情 報 保 護 學 會 誌
第21卷 第6號, 2011. 10

# 사이버전 대응을 위한 국방 정보보호환경 분석과 보안관리모델 연구방향 고찰

최 광 복*

요 약

국방 정보보호환경은 IT기술의 발전과 함께 사이버 공간이 제5의 전장으로 부각되면서 해킹을 통한 군사자료 유출, 시스템 파괴 등 외부로부터의 지속적인 위협에 직면해 있다. 본 논문에서는 이러한 사이버전 위협에 효과적으로 대응하기 위한 방안으로 보안사고사례, 조직, 제도, 인력양성, 법규 및 제도 등 국방 정보보호환경을 분석하고 이를 바탕으로 정보체계의 보안수준을 진단하기 위한 보안관리모델 개발의 필요성과 ISMS 방법론을 고려한 D-ISMS(Defence ISMS) 연구방향을 고찰한다.

## Ⅰ. 서 론

민간 사회의 IT 기술은 정보화 사회의 진전과 더불어 빠르게 발전하고 있다. 초고속 인터넷망 보급에 따른 인터넷 인프라를 기반으로 무선랜, IPTV, 인터넷 전화기, SNS, 스마트폰 등 다양한 서비스와 관련 기술이 속속 등장하고 있다. 우리나라의 스마트폰 사용자수는 이미 1,000만명을 넘어섰으며 트위터, 페이스북 등 SNS 사용자 역시 빠르게 증가하고 있다. 군 역시 전술 C4I체계, TICN 등 전장관리체계와 군수체계, 동원체계 등 다양한 자원관리체계가 속속 도입되고 있으며 2011년 말이면 10만명의 장병이 스마트폰을 사용할 것으로 예상될 정도로 민간 사회와 정보화 진전의 흐름을 함께 하고 있다.

그러나 이에 따른 부작용 역시 적지 않은 것이 사실이다. 네트워크 해킹에서 시스템 해킹, 웹해킹의 시대로 변화함에 따라 정보체계를 해킹하기 위해 악성코드를 제작·배포하고 좀비 PC를 확보하여 감염된 PC로부터 개인정보 및 저장된 파일을 절취하거나 DDoS 공격을 수행하여 특정 사이트를 마비시키는 공격기술이 보편화된 지 오래다.

이러한 공격기술은 민간에서 경쟁기업의 중요정보를 절취하거나 정상적인 영업을 방해하여 기업이윤을 증가시키려는 금전적인 목적에서부터에 국가차원에서는 군사적인 목적을 달성하기 위해 타국가의 정보체계를 해킹하여 군사자료를 절취하거나 국방정보체계를 마비시키기 위해 사이버 공격을 수행하는 등의 현실적인 위협으로 등장하고 있다.

사이버 공격은 네트워크라는 매체의 특성상 물리적·공간적 제약을 받지 않기 때문에 전 세계적으로 네트워크가 연결된 곳이라면 어디서든 수행될 수 있으며 값비싼 무기체계를 도입하지 않고도 상대적으로 저렴한 비용으로 사이버 전력을 양성하여 상대국가의 기간망을 공격하고 피해를 유발시킬 수 있다는 점에서 매우 유용한 공격수단으로서 각광받고 있다. 이러한 이유로 장래 사이버전은 더욱 더 치열해지고 광범위해질 것이며 소프트 공격무기부터 하드웨어적 공격무기까지 공격 수단 역시 점차 다양해질 것으로 예상된다.

본 논문에서는 이처럼 점증하는 국방 사이버 위협에 대응하기 위해 우리나라의 국방 정보보호환경을 살펴보고 사이버전 대응을 위한 보안관리 모델의 필요성과 연구방향을 고찰하고자 한다.

## Ⅱ. 국방 정보보호동향

### 2.1 우리나라의 사이버전 대응실태

우리나라를 둘러싼 주변 강대국들은 사이버공간을 육상, 해상, 공중, 우주에 이은 제 5의 전장으로 인식하

* 국군 기무사령부 (choik125@naver.com)

고 미래전에 대비하기 위해 사이버전 전력을 양성하여 전쟁에 활용하고자 하는 움직임이 매우 활발하다.

그러나 주변국의 기민한 움직임과는 달리 우리나라는 사이버전에 대한 대비가 부족했음을 인정하지 않을 수 없다. 사이버전에 본격적으로 대비하기 위한 조직인 사이버사령부가 창설되기 이전에도 기무사 국방정보전 대응센터와 각군 CERT를 중심으로 하는 정보보호 조직이 있었지만 관제업무, 침해사고 조사 등 방어 위주의 업무를 수행해온 것이 사실이다. 그 동안 빈번하게 발생했던 제 3국발 해킹공격에 대해서도 피해여부 확인과 함께 추가 피해를 예방하기 위한 보안교육, 강조지시 등 방어에 치중해왔다.

그 결과 2009년 7월 7일 발생한 7. 7 DDoS (Distributed Denial of Service) 공격을 통해 국방 정보보호 체계의 문제점이 드러났다. 민간 웹사이트가 대규모 좀비PC로부터 DDoS 공격을 받은 사건인 7.7 DDoS 공격은 북한 해커부대의 능력과 우리나라의 무력함이 극명하게 대비를 이룬 사건이라고 할 수 있다. 북한은 민간 파일 공유사이트를 해킹하여 인터넷 PC 사용자가 해킹된 파일 공유 사이트에 접속할 경우 악성코드에 감염되도록 하는 방법으로 8만대 이상의 좀비PC를 확보했고 이를 이용하여 한·미 정부 웹사이트, 보안회사 및 대형 포탈 웹사이트 등에 대해 DDoS 공격을 수행했다. 계획부터 실행까지 치밀하게 준비된 사이버 공격에 우리 군이 제대로 된 대응 능력을 갖추지 못했던 것이다.

