情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

# 지식경제사이버안전센터의 대응활동분석과 개선방안

이 승 원,[1†] 노 영 섭[2‡]
[1]지식경제사이버안전센터, [2]서울벤처정보대학원대학교

# Services analysis and improvement of MKE(Ministry of Knowledge Economy) Cyber Security Center

SeungWon Lee,[1†] YoungSup Roh[2‡]
[1]MKE Cyber Security Center, [2]Seoul University of Venture & Information

## 요 약

최근 사이버 테러는 국가와 민간을 넘나들며 그 경계가 제한되지 않고 있으며, 현대전의 양상은 사이버 공격을 활용하여 관련 정보를 유출하고 그 정보를 악의적으로 이용하여 국가 및 기업에 치명적인 피해를 끼치고 있다. 이에 정부는 2008년 7월 25일부터 지식경제부 산하 공공기관의 보안과 사고예방을 위하여 지식경제사이버안전센터를 운영하고 있다. 지식경제사이버안전센터는 보안관제센터로서 사이버공격 정보를 탐지・분석하여 즉시 대응 조치를 수행하고, 수집・탐지한 정보를 국가 사이버안전센터 및 회원기관과 공유한다. 또한 정보공유분석센터(ISAC, Information Sharing & Analysis Center)로서 전자적 제어・관리시스템을 포함한 주요정보통신기반시설에 대한 취약점분석 및 평가를 실시하고, 침해사고대응센터(CERT/CC, Computer Emergency Response Team/Coordination Center)로서 보안사고 예방활동 및 보안사고 대응서비스를 수행하고 있다. 이에 본 논문에서는 나날이 그 역할이 커지고 있는 지식경제사이버안전센터의 설립 목적 및 역할, 수행업무에 대한 서비스를 분석하고 문제점을 파악한 후에 개선 방안을 제시한다.

## ABSTRACT

Cyber attacks expose sensitive information and cause fatal damage in both the public and the private sectors. Therefore, MKE (Ministry of Knowledge Economy) Cyber Security Center was founded on July 25, 2008, to perform three major roles. First, it detects and analyzes cyber attacks for the both sectors. Second, its ISAC (Information Sharing & Analysis Center) service analyzes and evaluates the vulnerability of the communication and network infrastructure to security threats, including control systems. Third, it provides CERT/CC (Computer Emergency Response Team Coordination Center) service to prevent and to respond to computer security incidents. This study focuses on the MKE Cyber Security Center's service analysis, which is playing an increasingly larger role in the both sectors. Based on this analysis, after grasping the response services activity and pointing out the problems, this study suggests improvements to the MKE Cyber Security Center.

**Keywords**: MKE Cyber Security Center, ISAC, CERT/CC, CSIRT

## I. 서 론

2003년 '1.25 인터넷 대란'으로 대부분 인터넷망이 마비됨에 따라, 정부는 인터넷침해사고를 방지하기 위한 여러 가지 대책을 수립, 시행하여 왔고, 침해사고

접수일(2011년 7월 28일), 수정일(2011년 10월 31일), 게재확정일(2011년 12월 30일)
† 주저자, swlee1201@gmail.com
‡ 교신저자, ysroh@suv.ac.kr

가 일어난 1년 뒤인 2004년 1월에 보안에 대한 취약성과 관리소홀 방지를 위한 국가사이버안전센터 운영을 시작했다. 아울러 정부는 2009년 7.7 대란으로 국가의 주요 홈페이지가 DDoS (Distributed Denial of service) 공격을 받은 이후 이러한 사이버 공격으로부터 중요자료 및 국가정보통신망을 보호하기 위한 노력을 기울이고 있다.

2011년 들어 3.4 DDoS 주의 경보 발령 시에도 좀비PC 감염대수는 11만여 대로서 7.7 DDoS 대란 시와 비슷한 규모이나, DDoS 대응 장비 도입 등 전반적인 보안수준 향상으로 사이버 공격으로 인한 피해가 최소화되었다. 소셜 네트워크 서비스 (SNS, Social Networking Service)를 이용한 좀비PC 감염 등 DDoS 변종 공격의 지속적인 확대가 예상되고, 지경부 산하 주요정보통신기반시설의 제어시스템을 직접 파괴하려는 스턱스넷(Stuxnet)은 지속적으로 국가안전을 위협할 것으로 예상되어, 국가사이버안전센터와 함께 중앙행정기관, 지방자치단체 및 공공기관 사이버안전센터의 필요성이 증가하고 있다.

관련 용어의 법률적 정의를 보면 '사이버안전'이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성・무결성・가용성 등 안전성을 유지하는 상태를 말하며, '사이버 공격'이라 함은 해킹・컴퓨터바이러스・논리폭탄・메일폭탄・서비스 방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입・교란・마비・파괴하거나 정보를 절취・훼손하는 일체의 공격행위를 말한다[1].

'보안관제'란 조직의 정보기술 자원 및 보안시스템을 안전하게 운영하기 위하여 사이버 공격 정보를 탐지 및 분석하여 즉시 대응하는 일련의 업무를 말한다[2].

또한 '정보보안' 또는 '정보보호'란 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 회손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 마련하는 것을 말한다[3].

또한 '전자적 침해행위'라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리・메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말하며, '침해사고'람 전자적 침해행위로 인하여 발생한 사태를 말한다[3].

본 논문에서는 지식경제사이버안전센터의 설립배경, 역할, 수행업무 등을 상세히 분석하고, 향후 개선에 대한 방안을 제시하고자 한다.

