네트워크 중심전(NCW)하의 국방정보체계 제대별/기능별 정보보호지침 연구*

권 문 택**

요 약

본 연구는 네트워크 중심전(NCW) 환경하에서 국방정보체계에 대한 정보보호 지침을 마련하고자 수행하였다. 본 연구에서는 국방정보체계 분야에 다년간 근무했던 전문가들로 워킹그룹을 편성하여 그룹의사결정기법을 활용한 연구방법을 통해 네트워크 중심전(NCW)하에서의 정보보호 지침을 제대별, 기능별로 도출하였다. 본 연구에서 제시하는 제대별, 기능별 정보보호 지침을 활용하여 현존하는 국방정보체계의 정보보호 수준을 평가하고 미흡한 점을 보완한다면 보다 완벽한 정보보호 대책을 마련할 수 있을 것이다.

A Study on the Defense Information System Security Guideline for Network Centric Warfare

Moon Taek Kwon**

ABSTRACT

Information security is a critical issue for network centric warfare(NCW). This paper provides defense information system security guidelines for NCW, which is a result of the research through a group decision making process. The purpose of the research is to intended to help military officers establish information system security measures within their organization.

Key words : Information Security, Network Centric Warfare, Defense Information System

* 본 논문은 경희대학교 2005년 교비공모 연구과제지원으로 수행한 연구결과의 일부입니다.
** 경희대학교 테크노경영대학원

1. 서 론

21세기 들어오면서 인터넷을 비롯한 정보통신 기술의 급격한 발전으로 이를 활용한 군사혁신이 가속화되기 시작하였다. 군사혁신의 핵심 요체는 치명적인 대량 살상무기체계의 발전뿐만 아니라 정보통신 기술을 활용한 네트워크 중심(Network Centric)의 군사전략 변화라고 할 수 있다. 네트워크 중심의 군사전략이라는 정보기술을 지휘통제 기능에 접목하여 전장의 모든 부대와 개인들을 네트워크로 연결한다는 개념으로서, 이를 통해 정보의 수집, 가공, 처리 및 명령하달이 실시간으로 이루어짐으로서 즉각적인 타격을 통해 적을 제압하고자 하는 전쟁 수행 개념이다. 이러한 전쟁 개념을 '네트워크 중심전'이라고 한다.

네트워크 중심전(NCW : Network Centric Warfare)이라는 용어는 1998년 미국의 가스트카와 세브로스키[1]제독이 미 해군 저널 'Proceedings of the Naval Institute'에 기고한 'Network Centric Warfare : It's Origin and Future'라는 제목의 글에서 처음 소개된 바 있다. 이후 미군은 네트워크 중심전(NCW)에 대하여 많은 연구를 하였으며 이에 대한 개념이 진화되면서 정립되었는데, 이 개념을 요약한다면 "전투공간내의 모든 전투원에게 정보공유 능력을 제공하고, 전투공간에 대한 공통상황인식과 동시의사결정력을 제고함으로서 정보우위를 달성하고 전투력의 상승효과를 유발하도록 하는 정보기술 기반의 전쟁개념"이라고 정리할 수 있다.

네트워크 중심전(NCW)의 핵심 포인트는 지리적으로 분산된 전력을 효율적으로 운용하고, 정확한 표적정보 획득 및 정보의 공유, 다원화된 전투 공간의 효과적 연결 및 통합을 위한 통합정보의 공유가 절실히 요구된다. 그러나 이러한 요구사항이 원활하게 지원되기 위해서는 무엇보다 네트워크 시스템을 구성하고 있는 컴퓨터와 통신망에 대한 정보보호체계의 구축이 시급이 요구되고 있다.

이러한 상황 인식하에 최근 국방 정보화 분야에서는 인터넷 망 등 정보기술을 활용하는 네트워크 공간에서의 정보보호를 위하여 관련 기술 및 정책에 대해 많은 연구와 노력을 기울여 왔다. 그러나 가장 큰 문제점 중의 하나는 국방정보체계를 보호하기 위한 제대별, 기능별 가이드라인이 되는 지침이 미흡하다는 것이다.

