네트워크 중심전(NCW)하의 정보보호체계 구축방안 연구 : 정보보호체계 평가지표 개발을 중심으로

권 문 택*

요 약

본 연구는 네트워크 중심전(NCW)을 원활하게 구현하기 위해 구축된 정보보호체계의 수준을 평가하고 미흡한 부분을 도출함으로서 미래전에 대비하는 예방적 지침을 마련하고자 수행하였다. 본 연구에서는 국방 정보체계 분야에 다년간 근무했던 전문가들로 워킹그룹을 편성하여 그룹의 사결정기법을 활용한 연구방법을 통해 NCW하에서의 정보보호체계 수준을 평가하는 지표를 개발하였다. 본 연구에서 개발 제시한 평가지표를 활용하여 시스템 수준을 평가하고 미흡한 점을 보완한다면 보다 완벽한 정보보호 대책을 마련할 수 있을 것이다.

A Study on the Information Security Plan for Network Centric Warfare : Development of Information Security Governance Assessment Index

Moon Taek Kwon*

ABSTRACT

Information security is a critical issue for network centric warfare(NCW). This paper provides a information security governance index 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 organization's planners determine the degree to which they have implemented an information systems governance framework at the strategic and tactical level within their organization.

Key words : Network Centric Warfare, Group Decision Making, Information Security Governance Assessment Index

* 경희대학교 테크노경영대학원 교수

1. 서 론

21세기 들어오면서 미국을 비롯한 서방 선진국들은 군사혁신의 가속화를 추진하면서 기존의 플랫폼(platform) 중심의 군사혁신을 네트워크 중심(network centric)의 군사혁신으로 변화를 추구하게 되었다. 이는 정보기술을 지휘통제와 통신체계에 긴밀히 접목하면서 모든 부대와 개인들을 네트워크로 연결한다는 개념으로서, 이를 통해 정보의 수집, 가공, 처리 및 명령하달이 실시간으로 이루어짐으로서 즉각적인 타격을 통해 적을 제압하고 부대의 기동성을 증대시킴은 물론 시간적인 제한을 최소화하는 네트워크 중심의 전쟁 개념을 발전시키는 계기가 되었다.

'네트워크 중심전(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 NCW에 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.

NCW의 핵심 포인트는 지리적으로 분산된 전력을 효율적으로 운용하고, 정확한 표적정보 획득 및 정보의 공유, 다원화된 전투 공간의 효과적 연결 및 통합을 위한 통한 정보의 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 국방 정보보호체계 구축을 위해 참고가 될 만한 평가지표와 가이드라인이 미흡하다는 것이다.

정보보호체계 평가지표와 가이드라인이 사전에 준비되어 있고 이를 활용하여 정보보호체계 구축에 임한다면 혼선을 줄이고 효율적인 업무 수행이 가능할 것이다. 왜냐하면, 실제 사이버테러정보전 공격행위가 발생하기 전에 평소 지휘관, 참모 및 실무자가 구체적인 정보보호체계 평가지표를 가지고 조직내의 대비수준을 점검하여 미비점을 보완한다면 큰 문제가 발생하지 않기 때문이다.

또한 지금까지는 정보보호 대책이 주로 정보보호 담당자 위주로 수행되어 왔기 때문에 관리적 차원에서 국방 조직내의 구성원이 쉽게 따라 할 수 있는 매뉴얼화 된 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 NCW하에서의 정보보호 대책을 위해 예방차원에서의 정보보호 시스템 준비 실태를 평가하고 미흡한 점을 보완하여 완벽한 대비태세를 준비하기 위한 평가지표와 가이드라인을 제시하고자한다

2. 연구방법

2.1 연구방법의 기본 틀

본 연구를 위해 채택한 연구방법은 의사결정이론에 근거한 전문가 워킹그룹을 활용한 그룹의사결정기법이다. 일반적으로 다양한 의견을 가지고 있는 어떤 도메인에 대한 종합안을 도출하기 위해

서는 그 도메인에 정통한 전문가 워킹그룹을 편성하여 의견을 취합하는 방식이 적합하다[4, 9]. 본 연구에서는 이와 같은 관점 하에 전문가 워킹그룹을 활용한 그룹의사결정기법을 사용하였다.