그러나 7.7 DDoS 공격이 군이 사이버전에 대비하기 위한 조직과 인력을 정비하는데 있어 전화위복의 계기가 되었음은 주지의 사실이다. 빈번하게 발생해왔던 제 3국발 해킹공격과 북한의 소행으로 알려진 7.7 DDoS 공격을 계기로 사이버방호 전담부대 창설과 체계적인 사이버전사 양성의 필요성이 제기되었고 군내외적으로 공감대가 형성되어 2010년 1월 11일 마침내 사이버전을 전담하는 사이버사령부가 창설되기에 이르렀다. 현재 사이버사령부는 사이버전을 전담하는 핵심부대로서 조직과 인력을 확충하여 각 군과 더불어 사이버 위협에 대응하기 위한 전력을 갖추는데 역량을 집중하고 있다. 특히, 최근에는 2011년 7월 1일부터 정보본부예하에서 국직부대로 전환하여 독자적 권한을 확보하고 고려대학교에 사이버국방학과를 신설하여 연간 30명의 졸업생을 군 정보보호 조직에서 근무토록 할 예정으로 있는 등 다방면에서 사이버 역량 확충을 위한 활동을 강화하고 있다.

## 2.2 보안사고사례 분석

국군 기무사령부(이하 기무사)에서 국회에 제출한 자료[1]에 의하면 2010년을 기준으로 최근 5년 동안 보안사고나 보안규정을 위반한 장병은 2,550여 명으로 육군이 1,900여명으로 가장 많았고, 공군 266명, 해군은 242명으로 나타났다. 유형별로는 군사비밀 누설이 71명, 군사비밀 분실은 59명이며 지난 3년간 누설되거나 분실된 군사비밀의 보안수준은 2급 비밀이 17건, 3급 비밀은 12건이었다. 이와 관련, 2,180명이 경고 처분을 받았고 병사 포함 280여명은 정직과 영창 등의 징계 처분을 받았다. 특히, 최근 3년간 사이버상에서 발생한 보안사고는 총 100여건 수준이며 이중 해킹으로 인한 군사비밀 유출사고는 약 1/5 가량으로 연도별로 점차 증가되고 있는 추세다. 군에서 보안사고 예방을 위한 노력을 강화하고 있음에도 불구하고 오히려 보안사고가 증가세를 유지하고 있는데 이는 내부자에 의한 군사자료 유출뿐만 아니라 첨단 정보통신 기술 발전에 따른 외부로부터의 해킹공격과 그로 인한 군사자료 유출 역시 증가하고 있기 때문으로 판단된다. 최근 발생한 주요 보안사고 중 외부자 또는 내부자에 의해 군사자료 및 군사기밀이 외부로 유출되거나 군 정보체계가 공격을 받은 보안사고 사례를 유형별로 분류하면 다음과 같다.

### 2.2.1 서버해킹

서버 해킹을 통해 공개·비공개자료 또는 개인정보를 입수하는 경우이며 이러한 개인정보는 차후 사회공학적 기법을 이용하여 악성코드가 포함된 해킹메일을 발송하는데도 악용된다. 북한 해커가 이러한 수법을 자주 활용해 왔는데 주로 군인공제회, 각군 사관학교 동기회, 연구소 등 안보관련 기관·단체 사이트를 주요 해킹 목표로 설정하고 등급별로 남측 인사들의 개인 신상정보를 관리하고 있는 것으로 알려져 있다[2]. 그러나 인터넷에 연결된 서버는 보다 향상된 정보보호시스템으로 보호되고 있어 해킹이 어려워지고 있으며 인터넷 서버에 고가치 자료가 저장된 경우도 감소하고 있으므로 서버를 직접 해킹하는 빈도는 점차 감소하고 있다.

### 2.2.2 PC 해킹

서버에 대한 직접적인 해킹 공격이 감소하고 상대적

으로 쉽게 해킹할 수 있는 PC에 대한 공격이 증가하고 있다. 해커는 사전에 확보한 개인정보를 분석하여 주요 직위자를 선별하고 이들에게 해킹 메일을 발송한다. PC 사용자가 메일을 열람하면 PC는 악성코드에 감염되고 내부에 저장된 군사자료는 해커에게 발송된다. 최근 사이버사령부는 '출처가 의심스러운 메일은 열어보지 말라'는 긴급 경고문을 일선부대 장교들에게 보내기도 했는데 해킹 메일을 분석한 결과, 악성코드가 포함된 메일이 60여명의 육사 출신 장교에게 발송됐고 수신자가 내용을 열람하거나 첨부파일을 실행할 경우 PC가 악성코드에 감염되어 PC 내부의 군사자료가 모두 해커에게 유출되도록 설정되어 있는 것으로 밝혀졌다[3]. 이러한 유형의 해킹공격을 예방하기 위해서는 사용자의 각별한 주의가 요구되기 때문에 정보보호시스템만으로는 방어할 수 없는 공격 형태라고 할 수 있다. 이외에도 사용자가 취약한 이메일 계정을 사용하는 경우 직접 해당 사용자의 메일 계정에 접속하여 메일함에 저장된 군사자료를 절취하거나 타인에게 사회공학적 기법을 이용하여 해킹메일을 발송하기 위한 수단으로 악용하는 경우도 발견되고 있다.