국방정보체계는 일단 구축이 된 후에는 국방부 본부로부터 말단 대대급 기동부대까지 일사 분란하게 연동되어 운용이 되어야 하며, 이를 통하여 먼저보고, 먼저 결심하고, 이를 통해 즉각적인 타격태세로 연결이 되어야만 전장에 대한 혼선을 줄이고 효율적인 업무 수행이 가능한 것이다. 이를 위해서는 네트워크 중심전(NCW)에 의한 사이버 공격을 당하기 전에 평소 국방부 본부로부터 말단 제대까지 장관, 지휘관, 참모 및 실무자가 구체적인 국방정보체계 보호에 대한 인식을 같이하고 조직내의 대비수준을 점검하여 미비점을 보완하여 나가야만 제대로 방비가 가능하고 큰 문제가 발생하지 않을 것이다.

또한 지금까지는 정보체계에 대한 정보보호 대책이 주로 정보보호 담당자 위주로 수행되어 왔기 때문에 관리적 차원에서 국방 조직내의 구성원이 쉽게 따라 할 수 있는 매뉴얼화된 지침 개발에는 비교적 관심을 덜 기울여 왔고, 이 때문에 현 시점에서 일부 보안 전문가들 이외에는 국방 조직내의 지휘관, 관리자등 일반 구성원들의 외면을 받아오고 있는 실정이다.

따라서 본 연구자는 이러한 문제점을 인식하고 국방 정보체계 분야에 다년간 근무했던 경험과 학문적인 연구방법론을 바탕으로 네트워크 중심전(NCW)하에서의 국방정보체계 정보보호 지침을 도출하여 완벽한 대비태세를 준비하기 위한 가이드라인으로 제시하고자한다.

2. 국방과 네트워크 중심전(NCW)

2.1 국방의 개념

전통적으로 국토방위 즉 국방의 정의는 '적의 침략으로부터 국민과 영토를 보호하는 것'이라고 그 개념이 정의되고 있다. 이 개념을 구체적인 실행 차원에서 달리 표현 한다면 국방이란 "적의 침략으로부터 국민과 영토를 보호하고 핵심가치를 적의 위협으로부터 보호하기 위한 능력을 확보하는 것"이라고 정의 할 수 있다.

이와 같이 국방의 본질이 적의 '위협'으로부터 국가의 '핵심가치'를 '보호하는 것'이라면 자연히 보호해야할 대상, 위협의 실체와 종류, 수단 세 가지 요소가 필수적으로 정의 되어야 한다.

따라서 먼저 보호를 해야 할 대상으로서 국가의 생존과 관련되는 핵심 가치를 식별한다면, 국가 정보체계 인프라로서 국방망, 공안망, 금융망 등이 될 것이다.

둘째, 위협의 실체에 관한 것이다. 위협은 국가의 핵심가치를 침해하려고 하는 적대 세력 및 수단이라고 설명될 수 있는데 이러한 측면에서 현존하는 대한민국 국방의 위협실체는 북한이라고 할 수 있으며, 위협의 유형은 치명적인 살상 및 파괴가 동반되는 무력침공이라는 군사적 위협이 우선 거론 될 수 있고 여기에 더하여 다양한 형태의 위협, 예를 들면 정보전 위협 등 비살상적인 위협이 존재한다.

셋째, 국방에 대한 위협이 살상과 파괴가 동반되는 군사적 위협과 살상이 수반되지는 않으나 통신마비 등 국방에 치명적인 위해를 가하는 비군사적 위협이 존재한다면 이에 대한 대응도 군사적, 비군사적 측면에서 다양하게 전개되어야 할 것이다.

2.2 네트워크 중심전(NCW) 대상과 주체 및 위협

본 연구에서는 이러한 관점에서 1) 국가 안보를 위해 보호되어야 할 대상으로서 국방정보체계, 2) 현존하는 위협의 실체로서 비살상적인 사이버 정보전 공격, 3) 방어 수단으로서 국방정보체계에 대한 정보보호 대책으로 규정하고 네트워크 중심전(NCW)하에서 국방정보체계 정보보호 대책을 강구하고자 한다.

네트워크 중심전(NCW) 환경하에서 예상할 수 있는 공격은 다양한 수단을 활용한 사이버정보전으로 국방정보체계를 공격하여 지휘통제 기능을 마비시키고, 아울러 연합작전을 불가능하게 하기 위해 미군과의 통신투절을 목적으로 할 것이다.

공격주체는 적의 군부대에서 양성한 정보전 전사 및 적대적인 해커 등이 될 것이며 심지어는 개인적인 적대감을 품고 있는 해커가 될 수 있을 것이다. 이들 공격자의 공통적인 공격 목적은 국방기능을 마비시켜 혼란을 야기 시키고 궁극적으로는 방위능력을 훼손시키는 목적을 가지고 있을 것이다.

