국가 사이버 안전관리규정"은 국가사이버 안전에 관한 조직체계와 운영에 관한 사항을 규정하기 위한 것으로 국가 사이버안전체계의 수립, 국가 사이버안전 관련 정책을 수립하고 조정하기 위해 국가 사이버안전 전략회의를 국정원장이 위원장이 되고 외교통상부, 국방부, 법무부, 정통부, 행자부, NSC사무차장 등 6인이 위원이 되어 운영하도록 규정하고 있다. 구가 사이버안전센터의 설립과 운영에 관한 사항과 공공기관의 침해사고에 대한 사고통보와 복구, 예경보의 발령 근거를 마련하고 있다. 또 중요한 사항으로는 사고의 조사와 처리에 관한 근거를 두고 있으며 정보공유를 위해 타 기관이 운영하고 있는 CERT, 정보공유 및 분석센터, 기타 유사 업무를 수행하는 조직과의 업무 협력을 하도록 하고 있다. 나아가서 사이버 안전을 위한 기술개발과 인력 양성을 할 수 있도록 하고 있다. 이러한 근거를 기반으로 국가사이버 안전센터와 인터넷 침해사고대응지원센터, 국방 정보전 대응 센터와의 정보공유와 협력관계를 강조하고 있다.

이러한 체계를 가진 우리나라의 침해사고 대응체계에는 몇 가지 문제점이 있다. 그들을 살펴보면, 첫 번째가 국가 안보나 대 테러 측면에서 침해사고에 대한 대응기능을 가지고 있지 않다는 것을 확인할 수 있다. 우선 침해사고의 가장 중요한 목표나 대상이 될 수 있는 것이 주요 정보통신 기반시설이다. 그리고 국가 경제의 동력이 되는 생산시설이나 산업시설, 연구시설 등 일 것이다. 그러한 침해 대상 목표에 대한 등급의 분류와 그에 상응하는 침해사고 대응체계가 갖추어져 있어야 함에도, 현재는 소관 부처의 장에게 보고절차, 긴급 대응절차를 일임하고 있다. 또 국정원의 협조체계에 의하면 대응센터들이 국가사이버 안전센터에 상호협력 하도록 되어 있어 구속력이 없고 법적으로 불이행에 대한 제재를 가할 수 없다. 또 일반 안보와 관련된 국가 최고 안보기구인 국가안전보장회의에 대해서는 사고와 관련된 직접적인 보고를 하는 규정이 없고 기존의 업무의 일부로서 위기관리 센터에 보고하는 것으로 되어 있어 그 시행력이 약하고 심각한 상황이 발생할 경우 국가적으로 대응할 수 있는 능력이 의심된다. 따라서 법적으로나 제도적으로 체계가 이루어지도록 하여야 하며, 임시적이고 정권 차원의 묵시적인 업무의 분장이나 위임은 책임과 의무가 결여되어 있어서, 국가안보에 위협이 될 것이다.

두 번째, 사이버 침해사고에 대한 총체적인 정책의 수립과 집행을 하고 그에 상응하는 책임질 부서가 없다. 이는 아직도 정부가 침해사고를 단순히 인터넷 상에서 발생하는 사고에 불과하고 그것이 국가 안보와 직결된다는 것을 인식하지 못하고 있다는 것이다. 실

제로 정보통신 전문가나 국방 정책 전문가, 국가 안보 전문가들의 일부를 제외하고 사이버테러나, 정보전에 대한 심각성을 인식하고 있는 정치인이나 행정가들이 거의 없다는 것이다. 따라서 사이버 침해사고나 사이버테러에 관련된 국가안보 정책과 관련한 정부 내의 임무부여와 책임이 명시되어 있지 않은 원인이 되고 있다. 이는 미국과 캐나다, 유럽 연합 등이 사이버 침해사고를 국가 안보의 핵심위협으로 판단하고 부서를 통합하고 정보를 공유하는 체제를 갖추고 임무와 책임을 통합 관리하는 형태의 정부 조직으로 전환한 것과는 너무나 대조적인 상황이라 하겠다. 이러한 것이 명확히 정의되지 못한 상태에서 마련되어 시행하는 예. 경보체제, 침해사고 보고, 침해사고 대응 및 복구체제 등은 당연히 일관성이나 합리성이 결여된 효과 없는 것이 될 수밖에 없을 것이다.

