국방주요정보통신기반시설 중심의 정보보호기술구조 연구

A Study on the Information Security Technical Architecture focusing on the Primary Defense Information Infrastructure

최 지 나* 남 길 현*
Choi, Ji-Na Nam, Kil-Hyun

ABSTRACT

The purpose of this thesis is to research and propose a practical Information Security Technical Architecture on Primary Defense Information Infrastructure with regard to requirement of information security. The scope of this research is limited to national defense information master plan & security rule, and U.S. DoD's IATF is used to plan a detailed structure. The result of this research can be used as a guide book for providing security for Army IT infrastructure now and in the future as well as to devise a plan for research and development in information protection technology.

주요기술용어(주제어) : IA(Information Assurance, 정보보증), Defense-in-depth Strategy(종심방어전략), Multi-Level Security(다단계 정보보호), Sequence Diagram(순차 도표)

1. 서 론

국방부는 2005년 10월 현재 국군통신사령부의 국방정보통신망을 포함한 5개 시설을 잠정적인 국방주요정보통신기반시설로 지정하고 있다. 그러나, 이의 보호를 위한 현 규정은 군의 주요정보통신기반시설의 정보보호 요구사항을 충족하기엔 미흡함이 있어, 기반시설에 대한 군의 정보보호 요구사항을 분석·반영한 실제적인 정보보호기술구조의 연구가 필요하다.

국방 정보보호기술구조에 대한 기존 연구 중 대표적인 것으로는 "국방정보체계기술구조(DITA : Defense Information system Technical Architecture)[1]"가 있으나, 이는 미 국방부의 "합동기술구조(JTA : Joint Technical Architecture)"를 준용하고 있어, 국방 환경에 맞지 않는 표준들이 다수 포함돼 있다. 그리고, 최근 발간된 "국방정보보호기술구조 연구[2]"는 국방 전 분야의 정보보호기술을 포괄적인 시각으로 평이하게 다루고 있어, 실무 적용을 위해서는 국방주요정보통신기반시설에 대해 적용 가능한 요소를 발췌하고 특성화하는 작업이 추가로 수행되어야 한다.

본 논문은 2장에서 국방주요정보통신기반시설의 운영현황 및 관련 정보보호 기술을 알아보고, 3장에서 국방주요정보통신기반시설의 보안취약점을 분석하여 국방 환경에 적합한 정보보호기술구조를 제시하고자 한다. 이때 IATF의 종심방어전략(Defense-in-depth Strategy)과 계층적 접근방법을 접목하고자 한다. 마지막 4장에서는 결론 및 향후 연구과제를 제시한다. 단, 국방주요정보통신기반시설에 대한 세부내용은 비

† 2006년 1월 31일 접수~2006년 3월 17일 게재승인
* 국방대학교(Korea National Defense University)
주저자 이메일 : chgina1@hanmail.net

공개 사항이므로 기술하지 않으며, 국방주요정보통신기반시설에서 큰 비중을 차지하는 국방 전용네트워크 분야의 정보보호 방안에 집중하여 내용을 전개할 것이다. 또한, 네트워크기반 관련 사항은 "차세대 국방 정보통신망 최적화 설계 연구[3]"를 바탕으로 하고자 한다.

2. 국방주요정보통신기반시설 현황 및 관련 정보보호기술

가. 주요정보통신기반시설 지정·운영 현황

정보통신부는 2001년 1월 정보통신기반보호법을 제정하여 국가주요정보통신기반시설 관련 조항을 마련하고, 국방 분야에 대해서는 자체적으로 지정·운영하도록 규정하였다[4,5]. 이에 따라 국방부는잠정적으로 국군통신사령부의 국방정보통신망, 합참의 CPAS, 육군의 지상전술C4I, 해군의 KNTDS, 공군의 제2MCRC 등 5개 시설을 주요정보통신기반시설로 지정하고 "국방 정보통신기반 보호지침[6]"을 2002년 4월 국방부 훈령 704호로 제정(2004년 7월 개정)하여 기본적인 가이드라인을 제시하고 있다. 이 지침은 목표와 조직 구성 및 임무와 역할을 규정하고 국군기무사령부를 정보보호 지원기관으로 지정하고 있으며, 취약점 분석/평가, 보호대책, 침해사고 예방/대응 등에 관해 기술하고 있다.

