情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

네트워크 중심전에서의 정보보장

김 관 호*

요 약

정보화의 선진국인 미국은 정보전 시대에서는 인적자원의 능력에 따라 전쟁의 승패가 좌우됨으로 교육을 통해 관련 개념을 통일 시키고, 통일된 개념 하에 소요되는 인력을 분야별로 육성 및 관리하여 수행해야 할 작전 범위와 영역에 적합하게 조직화를 시키고, 수행절차를 각종 규정을 통해 강력하게 추진하고 있는데 우리도 이와 같은 선진국의 사례를 분석하여 단순히 소프트웨어나 하드웨어, 기술적인 도구를 확보하면 정보보호가 가능하다는 생각에서 벗어나 개념정립으로부터, 방어전략의 수립, 규정과 지침작성, 필요한 인적자원의 확보 및 관리, 작전수행 방법의 정립, 필요한 기술의 확보 등 체계적인 준비가 필요할 것으로 판단이 된다.

Ⅰ. 배 경

미 국방성 C3I차관보와 정보체계국, 그리고 합참은 미래 디지털 전장 환경인 네트워크 중심 전에서는 우리가 알고 있는 방화벽이나 침입탐지 체계만으로는 전쟁을 위해 필요한 정보보호를 보장할 수 없어 디지털 전장에서 정보보장을 위해 필히 알아야 할 교육프로그램을 만들었는데 그 내용을 소개함으로써 선진국은 어떻게 미래 전을 준비하고 있는가를 이해하고 부족한 분야를 인식하여 체계적인 준비를 하기 위함입니다.

이 교육프로그램이 등장된 배경은 디지털 전장은 네트워크를 기반으로 전장의 가시화를 실현하고 이를 통해 공통된 상황인식을 함으로써 전쟁의 속도, 정확성, 융통성을 증가시켜 전쟁의 효율성을 증대시키는 개념으로 작전의 계획, 명령, 협조 및 실시에 필요한 데이터의 저장, 처리, 전송을 위해 디지털 전자정보기능에 대한 의존도가 증가하고 있습니다.

아군의 정보체계에 대한 무력화를 시도하는 적은 네트워크 기반 시스템의 보안 취약점을 이용한 공격위협을 증가시켜 아군은 적의 공격에 대응하기 위해 계층화된 방어전략(Layered Defense)을 수립하여 아군 네트워크 체계의 취약점을 감소시키고 이를 보호하며, 적의 네트워크 공격위협을 사전에 탐지하고 대응하는 개념을 정립해야 디지털 전투를 하기위해 필요한 전자정보기능에 대한 정보를 보장(Information Assurance, IA)할 수 있다는 것입니다.

Ⅱ. 주요내용

첫째, 기본적인 내용으로 디지털 전장에서 정보보장을 하기 위해 알아야 할 개념과 용어를 소개하고

둘째, 계층화된 방어전략의 개념과 정보환경 분석 및 방어를 하기위한 전략의 우선순위 등을 소개하며

셋째, 정보보장을 위해 필요한 인력의 교육 및 훈련, 인증, 인원의 모집 및 지휘관의 역할을 소개하고

넷째, 정보보장을 위한 작전요소의 개념, 개념을 구현하기 위한 지침과 교리 및 징후와 경보, 사고대응 등을 설명하며

다섯째, 효과적인 사이버 방어를 위해 필요한 기술요소로 네트워크 방어의 중요기술 등을 소개하고 있습니다.

Ⅲ. 기본개념

- 정보작전
- 정보우위
- 정보보장
- 네트워크 작전
- 네트워크중심전의 위협분석

첫 번째 과정은 모두가 알아야 할 기본적인 내용으로 정보작전의 개념과 육군 비전이 구현되기 위한 조건, 정보보장의 의미, 네트워크의 작전, 위협 요소 등으로 구성되어 있으며 정보작전은 정보보장을 위해 기본적으로 알아야할 개념으로서 정보작전(Information Operations, IO)은 아군의 정보 및 정보체계를 보호하면서 적의 정보 및

* 정보통신학교 전술학 처장

정보체계에 영향을 가하는 행위로서 물리적 공격, 심리전, 컴퓨터 네트워크 공격, 컴퓨터 네트워크 방어, 물리적 보안, 작전 보안, 정보보장 등을 이야기하며 현재 미 육군이 추진하고 있는 비전을 달성하기 위해서는 정보우위(Information Superiority)가 필수적인데 이는 정보보장에 의해 달성되며 정보우위는 아군의 정보수집, 처리, 유포 등에 대해 적으로부터 방해를 받지 않으면서 적의 정보수집, 처리, 유포 등을 방해하거나 또는 이용하는 능력 정보, 지휘, 통제, 통신, 컴퓨터 및 정보작전의 우세를 통해 달성된다고 정의하고 있습니다.