공격방법은 다양하게 전개 될 것이 예상 되는데 주요 예를 든다면 해킹, 바이러스, 웜, 스파이웨어, 스팸메일, 논리폭탄을 비롯하여 초미세형 로봇, 전자적 미생물 등이 될 것이다.

따라서 본 논문에서는 네트워크 중심전(NCW) 환경하에서 만약 적으로부터 침해를 받아 마비된다면 국방에 큰 위협이 될 수 있는 국방정보체계에 대한 정보보호차원에서 강구되어야 할 대책을 제대별, 기능별로 체계화 하여 제시하고자 한다.

3. 연구방법

3.1 연구방법의 기본 틀

본 연구를 위해 채택한 연구 방법은 전문가 그룹의사결정기법이다. 일반적으로 객관적인 데이터에 의해 계량화 될 수 없고 참여자의 의견이 다양하게 표출될 수 있는 어떤 문제에 대한 합리적인

의사결정은 그 분야에 정통한 전문가 워킹그룹을 편성하여 의견을 취합하는 방식이 적합하다[4, 9]. 본 연구에서는 이와 같은 관점 하에 전문가 워킹그룹을 활용하여 네트워크 중심전(NCW) 환경하에서의 국방정보체계에 대한 제대별, 기능별 정보보호 지침을 도출하였다.

본 연구에서 수행한 전문가 워킹그룹을 통한 그룹의사결정기법은 참가자들끼리 서로 자유로이 의견을 제시할 수 있는 브레인스토밍기법과 함께 참가자들이 자기의 생각을 조용히 기술하는 브레인라이팅기법을 사용하였으며, 최종적인 검증을 위해 전문가 설문을 실시하였다.

또한 군 부대의 특성상 부대의 규모와 업무의 수준에 부합되는 정보보호 대책을 도출하기 위해 국방부, 육군본부 등 정책 부서와 야전부대를 구분하여 제대별, 기능별 정보체계 보호 대책을 도출하기 위하여 각 각 별도의 전문가그룹을 활용하였다.

3.2 전문가 그룹 편성

본 연구를 위한 전문가 집단은 네트워크 중심전(NCW) 환경에 대한 국방정보보호에 관환 내용이기 때문에 문제 영역에 부합되는 전문가로서 국방부 본부 및 육군의 정보통신 병과 현역 및 예비역 장교들로 구성하였다. 워킹그룹에 참여한 전문가들은 5년 이상 국방정보체계 분야에서 정보보호 계획 수립, 시스템 개발, CERT 요원으로서의 경험을 가진 자들로서 이 분야에 충분한 전문지식을 가진 우수 요원들이다. 참여자들은 주로 전산 또는 전자공학을 전공하고 본 연구에 관심을 가지고 참여하였으며, 참가인원은 정책부서인 국방부 및 육군본부에서 5명, 야전부대 근무 경력자 5명 등 총 10명이다.

본 연구에 참여한 워킹그룹의 그룹의사결정 참여자들은 학력이나 경력 및 경험면에서 본 연구의 취지에 매우 적합한 인력으로 판단되며, 연구에 적극적으로 협조를 하였기 때문에 네트워크 중심전(NCW) 환경하에서의 국방정보체계에 대한 정보보호 지침을 도출하는데 큰 무리는 없다고 판단되었다.

3.3 제대 및 기능 구분

본 연구에서는 연구 목적을 위하여 국방정보체계와 관련된 제대, 기관 및 부서 분류를 1) 정책부서, 2) 전략제대급 부대, 3) 군단급 이하 전술부대 전산실, 4) 시스템 도입 및 개발부서로 구분하였다.

첫째, 정책부서는 군의 최고위급 제대 부서로서 국방부 본부, 합동참모본부 및 육, 해, 공군 본부의 정보화 담당 부서로서 주요 임무 및 기능은 국방 및 군의 나아갈 비젼과 정책을 수립하고 예산을 편성하며, 인력 계획 및 교육훈련 방침을 수립하고, 중/장기 시스템 도입정책을 수립 하는 등 거시적이고 정책적인 업무를 수행하는 부서이다.

둘째, 전략제대급 부대는 각 군의 군사령부 급 부대를 의미하며 주요 임무 및 기능은 상위 개념의 국방 정책에 부합하면서 야전군 차원에서의 정보화 계획 수립 및 지휘통신체계 운용과 예하 부대의 정보통신 업무에 대한 지휘통제 업무를 수행한다.