## II. 현황

### 2.1 설립 목적

지식경제사이버안전센터의 주요 설립목적은 첫째 지식경제부 산하의 공공기관의 위탁을 받은 보안관제센터의 역할을 수행한다. 회원기관의 정보통신망에 대한 모니터링 및 조기 예·경보를 실시하는 것이다. 중앙행정기관의 장, 지방자치단체의 장, 공공기관의 장은 소관 정보통신망에 대한 사이버 공격 정보를 수집・분석・대응할 수 있는 자체 보안관제센터를 설치・운영하여야 한다[1]. 보안관제센터를 운영하는 기관은 보안관제 업무를 하루 24시간 중단 없이 수행하여야 하며 필요한 전담인력을 배치하여야한다고 규정하고 있다. 다만, 불가피한 사유가 있을 경우에는 여타 국가・지방자치단체・공공기관이 운영하는 보안관제센터에 관련 업무를 위탁할 수 있다. 또한 보안관제센터를 운영하는 기관의 장은 필요한 경우에 지식경제부 장관이 지정하는 보안관제전문업체의 인력을 파견받아 보안관제업무를 수행할 수 있다.[1,2]

보안관제센터를 설치・운영하는 기관의 장은 수집・탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다[1].

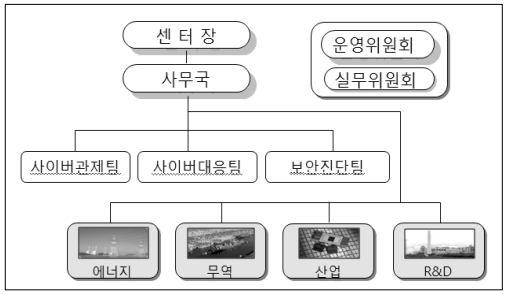
둘째, 보안관제와 더불어 침해사고 발생시 신속한 침해사고 원인 분석 및 적절한 대응조치의 전파·지원 기능을 수행하고 있으며, 국가사이버안전센터와 침해사고의 정보를 공유하고 있다. 이는 침해사고대응센터(CERT/CC, Computer Emergency Response Team Coordination Center)로서도 역할을 수행하고 있음을 의미한다. 공공기관의 장은 사이버공격 정보를 수집할 경우, 피해 유무를 파악하고 공격 IP차단, 로그자료 보존 등 초동조치를 신속하게 취하여야 하며, 이 경우 사고 원인 규명 시까지 피해시스템에 대한 증거를 보존할 필요성이 제기되기도 하며, 때로는 피해를 최소화하는 조치를 취해야 한다. 이에 대한 법적 요건은 정보공유・분석센터이다.[4] 금융・통신 등 분야별정보통신기반시설을 보호하기 위하여 정보공유・분석센터를 구축・운영할 수 있는데 그 수행업무는 ① 취약점 및 침해요인과 그 대응방안에 대한 정보제공, ② 침해사고가 발생하는 경우 실시간 경보・분석체계 운영으로 규정되어 있다[4]. 정보공유・분석센터의 기준은 납입자본금은 20억원 이상, 시행규칙에 명시된 기술인력의 자격기준 15인 이상, 시설 및 장비, 정보보호관리 규정 등에 충족해야 한다[4]. 지

경부 회원기관의 취약점 및 침해요인과 그 대응방안에 대한 정보제공, 침해사고가 발생하는 경우 실시간 경보·분석체계 수행과 더불어, 취약점분석 및 평가의 전담반 역할을 수행하는 정보공유·분석센터의 역할을 담당하는 것이다. 정보공유·분석센터에 업무종사자의 인적사항 등은 관계 중앙행정기관에게 통지하고, 중앙행정기관의 장은 행정안전부 장관에게 통지하도록 되어 있다[4].

셋째, 회원기관의 주요정보통신기반시설에 대하여 취약점 분석서비스를 수행한다. 정보통신기반시설에는 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 등이 있고[4], 지식경제부 산하의 전력, 석유, 가스망 등이 포함되어 있다. 주요정보통신기반시설을 관리하는 장은 최소한 2년에 한 번씩 취약점분석 및 평가를 시행하고 그 결과에 따라 소관 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·관리적·기술적 대책을 포함한 주요 정보통신 기반시설 보호대책을 수립·시행토록 명시되어 있다[4]. 주요정보통신기반시설을 관리하는 장은 취약점분석 및 평가를 위해 시행령에 정한 기준에 따라 취약점분석 및 평가의 전담반을 구성토록 되어있다. 취약점분석 및 평가의 전담반 구성을 위하여 반장, 관리기술 담당, 메인프레임 담당, 응용프로그램 담당, 서버 담당, 정보보호 담당, 네트워크 담당 등 적정 인원으로 전문인력을 확보토록 하였다[4]. 다만, 취약점분석 및 평가 시행을 한국인터넷진흥원, 정보공유·분석센터(ISAC, Information Sharing & Analysis Center), 정보통신산업 진흥법에 따라 지정된 지식정보보안 컨설팅 전문업체, 한국전자통신연구원 등에 위탁할 수 있는데, 이때는 취약점분석 및 평가의 전담반 구성을 면제하고 있다[4].

지식경제사이버안전센터는 보안관제센터 기능과 정보공유·분석센터로서의 침해사고대응 기능이 병존한다고 봐야 하며, 이와 함께 정보공유·분석센터 자격으로 인해 지식경제부 산하 회원기관에 지정된 주요정보통신기반시설에 대하여 취약점분석 서비스를 제공하고 있다.

지식경제사이버안전센터는 에너지·무역·산업·R&D 등 지경부 산하 공공기관의 정보통신기반시설에 대한 사이버안전체계를 확보, 국가안보 및 국민생활 안정에 기여하기 위해 설립·운영하고 있다. 구체적으로 지식경제사이버안전센터 조직은 [그림 1]과 같이 사이버관제팀, 사이버대응팀, 보안진단팀으로 구성되어 있다. 사이버관제팀은 관제서비스, 사이버대응팀은 침해사고




[그림 1] 지식경제사이버안전센터 조직

대응서비스, 보안진단팀은 취약점분석평가 및 교육서비스를 담당라고 있다.