나. 주요정보통신기반시설의 정보보호 목표 및 기술 범주

주요정보통신기반시설에 대한 정보보호 목표는 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 확보하는데 있으며, 요구되는 기능은 신분확인(Identification), 인증(Authentication), 접근제어(Access Control), 운영관리(Administer), 감사(Audit), 암호화(Encryption), 백업(Backup) 등으로 구분할 수 있다[7,8]. 이들 각각의 기능 구현을 위해서는 다양한 정보보호기술들이 복합 작용한다. 본 논문에서 다루는 정보보호기술은 DITA 등 기존 연구에 제시된 표준화 기술과 신기술 중 국내·외 동향, 활용도, 발전가능성 등을 고려하여 선정하였다. 기본적인 범주 및 세부기술은 다음과 같다.

1) 신분확인(Identification) 기술 : 사용자 ID와 패스워드, 스마트카드, 생체인식, 토큰, RFID(Radio Frequency IDentification) 등

2) 인증(Authentication) 기술 : 생체인증, 전자서명, PKI, X.509 인증서 등

3) 접근제어(Access Control) 기술 : 보안 운영체계, 암호기술, 원격제어기술, 침입차단시스템, IPSec(IP Security), NAT(Network Address Translation), NetSwitch, Tamper-proofing 등

4) 운영관리(Administer) 기술 : 권한관리, 물리적 보호기술, 암호 API, 전자서명 등

5) 감사(Audit) 기술 : 감사도구, 모니터링/필터링, 바이러스 방어기술, 침입탐지기술, 해킹 방지기술 등

6) 암호화(Encryption) 기술 : 암호알고리즘 및 구현기술, 키 관리, PCC(Programmable Cryptography Chip) 등

7) 백업(Backup) 기술 : 실시간 백업, 장비 이중화

3. 국방주요정보통신기반시설의 정보보호 기술구조 제안

본 장에서는 국방주요정보통신기반시설의 보안요구사항과 소요 보안기술을 바탕으로 정보보호기술구조를 설계한다. 이때, 서론에서 밝힌 바와같이, 국방주요정보통신기반시설의 네트워크 분야로 대상 영역을 한정한다.

정보보호기술구조 설계 방향 도출을 위하여 우선, 국방주요정보통신기반시설의 보안대상 영역을 식별하고, 식별된 영역의 보안 취약점을 도출한 후, 그것의 극복을 위한 방안을 모색하여 정보보호기술구조 설계에 반영한다. 보안대상영역 식별 방법은 미 국방부의

IATF를 준용하였는데, 이를 간략히 소개하겠다.

가. 미 국방부의 IATF

미 국방부는 사이버 공격의 유형을 표 1과 같이 5가지로 분류하고, IATF(Information Assurance Technical Framework : 정보보증기술프레임워크) 및 종심방어전략을 통해 이를 방어해 낼 수 있다고 보았다[9].

[표 1] 사이버 공격의 유형

공격유형	기 술
내부자 공격 (Insider)	• 정보보호 처리 시스템의 물리적 경계 내에 있거나 직접적인 접근 권한을 갖고 있는 인가된 사람에 의해 수행되는 공격 [예] 데이터/보안매커니즘 변경, 비밀채널설정 등
수동적 공격 (Passive)	• 시스템 및 네트워크에서 유통되는 데이터와 이를 통해 추출 가능한 정보를 수동적으로 감시하는 공격 유형 [예] 정보의 모니터링, 스니핑, 암호문 분석 등
능동적 공격 (Active)	• 대표적 공격 유형으로, 보호수단 우회/파괴, 악성코드삽입, 정보의 탈취·삭제 등 정보/정보시스템의 기밀성, 가용성, 무결성에 직접적인 영향을 미치는 공격 유형 [예] 정보변조/위조, 사용자가장, 서비스거부공격
근접 공격 (Close-in)	• 비인가자가 정보를 변조, 수집하거나 정상적 접근을 방해하기 위해 네트워크, 시스템, 시설에 물리적으로 접근하여 수행하는 공격 [예] 데이터변경, 정보수집, 물리적 파괴 등
배포공격 (Distribution)	• 생산에서 설치의 과정이나 사이트 이동 중에 악의적 목적으로 H/W, S/W를 수정, 변경 [예] S/W, H/W악의적 수정, 백도어 설치 등