#### 2.2.3 인터넷으로 군사자료 전송

현역 간부가 업무참고 목적 또는 교육 자료로 활용할 목적으로 군사비밀을 이메일로 발송하거나 군사비밀을 자가 인터넷 PC에 저장하고 있다가 P2P 사이트, 메신저 등의 인터넷 공유프로그램을 사용하는 과정에서 PC에 저장되어 있던 군사자료가 인터넷상으로 유출되는 경우이다. 기타 군사자료가 저장된 보조기억매체를 인터넷 PC에 연결하는 과정에서 파일공유사이트나 메신저 또는 악성코드에 의해 군사자료가 외부로 유출되는 경우도 발견되고 있다. 이 경우는 본인이 인지하지 못한 채로 저장된 군사자료가 인터넷 상에 공유되거나 악성코드에 의해 군사자료가 해커에게 유출된다는 특징이 있다.

#### 2.2.4 언론, 국회, 예비역에 의한 군사자료 유출

군 내부자가 기자에게 군사자료를 직접 제공하거나 기자의 요청으로 직무상의 내용을 구두로 설명하는 과정에서 부지불식간에 군사비밀 관련 내용을 누설하여 언론을 통해 보도되는 경우다. 이외에도 국회 제공 자료가 국회의원이나 국회의원 보좌관의 관리소홀로 인해 구두 또는 문건으로 외부에 누설되기도 한다. 예비역에 의한 군수자료 유출은 주로 방위산업체와 연관되어 있다. 예비역이 군내 근무 연고자 또는 선후배를 통해 군사비밀을 탐지·수집 후 민간업체 취직을 목적으로 업체에 제공하거나 이미 취직한 회사 또는 본인 소유회사의 사업수주를 용이하게 하기 위해 군사비밀을 임의 유출하는 경우이다.

#### 2.2.5 정보체계 파괴를 목적으로 해킹공격

군사자료 수집 목적이 아닌 전산망 마비를 목적으로 군 전산망을 공격하는 경우이다. 우리 군에 아직까지 이러한 유형의 해킹 공격이 발생하지는 않았으나 향후 발생 가능성이 존재하기에 해킹공격의 한 가지 유형으로 소개한다. 유사 사례를 소개하자면 최근 북한의 소행으로 알려진 농협 해킹사건이 해당될 것이다. 협력업체 직원의 노트북 컴퓨터를 미상경로를 통해 감염시킨 후 해당 노트북을 활용하여 농협 금융망에서 운영되는 다수 서버에 삭제 명령을 실행시켜 금융거래 자료를 무차별적으로 삭제시킨 경우이다[4]. 미국과 이스라엘이 스턱스넷을 개발하여 폐쇄망 형태로 운영되는 이란 부세르 원전의 SCADA (Supervisory Control And Data Acquisition) 시스템을 감염시키고 원심분리기 1,000여대의 고장을 유발한 사건[5]도 비슷한 맥락이라고 할 수 있다. 즉, 폐쇄망 또는 보안성이 높은 네트워크를 직접 공격할 수 없을 때 보조기억매체나 보안에 취약한 내부자를 통해 내부 네트워크에 바이러스를 침투시키거나 악성 쉘스크립트를 실행시켜 공격하는 경우이다.

이상과 같이 최근에는 내부인이 출력물 또는 구두 형태로 군사자료를 유출하는 경우를 제외하고는 대다수가 해킹메일 열람, 보조기억매체 사용, 인터넷 공유 등 다양한 경로를 통해 군사자료가 유출되고 있고 기술발달로 새로운 공격 기법들이 지속 발견되어 기존의 보안지원 시스템으로는 효과적으로 보안사고를 예방하기가 어려운 형편이다. 따라서 급변하고 있는 보안환경을 고려하여 최근의 해킹공격 유형에 적시성 있게 대비할 수 있는 근본적인 수준의 보안관리 모델의 필요성이 제기된다.

## Ⅲ. 정보보호 주요활동

3장에서는 국방 정보보호 조직, 대외정보공유, 관제시스템, 보안감사 등 국방 분야의 정보보호 주요활동에

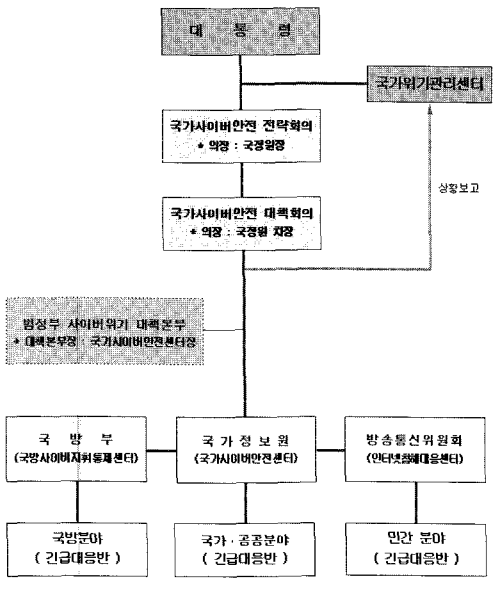
대해 소개한다.