또한 정보보장은 정보 및 정보체계의 가용성(Avalibility), 무결성(Integrity), 신뢰성(Authentication), 보안성(Confidentiality), 수용성 (Non-reputation) 등을 보장함으로써 정보 및 정보체계를 보호하고 방어하는 정보작전의 핵심요소로서 정보보장은 정보 및 정보체계의 보호, 적의 공격위협의 탐지 및 대응능력이 통합되어 있으며 유사시 아군 체계의 복구 기능을 제공하는 것을 의미합니다.

네트워크 작전(Network Operations, NETOPS)이란 국가 및 군 내부의 모든 정보통신망은 임무달성을 위해 필요한 정보우위를 제공하며 네트워크 작전은 이에 필요한 네트워크를 관리하는데 있어 조직적이고 절차적인 체제를 제공하는 것으로 정보의 중요성 및 전송에 대한 우선순위 결정을 하는 정보분배 관리(Information Dissemination Management, IDM)와 시스템 운영의 범위, 트래픽 양, 정보 처리량 등을 가시화 하는 네트워크 관리(Network Management) 기능과 정보 및 정보체계에 대한 보호 및 방어 기능으로 구성되어 있습니다.

정보보장을 위협하는 요소는 크게 3가지로 구분되는데 자연환경적 위협은 자연적 요소와 영향에 기인하는 것으로 바람, 번개, 홍수, 화재, 방사능 등이 있으며 인위적, 물리적 위협은 인간에 인해 영향을 받았거나 사용되었던 요소 등에 기인하는 것으로 구조물, 기계, 도구, 열, 물, 화학제품, 가스 등이며 마지막 위협은 인적 자원에 의한 위협으로 이는 정보체계에 대한 가장 큰 위협으로 해커, 조직, 적극적인 네트워크 기반 공격, 내부인원에 의한 공격, 하드웨어 및 소프트웨어 유포 공격 등이 있습니다.

컴퓨터 네트워크 공격(Computer Network Attack, CNA)은 컴퓨터 및 컴퓨터 네트워크 또는 이에 속한 정보에 대한 유통 중단, 접근거부, 성능약화 및 파괴를 위한 활동이며 공격의 형태는 수동적 가로채기 공격(트래픽 감시, 복사, 분석, 암호해독, ID 및 패스워드 획득), 적극적인 네트워크 기반 공격(보안장치 파괴, 악성코드 유포, 정보의 절취 및 변형 등의 행위로서 네트워크 백본, 전송 정보, 지역 통신망에의 침투 또는 정상적인 원격접속을 통한 공격), 내부인원에 의한 공격(네트워크 접근이 인가된 인원에 의해 발생, 정보의 도청, 절취 또는 정보 손상 및 다른 사용자의 접근 거부), 하드웨어 및 소프트웨어 유포 공격(하드웨어 및 소프트웨어에 대한 변형 또는 교환)등이 있습니다.

Ⅳ. 계층화된 방어전략

두 번째 과정은 계층화된 방어전략(Layered Defenses)개념이 왜 필요한 것인가를 교육 시키는 것으로 이 개념은 마치 중세기 전투에서 성(Castle)을 방어하는 것과 같은 것으로 이 개념이 등장하게 된 이유는 최초의 컴퓨터는 단독으로 사용을 하였으나, 인터넷이 발달되어 수 백 만개의 호스트로 연결된 네트워크가 등장하면서 단순접속체계로서는 취약점을 방어할 수 없기 때문에 인적자원과 작전, 기술 등을 통합하여 다중계층 및 다차원적인 보호 체계를 구축해야 적의 공격에 대한 취약점 감소, 아군 체계를 보호할 수 있으며, 또한 강력한 방어 체계 구축을 위해서는 아군 체계들이 상호지원 계층으로 구성되어 적 공격의 탐지 및 대응을 할 수 있도록 하고 아군의 체계를 공격하려고 시도하는 적에게 공격이 실패할 때까지 계속 시도하도록 다중 방어체계를 구축하여 결과적으로 적이 계속 공격하다가 실패되도록 유도하는 개념으로 특히, 이때 아군 정보체계는 모든 접근경로가 적의 공격이나 침투로부터 보호되어야 만이 이 작전 수행이 가능합니다.