세 번째로, 예 경보체계의 모순이다. 국정원의 업무체계에서는 국방 분야, 민간 분야, 정부 및 공공 분야로 나누어서 각각의 대응 센터에서 소속기관들의 보고사항 등을 분석하여 예. 경보를 발령하는 것으로 되어 있다. 그러나 정보통신 기반 보호법에 의하면 정보통신부와 국가정보원이 각각 예.경보를 발령하는 것으로 되어 있다. 이는 한 개의 국가에서 동일한 사이버 공간에 대해 두 개의 기관에서 서로 다른 경보를 발령할 수 있다는 것이고, 실제로 그러한 사례가 발생하였다. 또한 예. 경보를 발령하는 방법이나 수단에 대해서는 언급을 하지 않고 있다. 이는 지휘계통을 통한 하달이나 전파를 의미하는 것으로 판단된다. 그러나 불과 수 초내지 수 분만에 상황이 종료되는 사이버 침해에서 일반적인 안보 상황의 경보하달과 같은 방법의 하달은 의미가 없다.

네 번째, 침해사고 보고 체계에 대한 모순이다. 침해사고가 발생하였을 경우 중요정보통신 기반 시설을 관리하고 있는 관리기관은 소관부처가 마련한 보고체계에 의해서 보고를 하게 되어 있다. 그리고 소관부처는 국가정보원이 정한 보고체계에 의해서 국가 사이버 안전센터에 보고를 할 것이다. 그러나 민간 분야에서는 보고 자체가 의무 사항이 아니다. 따라서 중요정보통신 기반 시설을 제외한 민간 분야의 침해사고에 대해서는 자발적인 신고에 의존할 수밖에 없는 상황이다. 특히 침해사고가 빈번히 발생하는 기관은 기관의 대외 이미지 추락을 염려하여 보고를 기피하는 경향이 있는 것이 침해사고의 특징이다. 따라서 정확한 사고의 파악조차 현재와 같은 상황에서는 불가능하게 되어 있다. 따라서 신뢰관계를 형성할 수 있는 조치가 필요하다.

다섯째, 민간과의 협력 체계가 민간의 사고보고나 민간의 대응조치를 위한 체계를 마련한기 위한 활동이 되지 못하여 실질적으로 침해사고 대응 능력이 없는 중소기업이나 개인사용자들은 침해사고로부터 완전히 노출된 상태에 처해 있다. 현재 민간과의 협조체계는 국가 정보원에서 운영하고 있는 국가정보보안 협의회는 국정원의 사이버 보안 업무를 추진하기 위한 자문기구로서의 역할을 하는 것일 뿐 민간이나 개인 사용자 등의 인식확산이나 지원을 위한 기구라고 할 수 없다. 또 개인정보관리 책임자 협의회나 금융정보보호 협의회 역시 각 분야의 정책시행을 위한 자문 기구에 불과하다. 정보보호 실천 협의회는 민간에게 정보보호의 중요성을 인식시키기 위한 기구로서 다양한 대 국민 홍보활동을 하고 있는 것으로 판단된다. 그러나 홍보와 더불어 국민들이 신뢰를 가지고 침해사고를 보고하고 이를 토대로 대응책을 수립하고, 그들을 침해사고로부터 보호하고 침해사고 발생 시에 복구를 하여 주어 국민 개개인이 사이버 공간의 안전을 위한 국가 노력에 적극 참여하는 기반을 만들어야 할 것이다.

여섯째, 정보통신 기반 보호법이나 사이버안전에 관련된 법에서는 주요기반 시설에 대해서 취약점의 분석 평가와 대응 조치 계획의 수립과 시행을 하도록 규정하고 있다. 또 국가정보원은 국가기관에 대해서 사이버 안전 조치의 이행이나 안전정도를 감사할 수 있도록 되어 있다. 그러나 계획의 불이행이나 감사 지적사항에 대한 후속조치가 미흡하여 위험 요소가 쉽게 제거되지 못하고 있는 실정이다.