## 2.2 국가사이버안전센터와 관계

현재 국내에서 사이버테러 대응체계는 국가사이버안전체계의 수립 및 개선, 기관 간 역할조정 등 국가사이버안전에 관한 중요 사항을 심의하기 위한 '국가사이버전략회의'와 전략회의의 효율적 운영을 위한 '국가사이버안전대책회의'가 설치됨으로써 사이버안전체계가 설립되었다[6,7]. 공공분야는 국정원의 '국가사이버안전센터'가 기능을 수행하고, 민간분야는 방통통신위원회의 '인터넷침해사고대응센터'가 업무를 담당하며, 국방분야는 2010년 1월 창설된 '국군사이버사령부'가 담당하고 있다.

국가사이버안전센터의 설립 목적은 "국가사이버안전관리규정"에 "사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터를 둔다."고 규정되어 있다[1].

국가사이버안전센터의 역무는 ① 국가사이버안전정책의 수립, ② 전략회의 및 대책회의의 운영에 대한 지원, ③ 사이버위협 관련 정보의 수집·분석·전파, ④ 국가정보통신망의 안전성 확인, ⑤ 국가사이버안전매뉴얼의 작성·배포, ⑥ 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, ⑦ 외국과의 사이버위협 관련 정보의 협력 등이다[1].

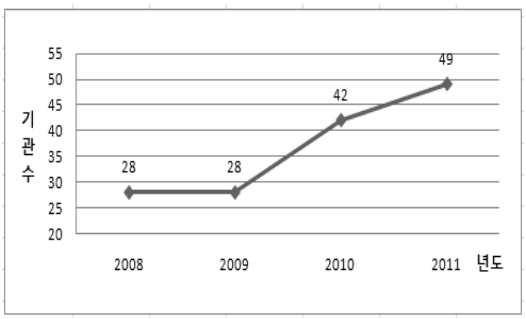
사이버공격과 관련한 정보의 협력은 국가정보원과 각급기관 간에 지체 없이 이루어져야 한다. 즉, 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체 없이 그 사실을 국가정보원장에게 통보하여야 한다. 국가정보원장은 관련 정보를 제공받은 경우 대응에 필요한 조치를 강구하고 그 결

과에 대해 정보를 제공한 해당기관의 장에게 통지하도록 명시되어 있다[1].

## 2.3 서비스 분석

### 2.3.1 서비스제공 대상 기관

지식경제사이버안전센터는 [그림 2]와 같이 2008년 8월 개소 당시 전력·가스·석유 등 에너지 분야 28개 기관에 서비스를 제공하였으며, 2010년에는 서비스 범위를 무역·산업 분야로 확대하여 14개 기관이 추가된 42개 기관에 서비스를 제공하였고, 2011년에는 R&D분야 7개 기관이 추가되어 49개 기관에 대해서 사이버안전서비스를 제공 중이며 앞으로 단계적으로 회원기관의 확대를 추진하고 있다.




[그림 2] 지식경제사이버안전센터 회원기관 현황

### 2.3.2 사이버안전서비스 유형

지식경제 사이버안전센터의 사이버안전서비스의 세부업무로는 ① 사이버공격 실시간 관제·분석, 예·경보 및 기술지원, ② 취약점 및 침해요인에 대한 대응방안 관련 정보 제공, ③ 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원, ④ 정보통신기반시설의 취약점분석 및 평가 및 보호대책 수립 지원, ⑤ 정보보호·사이버안전 교육 및 훈련 서비스 제공, ⑥ 정보보호·사이버안전 관련 국내외 기술·연구 조사 및 각종 간행물 발간, ⑦ 기타 사무국 및 운영위원회에서 정한 업무로 규정하고 있다[5]. 이를 기준으로 볼 때 사이버안전서비스는 관제서비스, 침해사고대응서비스, 취약점분석 및 평가 서비스, 사이버공격탐지 프로그램 개발 및 적용, 보안관련 최신기술 정보공유서비스, 보안기술에 대한 교육서비스 등 다양한 서비스가 제공되고 있으며 이를 기준으로 살펴보기로 한다.

관제서비스로는 24시간 관제전문요원이 관제센터에 상주하면서 실시간 모니터링을 통해 사이버 공격 징후 발생 시 사전탐지·초동 대응을 수행하며, 특히 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 등 침해사고 경보를 탐지할 경우에는 회원기관에 대응조치를 제시한 후 메일로 즉각 전파한다. 이들 내용은 즉시 종합보안관제 시스템에 등록되며, 사후에는 조치결과를 입력하도록 설계되어 있다. 관제와 더불어 Help Desk가 운영되어 침해사고의 구체적 대응요령은 이메일, 문자메시지, 전화 등을 활용하여 제공되며, 감염된 서버 및 PC의 조치 요령, 유해 IP차단 등의 안내로 사이버공격에 대한 확산을 방지한다.

침해사고 대응서비스로는 해킹, 웜/바이러스 감염 등의 침해사고가 의심되는 컴퓨터를 신속히 조사하여 원인을 규명하고, 피해 확산을 방지하기 위한 종합적인 대응방법을 지원한다. 사고의 심각성이 크고, 피해가 확산될 경우에는 회원기관 사고 현장을 직접 방문하여 사고 조사 및 복구를 지원하고, 조사에 시간이 필요하다고 생각될 경우에는 하드디스크를 수거하거나 PC/서버를 수거하여 사이버안전센터에서 디지털 포렌식(forensic) 도구를 이용하여 분석한다. 회원기관의 침해사고지역이 원격지에 위치한 경우에는 신속한 대응을 위해 자체 개발한 침해사고 분석 수집프로그램을 배포하여 자동으로 정보를 수집, 분석하여 침해결과에 효과적으로 대응· 조치하도록 지원하고 있다.

