情報保護學會論文誌
第19卷 第1號, 2009. 2

국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구

김 영 진,[1†] 이 수 연,[1‡] 권 헌 영,[2] 임 종 인[1]

[1]고려대학교 정보경영공학전문대학원, [2]광운대학교 법학과

A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services

Young-Jin KIm,[1†] Su-yeon Lee,[1‡] Hun-Yeong Kwon,[2] Jong-in Lim[1]

[1]Graduate School of Infomation Management and Security CIST, Korea University, [2]Department of Law, Kwangwoon University

요 약

국가 · 공공기관의 정보통신망에 대한 최근의 사이버공격은 날로 지능화 · 고도화 되어 갈 뿐 아니라 심지어 경쟁상대국이 국가기밀이나 첨단산업기술 절취를 위해 국가차원에서 조직적으로 감행하는 경우도 있어 새로운 국가안보의 위협요소로 대두되고 있다. 이러한 사이버공격에 효율적으로 대응하기 위해서는 기존의 정보보호시스템 운용만으로는 한계가 있어 사이버공격을 실시간 탐지, 분석·대응하는 보안관제가 그 중요성을 더해가고 있다. 이에 본 논문에서는 국가 전산망에 대한 사이버위협 실태 및 대응방안을 살펴본 후 현재 우리나라 국가·공공기관에서 이러한 사이버 공격에 대응하기 위해 실시하고 있는 보안관제 업무의 수행체계·방법 등 실태 분석을 통해 국가 전산망 보안관제 업무를 효율적·체계적으로 수행하기 위한 방안을 모색해 보고자 한다.

ABSTRACT

Recently, cyber attacks against public communications networks are getting more complicated and varied. Moreover, in some cases, one country could make systematic attacks at a national level against another country to steal its confidential information and intellectual property. Therefore, the issue of cyber attacks is now regarded as a new major threat to national security. The conventional way of operating individual information security systems such as IDS and IPS may not be sufficient to cope with those attacks committed by highly-motivated attackers with significant resources. As a result, the monitoring and control of cyber security, which enables attack detection, analysis and response on a real-time basis has become of paramount importance. This paper discusses how to improve efficiency and effectiveness of national cyber security monitoring and control services. It first reviews major threats to the public communications network and how the responses to these threats are made and then it proposes a new approach to improve the national cyber security monitoring and control services.

Keywords : National Security, Security Monitoring and Control, Cyber Attack

접수일(2009년 1월 12일), 게재확정일(2009년 2월 11일)

† 주저자, yjkim243@korea.ac.kr
‡ 교신저자, lsyeon@korea.ac.kr

Ⅰ. 서 론

우리나라는 2008년 현재 초고속 인터넷에 100가구당 91가구가 가입하여 세계 1위, 인터넷 이용자 수는 100명당 71명으로 세계 6위, 컴퓨터 보유대수는 100명당 54대로 세계 17위 등 국가정보화지수가 세계 8위를 차지하는 등[1] 정보화는 선진국 수준에 이르고 있으나 이에 따른 국가 정보보호대책은 미흡하여 국가·공공분야 전산망 해킹사고는 2008년 들어 10월까지 6,496건이나 발생하는 등 매년 증가 추세에 있다. 해킹공격의 수법은 점차 지능화·첨단화·조직화 되어 가고 있으며, 공격목적 또한 해커의 실력과시 등 단순 공격에서 국가기밀이나 첨단산업기술 등 정보절취 또는 국가정보통신망 마비를 노린 사이버정보전 양상으로까지 변화되고 있어 국가안보의 직접적인 위협요인으로 대두되고 있다.

이에 반해, IT 환경은 BT·NT 등과 융합되어 새로운 유비쿼터스 환경으로 진화되고 있으며, 인터넷·웹 기반의 IT 기술은 점차 WiBro, RFID 등 유무선 통신·방송기술과 융복합되어 'Always Connected' 환경으로 발전하고 국가·공공분야 행정환경도 오프라인, 제한된 비공개 업무환경에서 점차 인터넷 기반의 공개서비스로 진화함에 따라 정보보호 환경은 날로 취약해져 가고 있는 추세이다. 그 결과, 침입차단·탐지 등 정보보호시스템 운용만으로는 이러한 사이버공격이나 취약요인에 철저히 대처할 수 없는 한계상황에 직면해 있다. 이에 따라, 최근에는 민간분야는 물론 국가·공공분야에서도 정보통신망이나 정보화시스템에 대한 사이버공격을 실시간 탐지, 분석·대응하기 위해 점차 사이버 보안관제센터를 설립, 운영하고 있다. 그러나 아직까지 보안관제에 관한 명확한 법 규정이나 관련 지침이 없고 보안관제시스템 구축, 운영에 대한 표준화는 물론 각 보안관제센터간 사이버 위협정보나 관제기술 공유 등을 통한 사고 재발방지 등을 위한 공동 대응방안도 마련되어 있지 않아 효율적인 보안관제업무 수행에 차질이 초래되고 있는 실정이다.