미 국방부는 1990년대 중반부터 정보통신 환경 변화와 미래 임무 환경 변화에 따른 새로운 위협에 대응하기 위해 정보보호의 개념을 "정보보증(IA : Information Assurance)"이라는 용어로 재정립하고, 관련 체제의 정비 및 활동을 추진 중이다. 이러한 목표 달성을 위해 미 국방부가 제시한 방안이 IATF 및 종심방어전략이다.

종심방어전략(Defense-in-depth Strategy)은 다중 계층, 다중 차원의 보호수단을 구축하는 접근 방법으로, 하나의 방어 장벽이 공격자에 의해 침투되거나 돌파되어도, 연속적인 다른 방어수단을 통해 이에 대응하는 개념이다. 종심방어전략의 구현 분야는 기술적인 측면으로만 제한하지 않고, 인력(People), 운영(Operation), 기술(Technology)을 주요분야로 설정하여 모든 분야의 균형적 발전을 강조하고 있다.

또한 종심방어전략은 복잡한 정보통신 기반구조 환경에서 기술적 보호수단을 효율적으로 구현하기 위하여 계층적 접근방법을 채택하고 있다. 계층적 접근방법은 정보보호 요구사항이 도출되고 처리되어야 할 대상영역을 설정하고, 높은 보증수준의 보호수단 구축을 집중하는 방법이다. 4가지 대상영역은 다음과 같다.

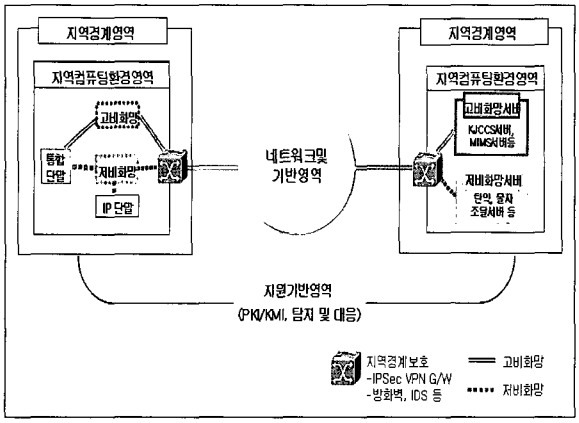
- 지역컴퓨팅환경영역(Local computing environment)
- 지역경계영역(Enclave boundary)
- 네트워크및기반영역(Network and Infrastructure)
- 지원기반영역(Supporting Infrastructure)

IATF는 미 국가 및 국방 사용자들이 종심방어전략의 기술적 구현을 위해 공통적으로 참조하여야할 정보 및 지침을 제공하고자 개발·관리되는 기술참조 문서로서, 미 NSA 주도하에 작성되었다.

나. 국방주요정보통신기반시설의 보안대상 영역

영역의 구분은 효율적인 정보보호 정책 및 기술을 적용하기 위해 중요한 요소이다. 본 논문에서는 우리 국방 환경과 IATF에서 상정한 영역 구분이 상당부분 일치하여 적용에 무리가 없으며[2], 차후 표준화 기술의 적용시 유리한 점이 있으므로, 이를 준용하고자 한다.

국방주요정보통신기반시설은 그림 1과 같이 물리적 영역을 기준으로 지역컴퓨팅환경영역, 지역경계영역,



[그림 1] 국방주요정보통신기반시설의 보안대상 영역

네트워크및기반영역, 지원기반영역의 4개영역으로 구분하며, 이에 추가하여 비밀등급에 따른 논리적 영역을 저비화망과 고비화망으로 구분하도록 한다. 이때 저비화망에서는 "군사보안업무시행규칙[10]"에 의해 대다수 평문으로 분류되는 정보를 취급하는 "자원관리정보체계"가 운용되며, 고비화망에서는 비밀로 분류되는 정보를 다루는 "전장관리정보체계"가 운용되는데, 국방주요정보통신기반시설은 전장관리정보체계에 포함되므로, 이의 전산망은 고비화망으로 분류할 수 있다.