셋째, 군단급 이하 전술부대 전산실은 군단, 사단, 여단급 부대에서 운영하는 전산실을 말하며 주로 해당 부대의 시스템 운영과 네트워크관리 등을 담당한다.

넷째, 시스템 개발 및 도입부서는 국방부 본부, 각 군 본부의 정보화 업무개발 및 도입업무를 수행하는 부대 또는 부서를 말한다. 현재 국방부 및 각 군의 정보화 업무 개발 및 도입은 국방부 본부는 '국방정보전산관리소'에서 주로 담당하며, 육·해·공군의 업무는 각 군에 속한 '정보체계관리단' 또는 '중앙전산소'에서 담당하고 있다.

4. 제대별/기능별 국방정보체계 정보보호 지침 도출

4.1 그룹의사결정 그룹편성

본 연구에서는 전술한 바와 같이 네트워크 중심전(NCW) 환경하에서 국방정보체계 정보보호 지침을 제대별, 기능별로 도출하기 각 해당부서 또는 부대의 정보통신분야에서 근무한 경력이 있는 정보통신병과 현역 및 예비역 장교들로 그룹의사결정 워킹그룹을 편성하였다.

워킹그룹은 정책부서인 국방부 본부 및 각군본부 정보통신 참모부에서 근무한 경험이 있는 현역 및 예비역 장교 5명, 군사령부 급 전략제대 와 군단급 이하 전술제대 전산실에서 근무한 경력이 있는 전문가 5명으로 구성하였다.

4.2 정보보호 지침 도출방법

연구자는 본 연구에 참가하기로 동의한 참가자들에게 연구 취지와 가치에 대하여 공감대를 형성하기 위하여 본 연구 결과가 장차 네트워크 중심전(NCW) 환경하에서 적의 정보전 공격에 대비하여 제대별, 기능별로 국방정보체계를 보호할 대책을 마련하는데 중요한 기초 지침이 될 수 있다는 점을 설명하고 공감대를 형성하였다.

공감대 형성 후 연구가가 사전에 수집한 다양한 정보보호 점검표 또는 가이드라인 자료를 나누어 준 후 그들이 그동안 생각하고 경험했던 내용을 바탕으로 제대별, 기능별 정보보호지침에 대한 내용을 구상하도록 7일 간의 연구 기간을 부여하였다.

7일 간의 연구 기간이 부여된 이후에는 참가자 전원이 한 장소에 모여 전문가 워킹그룹을 통한 그룹의사결정기법에 대하여 설명을 다시 들은 후 다른 구성원과 토론 없이 핵심 지침들을 나누어 준 양식에 자유로이 기술하도록 하였다. 이렇게 기술한 내용을 가지고 각 팀별로 별도로 소회의실에 모여 항목별로 정리한 후 1차 정리된 결과를 보면서 참가자 전원이 토론을 통해 의견을 나누고 새로운 아이디어가 나오면 타당성을 검토 후 첨가하면서 아이디어를 교환하고 공감대를 형성하여 나가면서 주요 지침들을 식별하여 정리하였다.

2단계 최종 종합 단계에서는 효과적인 결과를 도출하기 위해 하나하나의 결과를 파워포인트 화면에 전시하면서 수정 기록하였으며 도출된 내용들을 하나하나 그 타당성에 대하여 재 토론을 하면서 확정해 나갔다. 이와 같은 과정을 거쳐 확정된 제대별, 기능별 국방정보체계 보호지침 초안은 별도로 국방정보통신 업무에 종사하는 15명의 전문가에게 설문조사 및 방문 또는 면담을 통해 최종 점검하고 정리하였으며, 그 결과는 다음과 같다.

5. 제대별/기능별 국방정보보호 지침

5.1 정책부서에서의 정보보호 지침

전술한 바와 같이 국방 업무에서 정책부서는 국방부 본부, 합동 참모본부 및 육해공군 본부에 해당된다. 현재 한국군에는 국방부 본부, 합동참모본부, 각 군 본부에 정보체계 업무를 관장하는 참모부가 편성되어 운영되고 있다. 이 부서들은 실제 시스템을 운영관리하지는 않으나 국방정보체계에 대한 정책수립과 예산 편성, 중장기 발전 계획수립, 법규 및 규정 제정 등 거시적인 차원의 업무를 주로 수행하고 있으며 실무자들의 직급은 최소 중령급 이상으로 보직되어 있다.