취약성 분석.평가 서비스로는 전자적 침해행위로부터 보호가 필요하다고 인정되는 정보통신기반시설인 주요정보통신기반시설로 에너지 등의 업무와 관련된 전자적 제어시스템에 대해 시행하고 있다. 서비스범위로는 정책, 조직, 인원 등 관리적 보안, 시설물, 통제구역설정, 출입보안 등 물리적 보안, 서버, 네트워크, 웹 등 기술적 보안에 대해 정보보안 관리실태 평가항목과 국가기반시설 전자제어시스템 보안가이드라인을 기본으로 하며, 보안기술검증을 통한 해킹 가능성을 사전 점검하는 서비스가 함께 제공된다. 취약성 분석 및 평가절차로는 환경자산분석, 영역별세부평가, 정보보호 종합 대책 수립으로 구분된다.

보안관련 최신기술 정보공유서비스로는 매일 최신 보안동향을 파악하여 제공하는 일일보안 동향 서비스, 유해IP 차단 리스트와 최신 사이버공격 동향 및 사례 등을 제공하는 주간 동향 서비스가 있다.

보안교육 서비스로는 교육을 통한 정보보호 실무지식 배양을 목표로 실무자반 교육, 관리자 리더쉽 함양

및 보안의식 강화를 위한 관리자반 교육 등이 연간 12회 이상 제공되고 있으며, 각 기관의 특성을 고려하여 기관요청에 의한 직접방문 교육 등 고객맞춤형 특별반을 운영되고 있다.

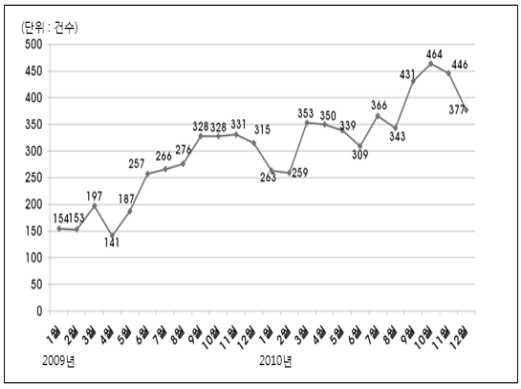
#### 2.3.3 기관 간의 네트워크 구축

지식경제사이버안전센터와 회원기관 간에는 전용회선이 구축되어 있어 회원기관의 정보보호설비에 대한 사이버 공격에 대한 침입시도를 탐지하여, 침입정보를 분석하고, 공격유형을 파악하고, 해당 기관의 시스템 정보를 확인하여 대응책과 함께 사이버위협정보를 제공한다. 새로운 탐지 패턴 유형이 적용 될 때는 자동배포시스템에 의해 회원기관에 설치되어 적용된다.

## III. 대응활동 및 문제점

### 3.1 대응활동

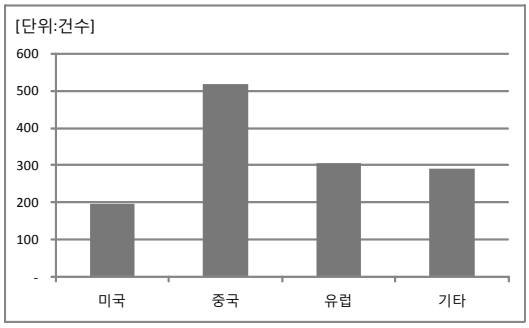
#### 3.1.1 사이버 공격 탐지 활동




〔그림 3〕 2009년, 2010년도 월별탐지실적

지식경제사이버안전센터의 주요 침입탐지실적은 〔그림 3〕과 같이 2008년에는 약 6개월에 걸쳐 796건, 2009년에는 2,933건, 2010년에는 4300여건에 이르고 있으며, 그 추세는 점증하고 있음을 알 수 있다.

2010년에는 발생한 주요 공격에 대한 침입탐지 실적은 4300여건이다. 이 중 해외 경유국을 통한 공격은 1,310건이다. 이를 미국, 중국 외는 기타 대륙별 합계로 경유지 현황을 파악하면 〔그림 4〕과 같이 미국은 197건으로 15%, 중국은 517건으로 40%, 유럽은 305건으로 23%, 기타 291건으로 22%에 이르

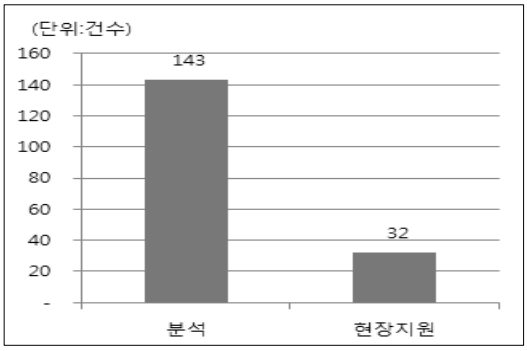



〔그림 4〕 2010년도 국가별 경유지 비율

고 있다.

#### 3.1.2 침해사고대응

〔그림 5〕와 같이 2010년의 탐지실적은 4300여건에 이르고 있으나 이중 실제 대응한 서비스는 〔그림 8〕과 같이 143건에 대해 분석하였고 32건에 대해 현장조사를 시행하였으나 탐지된 침해사고는 대부분 단순 바이러스로 파악되었다.