이 같은 전략이 수행되는 정보환경(Information Environments)은 크게 4가지 영역으로 단일체계로 된 지역 컴퓨팅 환경, 망과 망이 연결되는 통신망 경계 지역, 네트워크 레벨, 기반체계를 지원하는 영역으로 구분 합니다.

- 정보환경
  - -지역 컴퓨팅 환경
  - -통신망경계지역
  - -네트워크 레벨
  - -기반체계
- 방어전략 적용
  - -우선순위 부여
  - -보안수단

지역 컴퓨팅 환경(Local Computing Environments or Enclave)이란 네트워크 내의 모든 데이터, 애플리케이션, 인원 및 설비를 포함한 모든 요소가 단일체계 속에서 일관된 정책에 의해 관리되고 있는 물리

적인 환경을 의미하며 그 예로는 소규모 조직의 컴퓨팅 환경, 서비스계층 네트워크, 차별화된 LAN, 원격 LAN, 특정 체계, 가상 사설망의 형태가 있으며 이와 같은 영역으로 구분하는 목적은 호스트와 애플리케이션 보호, 지역 통신망 내부 및 외부로부터 데이터의 보안성 및 무결성 보장, 내부 인원으로부터 체계 보호, 보안체계의 변형 없이 애플리케이션들을 용이하게 통합할 수 있는 것을 보장하기 위함이며 통신망 경계 지역(Enclave Boundary)은 LAN 또는 유사 네트워크가 서비스 계층에 접속하는 지점을 의미하며 이같이 구분하는 목적은 통신망 경계 부분에 대한 변형(침투), 노출 및 외부로의 데이터 전송에 대한 보호, 지역 통신망의 물리적, 논리적 경계 부분에 대한 보호, 체계 가용성 보장을 위한 지역 통신망 내부의 시스템 및 네트워크 보호이며 네트워크 레벨 영역이란 전송 및 교환 기능을 포함한 정보 전송체계 보호를 위한 것으로 네트워크의 기반망을 견고하게 설치 및 유지하는 것과 기반구조에 유통되고 있는 데이터에 대한 보호, 외부의 침입에 대한 네트워크의 대응 및 복구 능력을 보장하며 기반체계를 지원하는 영역이란 네트워크, 지역 통신망 및 컴퓨팅 환경에 대한 보안 서비스 제공, 암호화 및 암호키 관리, 탐지 및 보고, 대응기능을 의미하며 지원의 목적은 암호키 관리 및 네트워크 접근 시도 시 정확한 인증을 가능하게 하고, 신속한 침입탐지 및 침입에 대한 반응을 지원하는 것입니다.

또한, 계층화된 방어전략(Layered Defenses)은 가용한 자원 범위 내에서 최대의 효과가 이루어 질 수 있도록 우선순위 부여되어야 하며 임무수행에 요구되는 가용자원 사용의 우선순위는 위기관리로부터 도출되며 이는 위험분석(정보와 정보체계의 가치 및 가능한 위협과 잠재적인 위험의 특성 및 범위에 초점)후 가용자원 내에서 위험을 최소화할 수 있는 보안수단을 강구함으로 가능한데 보안수단은 반드시 소프트웨어, 하드웨어, 네트워크 디자인을 포함하고 체계가 야전에 배치되기 전부터 계획되어져야 하고 지속적이고 신뢰성 있게 작동해야하며 임무, 중요성, 위협 및 기술의 변화를 수용할 수 있도록 관심이 필요하며 특히 작전수행 시 조직 상호간에 정보를 공유하고 협조하여 이와 같은 방어체계가 조직 상호간의 업무 수행에 방해와 부담이 되어서는 안 된다는 것을 강조하고 있습니다.