전문가 워킹그룹을 통한 그룹의사결정기법은 문제의 성격에 따라 아이디어를 창출하는 브레인스토밍(Brainstorming)기법, 아이디어를 조용히 기술하는 브레인라이팅(Brainwriting)기법, 브레인라이팅 기법에 토의 및 투표 과정을 더한 명목집단기법(Nominal Group Technique : NGT), 서베이(Surveys)기법 등이 있다. 본 연구는 이러한 그룹의사결정기법을 종합적으로 활용하여 NCW하에서의 정보보호체계 수준 평가지표를 개발하였다.

2.2 정보보호수준 평가지표 개발 방법

본 연구를 위한 워킹그룹 전문가 집단은 필자가 활용 가능한 국방부 산하 육군의 정보보호 분야 인력을 활용하였다. 이들은 육군의 정보통신 병과 현역 및 예비역 장교들로서 정보보호 계획 수립, 사업집행, CERT 요원으로서 시스템을 실제로 운영한 경험을 가지고 있어 이 분야에 충분한 전문지식을 가진 우수 요원들이다. 이들의 주요 학문적 배경은 전산 또는 전자공학을 전공하고 5년 이상 전산실에서 정보보호 업무에 근무한 경력자들로서 본 연구에 흥미를 갖고 참여하였으며, 참가인원은 총 6명이다.

본 연구에 참여한 워킹그룹의 그룹의사결정 참여자들은 조직 규모나 정보시스템 운영면에서 어떤 조직보다도 큰 군 정보통신 병과 조직에서 다년간 경험을 쌓은 요원들이므로 연구를 위한 워킹그룹으로는 매우 적합한 조직으로 판단되며, 또한 연구 참여자들이 적극적으로 협조를 하였기 때문에 여기에서 제안한 기본 평가지표는 미래의 NCW에 대비한 정보보호체계 수준 평가 지침으로서 활용하는데 큰 무리는 없을 것이다.

3. 정보보호체계수준 평가지표 개발

3.1 제 1단계 : 연구에 대한 공감대 형성단계

제 1단계에서는 본 연구에 참가하기로 동의한 참가자들에게 연구 취지와 가치에 대하여 공감대를 형성하는 단계이다. 그룹의사결정에서 가장 중요한 성공요소는 의사결정 주제에 대한 참가자들의 공감대 형성과 이를 통한 적극적 참여의지이다. 따라서 연구자는 제 1단계에서 연구 참가자들에게 본 연구 결과가 NCW하에서 사이버테러정보전에 대비하여 조직의 정보보호체계 수준을 측정하고, 향후 발전방향 수립에 유용하게 활용될 수 있는 모델이 될 수 있다는 점에 대하여 설명을 하고 공감대를 형성하였다.

공감대 형성 후 정보보호체계 구축과 관련된 자료를 나누어 준 후 그들이 그동안 생각하고 경험했던 내용을 바탕으로 조직업무의 IT의존도 평가지표를 구상하도록 약 5일간의 연구 기간을 부여하였다. 이 때 나누어 준 자료는 연구자가 사전 수집한 선행 연구 자료를 정리한 것이다.

3.2 제 2단계 : 조직업무의 IT의존도 수준평가지표 결정

이 단계에서는 참가자 전원이 한 장소에 모여 전문가 워킹그룹을 통한 그룹의사결정기법에 대하여 설명을 다시 들은 후 다른 구성원과 토론 없이 조직업무의 IT의존도를 측정 할 수 있는 핵심 평가지표들을 5일전에 나누어 주었던 양식에 자유로이 기술하도록 하였다. 이렇게 기술한 내용을 가지고 각 분야별로 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 <표 1>과 같이 주요 평가지표들을 식별하여 정리하였다.

여기에서 매 평가지표마다 수준측정을 위한 점수 부여를 최고점수 5점, 최하 점수를 1점으로 배분하여 정성적 수준 평가항목을 계량화 하도록 하였다.