따라서 본 논문에서는 국가 전산망에 대한 사이버위협 실태 및 대응방안을 살펴본 후 현재 국가·공공기관에서 이러한 사이버 위협에 대응하기 위해 실시하고 있는 보안관제 업무 수행체계·방법 등 실태 분석을 통해 국가 전산망 보안관제업무를 효율적·체계적으로 수행하기 위한 방안을 모색해 보고자 한다.

Ⅱ. 보안관제의 개념 및 외국의 사례

2.1 보안관제의 개념

지금까지 전산망 보안관제에 관해 법 규정이나 학술적으로 개념정의가 되어 있지 않은 실정이다. '보안관제'(保安管制)란 용어는 영어로는 'Security Monitoring' 또는 'Security Monitoring & Control' 등으로 사용되고 있는데 Monitoring의 사전적 의미는 '컴퓨터의 프로그램 수행중 일어날 수 있는 여러 가지 오류에 대비하기 위한 감시활동'이라고 설명되어 있으며 우리나라 국어사전에는 '관제'에 대해 '국가나 공항 따위에서 필요에 따라 강제적으로 관리하여 통제하는 일을 말함'이라고 되어 있다. 그러나 이러한 설명은 현재 우리나라 보안관제서비스 업체나 국가·공공기관 등에서 수행하고 있는 전산망 보안관제의 개념과는 다소 거리가 있다. 우리나라에서는 1999. 9. 21.부터 안랩코코넛이 민간업체를 대상으로 보안관제서비스 사업을 최초 시작한 이래 현재까지 보안관제의 개념에 관한 명확한 정의가 없는 상태에서 민·관·군에서도 '보안관제'란 용어를 도입하여 사용해 오고 있다.

외국의 경우에도 보안관제의 개념에 대한 정의를 찾아보기가 어려우나, 미국의 학자가 전산망 보안관제에 관해 '네트워크 트래픽 분석도구를 이용하여 24시간 서버와 네트워크를 통해 통신한 방대한 데이터에서 잠재적인 침입자의 공격시도를 규명하고 이러한 과정에서 분석된 내용을 토대로 불명확했던 침입시도를 규명하는 일련의 행위[2]라고 정의한 바 있다. 하지만 이것도 우리나라에서 수행하고 있는 보안관제의 일부 업무만을 설명한 것에 불과하다.

여기서 보안관제의 개념 정의에 앞서 검토되어야 할 사항은 관제업무의 내용과 범위이다. 다시 말하면, 사이버공격을 탐지, 분석, 대응하는 세부 내용은 무엇이고, 이중 어느 단계까지의 업무를 보안관제의 범위에 포함할 것인지 여부에 대한 검토가 있어야 할 것이다. 우선 보안관제와 관련하여 사용되는 용어의 개념을 살펴보면 다음과 같다.

2.1.1 사이버 공격[3]

‘사이버 공격’은 정보통신시스템에 저장되어 있거나 정보통신망을 이용하여 소통되는 정보의 절취나 위변조 및 가용성(Availability) 등을 저해하는 일체의 행위로서, 해킹, 전자우편 폭탄, 해킹프로그램이 은닉된 이메일, 서비스 장애(Dos), 트로이 목마(Trojan Horse), 논리폭탄(Logic bomb), 웜(Worm), 트랩도어(Trap Door), 스니핑(Sniffing) 등이 공격수단으로 사용되고 있다.

2.1.2 사이버공격 탐지

국가전산망에 대한 전체적인 트래픽 급증·급감 및 내부 정보를 절취하기 위한 해킹시도 및 악성해킹프로그램 유포 등과 같은 사이버공격 시도를 보안관제시스템을 이용하여 사전에 알아내는 행위로서 웜바이러스(봇계열, 전자우편 등), DNS 정상작동여부, 홈페이지 단절·지연·오류 등의 현상을 실시간으로 탐지한다. 또한 국가전산망이 해킹 경유지로 악용되지 않도록 보안취약점을 발굴하는 활동도 이에 포함된다.

2.1.3 탐지결과 분석

경유지악용, 해킹메일 유포, 홈페이지 위변조, 정보자료 절취 등과 같은 해킹시도를 탐지한 뒤, 최신 해킹기술 및 침해당한 전산망의 관련 로그정보를 수집하여 공격자정보, 공격시간, 공격방법 등을 알아내고 자료절취 및 관리자권한 피탈 등의 피해규모를 파악하는 행위를 말한다.

2.1.4 대 응

해킹사실을 피해기관에 통보하고 분석단계에서 파악된 공격자 정보와 취약점 정보를 활용하여 피해시스템이 정상적으로 운영될 수 있도록 신속하게 전문기술을 제공하며 또한 공격에 사용한 해킹도구 및 해킹기법을 토대로 同 해킹공격 탐지기술(Signature)을 개발하여 보안관제업무에 활용함으로써 동일한 침해사고 발생을 미연에 방지한다.