〔그림 5〕 침해사고 대응활동 건수

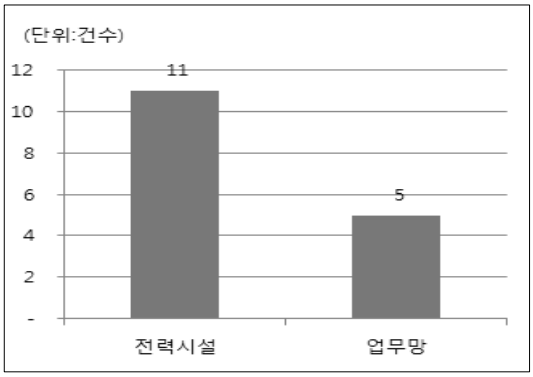
일부 침해사고대응 사례로는 해커가 사용자 명의를 위장하여 정보유출악성코드가 첨부된 이메일을 보내 사용자 컴퓨터에 설치되었으나 이를 탐지 분석하여 수집된 정보가 해커에게 전송되는 것을 차단하고 설치된 해킹프로그램을 제거하여 정보유출 피해를 예방하였으며, 또 홈페이지 해킹 후 청보탈취용 해킹도구를 설치하였으나 실시간 감시를 통해 이를 차단하고 취약점을 제거토록 조치하여 정보유출을 방지하였다. 다만 포렌식으로 분석한 일부 침해사고에 대해서는 바이러스 백신에 반영되지 않은 경우가 존재하였으며, 이 경우 악성코드를 제거하는 프로그램을 개발하여 회원기

관에 배포하였으며, 일부는 백신치료가 되나 일부는 치료되지 않았는데, 이에 대해서는 악성코드를 제거하는 프로그램을 개발하여 배포하였다.

주요 탐지패턴 개발사례를 보면, 업무망에서 P2P, 웹하드 등의 불법공유프로그램을 사용할 때 악성코드 및 중요자료가 노출될 위험이 존재하는데 이를 탐지할 수 있는 탐지패턴은 2010년 6월에 적용하였으며, 최신정보를 습득하여 사전 예방하는 패턴을 개발한 사례로는 스턱스넷(Stuxnet) 바이러스 탐지 패턴을 2010년 10월에 적용하였다.

### 3.1.3 취약점 분석

취약점분석 및 평가 서비스 내역을 보면 2008년에는 광해관리공단에 대해서만 시행하였으며, 2009년에는 한전 등 7개 기관에 대해, 2010년에는 〔그림 6〕과 같이 16개 시설에 대해 수행하였는데 주요정보통신시설을 보유한 한전 등 11개 전력시설과 에너지기술평가원 등 5개 기관의 업무망에 대해 수행하였다.




〔그림 6〕 취약점분석 및 평가 서비스 활동 건수

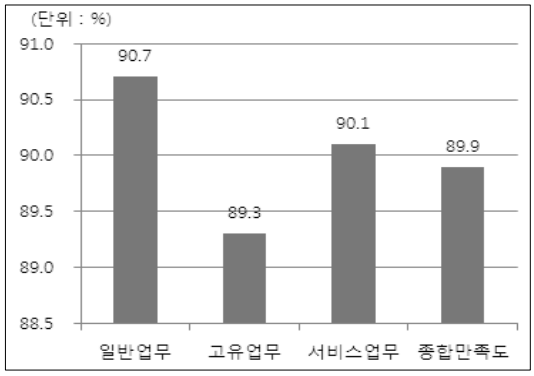
취약점분석 및 평가서비스 내용은 전력제어망으로는 발전제어(Process Control, Automatic Generation Control), EMS(급전자동화 시스템, Energy Management System), SCADA(집중원격감시 제어시스템, Supervisory Control and Data Acquisition), DAS(배전자동화시스템, Distributed Automation System)가 있고, 천연가스 배관망 역시 SCADA가 주를 이룬다. 이와 더불어 관련사의 업무망과 연계네트워크, 기관간의 네트워크에 대한 진단업무도 포함된다.

주요수행 취약점 분석 서비스 지적 사례로는 근본적인 업무망의 침해 가능성을 차단하기 위해 업무망에서 인터넷망을 분리하도록 망분리를 권고하였다. 또한 웹취약점 점검을 위해 인터넷망을 통한 홈페이지와 웹서버를 점검하고 발견된 취약점에 따라 정보유출에 대비한 소스코드 수정 및 비밀번호 관리방법 개선 등의 취약점 제거를 위한 대응책을 제시하였다.

## 3.2 문제점

### 3.2.1 야간, 공휴일 긴급 대응 미흡

회원기관에 대한 보안관제, 침해사고대응, 취약점분석 및 평가는 대체적으로 양호하다. 2010년 고객만족도는 〔그림 7〕과 같이 일반 업무에 대해서는 문의내용에 대한 적극적 청취도 및 친절도, 고객 요구사항에 대해 신속하게 처리하려고 노력하는 정도 등 9문항에 90.7점, 서비스와 고유업무에 대한 평가는 현장 기술지원 대응서비스 만족도, 취약점 분석평가에 대한 만족도는 11문항에 89.3점, 종합만족도는 89.9점으로 조사되었다.



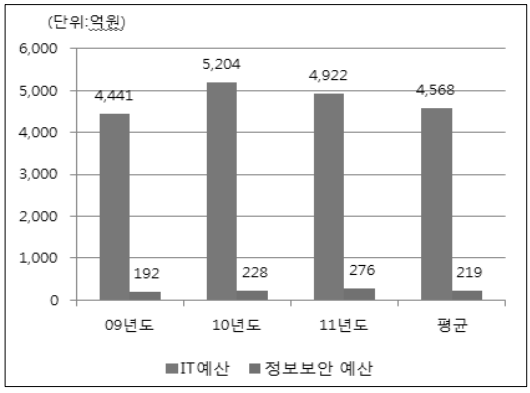

〔그림 7〕 고객만족도 조사

센터의 관제설비인 방화벽 및 침입탐지시스템 등 기본적인 보호시스템 구축실태는 양호하다. 24시간 상시관제 체제를 유지하고 있으나 침해사고대응 담당자의 역할분리로 인해 침해사고 야간 및 휴일 긴급 대응측면에서는 대처역량은 미흡하다고 조사되었다. 침해사고대응(CERT) 담당자의 주간 근무로 인해 평일에는 긴급대응서비스가 가능하나, 야간 및 휴일 침해사고 발생할 때에는 신속한 대응이 곤란하므로 이에 따른 제도 개선 및 추가 인력양성이 요구된다. 또한 긴급한 사이버침해 발생할 때에는 지식경제사이버안

전센터와 회원기관의 합동 조사가 진행된다. 이때 회원기관의 본사 보안담당자는 책임감을 갖고 긴급 대응 서비스에 대해 적극적으로 지원하여야 한다. 그러나 사업소에서 침해사고 발생 시에는 사업소담당자의 보안지식 미비로 공동 대처에 어려움이 발생된다. 따라서 명시적인 사업소담당자 지정 및 담당자의 보안 전문지식의 배양이 필요하다고 하겠다.