### 3.1 조직

국방분야의 정보보호활동은 국방부 정보화기획관실, 합참, 국방정보본부, 국군 기무사령부(이하 기무사), 사이버사령부, 국군 지휘통신사령부, 국방전산정보원, 각 군 CERT를 중심으로 이루어지고 있다. 이 중 각급부대에 설치되어 운영되는 CERT는 국방 정보보호 업무 수행의 가장 중요한 실무조직으로 각 부대에 대한 침해사고 관제, 침해사고 발생시 초동조치, 국방사이버지휘통제센터 통제하에 제반 사이버 위협 대응단계에 대한 조치사항 시행 등 각군의 정보보호 대응 기능을 수행한다.

### 3.2 대외정보공유

국가차원의 사이버 위협정보 공유체계는 [그림 1][6]과 같이 국가사이버안전전략회의와 국가사이버안전대책회의에서 각각 국가사이버안전에 관한 정책·제도에 관한 사항과 실무에 관한 사항을 결정하고 인터넷침해대응센터, 국가사이버안전센터, 국방사이버지휘통제센터에서 각각 민·관·군 분야의 사이버안전 대응 전담기관 역할을 수행한다. 인터넷 침해대응센터는 한국인터넷진흥원(KISA)에서 운영하고 있으며 현재 ISP 업체




〔그림 1〕 국가 사이버 위협 대응체계

등 민간기업에 대한 사이버 보안 지원을 담당하고 있다. 국가사이버안전센터(NCSC)는 1.25 인터넷 대란을 계기로 국가정보원에서 창설하여 정부·공공기관에 대한 사이버보안 지원 업무를 담당하고 있다. 국방사이버지휘통제센터는 사이버사령부에서 군 관련 사이버위협에 대응하기 위하여 운영하고 있는데 최초 기무사 국방정보전대응센터에서 수행하던 기능을 2010년부터 사이버사령부에서 이관 받아 해당 업무를 수행하고 있다. 국방사이버지휘통제센터는 정보화기획관실과 합참의 통제를 받아 각군 CERT에 사이버 위협 관련 상황을 전파하고 각군 CERT는 침해사고 발생시 상위 CERT 및 최상위 CERT인 국방사이버지휘통제센터에 해당사항을 신고한다.

기타 한·미 사이버위협 정보공유는 합참 및 연합사 정보작전방호태세 규정에 의해 수행되고 있으며, 사이버 위기상황 또는 각종 연습시 연합사 정보보증 수행부서인 IAWG(Information Assurance Working Group, 연합사 정보보증 수행부서)에 합참요원을 파견 운영하여 한·미 사이버 위협 협조체계를 유지하고 있다. 또한, 한·미 각군은 CENTRIXS-K 및 KJCCS의 웹메일을 사용하여 사이버 위협정보를 공유한다[7].

### 3.3 인력양성 및 전문화 교육

국방분야에서 정보보호전문인력 양성은 크게 육·해·공군 정보통신학교 교육과 기무사 국방정보보호교육센터에서 이루어지는 교육으로 나누어 볼 수 있다.

각 군 정보통신학교에서는 장교를 대상으로 초군반, 고군반 교육 또는 특기교육에 정보보호 과정을 편성하고 있고 부사관 대상으로는 육군은 초급반과 전산특기교육에 정보보호 교육을 실시하고 해·공군은 초·중·고급으로 세분화된 교육과정을 운영하고 있다. 기타 정보보호 전문 교육과정으로는 육군의 정보체계기본반, CERT운영자반, 정보보호실무자반이 있고, 해·공군은 각각 정보보호연수, 정보보호실무자반이 있다.

이처럼, 각군 정보통신학교에서는 초급수준의 정보보호교육을 하고 있는데 반해 기무학교 국방정보보호교육센터는 군 인력에 대한 정보보호 분야별 단과과정과 정보보호 초급·중급·고급의 세분화된 교육과정을 운영하며 정보보호 전문인력을 양성하고 있다.

그러나 각군 정보통신학교와 기무학교 국방정보보호교육센터 공히 기술적 차원의 정보보호 교육 과정은 운

영되고 있으나 관리적 차원의 정보보호 교육과정 및 커리큘럼은 운영되고 있지 않다. 즉, 정보보호 업무 실무자를 대상으로 하는 교육에만 집중되어 있고 보안 관리자 입장에서 정보체계와 이와 관련된 조직·인력에 대해 보안 수준을 유지하고 관리하기 위한 방안에 대한 교육은 별도로 시행되지 않고 있는 상황이다.

### 3.4 관련 법규 및 제도

국방 정보보호 관련 규정으로는 크게 군사보안업무훈령, 국방정보화업무훈령, 정보작전방호태세 규정, 사이버안전 국방분야 위기대응 실무매뉴얼 등이 있으며 군은 이러한 훈령·규정을 근간으로 국방정보보호 조직과 임무, 정보체계 및 조직·인력에 대한 보안수준 관리, 사이버 위협에 대한 대응태세 유지 등 국방 분야 정보보호 업무를 수행한다.