1) 지역컴퓨팅환경영역

국방정보통신망의 소규모 LAN구간으로 서버, 클라이언트 시스템, 시스템에 설치된 어플리케이션을 포함하며 기존시스템, COTS, GOTS 등 임무 목적에 따라 다양한 시스템과 어플리케이션이 사용된다[3].

2) 지역경계영역

지역컴퓨팅환경영역에서 외부로 정보가 유출 또는 유입되는 지점이다. 지역컴퓨팅환경영역을 보호하기 위해 불법침입 및 불법유출을 방지하기 위한 방화벽, 네트워크기반 모니터링도구, 네트워크기반 스캐너, 네트워크기반 침입탐지도구, 바이러스방어도구 등을 중요도에 따라 조합하여 설치한다.

3) 네트워크및기반영역

네트워크 간 연결을 제공하며, WAN, LAN, MAN 등과 위성, M/W, 광전송 등 전송체계를 포함한다. 기타 네트워크관리 등도 수반된다. 이 영역은 통신기간사업자와의 회선계약, 군전용위성 및 M/W 등에 의해 구축된다. 이 영역은 테라비트 스위칭이 가능한 TSR이 백본망을 구성하며, M/W와 군전용위성을 이용하여 유선백본망과 일부 트래픽을 분산하는 구조를 가진다. 그 외에도 네트워크 관리를 위한 망관리센터 등이 포함된다.

4) 지원기반영역

공통적 정보보호 요소 지원을 위한 기술, 시스템, 구조 등으로 구성된다. PKI/KMI와 탐지 및 대응을 위한 기반구조로 구성될 수 있다.

다. 국방주요정보통신기반시설의 보안대상 영역별 취약점 및 종심방어전략

본 절에서는 4가지 보안대상영역별 취약점을 분석하여 종심방어전략을 제시하고자 한다. 본 절에서 도출된 정보보호기술은 "라"절의 "국방 정보보호기술구조" 설계에 반영될 것이다.

종심방어전략은 인력(People), 운영(Operation), 기술(Technology)을 주요 분야로 설정하고 있는데, 각 분야에서 다루는 주요 내용은 다음과 같다.

- 인력(People) : 정책/절차, 교육/훈련 및 인식제고, 물리적/시설 보안, 시스템 보안관리 등
- 운영(Operation) : 정보보호기술/체계의 인증 및 인가, 정보보증 준비태세 평가, 키관리 등
- 기술(Technology) : 정보보증 구조틀/기준, 평가된 제품 획득/통합, 시스템 위험평가 등

또한, 종심방어전략은 복잡한 정보통신 기반구조 환경에서 기술적 보호 수단을 효율적으로 구현하기 위한 방법으로 계층적 접근방법을 채택하고 있는데, 이는 "다단계 정보보호(Multi-Level Security) 체계 구축"이라는 중·장기 국방정보보호 전략과도 일맥상통한다[11].

계층적 접근방법은 정보보호 요구사항이 도출되고 처리되어야 할 대상 영역을 설정하고, 대상 영역에 높은 수준의 보호수단 구축을 집중하는 방법으로, 대상 영역은 앞서 분류한 지역컴퓨팅환경영역, 지역경계영역, 네트워크및기반영역, 지원기반영역이다.

1) 지역컴퓨팅환경영역

이 영역은 국방정보통신망 LAN 구성 영역으로, 표 2는 국방주요정보통신기반시설의 예상되는 취약점과 그 대응책을 판단한 것이다. 이때 대응책은 종심방어전략의 관점에서 인력, 운영, 기술의 세가지 분야로 구분하여 도출하였으며, 국방 환경에의 적용시엔 동시에 고려되어야 한다. 이 영역의 보안 중점은 시스템 및 시스템에 설치된 어플리케이션의 보호이다.