V. 인적자원

세 번째 과정은 정보보장을 위해 필요한 인력은 기술을 사용하여 작전을 수행하는 핵심요소로서 이와 같은 결정적인 임무를 수행하기 위해서는 임무수행에 필요한 지식과 전문기술을 획득 및 유지하기 위한 교육, 훈련, 경험 등이 포함된 프로그램이 반드시 필요하며 특히, 전문화 와 인증(Certification)은 전문 간부 육성을 위한 동기부여 수단이며 인증을 통해 숙련되고 전문적인 사용자 집단 구축 가능합니다. 또한 최고 수준의 능력을 구비한 탤런트를 선발하는 것은 대단히 중요하나 사전에 배경 및 보안심사 등을 필히 확인을 해야 합니다.

- 방어전략 핵심요소
  - 교육 및 훈련
  - 인 증
  - 지휘주목

또한, 지휘주목, 적극적인 참여의식, 리더쉽은 모든 제대에서 가장 중요한 요소이며, 지휘관은 조직의 보안체계에 대한 핵심역할을 담당하는 자로서 완벽한 보안체계를 유지하기 위해서는 임무와 기능이 세부적으로 구별된 체계 구성승인담당관, 정보체계 보안 장교, 정보체계 보안 관리자, 체계 관리자, 네트워크 관리자 등 잘 훈련되고 전문화된 많은 인력들이 있어야 정보보장이 가능합니다.

VI. 작전요소

네 번째 과정은 정보보장을 위한 작전수행에 대한 개념을 구현하기 위한 것으로 구체적인 지침, 전문적인 관리 및 통제, 정보/징후와 경보, 사고에 대한 대응, 평가와 검사, 승인 및 인가 등의 범주로 구성 되어 있는데 지침(Guidance)에 대한 것 중 정책관련 분야는 국가의 모든 조직에서 작전명령, 지시, 규칙, 규약, 교범 및 표준의 결합된 형태로 나타나며 문서화된 계획은 정책 및 중요 계획요소의 명시 및 정보능력, 특성, 평가 및 검사, 보안대책 및 절차, 사건대응, 작전의 연속성, 개인보안, 훈련정도 등에 대한 구조 및 구성 등을 포함하며 특히, 표준운용절차(Standard Operation Procedure, SOP)는 일상적 작전 및 사고대응, 보고에 대한 내용을 정의합니다.

- 지 침
- 정 책
- 관리와 통제
- 정보징후와 경보
- 사고대응
- 평가와 검사
- 승인 및 인가

방어전략 정보보장 정책은 크게 3가지로 구분을 할 수 있는데 일반 정책(목표, 목적, 범위, 자원할당, 권한과 책임, 승인 등 조직차원의 보안대책) 특정사안 정책(Issue-specific Policy: 작전계획의 연속성 또

는 인터넷 접속 등의 특정 사안 기술) 특정체계 정책(System-specific Policy : 특정 체계에 대한 목표, 규칙, 절차 및 표준을 기술)이 있으며, 교리(Doctrine)는 국가 목표를 위한 행동지침에 대한 기초적 원칙 이며

성공적인 방어전략의 구축을 위해서는 전문가, 체계 감시, 정보체계에 대한 관리와 통제, 포괄적인 목록 및 구조가 요구되며 취약점에 대한 가시화 및 보안에 필요한 기술의 요구 및 상호운용성이 보장되는 보안체제의 구축이 요구됩니다.

정보, 징후 및 경보는 구성원들에게 잠재적 위협 및 공격에 대한 경고를 제공하며 방어 전략은 침입의 특징 및 범위와 영향, 원인, 취약점 등 광범위한 분야에 대한 노력을 요구하며

방어 사고대응은 침입탐지 후 관련 정보를 관리자와 분석 및 대응센터로 보고하며, 사고대응은 즉각적으로 침입 피해의 최소화 및 피해에 대한 복구활동을 포함하고, 침입에 대한 대응으로서 이에 대한 공격 결심 및 공격의 효과를 예측하고 침입자에 대한 추적 노력이 요구되며, 체계 관리자는 보안상태 또는 정보작전상태 강화를 선언하거나 공격받은 체계의 분리를 결심하고 합법적, 외교적 또는 군사적인 대응을 결정해야 하는 등 통합된 정보작전체계는 전체적인 방어노력에 큰 기여가 됩니다.