#### 3.5.1 군사보안업무훈령

군사보안업무훈령은 1965년 1월 10일 제정되어 2010년 9월 27일 최종 개정된 이래 총 17차례에 걸쳐 전면 또는 부분 개정되었다. 군사보안업무훈령은 국방부, 국방부 직할부대 및 기관과 육군·해군·공군 및 국방과학연구소 등 군 및 군 관련 기관에 적용되는데 그 구성을 살펴보면 총칙, 정신보안, 문서보안, 인원보안, 시설보안, 정보통신보안 등 8장, 216조항으로 구성되어 있으며 군 보안의 핵심 훈령으로서 군사보안 및 정보통신 보안을 포함한 제반 군사보안업무에 대한 총체적인 원칙을 제공하고 있다[8]. 군사보안업무훈령은 각 보안 분야별로 구성원들이 군 내부에서 준수해야 하는 사항을 상세히 기술하고 있으며 훈령이라는 용어가 의미하는 것처럼 법령의 성격을 내포하고 있다. 따라서 ISMS처럼 정보보호시스템의 수준을 진단하기 위한 목적보다는 각 분야별로 구성원이 준수해야할 보안사항을 규정하고 위규자에 대해서는 조항에 따라 처벌함으로써 군사자료가 무분별하게 대외로 유출되지 않도록 군사보안을 유지하는데 목적이 있다. 군사보안업무훈령은 기무사에서 국방부 정보본부와 협조하여 제개정을 담당하고 있는데 최근에는 국방 정보보호환경의 급변과 더불어 개정 주기도 점차 빨라지고 있는 추세다.

#### 3.5.2 국방정보화업무훈령

국방부 정보화기획관실에서는 국방정보화 기반조성 및 국방정보자원관리에 관한 법률('11.1.1)에서 정한 사항을 시행하기 위한 업무 절차 및 기준을 마련하고 국방정보보호훈령, IT신기술 국방적용 관련 협력업무 추진 훈령, 국방정보 체계사업관리지시, 국방정보화사업 예산집행조정 및 예산재사용 지시 등 산재된 기존의 정보화 관련 15개의 훈령·지침·지시를 통합하기 위해 2011년 2월 7일 국방정보화업무훈령을 제정하였다[9]. 신규 제정된 국방정보화업무훈령은 9장 360조로 구성되어 있는데 이 중 제 6장 국방정보보호 관리는 舊 국방정보보호훈령에 해당하는 부분으로 사이버사령부 창설 이후 각 기관의 임무와 기존 군사보안업무훈령에 비해 대폭 강화된 보안대책 검토, 보안측정 등의 보안수준 관리업무, 개인정보보호법 시행을 고려한 국방분야 개인정보보호에 관한 사항, 국방정보보호 협력체계 구축 등의 내용을 명시하고 있다. 이외에도 국방정보시스템 보호기준 및 보호요구사항에 ISMS기준을 적용하여 네트워크보호, 서버보호, 단말기보호 등 총 5개 분야에 76개의 정보시스템 보호통제항목을 제시하고 있어 군 정보시스템 관리자들이 지정된 기준의 보호요구수준을 준수토록 하고 있다. 그러나 국방정보화업무훈령은 다양한 훈령·지침·지시를 통합하여 국방 정보화분야에 대한 내용을 모두 다루다 보니 내용이 방대하고 보안에 관한 부분은 6장으로 국한되어 있어 보안실무자가 정보체계나 부대의 보안수준을 진단하는데 활용하기에는 다소 미흡한 점이 있다고 생각된다.

#### 3.5.3 정보작전방호태세 규정

정보작전방호태세 규정은 사이버위협에 효과적으로 대비하기 위해 2001년 4월 1일 합참에서 제정하여 2010년 7월 1일 개정되었다[6]. 이 규정은 최근 사이버사령부의 침해사고조사 절차를 반영하고 정보작전방호태세 위원회를 기존 3단계에서 1단계로 간소화하는 방향으로 개정될 예정이다. 정보작전방호태세 규정은 아군의 정보 및 정보체계에 대한 공격징후 또는 침해사고 발생시 신속한 대응으로 피해를 최소화하기 위한 정보작전방호태세에 관한 사항을 명시하고 있다. 정보작전방호태세 규정은 전장관리체계, 자원관리체계, 국방정보통신망, 인터넷망 등 국방정보체계에 대한 위협 발생

시 위협 수준에 따라 5단계, 4단계, 3단계, 2단계, 1단계의 등급으로 구분하여 사이버 위협에 대응하도록 하고 있다. 이러한 5단계 등급은 국정원의 국가사이버안전센터 및 한국인터넷진흥원의 인터넷침해대응센터에서 사이버 위협 대응 단계에 적용하는 정상, 관심, 주의, 경계, 심각 단계와도 일치한다. 국방사이버지휘통제센터는 정보작전방호태세 규정에 따라 평시 정보보호 훈련을 수행하거나 사이버 위기상황 발생시 국가사이버안전센터, 인터넷침해대응센터와 공조하여 사이버 위협 대응단계를 상향 조정하고 각 단계에 따라 요구되는 대응책을 강구한다.

#### 3.5.4 사이버안전 국방분야 위기대응 실무 매뉴얼

사이버안전 국방분야 위기대응 실무매뉴얼은 「국가위기관리기본지침(대통령령 제124호)」 및 「사이버안전분야 위기관리 표준매뉴얼」에 근거하여 국방정보체계에 대한 사이버안전분야 위기발생시 세부 대응절차 및 제반 조치사항 등을 규정하고 있다[10]. 본문은 제1장 개요, 제2장 위기경보 수준별 조치사항, 제3장 위기대응 조치 및 절차로 구성되어 있으며 사이버 위기경보에 대한 판단기준과 피해상황, 조치사항 등을 상세하게 설명하여 각군 정보보호실무자가 정보보호업무를 수행하는데 참고하도록 지침을 제공하고 있다. 정보작전방호태세 규정에서 제반 사이버 위협 대응 단계를 규정하고 있는데 반해 사이버안전 국방분야 위기대응 실무매뉴얼은 제반 위협단계를 판단하기 위한 징후와 상세 대응 지침을 기술하고 있다.