2) 지역경계영역

지역경계영역은 지역컴퓨팅환경의 내·외부로 정보가 유출 또는 유입되는 지점이며, 유통되는 데이터 흐름에 대한 통제와 감시가 주요 보안 중점으로, 이에 초점을 맞추어 취약점 및 대응방안을 강구하였다. 이 영역은 국방정보통신망이 제한된 접속점을 통해 상호 연결되고, 원격접속자 연결도 가능해야 하므로 취약성 극복을 위해 고려할 사항이 많다. 이 영역에서의 가장 큰 위협요소는 능동적공격이며, 근접공격과 배포공격은 지역컴퓨팅환경영역에서와 유사하다. 표 3은 예상되는 취약점과 그 대응책을 정리한 것이다.

3) 네트워크및기반영역

네트워크및기반영역은 테라비트 스위칭이 가능한 TSR이 백본망을 구성하며 초고속국가망의 백본에 연결되고, M/W와 상용위성 및 군 전용위성을 이용하여 유선백본망과 일부 트래픽을 분산하는 구조를 가진다. 2005년 현재는 ATM노드에서 암·복호화에 따른 보안취약성이 존재하고 있으나, ALL IP기반으로 통합되는 차세대 국방 환경에서는 IPSec VPN을 통하여 네트워크가 구성되어 암복호화에 따른 보안취약점과 유통과정에서의 정보 변조 및 파괴를 막을 수 있다. 그러나 IPSec만으로는 완전한 정보보호를 달성할 수 없으므로 공격유형에 따른 대응책을 수립하여야 한다[12].

국방주요정보통신기반시설의 차세대 네트워크는 IPSec VPN으로 구축되기 때문에 근접공격은 그 위험성이 적으며, 배포공격은 지역컴퓨팅환경영역에서의 배포공격의 유형과 대응책이 유사하다.

[표 2] 지역컴퓨팅환경영역 예상취약점/종심방어전략

공격유형	취약점/위협	종심방어전략	
		인력/운영분야	기술분야
내부자공격	• 정보유출/파괴 · 부적절한 접근통제 설정, 부적절한 단말 보호메커니즘	• 접근통제 정책수립 • 내부인원 신원조사 및 물리적 보안 조치 • 보안교육	• SecureOS 통한 강제적 접근통제 • 주요시스템 접근권한 분권화 • NetSwitch • 전자서명 • 군용암호/인증 알고리즘 • 바이러스 방어 시스템 구축
수동적공격	• 네트워크 모니터링 · 불법자료취득 · 암호알고리즘 분석 · 불법 모니터링 도구 탐지 및 접근통제 미흡	• 인가된 모니터링 도구에 대한 접근 통제 강화 • 비인가 소프트웨어 차단	• 주요데이터암호화 • 국방 PKI 구축을 통한 공개키 인증서 사용
능동적공격	• 관리자권한획득 · ID, P/W의 부적절한 관리 · 취약프로토콜 • 메일/SW의 악성코드 감염 • 무선LAN통한 불법접속	• 접근통제, 감사정책수립 • 무선 AP 관리절차 정립 • 생체인증을 통한 출입통제	• 사용자/SW 인증서 사용 • 호스트기반 침입탐지/취약성 분석, 악성코드/바이러스 탐지, 파일무결성검사기 • 무선단말 인증 강화 및 암호화 · 무선IPSecVPN
근접공격	• 전산시스템 물리적 접속 후 시스템 변조 및 정보 획득 • 노출된 LAN 케이블, 포트를 이용 불법접속	• 전산시스템 접근통제강화 • 전산실 출입통제 철저 • LAN 케이블, 포트에 대한 물리적 보안 대책 강구	• 물리적 Tamper-Proofing
배포공격	• 암호장비 및 소프트웨어제작 및 배포시 악성코드삽입	• 신뢰성 있는 제작업체 및 연구원 선정 • 장비/소프트웨어 설치후 보안성테스트 • 주요시스템 정비능력구비	• 물리적 Tamper-Proofing • 오류처리루틴, 오류확산방지 • 소프트웨어 전자서명