본 연구에서 전술한 절차를 거쳐 도출된 정책부서에서의 정보보호 지침을 정리하면 <표 1>과 같다.

5.2 전략제대에서의 정보보호 지침

군에서의 전략제대는 육군의 경우에는 1·2·3군 사령부, 해군은 1·2·3 함대 사령부, 공군은

〈표 1〉 정책부서에서의 정보보호 지침

구 분	정보보호 지침
정책분야	1. 국방부 본부는 문서화된 정보보호 정책기획서 작성 후 장관, 합참의장 승인 획득 2. 승인된 정보보호 정책기획서를 바탕으로 국방 정보보호 예산 편성 3. 정보보호 정책기획서를 바탕으로 각 군 정보보호 기본계획 작성 지침 하달 4. 각 군 본부는 정보보호 정책기획서 및 지침을 시행하기 위한 군별 정보보호 기본계획 (우선순위, 책임, 일정, 예산) 작성 및 참모총장 승인 획득 5. 정보보호 기본계획을 이행하기 위한 이행계획(지침, 절차 및 표준 점검표 포함) 작성 및 예하대 배포 6. 정보보호 기본계획을 매년 단위로 최신기술을 반영하여 업데이트 후 재 배포 7. 정보보호 이행계획 실천현황 점검계획 작성 및 예하대 배포
조직분야	1. 국방부 본부 및 각군 본부에 정보보호 팀을 최소 과급 이상으로 편성하고 전문성을 갖춘 관리자 임명 2. 정보보호 팀 요원은 정보보호 정책 수립, 위험분석, 평가 및 통제업무를 수행할 전문성을 갖춘 자로 보직 3. 필요시 외부 전문가를 활용할 수 있도록 정보보호위원회를 구성하여 활용
예산분야	1. 정보보호 정책기획서를 구현할 중장기 예산 편성(하드웨어, 소프트웨어 및 네트워크 예산 포함) 2. 예산편성의 연속성을 보장받기 위해 중기계획 예산항목으로 편성
책임할당	1. 정보호호 업무를 이행하는 책임과 역할을 부서별, 제대별로 명시하고 문서화하여 지침으로 배포 2. 국방요원 개인 각자에게 정보보호 직무기술서를 제작하여 배포 3. 정보보호 규정 위반시 인사규정을 명시하고 배포
교육분야	1. 각급 부대별 정보보호 인식제고 및 교육을 위한 지침 제공 2. 각급 부대별 교육 및 훈련 실시후 평가 지침 제공
시스템 도입	1. 시스템 도입시 정보보호 규정 준수 지침 수립 및 전파 2. 업무 개발시 개발 단계별 정보보호 규정 적용 지침 수립 및 전파
시스템 운영	1. 전산실 및 네트워크 운영시 준수할 정보보호 지침 수립 및 전파 2. 침해 사고시 대응책 및 수행절차 수립 전파 3. 데이터 보안 지침 수립 및 전파

전방작전사령부와 후방작전사령부를 지칭한다. 여기에 더하여 해병대는 해병대 사령부를 지칭한다. 전략제대에 해당하는 부대들에는 정책부서와 마찬가지로 정보통신 업무를 전담하는 참모 조직이 편성되어 운영되고 있으나 그 규모는 전자보다는 비교적 소규모로 편성되어 있다.

군 사령부급 전략제대의 정보보호 담당 부서는 정보통신 참모부내에 편성되어 운영되고 있는데 그 주요 업무는 상급 부서인 정책부서로부터 하달된 기본 지침에 따라 군사령부 고유의 특성에 부합하도록 조정하여 예하부대 업무를 통제하고 있다. 군사령부 급 정보통신 참모부도 실제 시스템을 운영하지는 않으나 군사령부 예하부대에 정보보호 대응팀 운영에 대한 통제를 주로하고 실무자들의 직급은 최소 소령급 이상으로 보직되어 있다.

본 연구에서 워킹그룹에 의한 전문가의사결정 과정을 통해 도출된 전략제대 정보보호 지침을 요약 정리하면 <표 2>와 같다.