현재 보안관제는 각 보안관제센터의 기술 수준이나 관제노하우 등에 따라 탐지, 분석, 대응활동이 다양한 형태로 이루어지고 있다. 따라서, ‘보안관제의 정의’는 보안관제 업무의 세부내용을 수행하는 범위에 따라 협의의 보안관제와 광의의 보안관제로 나누어 볼 수 있다. ‘협의의 보안관제’는 Monitoring 즉 사이버공격을 탐지하는 활동만을 일컫는 말이고, ‘광의의 보안관제’는 Monitoring & Control 즉 탐지, 분석, 대응까지 포함하는 일련의 활동을 포함하는 개념이라고 볼 수 있다. 보안관제 서비스는 일반적으로 보안관제 대상기관의 자체 보안관제 시설 및 기술의 부족, 전문인력 부재 등의 문제를 해결해 주기 위한 것이므로 단순히 탐지만 하여 결과를 통보해 준다면 보안관제 대상기관에서는 그것을 조치할 능력이 부족하여 보안관제의 효과가 반감될 수 있다. 우리나라 보안관제 서비스 업체나 국가·공공기관의 보안관제센터에서 사용하는 ‘관제’의 범위는 탐지 이외에 분석, 대응까지 포함하는 개념으로 사용하고 있는 실정이다. 현재 보안관제 서비스 업체에서는 통상적으로 보안관제의 업무범위를 사이버 공격을 사전에 탐지, 분석하여 동일 유형의 사고가 재발되지 않도록 대응하는 일련의 활동과정으로 보고 있다[4].

따라서, 본 논문에서는 이러한 현실을 반영하여 전산망 보안관제를 광의의 보안관제 개념으로 보고 ‘정보시스템이나 정보통신망의 자원의 손실이나 정보의 침해를 사전에 방지하기 위하여 이들을 대상으로 수행되는 각종 사이버공격이나 위협행위를 탐지, 분석, 대응하는 일련의 활동’이라고 정의하고자 한다.

2.2 외국의 보안관제 실태

외국에서는 미국·영국 등 소수의 국가를 제외하고는 대부분의 국가에서 현재까지 국가·공공기관을 대상으로 보안관제를 수행하지 않고 있는 것으로 확인되고 있다.

2.2.1 미 국

미국은 9.11 테러이후 사이버테러에 대비하기 위해 국토안보전략(National Strategy to Cyber Terrorism) 차원에서 적극적인 연구와 노력을 기울이고 있다.

현재, 美 연방정부기관 전산망에 대한 사이버위협징후 모니터링 등 관제업무는 국토안보부 (DHS: Department of Homeland Security)내의 국가사이버보안처(NCSD: National Cyber Security Division) 산하 US-CERT에서 수행[5]하고 있다.

① **NCSD**는「국토안보대통령명령(HSPD-7)」에 의거 2003. 6월에 설립되었으며 산하에 미국 사이버침해사고 대응팀(US-CERT)을 운영하고 있다. 2004년도에 미국내 600여개 기관중 15개 주요기관에 유해트래픽 감시시스템(Einstein)을 설치, 24시간 보안관제를 수행중이나 해킹 탐지엔 능력이 다소 부족하여 현재, 네트워크 패킷내에 해킹코드 은닉여부를 파악하기 위한 Einstein2를 개발중인 것으로 알려지고 있다. 또한, 사이버 위협경보발령 및 연방정부 정보통신망에 대한 취약성을 평가하고 CIIMG(Cyber Interagency Incident Management Group) 보안포털 사이트를 통해 CIA, 법무부, 국방부 등 관계기관과 실시간 정보공유체계를 유지토록 하고 있다.

최근 들어 국토안보부는 중국 등 해외 스파이로 추정되는 해커의 공격으로 인해 주요 정부기관의 컴퓨터시스템 정보가 노출되는 사고가 빈발하자 장관 직속의 '국가사이버안보센터(NCSC)'를 신설(2008. 3월), FBI・NSA・국방부 공조 하에 연방정부기관의 컴퓨터시스템에 대한 사이버테러를 감시하고 해킹 취약정보를 관리하는 등 모든 연방정부기관의 컴퓨터시스템과 인터넷보안을 총괄하는 범 부처기구로 운영하고 있다[6].

또한 국가 주요자산에 대한 사이버 공격에 대응할 수 있는 능력을 점검하기 위해 매 2년마다 사이버 훈련(Cyber Storm)을 실시하고 있다.

② **국가안전부(NSA: National Security Agency)** 정보보증국(IA)에서 국방망 일부 및 정보기관들이 사용하는 정보망 등 주요 국가기밀을 보관, 소통하는 정보시스템 보호를 목적으로 테러상황실(TOC: Threat Operation Center)를 설치, 24시간 보안관제 활동을 수행하고 있다.