일곱째, 국외 협력 체계의 구축에 대한 국가 차원의 정책이 부재하다는 것이다. 현재 사이버 테러나 침해사고와 관련하여 정부부처간의 협력 체제를 구축하여야 할 것이다. 즉 국제적인사이버 테러리스트에 관한 정보나, 사이버 테러 조직에 관한 정보, 그들의 동향 정보, 테러 발생 증후에 관한 정보, 등의 협조체제가 마련되어 있어야 할 것이다. 그러나 우리나라는 아직 테러와 사이버 테러에 관련된 법과 제도가 미비하여 책임 있는 정부부처가 없다. 이러한 상황에서 적극적인 정보교류를 위한 협력체계가 마련되기는 어려울 것으로 판단된다. 또 침해사고에 대한 협력체계 구축에 있어서도 미국의 FIRST, CERT/CC, 등과 기관별 혹은 센터별로 각각 협력 관계를 유지하려고 하고 있어 상대편에서 인식하기를 회원 중에 하나로 인식되어 그 이상의 정보 교류나 기술 교류가 이루어 지지 않고 있다고 판단된다.

Ⅲ. 결 론

침해사고에 대한 대응체계는 이제 정부와 공공, 그리고 주요 정보통신기반구조에 한하여 체계를 확립하는 것은 바람직하지 않다. 왜냐하면 공격기법이 점차 자동화, 지능화되어 가고 있고, 제 3의 시스템을 통한 우회, 집단 공격의 유형을 택하고 있어서 가정이나 개인 사용자 시스템이 정부나 공공기관 혹은 주요한 기반시설의 시스템을 공격하기 위한 거점으로 이용되고 있어 총체적인 대응을 하지 않으면 안 되기 때문이다.

무엇보다 중요한 것은 사이버 안보에 대한 정책수립, 상황의 파악과 분석, 대응 계획의 수립 등을 총괄하는 부서를 정하고 임무와 책임을 부여해야 한다. 이때 고려해야 할 사항은 국가안보 업무와 밀접한 관계를 유지할 수 있도록 하여야 하며, 테러에 대한 대응체제를 함께 갖추도록 해야 한다. 현재와 같이 국가정보원의"국가사이버 안전관리 규정"과 정보통신부의 정보통신기반보호법에 의한 체제로 이원화되어 있는 대응조직체계를 일원화하거나 대 테러법, 정보전 수행과 관련된 국방관련법을 제정하고 현재의 국가안전보장회의 법을 보강하여 사이버안보를 국가안보의 중요한 사항으로 포함시킴과 동시에 총괄적인 정책 수립과 시행, 사고대응과 정보공유 등이 이루어지도록 해야 한다.

두 번째가 사고의 보고, 정보공유, 대응책의 전개 등을 위한 조직 구조로서 컴퓨터를 인터넷에 연결하여 사용하는 사람들을 그들이 속한 조직이나 사용 환경, 네트워크의 연결 방법 등을 고려하여 그룹핑하여 조직화하고 보고활동과 정보공유 활동, 그리고 경보의 전달과 예방, 봉쇄, 복구 활동이 체계적으로 이루어 질 수 있도록 하여야 한다. 그들을 아래와 같이 그룹핑하고 그림 2과 같이 신뢰 네트워크를 구성하여 사고의 보고와 정보의 공유 환경을 형성해야 한다.