〈표 1〉 IT의존도 수준 평가지표

번호	질문내용	점수
1.1	조직 업무 전반에 대한 IT의존도 정도는?	
1.2	조직내에서 전자정보의 가치 정도는?	
1.3	시스템 서버 다운시 예상되는 업무상 피해 정도는?	
1.4	인터넷 통신망 장애시 예상되는 업무상 피해는?	
1.5	타 조직과의 업무 협조시 IT의존도는?	
1.6	조직내 컴퓨터 시스템 장애발생시 타 조직 업무 수행에 미치는 영향은?	
1.7	컴퓨터 및 인터넷 장애시 부대원 업무 수행에 미치는 영향은?	
1.8	사이버테러정보전 공격을 받았을 때 이에 대한 피해의 심각성에 대한 조직 구성원의 인식 정도는?	

주) 평가점수 부여 기준 : 매우 높다 - 5, 높다 - 4, 보통이다 - 3, 비교적 낮다 - 2, 아주 낮다 - 1.

3.3 제 3단계 : 수준평가 분야 결정

이 단계에서는 제 2단계에서 정리된 조직의 전반적인 IT의존도를 측정하는 지표를 결정한 후에 그 내용을 가지고 세부 평가 분야를 결정하기 위한 작업을 하는 단계이다. 제 2단계 내용을 가지고 다시 토론을 하여 그룹의사결정 방법에 의해 수준측정을 할 대상 분야를 작성하였다.

이를 위해서 참가자는 우선 각자 생각하고 있는 중요 분야를 항목으로 분류하여 카드에 적어 제출하고 카드를 모은 다음 그 결과를 칠판에 기록하면서 도출된 내용들을 하나하나 그 타당성에 대하여 재 토론을 하면서 확정해 나갔다. 이와 같은 과정을 거쳐 확정된 수준평가 분야는 1) 위협에 대한 조직대책 수준 평가, 2) 정보보호 조직/기능 수준평가, 3) 정보보호전략 수준평가, 4) 정보보호 정책 및 절차 수준 평가, 5) 정보보호 프로그램 관리 수준평가, 6) 정보보호 기술요소 수준평가이다.

3.4 제 4단계 : 분야별 세부 수준평가지표 결정

이 단계에서는 전항에서 완료한 수준평가 분야 하나하나에 대한 세부 수준평가지표를 결정하는 단계이다. 이 단계에서도 제 3단계와 마찬가지로 참가자는 각자 생각하고 있는 분야별 세부 평가지표를 카드에 적어 제출하고 카드를 모은 다음 그 결과를 칠판에 기록하면서 도출된 내용들을 하나하나 재 토론을 하면서 확정해 나가는 과정을 거쳐 일단 초안을 작성한 후에 이 초안에 대한 객관적인 검증을 위하여 전문가 서베이를 실시하였다.

서베이를 위해서는 잠정결정 된 초안에 대하여 연구에 참여하지 않은 군내 다른 정보보호 전문요원 중에서 이 분야에 최소한 5년 이상 종사한 전문가 4명의 협조를 얻어 초안에 대한 동의, 부동의 여부를 질문하는 방식으로 검증하였다. 이 때 참여한 참가자들은 객관성을 유지하기 위하여 상호간 참여자가 누구인지를 모르도록 하였으며 만약 응답자가 부동의 한다고 하였을 때는 부동의 부문에 대한 사유를 기술하도록 하였다.

서베이 의견에 대한 결과를 가지고 재 토의를 1차 반복 실시하여 최종 평가지표를 완성하였으며 그 결과는 <표 2>~<표 7>과 같다. 여기에서도 분야별로 매 평가지표마다 수준측정을 위한 점수 부여를 최고점수 5점, 최하 점수를 1점으로 배분하여 정성적 수준 평가항목을 계량화 하도록 하였다.

3.4.1 위협에 대한 조직대책 수준 평가 지표

이 평가지표는 평가시점에서 NCW하에서 사이버테러정보전 위협에 대한 조직의 대책 수준을 평가하는 지표로서 그 결과는 <표 2>와 같다.