③ **국방부(DoD: Department of Defense)**는 전략사령관 직속에 연합컴퓨터센터(JTF-CNO: Joint Task Force - Computer Network Operation)를 설치하여 국방 CERT(DISA: Defense Information System Agency)를 중심으로 전 세계에 주둔하고 있는 미군과 정보, 작전 수행 및 사이버공격을 상시 감시중에 있다. DISA는 15~20명 규모의 상황실을 24시간 운영하면서 바이러스・해킹공격 등의 유무를 모니터링하여 사이버공격 정보수집 및 대응활동을 수행중에 있다.

2.2.2 영 국

영국은 2007년 2월 창설된 국가기반보호센터(CPNI: Centre for the Protection of National Infrastructure)의 정보통신보안단(CESG) 초동대응팀(Incident Response Team (GovCertUK))에서 보안관제와 유사한 업무를 수행[7]하고 있다. 초동대응팀은 영국 정부의 컴퓨터 비상대응팀(The UK Govenrnment's Computer Emergency Response Team)을 말하며, CESG의 임무중의 하나인 정부시스템에 대한 전자적 공격의 위험과 후속 여파를 최소화시키는 기능을 수행한다. 이를 위하여 각종 공격형태를 파악하고 사건관련 정보를 수집하여 종합적인 안전대책을 강구하고 있으며, 사이버 위협수준에 따른 경계를 발령하고, 각종 권고발령과 지침을 수립 시행한다.

2.2.3 러시아[8]

연방보안부(FSB) 소속 정보통신정보국(FAPSI)에서 국가기관의 인터넷망에 대해 24시간 모니터링을 실시하고 있다. 사이버위협징후를 탐지, 분석한 후 같은 소속기관인 정보보안센터(ISC)에 통보, 피해 PC에 대한 사고조사, 취약점 개선 등 대응활동과 공격자 색출활동을 수행하고 있다. FAPSI는 ISP업체를 통해 인터넷망에 'SORM'이란 하드웨어 디바이스를 설치하여 인터넷 트래픽에 대해 필터링과 원격제어를 하고 있다.

2.2.4 일 본

일본은 2005년 4월 「정보시큐리티센터의 설치에 관한 규칙(내각총리대신결정)」에 의거 설립한 '내각관방

정보보호센터(NISC, National Information Security Center)'에서 2009년 1월 부터 중앙 성청(省廳)에 대해 24시간 해킹·웜 바이러스 등 사이버위협징후에 대한 모니터링을 실시하고 있으며, 탐지된 위협에 대해서는 공격자정보, 공격시간, 공격방법 등을 분석하여 해당 성청(省廳)에 지원하는 업무를 수행중이다.

Ⅲ. 보안관제업무 수행실태 및 문제점

3.1 국가·공공기관 사이버위협 실태

우리나라는 1980년대 말부터 국가·공공기관에 컴퓨터가 본격적으로 보급되기 시작하였으나 당시에는 인터넷이 서비스되지 않아 사이버위협은 그다지 많지 않았다. 1994. 6월부터 일반인을 대상으로 인터넷 상용서비스가 시작된 이래 국가·공공기관에서도 점차 인터넷을 도입하여 업무에 활용하기 시작하면서부터 사이버위협 요인도 그만큼 증대되어 갔다. 왜냐하면, 국가·공공기관에서 하나의 컴퓨터를 업무용과 인터넷용으로 함께 사용함에 따라 컴퓨터에 저장되어 있던 주요 업무관련 자료들이 해커들의 절취 표적이 되었기 때문이다. 2007년도에 국가사이버안전센터에서 탐지·처리한 전체 국가·공공기관의 사이버 침해사고는 총 7,588건으로 2006년도의 4,286건보다 2배 가까이 증가한 것으로 나타난 것이 그 예라고 할 수 있다[9]. 이러한 사이버공격은 점차 고도화, 지능화 되어가고 있어 사이버위협도 그에 따라 날로 증대될 것으로 예상되며, 사이버공격의 형태도 점차 변화하고 있다. 우선, 단순 과시형 공격에서 내부 정보 절취를 목적으로 하는 공격과 정상적인 서비스를 방해하는 DDoS 공격 등으로 변화되면서 전산망의 안전성을 위협하는가 하면, 심지어 금전을 요구하기도 한다. 또한 국가간의 외교문제에 있어서 경쟁 상대국의 국가기밀 및 첨단기술 절취를 목적으로 하는 공격이 증가하고 있으며 조직적인 공격을 위한 해킹부대를 설립, 국가간에 정보전 양상으로까지 발전하고 있는 추세이다.