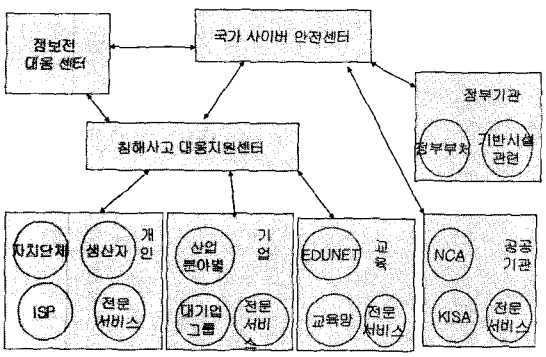

그림 2. 침해사고 대응 조직과 보고채널

- ☐ 정보통신 기반보호시설의 소유 혹은 운영 기관
- ☐ 국가 안보기관(국가 정보기관, 외교, 통일, 국방 등)
- ☐ 정부기관(중앙정부 및 지방 자치단체를 포함)
- ☐ 정부 산하 기관 및 투자 기관
- ☐ 각종 학교 및 교육 기관(초중고교 및 대학, 특수학교 등)
- ☐ 산업체(대기업과 중소기업의 구분, 산업 분야별 세부 구분 등이 필요)
- ☐ 가정과 개인 사용자

재원을 고려한 분야별 CERT나 영국의 WARP와 같은 조직을 구성하되 그림에서 표시된 것과 같이 기존의 조직을 확대 보강하도록 하고 규모에 따라 정보수집, 취약점 분석, 대응조치 방법의 수집과 배포 등의 기능을 보유한 종합 상황실에서부터 단순히 보고와 정보의 전달을 하는 가장 적은 규모의 조직 등으로 구성되어야 할 것이다. 또한 보다 안전한 사이버 환경을 원하는 기업이나 개인 등을 위하여 전문적인 보안관제 서비스를 하는 기업을 육성하고 그들이 수집한 정보를 공유할 수 있도록 하여야 할 것이다.

셋째, 예보와 경보는 무엇보다 먼저 사고보고와 침해사고에 대한 분석이 우선되어야만 가능한 절차이다. 조직적인 체계의 확립과 더불어 신뢰 네트워크의 구성과 정보의 전달을 위한 표준화된 보고 양식, 통계 형식 등이 중요하다. 안전한 네트워크를 구성하기 위한 기술적인 조치가 있어야 하는데 유럽과 같이 공개 소프트웨어를 기반으로 한 신뢰네트워크를 구성하여 특정 기업이나 국가의 제품으로부터 탈피하고 우리의 산업을 발전시킬 수 있는 계기를 마련해야 할 것이다. 또 보고 및 통계 양식은 국제 표준화 되고 있는 common language인 IODEF 등을 수용하도록 해야 할 것이다.

넷째, 경보의 발령은 물리적인 테러나 국가안보 상황에서의 사이버 테러의 영향을 고려하여 경보 단계를 정하여야 한다. 경보의 발령은 국가 차원에서 국민들에게 경고 수준에 따른 대응을 하라는 것이므로 단일한 체계가 돼야 한다. 현재와 같이 관련 기관의 홈페이지에만 상태를 나타내고 주요기관에게만 알리는 상황에서 조치를 할 것이 아니라 가능한 모든 사이버 공간의 구성원이 경고 사항을 알고 조치할 수 있도록 하여야 할 것이다. 실제 조치 내용을 인지한다고 해도 기술적으로 조치를 취할 수 없는 가정이나 중소기업이 대단히 많을 것이다. 가장 중요한 것은 이러한 조치가

가능하도록 중간단계의 지원 및 보고 체계를 갖추는 것이다. 따라서 우리나라의 경우 중간 단계의 대응기구들(지자체, 생산자 기구, ISP, 전문 서비스 업체 등)은 정보의 분석 능력은 구비하지 못하더라도 보고, 정보 수집과 그들의 DB화 등을 담당할 요원과 함께 발령과 예보 내용을 알리고 필요시 물리적으로 방문하여 조치를 취해줄 요원을 확보하여야 할 것이다. 이는 현재의 상황에서는 기초지방 자치단체마다 적어도 하나의 전문대학, 대학 등이 있으므로 이를 활용하여 파트타임의 업무를 부여하는 것도 좋은 방안이 될 것이다.