[표 3] 지역경계영역 예상취약점/종심방어전략

공격유형	취약점/위협	종심방어전략	
		인력/운영분야	기술분야
내부자공격	• 경계보호도구의 파괴 및 변조 · 부적절한 접근통제 설정 • 비인가자의 원격 접속 · 공개키인증서 부적절한 관리 및 사용	• 접근통제정책 수립 • 관리자의 자질 평가, 교육 • 원격접속용 공개키인증서에 대한 관리정책	• 중요 데이터의 분권화 관리 • 응용프로그램 수준의접근통제 • 네트워크 관리 정보 접근통제, 암호화 • 쌍방향인증, 암호기반인증 • 통합보안관제 시스템 연동 • 인증서 • 지역경계영역의 공개키인증서 접속
수동적공격	• 모니터링통한 불법 정보취득, 암호알고리즘 분석 · 부적절한 킷값 · ID, P/W의 부적절한관리	• 경계보호도구의 보호책 수립 • 저비화망에서 비문유통 금지	• IPSec 통한 암호화 • 적절한 킷값 사용
능동적공격	• 인가된 서버 및 사용자 위장 • 시스템 O/S, S/W 불법사용 • 경계보호도구 취약점 증가 • 불안전한 접근통제설정 • 암호화 및 인증 미비	• 접근통제정책 수립	• 암호화, 인증 강화 · IPSec VPN, 암호 API · NAT • 경계보호도구의 효율적 사용 · 모니터링, 방화벽 · 바이러스방어 · 취약성분석 · 능동형통합 보안도구 · 통합보안관제 시스템 연동
근접 공격	• 전산시스템 물리적 접속 후 시스템 변조 • 노출된 LAN 케이블, 포트를 이용한 불법 접속	• 전산시스템의 접근통제강화 • 전산실출입통제 • LAN 케이블 및 포트에 대한 물리적 보안 대책 강구	• 물리적 Tamper-Proofing
배포공격	• 암호장비, 소프트웨어 제작 및 배포시 악성 코드 삽입	• 신뢰성 있는 제작업체 선정 • 장비, 소프트웨어 설치 후 보안성 테스트 철저 • 주요시스템 정비능력 구비	• 물리적 Tamper-Proofing • 오류처리루틴, 오류확산방지 • 소프트웨어 전자서명

[표 4] 네트워크및기반영역 예상취약점/종심방어전략

공격유형	취약점/위협	종심방어전략	
		인력/운영분야	기술분야
내부자공격	• 망관리센터 관리자에 의한 정보침해 · 부적절한 접근통제 설정 · 보안대책 없이 원격접속으로 망관리장비 통제	• 접근통제정책 수립 • 관리자에 대한 자질평가와 교육	• SecureOS이용 강제적접근통제 • 주요시스템 접근권한분권화 • 네트워크통제 권한 분산 • 원격접속에 의한 망관리 시 암호화인증수행
수동적공격	• 모니터링을 통한 불법 정보 취득 · 위성 및 망관리 정보보호 대책 미비		• 위성/망관리 정보암호화/인증 • 프로토콜보안성 강화: SNMP, 무선MAC 등
능동적공격	• 네트워크 및 기반영역 기능저하 · 대역폭감소공격 및 통신교란공격 대응책 미비 · 통신기반 통제 마비 행위 대응책 미비	• 접근통제정책 수립 • 암호화, 인증 의무화	• 주파수호핑 및 이중화 구성 • 주요시스템 고정대역폭보장 • 장비간 암호화 및 인증 • 강력한 식별 및 인증에 의한 접근통제
근접공격	• 망관리센터에 대한 근접공격	• 망관리센터 접근통제강화 • 망관리센터에 대한 물리적 보안대책 강구	• 물리적Tamper-Proofing • 불법접속확인 · 침입탐지
배포공격	• 암호장비, 소프트웨어 제작 및 배포시 악성코드 삽입	• 신뢰성 있는 제작업체, 연구원 선정 • 장비 및 소프트웨어 설치 후 보안성 테스트 • 주요 시스템 정비능력 구비	• 물리적 Tamper-Proofing • 오류처리루틴, 오류확산방지 · ICMP • 소프트웨어 전자서명