국가간 사이버 정보전 준비실태를 살펴보면, 중국은 인민해방군내에 6천여명 규모의 전문 해킹조직을 운영하고 있고, 미국은 2001년 이후 국방부와 주요 정부기관 웹사이트에 해커가 침입, 기밀문서가 유출되는 사건이 빈발하자 중국정부를 배후로 지목하고 사이버보안을 더욱 강화하고 있다. 최근에는 사이버전에 대비한 가상공격 체계를 수립한 것으로 알려졌는데 미 공군이 2008년 10월까지 4대 편대로 구성된 사이버사령부를 신설해 적의 통신시스템을 교란하거나 데이터 패킷을 파괴하는 등 사이버 공격 정예부대로 양성한다고 밝힌바 있다[10]. 이는 그동안 미 정부가 사이버전 전략을 방어위주로 일관해 온 데서 선회하여 이제는 선제공격을 취할 수 있음을 공개적으로 시사한 것이어서 더욱 주목되는 부분이다. 최근 언론에 공개된 국내외 주요 사이버공격 사례를 살펴보면 아래[표 1]와 같다.

[표 1] 주요 사이버테러 사례[11]

구분	사 례	내 용
해외사례	그루지야-러시아간 사이버전 확산 (08. 8.)	양국간 영토분쟁으로 무력충돌과 병행하여 그루지야 주요부처 인터넷 사이트가 러시아(추정지)'로부터 무차별 DDoS 공격을 당해 사이트가 초토화됨 (WSJ, NYT 등 보도)
	독일 총리실, 외무부, 경제부 등 전산망 해킹 (07. 5.)	독일 시사주간지 슈피겔이 중국 해커가 정부 주요 부처 컴퓨터에 침투했다며 중국군대 소속 해커에 의한 것으로 파악 보도
	미 국방부 컴퓨터 네트워크, 1주일 넘게 내부조사 (07. 6.)	영국 파이낸셜타임스는 국방부 전산망이 와해 일보 직전까지 감에 따라 로버트 게이츠(Gates) 국방장관 집무실로 연결되는 전산망을 차단하였다며 중국 인민해방군이 해킹의 '진원지'임을 확인
	러시아 해커, 에스토니아 사이버 테러 (07. 6.)	에스토니아의 舊 소련군 동상 철거에 격분한 러 해커들이 에스토니아 대통령궁, 정부부처 등에 대한 사이버테러를 감행, 2개월간 행정업무 마비 등 국가적 혼란 야기
국내사례	이명박 방문일정 제하 해킹메일 (08. 3.)	'이명박 방문일정' 제하 해외발 이메일이 각급기관에 발송. 이에는 '대통령 출국일정'이라는 제목의 해킹프로그램이 은닉된 문서를 첨부
	한국원자력연구소와 외교부 등 10개 기관 및 국내 주요 언론사와 웹사이트 무더기 해킹 (04. 4.)	외국에서 국가지원을 받는 것으로 추정되는 조직적인 해커가 정보유출용 악성코드가 삽입된 문서를 첨부한 이메일을 이들 기관에 발송, 주요 기밀자료 절취 시도

3.2 보안관제업무 수행실태 및 문제점

우리나라 국가·공공기관에 대한 보안관제업무는 2002년 12월 금융결제원에서 18개 시중은행에 대한 보안관제를 위해 설치한 금융 ISAC을 시작으로 각급기관이 독자적으로 수행해 오다가 2003년 1.25 인터넷 대란을 계기로 2004년 2월에 국가사이버안전센터가 출범하여 국가·공공기관을 대상으로 국가차원의 종합 보안관제센터 기능을 수행하게 되었다.

2008년 12월 현재 우리나라의 보안관제기관은 국가사이버안전센터를 비롯하여 각 중앙행정기관이 설립한 분야별 보안관제센터 및 각 개별기관별로 운영중인 단위보안관제센터 등이 있다.

국가사이버안전센터는「국가사이버안전관리규정(대통령훈령 제141호)」에 의거 2004년 2월 국가정보원내에 설립되어 국가 주요 정보통신망을 대상으로 범국가차원의 보안관제업무 수행을 위해 각급기관 전산망의 특성·중요도 및 보안시스템 운영환경 등을 고려한 24시간 사이버공격정보 탐지 및 종합분석·대응체계를 유지하고 있다. 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를 발령한다[12]. 또한, 첨단 사이버공격에 효율적으로 대처하기 위하여 최신 보안관제기술을 개발하여 관제업무에 활용하는 한편 여타 관제센터에도 지원하고 있는데, 이러한 활동에 대한 법·제도적 근거는 다음[표 2] 보안관제 업무 수행을 위한 내용 및 관련 규정과 같다.

분야별 보안관제센터는 중앙행정기관 자체 및 소속·산하기관의 전산망을 대상으로 사이버위협을 탐지, 차단하는 업무를 수행하고 있으며 단위보안관제센터는 해당 기관 자체 전산망에 대한 보안관제업무를 수행하고 있다.