〈표 2〉 위협에 대한 조직대책 수준 평가지표

번호	질문내용	점수
2.1	조직 전반에 대한 문서화된 정보보호를 위한 절차를 규정한 매뉴얼 준비 실태는?	
2.2	조직 자체적으로 사이버테러정보전에 대한 훈련이나 교육을 정기적으로 실시하는 수준은?	
2.3	사이버테러정보전에 대비하여 조직내 중요 IT자산과 기능들에 대해서 사전 분류작업을 통해 문서화하고 이에 대한 조직원의 인식 및 관리 수준은?	
2.4	사이버테러정보전이 발생하여 조직내 중요 IT자산과 기능 손실시 이를 신속히 복구할 수 있는 예산의 확보 수준은?	
2.5	조직내 각 기능부서별로 문서화된 정보보호 대책 수립 여부?	
2.6	조직내 각 기능부서별로 문서화된 정보보호 대책 에 따라 실행할 준비 실태는?	
2.7	새로운 사이버테러정보전 기술에 의한 피해 발생시 이에 대비한 조직내 문서화된 정보보호 대책의 주기적인 갱신 실태는?	
2.8	상급조직 조치와 연계하여 조직내 문서화된 정보보호 대책에 대한 즉각적인 갱신 실태는?	

주) 평가점수 부여 기준 : 매우 좋다 - 5, 좋다 - 4, 보통이다 - 3, 비교적 나쁘다 - 2, 아주 나쁘다 - 1.

〈표 3〉 정보보호 조직/기능 수준 평가지표

번호	질문내용	점수
3.1	조직내에 정보보호 전담 조직 편성 여부 및 규모와 수준?	
3.2	조직내 정보보호 전담 조직 부서장의 전문성 및 경험 수준?	
3.3	조직내 정보보호 전담 부서의 독자적 권한 행사 권한 부여 여부와 능력 정도?	
3.4	정보보호 조직의 업무 관장 범위정도(아키텍처, 장비, 절차 및 추적 기능)는?	
3.5	침해 피해 발생시 피해복구에 대한 독자적 조치를 할 수 있는 권한?	
3.6	정보보호 조직원에 대한 신기술 습득 등 항시 보수교육을 받을 수 있는 프로그램 시행 여부?	
3.7	정보보호 조직이 조직내 타 기관과 독자적으로 협조할 수 있는 권한?	
3.8	정보보호 업무에 대한 조직내 최고경영자의 관심과 이를 수행하기 위한 문서화된 책임과 권한 부여 수준?	
3.9	정보보호 정책과 프로그램에 대한 조직내 단위 부서장의 구체적 관여 수준?	
3.10	조직내 일반 구성원에 대해서 정기적으로 정보보호 보안교육 및 이에 대한 실습 시행 수준?	

주) 평가점수 부여 기준 : 매우 좋다 - 5, 좋다 - 4, 보통이다 - 3, 비교적 나쁘다 - 2, 아주 나쁘다 - 1.

3.4.2 정보보호 조직/기능 수준 평가지표

이 평가지표는 평가시점에서 NCW하에서 사이버테러정보전에 대비한 정보보호 조직 및 이를 수행하는 기능의 준비태세에 대한 수준을 평가하는 지표로서 그 결과는 <표 3>와 같다.

3.4.3 정보보호전략 수준 평가지표

이 평가지표는 평가시점에서 NCW하에서 조직의 사이버테러정보전에 대비한 정보보호 전략의 수준을 평가하는 지표로서 그 결과는 <표 4>와 같다.