## Ⅳ. 사이버전 대응을 위한 국방 보안관리모델

### 4.1 보안관리모델 개발을 위한 고려사항

지금까지 국방 정보보호동향, 국방 정보보호주요활동에 대해 살펴보았다. 이상의 내용을 분석해보면 하드웨어적인 측면에서의 정보보호 시스템 구축, CERT 조직 편성, 전문화 인력 양성면에 있어서 일부 보완이 필요하기는 하지만 전반적인 정보보호 환경은 양호하다고 평가한다. 전장관리체계 관제에 관한 사항은 합참을 중심으로 전장관리체계 상호연동 확대와 더불어 통합 보안관제체계 구축을 추진하고 있는 상황이므로 본 논문에서는 고려대상으로 간주하지 않는다. 반면에 군사보안업무훈령, 국방정보화업무훈령 등에 근거해서 특정 정보체계의 보호수준이나 특정부대의 정보보호수준을 진단하기 위해 수행되는 보안감사, 보안측정, 취약점 분석 평가 등의 업무를 분석해 보면 사이버전을 대비하기 위한 국방정보보호 관리 모델이 부재하다는 점에서 개선의 여지가 많은 것으로 평가된다. 구체적 내용은 다음과 같다.

#### 4.1.1 정보체계 전반의 보호수준에 대한 정량적 평가기준 필요

군에서는 특정 부대의 보안수준을 평가하기 위한 방법으로 보안감사, 정보작전방호태세 훈련, 취약점 분석·평가, 보안점검, 취약점 진단, 보안측정 등의 방법을 활용하고 있다. 그러나 모든 방법이 공통적으로 평가 기준이 세밀하게 점수화되어 있지 않기 때문에 정량적으로 부대 정보체계의 정보보호 수준을 진단하는데 한계가 있다. 보안감사의 경우 2년마다 특정 부대의 전반적인 보안수준에 대해 진단하는데 매 2년마다 동일부대를 감사한다고 해도 ISMS 통제항목을 적용하는 것과 같이 객관성이 완전히 보장되지 않는다는 단점이 있다. 정보작전방호태세 훈련 역시 대응훈련을 하기 위해서 여러 명으로 팀을 구성해야 하며 전방위적인 사이버 훈련보다는 특정 정보체계에 대한 단편적인 훈련에 그친다는 점에서 정량적인 보안수준 진단활동이 아닌 사이버 위협에 대응하는 훈련에 중점을 두고 있다고 할 수 있다. 취약점 분석·평가는 특정 정보체계에 대해서 매 2년마다 수행되는데 정보체계 보안성 수준에 따라 5단계에 걸친 정량적인 평가를 하기는 하지만 부대 전반적인 정보체계의 수준을 진단하는 것이 아니라 특정 정보체계에 대한 취약점을 진단하고 있어 역시 한계가 있다. 보안점검 및 일반적인 취약점 진단 활동은 진단 범위가 좁고 특정 사항에 대해 보안성을 점검하는 등 단편적이고 일회성이 짙은 성격의 보안지원활동이므로 역시 단위부대 전반에 대한 보안수준을 정량적으로 진단하기에는 부적절하다. 보안측정 역시 부대의 전반적인 보안수준을 진단하는 것이 아닌 특정 정보체계가 전력화를 하는데 있어 보안취약점을 분석하고 그 대책을 제시한다는 점에서 부대의 정보보호 수준을 진단하기 위한 정보보호 관리 모델과는 거리가 있다.

#### 4.1.2 보안 관련 훈령의 이원화

현재 국방 정보보호 관련 규정은 크게 군사보안업무훈령과 국방정보화업무훈령으로 나누어 볼 수 있다. 군사보안업무훈령은 보안수준관리단계에 따라 보안대책 검토, 보안측정, 보안감사를 통해 정보체계의 보안수준을 관리토록 규정하고 있다. 국방정보화업무훈령은 군사보안업무훈령에 기초하고 있으나 보안대책 검토, 보안측정을 보다 강화하여 군사보안업무훈령에 비해 보안대책 검토는 4회 이상 가능토록 하고 있고 보안측정은 매년마다 보안측정이 종료된 정보체계의 보호대책 적절성을 검토하여 부적절시 재보안측정을 하도록 규정하고 있다. 또한 국방정보화업무훈령은 군사보안업무훈령에 명시되지 않은 취약점 분석·평가 업무를 명시하고 가·나·다급 정보체계에 대해서도 취약점 분석·평가 업무를 수행토록 하여 정보통신기반보호법보다 취약점 분석·평가 수행기준을 강화하고 있다. 이처럼 군 정보보호 관련 법규는 양대 훈령으로 이원화되어 있는데 이러한 체계가 오히려 군 정보보호 업무를 수행하는데 있어 복잡하고 혼란을 가중시키고 있다. 따라서 군사보안업무훈령과 국방정보화업무훈령을 모두 고려하여 정보체계의 보안수준을 진단할 수 있는 새로운 모델이 요구된다.