이상에서 살펴보았듯이 보안관제센터는 각급기관이 지속적으로 확대 설립하고 있으나, 다음과 같은 문제점이 상존하고 있는 실정이다. 첫째, 사이버공간에 대한 국가안보 및 국가이익 보호차원의 방어체계가 미흡하다. 육·해·공 등 물리적 공간에 대한 방어체계와 달리 사이버공간에 대해서는 각 보안관제센터가 사이버공격을 탐지 차단하고 있는데, 대부분 웜·바이러스 등 단순 사이버공격을 탐지 차단하는 수준에 머물고 있어 첨단 방

[표 2] 보안관제 업무 수행을 위한 내용 및 관련 규정

구분	주요내용	법적근거	
		관련규정	세부내용
사이버 위협 탐지 활동	보안관제	국가사이버 안전관리 규정[13]	제8조(국가사이버안전센터) 제2항 제3호 제14조(전문기관간 협력) 제1항
	예·경보 발령 및 전파	국가사이버 안전관리 규정	제8조(국가사이버안전센터) 제2항 제3호 제11조(경보발령) 제1항 제12조(사고통보 및 복구) 제1항
대응·복구 활동	사고조사 및 복구	국가사이버 안전관리 규정	제13조(사고조사 및 처리) 제14조(전문기관간 협력) 제1항 제15조(연구개발) 제1항
		국가정보 보안기본 지침[14]	제107조(정보보안사고 처리 및 조사)

위산업기밀이나 국가 핵심기술 등 국가안보 또는 국가이익을 침해하는 해킹공격 탐지 차단에는 미흡하다. 둘째, 대부분의 보안관제센터는 보안관제 전담조직과 전문 인력이 부족하고, 24시간 관제업무를 수행하지 않는 기관도 있어 사이버공격 탐지, 분석, 대응역량이 크게 미흡한 실정이다. 셋째, 각 보안관제센터별로 관제업무 수행형태나 방법, 기술수준, 관제시스템 규격 등이 상이하여 상호 관제정보 공유가 곤란할 뿐 아니라, 공유가능한 정보도 각 관제센터간 협조미흡 등으로 서로 공유되지 않아 동일한 침해사고가 다른 기관에서 재발되는 경우도 있다. 넷째, 보안관제활동 수행에 따른 명확한 법적근거가 없어 각급기관이 관제활동 수행에 다소 어려움을 겪고 있다. 현재는「전자정부법[15]」제27조 제3항에 행정기관의 장이 전자문서를 보관·유통할 경우 국가정보원장이 제시하는 보안조치를 수행토록 규정하고 있고,「국가사이버안전관리규정(대통령훈령)[13]」제10조 제1항에 국가·공공기관 및 지자체는 사이버공격정보를 입수한 경우 국가정보원에 즉시 제공토록 규정하고 있을 뿐, 보안관제와 직접 관련된 법 규정이나 세부지침·기준이 없어 체계적이고 효율적인 수행이 곤란하다. 따라서 사이버공격을 국가차원에서 효율적으로 탐지·분석·대응할 수 있는 국가 전산망 보안관제체계 구축 필요성이 긴요한 실정이다.

Ⅳ. 국가 보안관제업무의 효율적 수행방안

4.1 보안관제센터 구축 및 운영기준 표준화

국가·공공기관에 대한 보안관제 업무를 효율적·체계적으로 수행하기 위해서는 각 보안관제센터간에 관제기술 및 입수한 사이버위협정보를 신속하게 교류하여 공동대응체제를 갖추는 것이 중요하다. 왜냐하면 사이버공격자는 자신의 공격이 보안관제에 탐지, 차단당하지 않도록 하기 위하여 지속적으로 새로운 기법을 개발하여 공격하기 때문이다. 따라서 이러한 보안관제기술 및 위협정보를 신속하게 공유하기 위해서는 각 보안관제센터의 관제시스템 구축 및 운영에 관한 국가차원의 표준화가 이루어져야 한다. 개별 기관의 특성에 맞는 보안관제센터 구축이 필요한 경우에는 정보공유 인터페이스를 표준화하면 될 것이다. 이러한 표준화가 이루어지면 사이버 위협정보 탐지, 대응수준이 지금보다 한층 높아져 국가·공공기관 전산망에 대한 보안수준도 크게 높아질 것이다.

4.2 보안관제 의무화

국가·공공기관의 전산망은 상호 연동되어 있기 때문에 어느 한 기관에서 보안관제를 철저히 하여 사이버위협을 탐지, 차단한다고 하더라도 다른 기관의 전산망이 보안취약으로 사이버공격을 당하거나 악성코드에 감염될 경우 안전성을 보장하기는 어려울 것이다. 따라서 국가 전체 전산망의 안전성을 높이기 위해서는 헌법, 사법, 입법기관을 포함한 모든 국가·공공기관 및 지방자치단체의 정보통신망에 대하여 보안관제를 의무적으로 실시하도록 하여 국가차원에서 체계적으로 사이버공격을 탐지, 차단하여야 할 것이다. 보안관제를 수행하는 방법에는 해당 기관이 보안관제센터를 직접 구축하거나 관계 중앙행정기관이 운영하는 보안관제센터 또는 국가사이버안전센터에 위탁하는 방법이 있다.