〈표 4〉 정보보호 전략 수준 평가지표

번호	질문내용	점수
4.1	정보위험분석과 정보보호 전략에 바탕을 둔 조직내 공식적인 정보보호 아키텍처 수립 여부 및 그 수준?	
4.2	새로운 정보보호 위협에 대한 대비책으로서 정보보호 아키텍처의 주기적인 업데이트 여부 및 그 수준?	
4.3	새로운 정보보호 아키텍처 개발시 기존 시스템에 대한 보완기능의 존재여부 및 그 수준?	
4.4	새로운 IT시스템 도입시 기존 시스템과 연동하여 정보보호 기능을 수행할 수 있는지를 체크할 절차나 과정 존재여부 및 그 수준?	
4.5	신규 시스템 도입시 기존의 정보보호 시스템의 아키텍처를 그대로 적용하기 곤란할 때 시스템 도입을 중단하거나 부합되는 다른 시스템을 도입할 가능성 여부?	
4.6	정보보호의 대상이 되는 시스템이나 정보자산을 평가할 수 있는 기능이나 절차 존재 여부 및 그 수준?	
4.7	조직내에서 운용되는 모든 정보시스템에 대한 보안 점검 규정이나 관련 시스템 존재 여부 및 그 수준?	
4.8	조직내 정기적인 보안 패치 관리 절차나 권한 및 책임 부서와 이에 관한 규정 존재 여부 및 그 수준?	

주) 평가점수 부여 기준 : 매우 좋다 - 5, 좋다 - 4, 보통이다 - 3, 비교적 나쁘다 - 2, 아주 나쁘다 - 1.

3.4.4 정보보호 정책 및 절차 수준 평가지표

이 평가지표는 평가시점에서 NCW하에서 조직

의 사이버테러정보전에 대비한 정보보호 정책과 절차의 수준을 평가하는 지표로서 그 결과는 <표 5>와 같다.

〈표 5〉 정보보호 정책 및 절차 수준평가지표

번호	점검 내용	점수
5.1	조직내에서 정보보호업무 실시를 위한 조직 구성원 개개인의 책임을 명기한 규정 수립 및 그 수준?	
5.2	조직구성원 개개인이 평소 보안 의식을 가지고 컴퓨터, 이메일, 인터넷 및 인트라넷 등을 사용하는지 여부와 그 수준?	
5.3	조직 구성원들이 조직내 정보자산에 대한 보호절차를 준수하고 개개인의 업무 수행중 발생하는 자료를 보호하기위한 조치여부와 그 수준?	
5.4	조직내 정보시스템이 시스템에 대한 접근통제, 인증 및 허가 절차를 엄격히 따르도록 구축되어 있는지 여부?	
5.5	정보시스템내의 데이터 분류, 저장 및 유지, 공유 및 파기를 위한 절차 수립 여부 및 그 이행 수준?	
5.6	조직내 정보보호 취약성 관리 및 재난 복구를 위한 우발계획 수립 여부 및 그 수준?	
5.7	사이버테러정보전에 의한 침해사고 발생시 이에 대한 즉각적인 보고 및 대책 수립, 규정 준수여부에 대한 모니터링, 정보보호 강화 절차 수립여부 및 그 수준?	
5.8	사이버테러정보전에 의한 침해 발생시 즉각적인 조사 및 복구, 데이터 백업절차 수립 여부 및 그 수준?	
5.9	정보시스템에 대한 다중적인 물리적 정보보호 수단, 절차 수립 여부 및 그 수준?	
5.10	중요 하드웨어 장비 보호를 위한 대책 수립 여부(무정전 공급기, 전력 불안, 암호 키 등) 및 그 수준?	

주) 평가점수 부여 기준 : 매우 좋다 - 5, 좋다 - 4, 보통이다 - 3, 비교적 나쁘다 - 2, 아주 나쁘다 - 1.

3.4.5 정보보호 프로그램 관리수준 평가지표

이 평가지표는 평가시점에서 NCW하에서 조직의 사이버테러정보전에 대비한 정보보호 프로그램 관리수준을 평가하는 지표로서 그 결과는 <표 6>과 같다.