5.3 각급 부대 전산실에서의 정보보호 지침

군의 여단급 이상 부대에는 정보체계 운영 담당 부대 또는 부서(통상 전산실)가 편성되어 있으며 이들 부대 또는 부서는 시스템 및 네트워크를 직접 운영하는 책임을 가지고 있다. 예를 들면 국방부 본부에는 '국방전산정보관리소'가 독립 기관으로 편성되

〈표 2〉 전략제대 정보보호 지침

구 분	정보보호 지침
조직분야	1. 사령부내에 정보보호 팀을 최소 과급 이상으로 편성하고 전문성을 갖춘 관리자 임명 2. 정보보호 팀 요원은 침해사고 대응책, 위험분석, 평가 및 통제업무를 수행할 전문성을 갖춘 자로 보직
예산분야	1. 사령부 예하제대 정보보호 예산 편성 2. 사령부 예하제대 하드웨어, 소프트웨어 및 네트워크 예산 집행
책임할당	1. 사령부 예하 정보보호 인력의 책임과 역할을 명시하고 문서화 2. 정보보호 규정 위반시 자체 인사규정을 명시하고 배포
시스템 운영	1. 전산실 및 네트워크 운영 요원에 대한 운영 지침 수립 및 전파 2. 침해 사고, 데이터보안 감독
정보자산관리	1. 사령부 및 예하부대 정보자산 현황조사 및 책임관 임명 2. 정보자산의 가치 분류 및 보안 등급 부여 지침 수립 및 전파 3. 물리적 보안대책을 위한 지침 수립 및 전파

어 있으며, 각군 본부에는 '정보체계관리단', 또는 '중앙전산소'라는 이름의 부대가 편성 운영되고 있다.

한편 군단급 이하 기동부대, 즉 군단, 사단, 연대 등 전술제대급 부대는 유사시에 부대가 수시로 기동하면서 전투 행위를 하여야 하기 때문에 규모를 갖춘 정보통신 참모부 또는 전산실을 별도로 편성 운영하기보다는 소규모의 전산팀을 편성하여 시스템 운영과 네트워크 관리에 중점을 두고 운영하고 있으며, 책임자 급 실무자는 통상 소령급 장교로 보직을 하고 있다.

본 연구에서 도출된 전산실의 정보보호 지침을 정리하면 <표 3>과 같다.

5.4 정보체계 도입 및 개발부서에서의 정보보호 지침

국방부 본부 및 산하에는 주요 제대마다 정보체계 도입 및 업무개발 조직이 편성되어 운영되고 있다. 최상위 제대인 국방부 본부에는 '국방전산정보관리소'라는 독립 조직이 편성되어 있으며, 육군본부에는 '육군정보체계관리단', 해군본부에는 '해군중앙전산소', 공군본부에는 '공군중앙전산소'라는 명칭의 정보체계 담당 부대가 편성되어 있으며 각각 해당 군의 정보체계 도입 및 개발업무를 주관하고 있다. 각 군의 예하 제대에도 주요 사령부 급에는 규모의 차이는 있지만 전산실이 편성되어 소규모 업무 개발은 직접 수행하고 있다.

이들 부대 또는 부서들이 수행하는 주요 업무는 각 군에서 운영되는 업무를 개발하거나 컴퓨터를 비롯한 장비 도입과 운영, 네트워크 시스템 구축 및 운영을 담당하고 있으며 이 분야에 대해서는 거의 모든 권한과 운영 책임을 가지고 있다. 이 외에도 군수사령부, 교육사령부 등 주요 사령부에도 별도의 전산실에서 시스템 도입 및 개발 업무를 수행하고 있다.

따라서 국방정보체계의 원활한 운영과 정보보호 수준은 상당부분 이들 부서 및 부대가 얼마나 조직적이고 체계적으로 시스템 도입과 업무개발을 관리하느냐에 달려 있다고 해도 과언이 아니다. 이런 맥락에서 본 연구에서는 이들 조직에서 시스템 도입과 개발시에 준수해야 할 정보보호 지침을 별도로 분리하여 도출하였다.

본 연구에서 도출된 정보체계 도입 및 개발부서에서의 정보보호 지침을 정리하면 <표 4>와 같다.