4.3 단계별 중첩 보안관제 실시

각 보안관제센터에서 일일 평균 탐지 처리하는 사이버 위협정보는 적게는 수백만 건에서 많게는 수억 건에 이르고 있다. 따라서 수많은 사이버 위협정보를 효과적으로 탐지, 분석, 대응하기 위해서는 각 보안관제센터간에 유기적이고 단계적인 중첩 보안관제체계를 구축할 필요성이 있다. 일일 평균 수백만 건에서 수억 건에 이르는 각종 사이버공격을 어느 한 기관에서 완벽하게 탐지해 내는 것은 현실적으로 불가능하기 때문이다. 따라서, 군에서 실시하고 있는 3선 방어개념과 유사한 제도를 보안관제업무에도 도입하여 단위 보안관제센터, 분야별 보안관제센터, 국가사이버안전센터 간에 상호 임무를 분담하고 단계적으로 중첩하여 사이버공격정보 탐지활동을 수행한다면 보안관제의 효율성이 대단히 높아질 것이다.

4.4 보안관제정보 공유 제도화

어떤 신종 사이버공격이 어느 한 보안관제센터에서 탐지, 차단된 경우에도 다른 보안관제센터에서는 탐지되지 않고 공격에 성공할 가능성은 얼마든지 있다. 그렇기 때문에 이러한 보안관제 정보는 각 보안관제센터간에 위협정보 및 탐지기술과 같은 정보를 공유하여 공동대응체제를 갖추는 것이 무엇보다도 중요하다.

따라서, 사이버공격 처리현황 및 사이버공격 탐지·분석과정에서 수집된 각종 정보들 즉, 해커가 사용하는 IP정보(공격자 정보), 중간경유지와 해킹메일에 대한 내용 등을 체계적이고 신속하게 공유할 수 있도록 제도화하는 것이 필요하다. 각 보안관제센터는 이러한 정보를 활용하여 해킹 탐지기술 등 보안관제기술을 개발하고, 개발된 관제기술은 각 보안관제센터와 공유함으로써 전체적인 보안관제 수준을 높일 수 있다. 보안관제정보 공유를 제도화하는 방법에는 국가사이버안전센터가 전체 보안관제센터의 보안관제 관련정보를 실시간 공유할 수 있도록 통합보안관제시스템을 개발, 운용하면서 분야별 및 단위보안관제센터의 보안관제결과를 종합, 배포한다. 또한, 정기 또는 수시로 각 보안관제센터 운영기관이 참석하는 회의를 개최하여 관련 정보를 공유하는 한편, 민관을 아우르는 사이버공격정보를 종합 분석, 국가차원의 보안대책을 수립 지원하기 위하여 '민관 사이버위협 정보공유·분석센터' 같은 기구를 설립, 운영하는 방법 등을 생각해 볼 수 있을 것이다.

4.5 보안관제역량 제고방안 마련 시행

각 보안관제센터간에 보안관제 기술 수준이 차이가

있을 뿐 아니라 탐지하는 사이버공격정보 및 분석·대응 능력도 상이하기 때문에 각 보안관제센터의 보안관제 역량을 제고하기 위해서는 국가사이버안전센터 등에서 보안관제 관련 직무전문 교육과정을 마련하고 모든 보안관제요원에 대해 사이버위협정보 탐지·분석 및 대응기법 등에 대한 교육을 주기적으로 일정시간 이상 이수토록 의무화하는 것이 필요하다. 또한, 해커의 첨단 공격기법을 이용한 사이버공격을 탐지, 차단할 수 있는 고성능 탐지시스템을 개발, 보급하고 모든 보안관제센터는 관제대상기관 등을 고려하여 적정수의 보안관제 전문 인력을 확보하고 24시간 무중단으로 사이버공격 정보를 탐지, 차단할 수 있는 근무체제를 마련하도록 하여야 할 것이다.

4.6 법·제도적 기반 조속마련 필요

이상에서 살펴본 보안관제의 효율적 수행방안을 실효성 있게 추진하기 위해서는 우선 보안관제에 관한 법적근거를 마련해야 한다. 모든 국가·공공기관에 대해 보안관제를 의무화하도록 규정하고, 법 시행을 위해 보안관제지침과 보안관제센터 구축·운영기준 및 각 보안관제센터의 보안관제 인력이 참고할 수 있도록 보안관제 실무매뉴얼 등을 제정, 시행하는 것이 필요하다. 또한 분야별 보안관제센터는 이에 따라 자체 실정에 맞는 세부지침과 기준을 마련하여 시행하면 체계적이고 효율적인 보안관제업무를 수행할 수 있을 것이다.