표 4의 네트워크간 통신교란 공격은 정보흐름 통제 정보들을 변조 및 파괴하는 것을 의미한다. 네트워크 및기반영역에 존재하는 장비들간의 통신이 변조되면 정상적 서비스를 제공할 수 없기 때문에 장비들간의 정보에 대한 인증과 암호화가 이루어져야 한다. 통신기반 통제 마비 공격은 통신기반의 전반적 통제를 어렵게 만드는 것을 의미한다. 망관리센터에서는 네트워크및기반영역에 존재하는 장비들에 접속하여 통제기능을 수행할 수 있다. 망관리센터는 인력적·운영적 보안대책과 함께, 기술적 측면에서 계층적 접근방법에 의한 다단계 정보보호 기술로 구축되어야 한다.

4) 지원기반영역의 보안취약성 및 대응방안

지원기반영역은 PKI/KMI와 탐지 및 대응을 위한 기반구조로 구성된다. PKI/KMI와 탐지 및 대응시스템은 정보보호를 달성하기 위한 기반인 만큼 가장 안전하고 보안성 있게 구축되어야 한다. 취약점 및 대응방안은 표 5와 같이 분석·도출하였다. PKI/KMI 시스템에서의 수동적공격 및 근접공격은 상대적으로 그 위험성이 적으므로 논의에서 제외하였다.

[표 5] 지원기반영역 예상취약점/종심방어전략

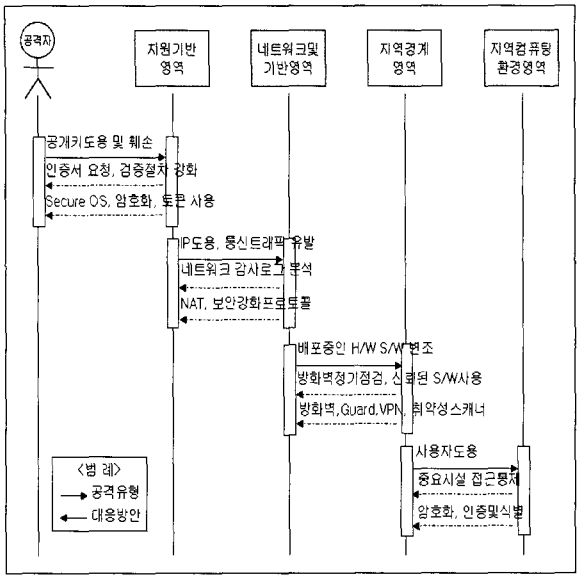
공격유형	취약점/위협	종심방어전략	
		인력/운영분야	기술분야
내부자공격	• 관리자 부주의에 의한 정보유출 • 부적절한 접근통제	• 시스템 운영 훈련 심화 • 시스템관리자 신원조사철저	• 사용자식별 및 인증대책 강화 • 주요시스템 접근권한 분권화 • 통신 내용 암호화 및 인증
능동적공격	• 시스템에 대한 물리적 접속후 시스템 변조 및 정보 획득	• 사이버테러에 대한 대응 계획 수립	• 주요 데이터 백업대책 강화 • 통합보안관제 체계 구축
배포공격	• PKI/KMI시스템 악성코드 삽입으로 시스템 결함 유도	• PKI/KMI 시스템 구축전 충분한 테스트 및 인증체계 마련	• 물리적 Tamper-Proofing

5) "정보탈취/파괴" 공격의 종심방어전략 적용 사례

본 절에서는 위에서 정리한 보안대상 영역별 취약점에 대한 방어전략을 응용하여, 실제 국방 환경에서 발생할 수 있는 구체적 공격유형인 "정보탈취 및 파괴" 공격에의 적용 사례를 예시하고자 한다. 이때 공격자의 의도는 국방 인트라넷 환경 내에 무단 침입하여 국방주요정보통신기반시설에 대한 접근권한을 획득하고, 목표 정보를 수집한 후 자신의 시스템으로 복사하고, 원본 정보를 파괴하고자 하는 상황으로 가정하였다. 이때 각 대상영역별 유추되는 위협과 대응방안은 표 6과 같다. 이 공격은 능동적공격과 근접공격, 배포공격이 혼합된 형태로, 공격유형별 구분은 생략하고 보안대상 영역별로 도표화하였다.