#### 4.1.3 짧은 시간에 보안수준 진단 필요

군사보안업무훈령과 국방정보화업무훈령은 모두 보안준수 사항을 나열하는 규정의 형태를 갖추고 있어 '무엇을 하면 안 된다.', 또는 '무엇을 해야 한다.' 식으로 강제사항을 명시하는데 주안점을 두고 있는데 이러한 서술식 문장 사용이 실무자들의 입장에서 정보체계의 보안수준을 간편하게 진단하는데 오히려 방해요소로 작용하고 있다. 정보체계의 보안수준을 진단하기 위해서는 보안수준 진단 담당자가 훈령의 긴 서술식 문장을 모두 이해하고 각 정보체계에 문장 하나하나를 적용하여 이상 유무를 확인하는 방식으로 정보체계의 수준을 평가해야 한다. 따라서 우리는 이러한 단점을 극복하기 위해 훈령을 모두 이해하지 않더라도 필요한 점검항목 기준과 요구수준만 정보체계의 현재 상태에 대입함으로써 정보체계의 수준을 간편하게 진단할 수 있는 방안이 필요하다고 하겠다.

#### 4.1.4 방대한 분야 적용 및 과대인력 시간 소모

내용의 범위 측면에서 보면 군사보안업무훈령, 국방정보화업무훈령, 보안감사 업무, 취약점 분석·평가 등 기존의 훈령과 보안지원 업무는 모두 매우 방대한 분야를 다루고 있다. 군사보안업무훈령은 인원, 문서, 시설, 정보통신보안 등 다양한 분야의 보안사항에 대해 규정하고 국방정보화업무훈령은 정보시스템 획득 및 관리, 국방정보기술 아키텍처 관리, 국방정보화책임관(CIO) 협의회 운영 등 정보보호 분야 이외에 정보화 전반에 걸친 방대한 내용을 기술하고 있다.

투입 인력·시간 측면에서 살펴보면 취약점 분석·평가 업무는 한 팀을 구성하여 한 달여 동안 특정 주요 정보통신기반체계를 대상으로 상세하게 취약점 점검을 수행하는데 그 취약점 진단 결과가 자세하게 도출되는 것만큼이나 많은 인력과 시간이 소요된다. 또한, 2년에 한 번 시행하는 만큼 점검 주기도 길기 때문에 1년 이상의 시간이 경과했을 경우에는 새로운 보안 취약점이 다수 발생하여 해킹 위협에 상당 부분 노출될 위험성이 크다. 보안감사 역시 2년에 한 번 시행하며 보통 일주일 정도의 기간 동안 여러 명의 감사관이 문서, 시설, 인원, 암호, 정보통신 등 보안 전 분야에 대해 감사하는 만큼 감사주기도 길고 인력과 시간이 많이 소요된다. 이러한 다양하고 복잡한 규정과 정량화되지 못한 평가 요구항목 및 평가수준 등은 수시로 각급제대의 보안수준을 측정하기가 어렵고 많은 시간·인력이 요구된다. 따라서 훈령이 다루는 범위에 있어서나 업무를 수행하는데 있어서 투입되는 인력과 비용을 경감하고 부대의 정보보호 수준을 진단하기 위한 방안이 필요하다.

### 4.2 국방 보안관리모델 연구방향

이상과 같이 4가지 요소를 감안하여 국방 사이버 위협에 적절하게 대비할 수 있는 보안관리모델의 개발이 요구된다.

우선적으로 보안관리모델을 통해 최근 들어 그 강도와 폐해의 심각성이 나날이 급증하고 있는 북한의 사이버공격에 적극 대응할 수 있어야 하겠다. 북한의 사이버 공격은 일 년 내내 쉼 없이 지속되고 있다. 전부대의 인터넷이나 홈페이지 그리고 장병들의 가정에 설치한 인터넷을 통하여 사이버 공격을 자행하고 있다. 따라서 각급부대의 정보통신체계에 대한 위협이 급증하고 있으며

그 취약점도 변화하고 있기 때문에 여러 각도에서 취약점을 분석해내야 한다. 상시적인 관제는 물론이고 사이버 공격자의 입장에서 보았을 때 각급 부대의 어느 자산이 가장 공격할 가치가 있으며 그에 대한 보안대책을 적절히 이행하고 있는지 확인 점검하는 개념이 도입되어야 한다.

또한, 북한의 사이버 공격이 보안의 3요소인 기밀성, 무결성, 가용성 중 어느 분야에 초점을 두어서 공격할 것인지 파악할 필요가 있다. 물론 모든 요소에 대하여 공격목표를 삼을 것이지만 우선적으로 평상시에는 기밀성과 가용성 파괴에 목표를 둘 것으로 보인다. 필요한 군사기밀을 해킹하여 우리군의 각종 작전계획이나 군사비밀을 절취한 뒤 결정적 시기에 각종 시스템을 사용불가능하도록 하는 방법을 구사할 것이라고 본다. 물론 무결성도 함께 무력화 시킬 것으로 본다. 그렇다면 평상시 각급부대에서 정보보호에 관심을 가져야 할 분야는 기밀성과 가용성을 저해하는 행위들을 보호할 수 있는 장비, 감시, 기술을 대응책에 우선 포함시켜야 한다는 의미이다.

다음으로 각급부대 지휘관이 쉽게 본인이 지휘하는 부대의 보안수준을 알 수 있어야 한다. 부대의 보안수준에 대하여 지휘관이 정확히 아는 것은 부대의 보안관리 측면에서 대단히 중요한 일이다. 해부대에 현재 예상되는 가장 높은 위협은 무엇이고 각 시스템의 취약점은 무엇이 있는지를 정확히 파악함으로서 보안수준을 평가할 수 있고 위험을 관리할 수 있기 때문이다. 따라서 지휘관이 용이하게 부대의 보안수준을 파악할 수 있도록 가급적 가시적 척도나 수준을 제시할 수 있는 틀이 개발되어야 한다.