〈표 6〉 정보보호 프로그램 관리 수준 평가지표

번호	질문내용	점수
6.1	조직내 물리적인 네트워크자산(라우터, 스위칭 시스템, DNS, 서버 등)과 논리적인 네트워크 자산(도메인 네임, 네트워크 어드레스, 엑세스 콘트롤 등)에 대한 현황관리 및 유지 상태?	
6.2	조직내 중요정보자산의 변동이 있을 때 이에 대한 적절한 구성관리 여부 및 그 수준?	
6.3	조직내 전반적인 정보보호 계획, 실행, 통제, 감사 및 보호기법들에 대한 정기적인 테스트 및 평가 여부 및 그 수준?	
6.4	조직내 각 부서별로 자체적인 정보보호 평가 및 감사 실시여부 및 그 수준?	
6.5	조직내 전반적인 정보보호 정책, 세부계획, 실행에 적절성에 대한 평가 실시 여부 및 그 수준?	
6.6	정기적으로 조직내 각 부서별로 자체적인 정보보호 평가 및 감사의 적절성 평가 여부 및 그 수준?	
6.7	정보보호 성과 점검을 위한 평가지표 작성 및 평가후 보고 여부 및 그 수준?	

주) 평가점수 부여 기준 : 매우 좋다 - 5, 좋다 - 4, 보통이다 - 3, 비교적 나쁘다 - 2, 아주 나쁘다 - 1.

〈표 7〉 정보보호기술 수준 평가지표

번호	질문내용	점수
7.1	인터넷 서버들에 대한 다층적인 정보보호 대책 여부(방화벽, 네트워크 IDS, 호스트 IDS, 애플리케이션 IDS 등)와 레이어 간 적절한 통제책 여부 및 그 수준?	
7.2	네트워크 시스템과 애플리케이션들에 대한 주기적인 취약성과 무결성 점검 여부 및 그 수준?	
7.3	조직내 네트워크, 시스템 및 애플리케이션에 대한 비인가자 접근과 비정상적인 프로그램(바이러스, 악성 코드 등) 접근 통제 여부 및 그 수준?	
7.4	하드웨어, 소프트웨어 구성변화, 엑세스 권한, 인가권자 변화 등 시스템 관리 활동에 대한 항시 모니터링 체제 존재 여부 및 그 수준?	
7.5	보안이 필요한 자료에 대한 암호화 여부와 계정, 암호키 등에 대한 적절한 관리여부 및 그 수준?	
7.6	엄격한 패스워드 변경절차에 입각하여 조직내 모든 시스템에 대한 패스워드 관리여부 및 그 수준?	
7.7	엄격한 규정(자동 타임아웃, 로그인 실패시 lockout 등)에 의해 조직내 모든 시스템의 세션과 사용자 관리 업무 수행 여부 및 그 수준?	
7.8	조직내 네트워크 도메인 네임과 어드레스(DNS, 서버 등), 원격 서비스들에 대한 정보보호 특별 조치 여부 및 그 수준?	
7.9	조직내 모든 PC, 워크스테이션 및 서버들에 대한 앤티 바이러스 프로그램 설치 및 정기적 패치 여부 및 그 수준?	

주) 평가점수 부여 기준 : 매우 좋다 - 5, 좋다 - 4, 보통이다 - 3, 비교적 나쁘다 - 2, 아주 나쁘다 - 1.

3.4.6 정보보호 기술요소 수준 평가지표

이 평가지표는 평가시점에서 NCW하에서 조직의 사이버테러정보전에 대비한 정보보호기술 수준을 평가하는 지표로서 그 결과는 <표 7>과 같다.

4. 정보보호체계 수준 평가 종합지표

전항에서 워킹그룹에 의한 그룹의사결정기법을 통해 개발된 정보보호체계 구축 수준에 대한 평가지표를 활용하여 현 조직의 정보보호체계 수준을 평가 한다면 1단계로 우선 조직의 IT의존도 수준을 평가할 수 있다. 연구자와 워킹그룹은 브레인스토밍 기법에 의한 토론을 통해 조직의 IT의존도 수준에 대한 지표를 5개 수준으로 구분하는데 의견을 모았으며 그 각각의 수준에 대한 점수 범위를 <표 8>과 같이 결정하였다. 여기에서 '매우 높은 수준'과 '매우 낮은 수준'의 점수 범위는 5점으로 하였으며, 그 이외는 범위를 10점으로 하였다. 그 이유는 일반적으로 최상위 그룹과 최하위 그룹은 발생 빈도수 면에서 비교적 드물게 일어나기 때문이다.