다섯째, 국가 사이버 안전센터나 침해사고 대응 지원센터는 현재도 취약성에 관한 DB와 분석, 동향 조사, 추세에 관한 예측 등과 해킹 사고에 대한 동향, 분석, 예측과 관련 DB들을 구축 보유하여 활용하고 있다. 상황 관제를 위해 국내의 주요 네트워크의 모니터링과 예경보 발령 등을 하고 있고 침해사고보고, 국외의 관련 정부 수집, 정보보호 제품에 관한 정보 수집등과 국제 협력 등을 수행하고 있다. 또한 해킹이나 바이러스와 관련된 기술의 연구와 개발, 시험망의 운영, 모의시험 등을 통한 예측과 도구의 개발 노력을 하고 있다. 그러나 국가 최고의 대응 기구로서 미국이나 유럽 등의 국가 CERT나 CERT/CC에서 하고 갖추고 있는 기능이나 연구들이 우리의 국가 수준의 센터에서도 이루어 져야 할 것이고 다른 나라와의 국제적인 협력의 대표기관도 창구를 일원화하여야 한다.

끝으로 침해사고 대응 기능을 수행하는 조직들은 임무를 수행하고 침해사고를 방지하기 위해 필요한 기술과 방법론, 절차 등, 예를 들면 정보보증, 생존성, 가정이나 개인 사용자를 위한 위험 분석 및 평가, 취약점이나 위협을 제거하는 방법 등에 대한 연구 개발 목표를 제시하고 이를 국가의 정보보호관련 연구 개발 사업에 반영하여야 할 것이다. 또한 정보보호 제품에 대한 규격과 각 규격에 합당한 기능 등에 대한 요구와 정보보호 제품에 대한 기준 등에 대한 제안을 하여 실질적이고 현실적인 상황을 반영한 안전한 제품이 보급되고 구매되도록 하여야 한다. 그러나 정보보호 산업을 육성하고 산업의 기술개발 능력을 고취하기 위해서 업체와 경쟁적으로 유사 아이템을 개발하거나 연구하는 우를 범해서는 안 될 것이다.

국가의 안보는 개인의 인권보다 우선한다. 그러나 개인의 사생활을 공개하거나 파괴하는 행위를 국가 기관이 해서는 안 될 것이다. 따라서 개인 정보의 철저한 보호와 산업의 경영, 기술 등의 비밀을 지켜주어야 할 것이며, 이러한 신뢰를 바탕으로 하지 않는 한 사이버 공간의 안전은 지켜질 수 없다는 것을 분명히 인식하여야 한다.

참 고 문 헌

[1] Critical alert for cyber terror security for national infrastructure (SCADA & DCS)

[2] Overview of attack trend, CERT coordination center, CMU, 2002

[3] The national strategy to secure cyberspace, Homeland Security,Feb., 2003

[4] Proposal for a establishing the European network and information security agency, commission of the European communities, 2003 (http://www.enisa.eu.int)

[5] http://www.niscc.gov.uk

[6] Computer security incident handling guide, NIST, 2004

[7] A policy framework for ISAC community, ISAC council, 2004, 1

[8] An information sharing vision to improve internet security, NSICC, 12, 2002

[9] http://www.uscert.org

[10] NISCC Assurance Report for "The CNI Organisation" June 2004, NISCC

[11] U.S department of Homeland security improve America's cyber security preparedness unveils national cyber alert system, DHS, Jan. 2004

[12] Emergency procedures, http://www.homeoffice.gov.uk/terrorism/emergency/index.html

[13] Responding to intrusions, CERT/CC, May, 2001

[14] 조기경보시스템 구축을 위한 자동화된"종합침해사고대응 시스템"설계 및 기능 연구, KEWIS, 최운호, 2004, 3

[15] 정보통신 기반 보호법, 2002

[16] 국가 사이버 안전관리 규정, 2005

〈著 者 紹 介〉

이 철 수(李 哲 洙)
정회원

1993년 3월~1998년 2월 : 한국전산원 원장
1998년 3월~2002년 6월 : 한국정보보호원 원장
2000년 8월~2002년 12월 : 정보통신대학교 초빙교수
2003년 1월~현재 : 경원대학교 교수
〈관심분야〉 정보보호, 전자정부