작전계획의 연속성 및 중요자산보장정책이란 그 자체의 기능유지 및 피해복구 노력으로 인해 중요자산 및 운용의 손실을 초래할 수 있으므로 작전계획은 위협이 될 수 있는 침입이나 다른 사고들에 대해 신속하고 적절한 반응을 할 수 있도록 작성되어야 하며 계획, 준비, 실행, 회복의 단계로 구성되고, 중요자산보장정책은 평화와 위기, 전쟁 등에 요구되는 중요 자산의 준비 및 작전 등에 대한 가용성을 보장합니다.

정보보장을 위해 내/외부 평가관에 의한 평가 및 검사는 정보보장 준비 상태에 대한 명확하고 정확한 진단에 필수적이며, 네트워크, 종단장치 및 구성요소에 대한 자동화된 검사장치 등의 기술도구들을 취약점 평가에 사용하고, 가장 효과적인 평가 및 검사 방법은 직접 체계에 침투를 시도하는 것입니다.

위험 환경에서 지역 통신망과 다른 시스템들이 네트워크에 접근을 시도할 때 자신들의 취약점을 다른 통신망에게 노출시키지 않는 것이 중요하며 승인 및 인가는 의도한 네트워크로의 접속을 승인하는 공식적인 절차의 완성단계로서 미국은 국방성의 정보기술 보안승인 및 인증절차를 통해서 체계에 대한 신뢰성을 보장하고 있습니다.

Ⅶ. 기술요소

다섯 번째 과정은 정보보장을 위한 기술로서 효과적인 사이버 방어를 위해 우수한 성능의 무기체계 및 이를 운용하는 기술은 필수적이며 적용되는 기술들은 권위 있는 기관에서 평가되고 이미 사용된 것들을 이용함으로써 효율성을 높일 수 있습니다.

구체적인 기술도구는 네트워크를 방어하는 기술, 독립된 통신망 경계영역 방어 기술, 지역 컴퓨팅 환경 방어기술, 기반체계 지원 등입니다.

네트워크 방어에서 지역 통신망 간의 연결 매개수단인 네트워크의 보호는 필수적이며 네트워크 방어의 중요 기술은 중복된 다수의 데이터 전송경로를 구성하는 것과 자동화된 감시 및 관리체계, 침입탐지 도구, 암호 기술, 체계별로 독립된 체계 구축 등이 있으며

- 네트워크 방어
  - 중복된 데이터 전송경로
  - 자동화된 감시 및 관리도구
  - 암호화
  - 보호된 분산체계
- 지역통신망 경계 지역방어
- 신기술 도입

중복된 다수의 데이터 전송경로를 구성하는 기술은 일부 네트워크의 기능이 약화 또는 상실되었을 경우 경로의 재설정을 통해 데이터 전송의 연속성을 보장하는 것과 지역 통신망은 유사시 외부 네트워크와의 접속을 차단하고 위험 데이터의 전송을 방지하기 위한 트래픽 필터링과 처리량을 통제하고 필요시 서비스 거부 등의 대책이 강구되어야 하며

자동화된 감시 및 관리도구는 보안체계에 대한 침투 시도 판단과 자동화된 경보, 상황묘사 및 대응행동을 제공할 수 있으며, 암호기술은 정보의 보안성 보장하고, 별도 구축된 보안 분산체계는 용도별, 기능별 단말과 전송선로 통신체계와 가입자와 통신장비, 통신선을 별도로 구성하는 것입니다.

독립된 통신망 경계영역 방어 기술은 외부의 위협으로부터 내부의 데이터와 서비스를 보호하는 것으로 자기방어 능력이 없는 지역 통신망 내부의 구성요소를 보호하는 것으로 구체적인 사례는 식별 및 인증도구(지역 통신망에 접속하는 원격 사용자 인증 및 통제), 방화벽(사설 네트워크와의 인증되지 않은 접근 및 접속을 방어), 악성코드 및 바이러스 탐지기(지역 통신망 경계 지역에서 유해 코드를 감시, 포착 및 파괴), 전자적 안전장치(지역 통신망 내부 정보의 불법적 유출 방지), 프락시 서버(접근이 제한된 네트워크로의 접근 차단), 감시 및 관리체계(지역 통신망으로부터 광역 통신망으로 접속할

경우의 가능성 있는 위협에 대응)등이 있습니다.