Ⅴ. 결 론

사이버공격기술이 날로 다양화·고도화 되어가고 있을 뿐 아니라 일부 국가에서는 상대국가의 국가기밀 절취나 사회교란을 목적으로 국가차원에서 조직적으로 사이버공격을 감행하는 정보전 양상을 띠고 있어 국가정보통신망에 대한 보호대책은 그 어느 때 보다도 중요성을 더하게 되었다. 몇 년 전까지만 해도 침입차단제품이나 침입탐지제품(IDS) 또는 침입방지제품(IPS) 등 정보보호시스템을 도입 운용하는 것이 정보통신망의 중요한 보호수단이었다. 하지만, 최근에는 정보보호시스템을 우회하여 공격할 수도 있으며 다양화되고 고도화된 기술이 출현하면서 정보보호시스템만으로는 정보통신망 보호에 한계가 있어 보안관제의 중요성이 날로 더해가고 있다.

따라서, 국가·공공기관 및 지방자치단체의 정보통신망을 안전하게 보호하기 위해서는 국가차원에서 이들 기관에 대한 보안관제대책을 마련하여 모든 기관이 보안관제를 의무적으로 수행하도록 하고 그 이행여부를 확인 감독할 수 있는 장치를 강구하여 실효성을 확보함으로써 국가보안관리 수준도 높아질 것이다.

그러나, 보안관제를 아무리 철저히 한다고 하더라도 알려지지 않은 신종 사이버공격은 보안관제 과정에서 탐지되지 않으므로 알려지지 않은 사이버공격을 탐지, 차단할 수 있는 기술을 지속적으로 개발해 나가야 한다. 또한, 일부 보안관제센터 운영 기관은 통신비밀보호법 위배 등을 내세워 보안관제 관련 정보공유에 소극적인 자세를 견지하고 있어 국가차원의 공동대응에 차질을 초래하고 있는데, 이에 대해서도 사이버공격으로 인한 피해와 개인정보 보호간에 보호법익을 비교 검토하여 피해를 최소화하는 방향으로 관련 법규를 정비해 나가야 할 것이다.

참고문헌

[1] 한국정보사회진흥원, 2008 국가정보화백서, pp. 42-44. 2008년 8월.

[2] R. Bejtlich, Tao of Network Security Monitoring, the beyond Intrusion Detection: What is Network Security Monitoring, Addison Wesley Professional, pp. 40-41. July 2004.

[3] 노훈, 이재욱, “사이버전의 출현과 영향, 그리고 대응방향,” 국방정책연구, 가을호, 2001년.

[4] 오자영, “보안관제 서비스란 무엇인가?,” 보안뉴스, 2006년 12월 25일.

[5] 미국 국토안보부 조직도 www.dhs.gov/xlibrary/assets/DHS_OrgChart.pdf.

[6] 조윤아, “미 백악관, 실리콘밸리 CEO를 사이버 안보 수장에 발탁,” 전자신문, 2008년 3월.

[7] 이연수, 이수연, 윤석구, 전재성. “주요국의 사이버 안전관련법 조직체계 비교 및 발전방안 연구,” 국가정보학회, pp. 125-128, 2008년 8월.

[8] 정보통신정보국(FAPSI) http://en.wikipedia.org/wiki/FAPSI#FAPSI.

[9] 국가정보원, 정보통신부, 2007 국가정보보호백서, p.16, 2007년 4월.

[10] 조윤아, “美, 사이버전 ‘선제공격’ 선언,” 전자신문, 2008년 4월 7일.
[11] 이연수, 이수연, 윤석구, 전재성, “주요국의 사이버 안전관련법 조직체계 비교 및 발전방안 연구,” 국가정보학회, pp. 112-113, 2008년 8월.
[12] 국가정보원, 정보통신부, 2006 국가정보보호백서, pp. 111-112, 2006년 3월.
[13] 국가사이버안전관리규정, 대통령훈령 제141호, 2005년 1월.
[14] 국가정보원, 국가정보보안기본지침, p. 67, 2006년.
[15] 전자정부법, 법률 제8852호, 2008년 2월.

<著者紹介>

김 영 진 (Young Jin Kim) 학생회원
2007년 6월~현재: 고려대학교 정보경영공학전문대학원 박사과정
<관심분야> 정보보호 법·제도 및 정책, 정보보호제품 평가인증

이 수 연 (Su yeon Lee) 학생회원
2009년 2월: 고려대학교 정보경영공학전문대학원 박사 수료
<관심분야> 정보보호정책, 네트워크 포렌식

권 헌 영 (Hun Yeong Kwon) 정회원
2005년 3월~현재: 광운대학교 법학과 교수
<관심분야> 정보통신정책, 사이버범죄, 법·제도

임 종 인 (Jongin Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책 자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신 정책 자문위원
<관심분야> 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식