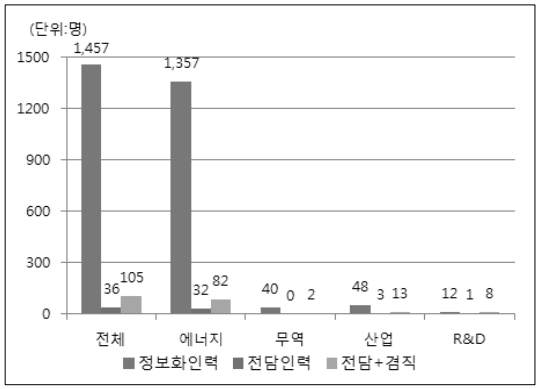
### 3.2.2 예산 및 인력 부족

한전 등 47개 기관의 정보보안 투자 예산 〔그림 8〕과 같이 정보화예산 대비 4.78%로 선진국에 비해 낮은 수준으로 정보보안 예산의 확충이 필요한 시점이라고 하겠다.




〔그림 8〕 지경부 산하 공공기관 4개년 정보보안 예산현황

회원기관의 2010년도 정보보안 전담인력 비율은 〔그림 9〕과 같이 기관당 2명 이내로 정보화인력 대비 2.5%이나, 대부분 다른 업무와 겸직하는 인력을 보안




〔그림 9〕 지경부 산하 47개 공공기관 정보보안 인력현황

업무에 투입하고 있으므로 이를 포함하여 보면 7.2%로써, 대부분의 회원기관이 보안조직을 별도로 운영하지 않고 있으며 전담보안 인력이 없음을 알 수 있다.

### 3.2.3 보안 인식 부족

대부분 회원기관이 인터넷과 업무망을 같이 사용하고 있기 때문에 내부업무시스템이 외부 사이버공격으로부터 보안위협에 노출되어 있다. 외부 해킹공격에 따른 정보유출과 업무서버의 데이터 삭제에 따른 정보의 손실 등이 우려된다. 또한 업무망을 통해 연계된 주요기반시설인 제어망까지 위협받고 있으나 전반적으로 위험에 대한 인식이 미약하다.

회원기관의 네트워크 보안수준이 강화되어 해커가 내부시스템을 공격하기 위한 통로로 집중적으로 홈페이지 등 웹(Web)서비스 영역을 주로 활용한다. 지경부사이버안전센터에서 수행한 모의해킹 결과 웹 취약점을 이용한 공격으로 내부시스템 침투가능성을 확인하고 취약점이 존재하는 소스코드의 수정을 권고하고 있으나 예산 등의 확보등 여러 사유로 대처가 부족하다.

국내외적으로 스턱스넷(Stuxnet)이 발견되는 등 제어시스템에 대한 보안 위협이 증가하고 있으나 이에 대한 긴급 대처가 부족하다고 볼 수 있다. 제어시스템은 작은 외부영향에도 오동작 하기 쉽고, 보안을 고려하지 않은 S/W개발로 인해 여러 취약점이 존재하며, 보안업데이트가 어려운 서버환경에서 운영되고 있으므로 제어시스템 운영자에게 보안에 대한 지식을 습득할 수 있는 기회부여가 필요하다고 하겠다.

특히 회원기관의 용역 및 하도급을 포함한 외주인력 비율이 전체 IT인력 대비 44.9%로 조사되었는데, 이는 외주용역관리가 대표적인 보안취약 요소임을 보여주고 있다. 즉, 외주용역인력이 사용하는 노트북·USB 등의 자산반출입을 통한 정보유출 및 보안사고 위험이 내재되어 있으므로 이를 예방하기 위한 철저한 관리가 요구된다.

## IV. 개선 방안

### 4.1 운영제도 개선

문제점에서 살펴 본바와 같이 24시간 상시관제 체제이나 야간 및 휴일의 침해 사고가 발생하면 긴급 대응측면에서는 대처역량은 일부 미흡하다고 볼 수 있

다. 긴급 침해사고대응능력을 강화하기 위해 관제인력의 대응능력 향상이 필수적이므로 이를 보완하기 위해 침해사고대응담당자와 함께 관제운영을 할 수 있도록 운영제도를 개선할 필요성이 제기된다.

지식경제사이버안전센터 설립목적에서 살펴본 바와 같이 보안관제센터를 운영하지 못하는 기관의 장은 보안관제센터를 운영하는 타 기관에 관제업무를 위탁할 있으나 침해사고가 발생할 때에는 회원기관의 협조가 불가피하다. 보안로그는 회원기관의 정보보호설비와 네트워크로 연계되어 탐지되므로 국가사이버안전센터, 지식경제사이버안전센터, 회원기관의 보안관제 3단계 보안관제가 수행된다. 문제점에서 제기한 바와 같이 회원기관의 사업소에서 침해사고 발생 시에는 침해사고 대응능력이 현저히 약화될 수 있으며 회원기관에서도 본사와 사업소 보안담당자 지정과 역할 등 운영제도의 개선이 요구된다.

### 4.2 보안전문업체와 협력 체제 강화

국가사이버안전관리규정에 의하면 "관제센터를 설치·운영하고 있는 기관의 장은 수집·탐지한 사이버공격 정보를 국정원과 관계기관에게 통보하여야 한다."고 규정되어 있다. 정보통신기반보호법에서도 정보공유·분석센터는 취약점 및 침해요인과 그 대응방안에 대한 정보제공이라고 규정되어 있다.