〈표 8〉 조직의 IT의존도 수준 점수범위

점수 범위	조직의 IT의존도 수준
35~40	매우 높은 수준
25~35	높은 수준
15~25	중간 수준
5~15	낮은 수준
0~5	매우 낮은 수준

또한 상기 점수 범위를 기준으로 조직의 IT의존도 수준 등급에 따른 6개 분야 평가 점수의 합계를 기준으로 '양호', '보통', '불량'으로 종합 판정하는 지표를 마련하였으며 <표 9>는 이를 나타내고 있다.

〈표 9〉 정보보호체계 수준 종합평가표

IT 의존도 수준	점수 수준	평가 점수	수준 판정	종합 평가 및 지침
매우 높은 수준	81% ~ 100%	209 ~ 260	양호	◦ 매우 높은 IT의존도 특성을 가지고 있으며, 이에 부응하여 매우 양호한 정보보호 대책이 수립되어 잘 이행되고 있음 ◦ 현 수준으로 계속적인 관심과 조직적인 관리를 통해 완벽한 정보보호 수행 요망
	61% ~ 80%	157 ~ 208	보통	◦ 매우 높은 IT의존도 특성을 가지고 있으며, 현 수준에서 일부 미흡하나마 비교적 정보보호 대책은 잘 이루어지고 있음 ◦ 그러나 일부 미흡한 분야에 대한 추가적인 대책강구를 통해 보다 세밀한 대책 보완이 요구됨
	0% ~ 60%	0 ~ 156	불량	◦ 매우 높은 IT의존도 특성을 가지고 있으나, 아주 낮은 수준의 정보보호 대책 수준 ◦ 조직 전체 수준의 전면적인 정보보호 대책 강구 시급히 요망됨
높은 수준	81% ~ 100%	193 ~ 260	양호	◦ 높은 IT의존도 특성을 가지고 있으며, 이에 부응하여 매우 양호한 정보보호 대책이 수립되어 잘 이행되고 있음 ◦ 현 수준으로 계속적인 관심과 조직적인 관리를 통해 완벽한 정보보호 수행 요망
	51% ~ 74%	131 ~ 192	보통	◦ 높은 IT의존도 특성을 가지고 있으며, 현 수준에서 미흡하나마 비교적 정보보호 대책은 잘 이루어지고 있음 ◦ 그러나 일부 미흡한 분야에 대한 추가적인 대책강구를 통해 보다 세밀한 대책 보완이 요구됨
	0% ~ 50%	0점 ~ 130	불량	◦ 높은 수준의 IT의존도에 비해 정보보호 대책 수준이 매우 불량하므로 조직 전체 수준의 전면적인 정보보호 대책 강구 시급히 요망됨
중간 수준	67% ~ 100%	173 ~ 260	양호	◦ 중간 수준의 IT의존도 특성을 가지고 있으며, 이에 부응하여 비교적 양호한 정보보호 대책이 수립되어 잘 이행되고 있음 ◦ 현 수준으로 계속적인 관심과 조직적인 관리를 통해 완벽한 정보보호 수행 요망
	45% ~ 66%	105 ~ 172	보통	◦ 중간수준의 IT의존도 특성을 가지고 있으며, 현 수준에서 미흡하나마 비교적 정보보호 대책은 잘 이루어지고 있음 ◦ 그러나 일부 미흡한 분야에 대한 추가적인 대책강구를 통해 보다 세밀한 대책 보완이 요구됨
	0% ~ 44%	0점 ~ 104	불량	◦ 비교적 중간수준의 IT의존도에도 불구하고 아주 낮은 수준의 정보보호 대책 수준이므로 조직 전체 수준의 전면적인 정보보호 대책 강구 시급히 요망됨