〈표 3〉 전산실 정보보호 지침

구 분	정보보호 지침
전산실 물리적 보호	1. 전산실은 진동, 먼지, 홍수 및 침수 등 위험에서 안전한 곳에 위치 2. 전산실 내 특별한 보호가 필요한 시설 및 장비의 보호구역 설정 및 이에 대한 보호대책 수립 3. 보호구역 등급에 따라 장비, 문서 및 매체의 입/출입 통제 실시 4. 전산실 건물은 내화 건축물로 구축하여 화재의 위험에서 안정성 확보 5. 전산실 출입 절차를 수립하고 이에 따라 출입통제 6. 전산실 내부에는 공조시설(항온항습기), 화재감지, 누수감지기, 무정전공급기 등 설치
장비보호	1. 장비들을 서버실, 네트워크실, 배전관, 매체보관실 등에 적절히 분리되어 설치 2. 화재, 온도, 습도, 환기 등 으로 보호될 수 있도록 배치 3. 무정전 전원 공급기, 전압조절기, 비상 발전기 등 전력공급 이상시 대책 수립 4. 데이터 송수신용 전력 및 통신 케이블 보호대책 수립 5. 장비 손상시 즉시 대처 할 수 있는 대책(장비보수, 정비업체 계약 등) 수립 6. 장비의 안전한 폐기 및 사용 대책 수립
전산실 운영	1. 전산실 운영 지침서 작성 및 절차 수립(운영요원 권한, 책임, 임무 및 기능 등 명시) 2. 정보처리 및 데이터 취급, 오류 및 예외사항, 위험 발생시 처리 절차 등 명시 3. 시스템 모니터링 절차 작성 및 배포 4. 장애 및 운영 일지 기록 및 주기적 검토
정보자산관리	1. 정보자산 책임관 임명 및 현황조사 유지 2. 정보자산의 가치 분류 및 목록 작성과 보안 등급 부여 3. 정보자산 폐기시 기록 유지 및 완전 삭제여부 점검
네트워크관리	1. 인가된자만 접근할 수 있도록 접근통제 절차 수립 2. 사용자 터미널과 서버간에는 물리적, 논리적 경로 통제책 수립 3. 원격 접속사용자의 적절한 인증 및 사용통제 4. 서버내 응용프로그램 및 데이터베이스에 대한 원격 접근 통제 5. 해킹 등 악성 소프트웨어 탐지 및 복구 대책 수립 및 시행
사용자 관리	1. 사용자 등록 및 해지를 위한 계정관리 절차 수립 및 운영 2. 시스템 운영 및 데이터 접근 권한에 대한 적절한 부여 및 통제 3. 데이터 접근 특수 권한 부여시 권한 종료시점 관리 4. 사용자패스워드 관리 절차 수립 및 준수
백업 및 복구	1. 정보자산에 대한 백업 및 복구 계획 수립 2. 중요정보에 대하여 주기별(일별, 주별, 월별 등) 정기 백업 실시 및 백업 현황 기록 3. 재난시 백업 매체 분산 저장 절차 절차 수립 및 시행 4. 백업 매체 보관 장소에 대한 물리적 보호 대책 수립 및 시행

6. 결론 및 기대효과

미래의 네트워크 중심전(NCW)은 전투공간 내의 모든 전투원에게 정보공유 능력을 제공하고, 전투공간에 대한 공통상황인식과 동시 의사결정력을 제고함으로서 정보우위를 달성하고 전투력의 상승효과를 유발하도록 하는 정보기술 기반의 전쟁개념이다. 이러한 개념의 새로운 전쟁 패러다임을 원활하게 구현하기 위해서는 무엇보다 네트워크 시스템을 구성하고 있는 컴퓨터와 통신망, 어플리케이션, 데이터에 대한 정보보호체계의 구축이 시급이 요구되고 있다.

이러한 상황 인식하에 최근 국방 정보화 분야에서는 수년간 인터넷 망 등 정보기술을 활용하는 네트워크 공간에서의 정보보호를 위하여 관련 기술 및 정책에 대해 많은 연구와 노력을 기울여 왔다. 그러나 가장 큰 문제점 중의 하나는 국방정보체계를 보호하기 위한 제대별, 기능별 지침이 미흡