지역 컴퓨팅 환경 방어기술이란 지역 통신망의 내부 네트워크를 포함하며 별도 보호된 분산체계 설치 및 종단장치 및 내부 구성요소와 관련된 주변장치를 보호하기 위해 방어의 효과가 확장되는 도구를 사용하는 것으로 주요 사례는 강력한 통제로서 지역 컴퓨팅 환경의 구성요소에 대한 접근 통제하고, 서비스의 사용 및 파일의 접근은 승인에 의해서만 인가하며, 암호화를 통한 정보의 보안성 유지, 전자서명의 생활화, 전기적 안전장치, 시스템 취약점 분석기, 감시체계, 불필요한 코드 감지기, 백업기술 등 입니다.

기반체계 지원은 크게 독립된 암호체계와 키관리를 통해서 불법침입에 대한 탐지, 보고, 대응을 지원하고, 정보보장을 위한 자원의 제공 및 유지, 보수, 군수지원 체계, 사고보고 및 대응능력, 암호화 능력과 같은 특성화된 지원 능력에 대한 지원이며 개발 진행중인 신기술에 대한 시험 및 평가를 통해 지속적으로 효율성 있는 기술을 정보보장에 적용하고, 정보보안과 관련된 신기술의 문제점 분석이 필요합니다.

지금까지 미 국방성과 합참에서 교육하고 있는 정보보장에 대한 내용을 요약하면

- 정보보장을 위해서는 지휘관으로부터 최하위 구성원까지 자원, 의지 및 기술을 활용한 임무 수행 절차의 정립이 필요하며
- 정보보장을 위해서는 수행에 관련된 모든 요소들은 방어전략을 통해 정보보장을 계획하고 통합하여 강력하게 시행하여야 하고
- 정보보장 작전 수행을 위해서는 특히 인적자원 능력의 통합, 발전을 위한 노력이 절대적으로 필요하며
- 방어전략은 변화하는 작전환경 및 기술의 발전, 적의 위협 및 취약점에 적극적으로 대처할 수 있도록 지속적 관심이 요구된다고 할 수 있습니다.

Ⅷ. 결 론

정보화의 선진국인 미국은 미래 정보전을 대비하기 위해서 정보보호를 어떻게 할 수 있는가에 대한 방안과 개념을 정립하여 작전 수행에 필요한 정보보장을 체계적으로 지원하고 있는데 특히, 정보전 시대에서는 인적자원의 능력에 따라 전쟁의 승패가 좌우됨으로 교육을 통해 관련 개념을 통일 시키고, 통일된 개념하에 소요되는 인력을 분야별로 육성 및 관리하여 수행해야 할 작전 범위와 영역에 적합하게 조직화를 시키고, 수행절차를 각종 규정을 통해 강력하게 추진하고 있다는 것을 알 수 있습니다.

따라서, 우리도 이와 같은 선진국의 사례를 분석하여 단순히 소프트웨어나 하드웨어, 기술적인 도구를 확보하면 정보보호가 가능하다는 생각에서 벗어나 개념정립으로부터, 방어전략의 수립, 규정과 지침작성, 필요한 인적자원의 확보 및 관리, 작전수행 방법의 정립, 필요한 기술의 확보 등 체계적인 준비가 필요할 것으로 판단이 됩니다.

〈著 者 紹 介〉

김 관 호 (Kim Gwanu-Ho)

육군사관학교 35기 현역 통신대령
한양대 산업대학원 전자통신공학/
아주대 C4I 석사
국방부 정보체계국 기획장교,
군사과학대학원 C4I 분야 시간강사
국방개혁위 정보화 담당관
육군최초 디지털부대 부대장
육군 최초 전술C4I체계 평가처장
현보직: 정보통신학교 전술학 처장
관심분야: 정보체계평가기법(CMM:Capability Maturity Model)의 군사적 활용방안 연구, 주파수 워게임 소프트웨어 개발, 상호연동을 위한 지침연구, TMN (Telecommunication Management Network), 정보전 대비 정보보호 정책, 정보화 전문인력 육성방안 네트워크 중심전을 대비한 군 전력의 Master Plan 작성