최근 사이버공격은 악성코드에 의한 DDoS 변종 공격의 증가와 더불어 사회기반 시설 제어시스템을 공격하는 스턱스넷 등 보다 지능적이고 다양한 신·변종 악성코드가 급증하고 있다. 국내외 최신 해킹공격 기술동향을 수집하여 사이버공격 분석 정보를 공유하고, 이를 바탕으로 사이버공격탐지패턴을 개발하여 참기기관에 배포하는 것 또한 정보공유의 필수적인 기능이다. 그러나 침해사고대응서비스에서 파악한 것처럼 포렌식으로 분석한 일부 침해사고에 대해서는 바이러스 백신에 반영되지 않은 악성코드가 발견되고, 일부는 백신반영이 완전하지 않아서 불완전한 치료가 종종 발생된다. 이에 대비한 정보공유를 위해 보안전문업체와의 협력은 필수적이다. 정보공유가 원활히 이루어지기 위해서는 상호 신뢰를 바탕으로 정보를 공유하는 양쪽 모두가 도움이 되는 방향으로 운영하여야 한다[8].

지식경제사이버안전센터는 국가정보원과 장비납품 관련업체로부터는 신규공격에 대한 방어 정보를 지속적으로 제공받고 이를 관제시스템에 반영하고 있다. 그러나 국내·외 보안전문업체들과 실시간으로 신규사이버공격에 대한 다양한 악성코드 및 공격정보를 공유할 수 있는 협력체계의 강화가 필요하다.

### 4.3 설비투자 확충

사이버공격 기술은 빠르게 진화하고 있기 때문에 기존 사이버방어 기술로는 탐지·대응하기 어려운 알려지지 않은 신종 악성코드에 의한 공격이 빠르게 증가하고 있으며, 사고 발생 시에는 그 피해 규모 또한 막대하다. 알려진 악성코드 공격에 따라 특정 탐지패턴에 따라 탐지하는 방식으로 방어하는 것은 한계가 있다. 지식경제사이버안전센터 보안관제는 사이버공격에 대한 방어의 관문으로써 최신 공격기술에 효율적으로 대응하기 위하여 관제시스템 모니터링 및 보안장비의 고도화 및 사이버침해에 대한 최신의 분석을 위한 포렌식 장비의 지속적인 업그레이드가 선결조건이 된다. 따라서 필요에 맞는 장비를 구비하여 최신의 사이버 침해사고에 주력할 필요가 있다[9].

[그림 8]과 같이 회원기관의 정보보안예산은 IT투자 예산 대비 5%수준으로 제약이 있으나 사이버공격 및 해킹기술의 발전에 부응하여 이를 체계적으로 방어할 수 있도록 최신 정보보호 솔루션 및 대응장비의 지속적인 도입이 필수적이며, 도입·설치된 장비를 통합적으로 연계하여 정보를 관리할 수 있는 종합상황관리시스템의 운영개선 및 업그레이드도 필요하다고 하겠다. 보안로그는 지식경제사이버안전센터와 회원기관의 정보보호설비와 연계되어 탐지되므로 최신신규설비에 대한 도입은 사이버안전센터에 국한된 것은 아니며, 회원기관의 정보보호설비의 교체도 필요하다고 하겠다. 이는 보안시스템 운영의 핵심은 좋은 자료를 얼마나 빨리 그리고 얼마나 많은 자료를 많이 게시하고 이를 관리하느냐에 달려 있기 때문이다[9].

### 4.4 전담 인력 충원

앞에서 살펴본 [그림 3]과 같이 서비스 기관을 보면 2008년 8월 센터 개소 시에 28개 기관에서 출발하여 2010년에는 49개 기관으로 75% 증가하였고, 주요 사이버 공격 건수로 보더라도 [그림 4]처럼 2009년에는 2,933건, 2010년에는 4300여건으로 47% 증가하였으나, 운영 인원은 2010년 들어 신규서비스인 웹 예방 진단 서비스를 위해 2명을 충원함으로써 약 6% 증가하였다. 또한 앞으로 외부 사이버공격에 의한 전자적 침해사고로부터 지식경제부 유관기관 정보통

신시설을 보호하기 위하여 회원기관 확대가 예상되고 있다. 따라서 사이버안전센터 담당업무의 서비스 수준 저하를 방지하기 위하여 업무량 증가에 따른 지식경제 사이버안전센터의 운영인력 증원이 필요하다.

그리고 〔그림 9〕에서 보는 바와 같이 회원기관의 정보보안 담당인력은 한전 등 몇 개 기관을 제외하고 2명 이내로 지식경제사이버안전센터와 유기적인 보안관제서비스 수행을 위해서는 해당기관의 인력확충도 필요하다.

### 4.5 인력양성

#### 4.5.1 서비스 인력의 능력향상

새롭게 출현하는 악성코드에 대한 정보를 신속하게 수집하여 참여기관에게 대응능력을 제고할 수 있도록 침해정보를 공유하기 위해서는 무엇보다도 신종 사이버 공격을 분석하여 대응방안을 신속히 찾을 수 있는 침해사고 대응 서비스 인력의 자질향상이 필요하다. 보안관제 절차는 예방, 탐지, 대응 서비스로 구분할 수 있다〔6〕. 예방부문은 취약점 점검 및 모니터링 등, 탐지부문은 네트워크 및 시스템 이벤트 등의 탐지활동, 대응부문은 웜바이러스 및 불법접근에 대한 침해사고 대응 및 스캐닝 수집활동 등이다. 이들 활동에 대한 최신의 정보분석 및 보안기술에 대한 대응능력 향상을 위한 지속적인 교육이 필요하다.