〈표 4〉 정보체계 도입 및 개발부서 정보보호 지침

구 분	정보보호 지침
시스템 도입관리	1. 외부 시스템 도입시 운영체제, 네트워크, 어플리케이션 별로 정보보호 요구사항 제시 2. 외부 업체의 부대 출입과 정보시스템 접근시 신원조회 철저 3. 외부 도입 시스템과 기존 시스템 연동 운영시 정보보호 대책 수립 및 통제
시스템 분석 및 설계	1. 시스템 개발시 개발 계획에 보안 요구사항의 명확한 설정(사용자 접근권한, 접근통제 유형 등) 2. 시스템 개발 설계서에 입력요구사항 정의 및 문서화 3. 입력데이터의 정확성, 무결성 및 신뢰성을 보장할 표준화 달성 4. 시스템 설계시 내부처리 무결성 회복 기능 포함 5. 출력 요구사항 정의 및 문서화(정확성, 무결성, 신뢰성 대책) 6. 시스템 설계시 사용자 인증 및 암호 요구사항 문서화 7. 시스템 설계시 사용자 인증, 데이터 분실, 수정 및 오남용 점검 요구사항 문서화
시스템 개발 및 구현	1. 시스템 개발시 보안요구사항 구현을 위한 프로그래밍 표준에 따라 코딩 2. 개발된 프로그램이 보안요구사항을 충족하는가 확인 3. 개발된 프로그램의 수정 권한의 확인 및 통제 4. 시험 데이터를 이용하여 실제 보안 요구사항 충족 여부 점검 5. 시험 데이터를 이용하여 원격 접속 및 데이터 보안 요구사항 점검
시스템 변경관리	1. 시스템 개발후 운영시 변경에 대한 관리지침 수립 2. 시스템 변경관리 권한자 선정 및 명확한 변경절차 부여 3. 시스템 변경시 변경 승인 절차 확립 4. 시스템 변경후 변경이력 등록 및 문서화 5. 시스템 변경후 보안요구사항 충족 여부 확인 및 사용 승인 절차 확립 6. 운영체제 변경시 시스템 변경의 경우 보안요구 사항 충족여부 점검 7. 외주 구매 패키지 변경시 보안요구 사항 재점검

하다는 것이다. 제대별, 기능별 정보보호 지침이 정립되어 있고 이를 활용하여 각 부대별로 정보보호 체계 구축에 임한다면 혼선을 줄이고 효율적인 업무 수행이 가능할 것이다.

본 연구는 이러한 인식하에 국방 정보체계 분야에 다년간 근무했던 경험과 학문적인 연구방법론을 바탕으로 네트워크 중심전(NCW)하에서의 정보보호 대책 수립을 위한 지침을 도출하여 가이드라인으로 제시하였다.

본 연구에서의 연구방법은 그룹 의사결정론을 전제로 전문가 판단과 그룹 참가를 바탕으로 한 연구 기법으로 실시하였다. 본 연구에서 제시된 제대별, 기능별 정보보호 지침은 정보보호 분야에 종사하는 국방 실무자들에게 추가적인 정보보호 대책을 수립하고 발전시키는데 도움이 될 것으로 기대된다.

참 고 문 헌

[1] Cebrowski, Arthur K. and Garst Ka, John J., “Network Centic Warfare : Its Origin and Future”, U.S Naval Institute Proceedings, January, 1998.

[2] Department of Defense, “Network Centric Wrafare”, DOD report to Congress, 2001.

[3] 국정원, 2005 국가정보보호 백서, 2005.

[4] 김성희, 정병호, 김재경, 의사결정 분석 및 응용, 영지문화사, 2000.

[5] 김유재, “정보전에 대비한 군 정보통신망 정보보호 대책 연구”, 1999.

[6] 김종훈 외, “국가 주요기반 구조 보호를 위한 정보전 대응체계 연구”, WISE, 제99호, 1999.

[7] 남길현, “한국의 정보보호 현황”, 제3회 해킹

방지 워크샵, 2000.
[8] 박창권, “네트워크 중심의 미래전 양상과 군 사혁신”, 합참, 제15호, 2000.
[9] 박홍국, 전기정, 의사결정지원시스템, 경문사, 1999.
[10] 이선호, “전략적 정보전의 신국면과 과제”, 군사세계, 1999.
[11] 이진수, “사이버테러와 국가안보”, 국방 정보화 심포지움, 2001.
[12] 최운호, “군 정보보호발전모델 및 사이버전 대응체계 구축방안”, 국방부, 2001.
[13] 한국국방연구원, “NCW의 기본개념 및 구현전략”, 제4회 국방정정책 세미나, 2006.
[14] 한국정보보호센터, 정보전 대응체계 구축 방안, 1999.

권 문 택

1970년 육군사관학교(이학사)
1981년 미국 University of Iowa (공학석사)
1987년 University of Wisconsin (경영정보학 박사)

경희대학교 테크노경영대학원 정교수
경희대학교 정보지원처장
경희사이버대학교 초대 학장
한국사이버테러정보전 학회 부회장