낮은 수준	81% ~ 100%	157 ~ 260	양호	◦ 낮은 수준의 IT의존도 특성을 가지고 있으며, 비교적 양호한 정보보호 대책이 수립되어 잘 이행되고 있음 ◦ 현 수준으로 계속적인 관심과 조직적인 관리를 통해 완벽한 정보보호 수행 요망
	81% ~ 100%	95 ~ 156	보통	◦ 낮은 IT의존도 특성을 가지고 있으며, 현 수준에서 미흡하나마 비교적 정보보호 대책은 잘 이루어지고 있음 ◦ 그러나 향후 IT의존도가 높아질 것에 대비하여 미흡한 분야에 대한 추가적인 대책강구를 통해 보다 세밀한 대책 보완이 요구됨
	81% ~ 100%	0 ~ 94	불량	◦ 낮은 수준의 IT의존도이고 또한 정보보호 대책 수준도 매우 불량하므로 향후 발전을 대비해서 조직 전체 수준의 전면적인 정보보호 대책 강구 시급히 요망됨
매우 낮은 수준	51% ~ 100%	130 ~ 260	양호	◦ 매우 낮은 IT의존도 특성을 가지고 있으나 양호한 정보보호 대책이 수립되어 잘 이행되고 있음 ◦ 현 수준으로 계속적인 관심과 조직적인 관리를 통해 완벽한 정보보호 수행 요망
	31% ~ 50%	79 ~ 130	보통	◦ 매우 낮은 IT의존도 특성을 가지고 있으며, 낮은 의존도에 맞추어 비교적 정보보호 대책은 잘 이루어지고 있음 ◦ 그러나 향후 시스템 도입 등 IT의존도가 높아질수록 미흡한 분야에 대한 추가적인 대책강구를 통해 보다 세밀한 대책 보완이 요구됨
	0% ~ 30%	0 ~ 78	불량	◦ 아주 낮은 수준의 IT의존도이기 때문에 현 시점에서는 큰 문제는 없으나 현재의 정보보호 대책 수준이 매우 불양하므로 향후 발전을 대비하여 조직 전체 수준의 전면적인 정보보호 대책 강구 시급히 요망됨

5. 결론 및 기대효과

미래의 네트워크 중심전(NCW)은 전투공간내의 모든 전투원에게 정보공유 능력을 제공하고, 전투공간에 대한 공통상황인식과 동시의사결정력을 제고함으로서 정보우위를 달성하고 전투력의 상승효과를 유발하도록 하는 정보기술 기반의 전쟁개념이다.

이러한 개념의 새로운 전쟁 패러다임을 원활하게 구현하기 위해서는 무엇보다 네트워크 시스템을 구성하고 있는 컴퓨터와 통신망에 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 국방정보보호체계 구축을 위해 참고가 될 만한 평가지표와 가이드라인이 미흡하다는 것이다. 평가지표와 가이드라인이 사전에 준비되어 있고 이를 활용하여 보호체계 구축에 임한다면 혼선을 줄이고 효율적인 업무 수행이 가능할 것이다.

본 연구는 이러한 문제점을 해결하기 위하여 국방 정보체계 분야에 다년간 근무했던 경험과 학문적인 연구방법론을 바탕으로 NCW하에서의 정보보호 대책을 위해 예방차원에서의 정보보호 시스템 준비 실태를 평가하고 미흡한 점을 보완하여 완벽한 대비태세를 준비하기 위한 평가지표와 가이드라인을 제시하였다.

본 연구에서의 연구방법은 그룹 의사결정론을 전제로 전문가 판단과 그룹 참가를 바탕으로 한 명목집단기법에 일부 서베이 기법을 가미한 형태의 연구 기법으로 실시하였다. 본 연구에서 제시된 평가지표와 종합평가지침은 정보보호 조직 및 관리체계를 수립하고, 기술적인 정보보호 대책 마련을 하는데 도움이 될 것으로 판단된다.

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 해킹방지 워크샵, 2000.
[8] 박창권, “네트워크 중심의 미래전 양상과 군사혁신”, 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 대학(공학석사)
1987년 미국 University of Wisconsin 대학(경영정보학 박사)
경희대 테크노경영대학원 정교수
경희대 정보처리처장
경희사이버 대학교 학장
한국지능정보시스템학회 회장
사이버테러정보전학회 부회장