일반회사나 기관에 비하여 군의 각급부대가 보유하고 있는 자산의 종류는 상대적으로 다양하고 그 피해로 인한 영향력도 금전적 피해보다 훨씬 치명적인 전투임무의 중단내지는 오류로 나타난다. 따라서 자산에 대한 가치 평가가 정교하게 이루어질 수 있는 틀이 요구된다.

각급부대의 인적 구성원들이 수시로 교체되고 그리고 보안에 대한 전문가가 그리 많지 않다는 점도 간과할 수 없는 중요 고려사항이다. 사회에서는 정보보안 전문가도 많고 그리고 보안전문업체로부터 보안컨설팅 등을 통하여 양질의 보안서비스를 제공받을 수 있으나 군부대는 민간 보안전문가들로부터 자문 정도는 받을 수 있으나 구체적인 보안서비스는 받을 수 없는 구조적 문제점을 가지고 있다. 부대별 정보부서가 있기는 하지만 보안업무를 전문으로 하기보다 전투중심의 정보임무를 주로 수행하고 있고 최근의 발전된 정보보호기법들에 대해서는 비교적 낮은 수준의 임무를 수행하고 있다. 이는 각급부대에 적용할 정보보호의 기본 틀이 보안전문가가 아니더라도 쉽게 이해할 수 있고 자주 사용할 수 있도록 충분히 간단하고 쉬워야 한다는 점이다.

가능하면 국제적으로 표준화되어 있어 그 수행결과를 신뢰할 수 있는 틀이어야 한다. 이런 측면에서는 국제적인 표준인 ISO17799와 K-ISMS나 G-ISMS를 참고로 하여 국방 보안환경에 맞도록 일명 D-ISMS(Defence-ISMS)를 만들어가는 것이 지름길이라고 생각된다.

결론적으로 국방 정보보호 관리제도의 도입은 사이버공격이 지금도 진행되는 현실을 정확히 직시하여 적극적인 예방 및 대응개념으로 발전되어야 할 것이며 각급부대의 판이한 보안환경과 보안대책들을 적절히 반영할 수 있는 탄력성이 있는 기본 틀이 되어야 할 것이다. 또한 각급부대의 보안 실무자들이 비교적 용이하게 사용할 수 있고 지속적으로 사용하여야 할 수 있는 틀이 되 국제적으로 표준화되어 있는 여러 제도들을 군 보안환경과 특성에 잘 맞도록 개선한 프레임워크로 발전되어야 할 것이다.

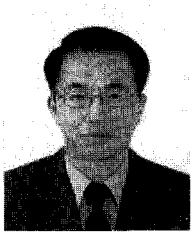
## V. 결 론

국방 정보보호 환경은 조직, 제도, 인력양성 측면에서 양호한 것으로 평가된다. 반면, 법규 및 제도, 정보체계 보안수준 관리 측면에서는 부족한 점이 노정되어 사이버전에 효과적으로 대비하기 위해서 일원화되고 단순화된 보안관리모델이 요구되는 것으로 판단된다. 이를 위해서 ISMS에 기반한 위험관리 방법론을 국방분야에 적용하여 사이버전에 적합한 D-ISMS를 개발하고 이를 단위부대에 적용하여 성능을 평가하는 방법을 고려할 수 있다. 이를 위한 구체적 방법으로 육군 사단급 부대를 표준 부대로 선정하여 정보체계 자산을 분류하고 개발된 통제항목을 적용하여 위험분석을 수행한 후 취약점, 또는 위협 수준을 고려하여 보호관리가 요구되는 것으로 판단되는 자산에 대해서는 적절한 보안대책을 강구한다. 이러한 국방 보안관리시스템을 도입, 발전시킬 경우 사이버전에 효과적으로 대응할 수 있는 보안관리 틀이 될 것으로 본다.

## 참고문헌

[1] YTN, "군 보안사고·보안규정 위반...5년 동안 2,557명", 2010년 8월.
[2] 연합뉴스, "북, 남측 165만명 개인정보 해킹 입수", 2009년 7월.
[3] 국민일보, "육군사관학교 동기 사칭... 北, 軍인사 상대로 해킹시도!(북한의 사이버해킹과 테러 막아내야", 2011년 5월.
[4] 서울중앙지검, "농협 전산망 장애사건 수사결과", 2011년 5월.
[5] 조선일보, "사이버 미사일 '스턱스넷(Stuxnet)' 이란 이어 中 공격", 2010년 10월.
[6] 합동참모본부, "정보작전방호태세 규정", 2010년 7월.
[7] 강신우, "국방 사이버전 대응체계 발전방안", 군사평론, 제398호, pp. 7-24, 2009년 4월.
[8] 국방부, "군사보안업무훈령", 2010년 9월.
[9] 국방부, "국방정보화업무훈령", 2011년 2월.
[10] 국방부, "사이버안전 국방분야 위기대응 실무매뉴얼", 2006년 12월.

## 〈著者紹介〉



**최 광 복 (Kwangbok Choi)**
정회원
1980년 2월 : 육군사관학교 졸업
1992년 2월 : 동국대학교 경영학과 석사
2005년 8월 : 경남대학교 국제 정치학 박사
2007년 3월~현재 : 수원대학교 컴퓨터학과 박사과정
관심분야 : 정보보호, 보안정책, 위험관리, IT 거버넌스, IT 감사