#### 4.5.2 참여기관 교육서비스 강화

지식경제사이버안전센터는 회원기관의 보안담당 인력과의 협업을 통한 CERT/CC 활동이 주 업무이다. 사이버 공격에 대해 회원기관의 대응능력 향상 없이는 효과적으로 대처하는 것이 불가능하다. 먼저 임직원에 대해 보안정책의 중요성을 인식시키고, 보안담당자의 대처능력을 향상하기 위한 최신 대응기법 교육은 지속적으로 제공되어야 한다. 지식경제사이버보안센터는 관리자반, 실무자반, 일반직원반 등을 운영하고 있으나 회원기관의 요구사항을 최대한 반영하여 보안사고 사례 중심의 교육을 포함하여 포렌식 분석기법 및 이론과 실무를 병행한 신규 교육서비스를 강화해야 한다.

## V. 결 론

지식경제사이버안전센터의 주요 업무는 지식경제부 산하 회원기관의 정보통신망에 대한 사이버 공격정보를 수집·분석·대응할 수 있는 통합 보안관제센터로서의 역할과, 주요 정보통신기반시설에 대한 정보통신기반시설의 취약점분석 및 평가와 더불어 보호대책 수립을 지원하는 정보공유·분석센터로서의 역할, 사이버 공격으로 인하여 발생한 사고의 조사 및 복구를 지원하는 침해사고대응센터로서의 역할을 수행하고 있다.

지식경제사이버안전센터는 고도화된 신종 악성코드의 출현과 지능화된 사이버공격 및 해킹 양상에 따라 회원기관 스스로 체계적인 방어를 할 수 있도록 사이버공격에 대한 정보를 분석하여 대응에 필요한 정보를 실시간으로 제공하며 이를 지속적으로 반영할 수 있도록 지원해야 한다. 이를 위한 개선방안으로는 첫째, 긴급 침해사고대응능력을 강화하기 위해 관제인력의 대응능력 향상을 위한 침해대응인력에 대한 보완과 함께 관제하는 제도의 개선이 요구되고, 둘째, 국내·외 보안전문업체들과 사이버공격에 대한 다양한 악성코드 및 공격정보를 공유할 수 있는 협력체계의 강화가 필요하다. 셋째, 최신 정보보호 솔루션 및 대응장비의 지속적 도입이 이루어져야 하며, 도입·설치된 장비들을 통합 및 상호 연계하여 정보를 관리할 수 있는 종합상황관리시스템의 운영개선이 필요하다. 넷째, 지식경제부 산하 회원기관 증가에 따른 운영인원의 확충이 필요하다. 다섯째, 내부적으로 예방·탐지·대응 서비스의 효과적인 수행을 위해서는 최신 정보 분석 및 보안 기술에 대한 대응능력 향상을 위해 지속적인 인력양성이 필요하며, 여섯째, 회원기관의 정보보호 인식재고를 위해 보안전문가를 양성하는 교육이 필요하다.

본 연구는 지식경제사이버안전센터의 설립 목적 및 역할, 업무 수행 현황에 대하여 분석하고, 수행 서비스를 중심으로 대응활동의 분석 및 문제점을 파악하였으며, 이에 따른 개선방안을 제안하였다.

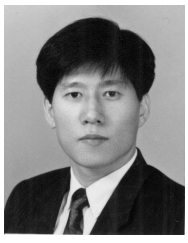
## 참고문헌

〔1〕 국가정보원, "국가사이버안전관리규정", 대통령훈령 제267호, 개정 2010년 3월 22일.
〔2〕 지식경제부, "보안관제전문업체 지정 등에 관한 공고", 제2010-478호, 제정 2010년 12월 21일.
〔3〕 방송통신위원회, "국가정보화 기본법", 법률 제10166호, 개정 2010년 3월 22일.
〔4〕 행정안전부, "정보통신기반 보호법", 법률 제9708호, 개정 2009년 5월 22일.

〔5〕 지식경제부, "지식경제 사이버안전센터 운영규칙", 훈령 제91호, 개정 2012년 2월 1일.
〔6〕 침해사고대응팀(CERT) 구축/운영 안내서, KISA안내・해설 제2010-13호, 한국인터넷진흥원・CONCERT, 2010년. 1월.
〔7〕 2011 국가정보보호백서, 방송통신위원회・행정안전부・지식경제부, 2011년 5월.
〔8〕 이연수, "국가정보의 보호를 위한 사이버안전법 제도 연구," 박사학위논문, 고려대학교, 2010년 6월.
〔9〕 이주호, "금융ISAC의 차별화된 정보제공서비스 개선 방향에 관한 연구," 석사학위논문, 성균관대학교, 2009년 6월.

## 〈著者紹介〉

이 승 원 (SeungWon Lee) 정회원
1982년 8월: 전남대학교 계산통계학과 졸업
1992년 8월: 고려대학교 경영대학원 경영정보 석사
1010년 3월~현재: 서울벤처정보대학원대학교 U-City학과 박사과정
1982년 12월~1992년 8월 한국전력기술(주) 근무
1992년 8월~현재 한전케이디엔(주) 근무
2011년 3월~현재 지식경제사이버안전센터 침해사고대응팀장
〈관심분야〉 CAD/GIS, U-City, 스마트그리드, 융합기술, 정보보호, 정보시스템감리



노 영 섭(YoungSup Roh) 정회원
1988년 2월: 인하대학교 전자공학과(공학사)
1996년 8월: 한국과학기술원 정보및통신공학과(공학석사)
2005년 2월: 고려대학교 전기,전자,전파공학과(공학박사)
1987년 11월~1998년 2월: LG전자 미디어통신연구소 선임연구원
1998년 3월~2001년 2월: 청강문화산업대학교 이동통신과 교수
2001년 3월~2005년 2월: 주식회사 싸이버뱅크 연구개발부문 상무이사
2005년 3월~현재: 서울벤처정보대학원대학교 유시티.융합기술경영전공
〈관심분야〉 임베디드시스템, 이동통신, IT융합기술, 정보보호