[표 6] "정보탈취/파괴"공격에 대한 종심방어전략

공격유형	취약점/위협	종심방어전략	
		인력/운영분야	기술분야
지원기반영역	• 공개키배포중훼손 • 키 부당접근권한 • 인가된 공개키 도용 • 기반 구조에 대한 악성코드삽입	• 올바른 시스템 설계, 구현 • 기반구조의 물리적접근 통제강화 • 인증서 요청, 검증절차 강화	• 통신과정의 암호화 • SecureOS사용 • 개인키 생성, 보호를 위한 토큰 사용
네트워크 및 기반영역	• 취약점 정보수집 및 IP 도용 • 통신 트래픽 유발로 대역폭 손실 • 무선환경에서 전파방해/차단	• 네트워크감사 로그 기록	• NAT 사용 • 보안성 강화 프로토콜 사용 • 무선주파수 출력통제 및 ECC
지역경계영역	• 프로토콜 취약점 이용한 공격 • 인가된 사용자/서버 도용 침투 • 배포중인 H/W, S/W 변조	• 방화벽의 정기적 점검 • 신뢰성 있는 S/W 사용	• 방화벽, Guard, VPN 채택 • 접근통제 • 취약성스캐너, IDS 사용
지역컴퓨팅환경영역	• 사용자 도용 • 정보 유출, 변조, 파괴 • 시스템 변경, 물리적 파괴	• 중요 시설의 접근통제강화	• 사용자 인증, 식별 강화 • 데이터 암호화 • 데이터별 접근권한 분권화



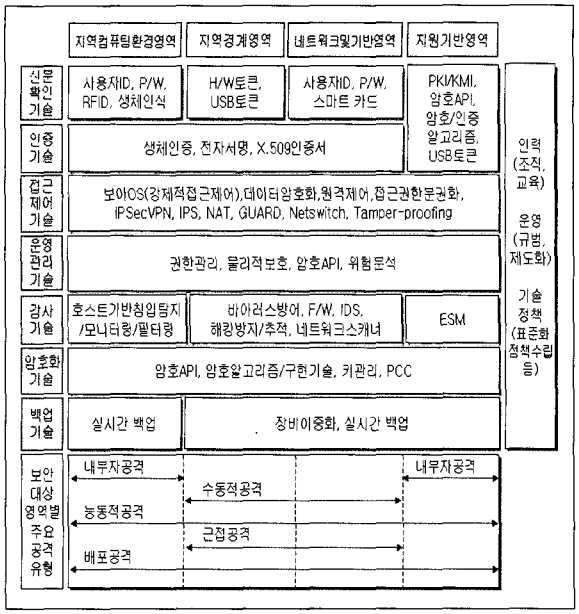
[그림 2] "정보탈취/파괴" 공격에 대한 종심방어전략 시퀀스 다이어그램

위 도표를 바탕으로 시퀀스 다이어그램을 작성하면 그림 2와 같다. 시퀀스 다이어그램은 소프트웨어공학적 개념으로서, 정보 및 행위의 순차 표현에 효율적인 도구이다. 이러한 시퀀스 다이어그램의 특성은 공간(보호대상 영역)의 흐름에 따라 포괄적 범주로부터 협의의 범주로 순차적 방어가 이루어지는, 종심방어전략의 개념을 표현하는 데에도 효율적일 것으로 판단된다.

그림 2는 정보 및 행위의 흐름이나 공격자를 기준으로, 국방주요정보통신기반시설의 4대 영역중 그 의미상 가장 외곽에 위치한 지원기반영역으로부터 지역컴퓨팅환경영역의 순으로, 공격과 대응의 순차적인 흐름을 도식하였다. 실제로 보다 손쉽게 공격과 대응의 흐름을 읽을 수 있다. 정보보호 정책수립 및 검증과정에서도 시퀀스 다이어그램을 활용하여 가독성을 높임으로써 업무효율을 향상시킬 수 있을 것으로 판단된다.

라. 국방주요정보통신기반시설의 정보보호기술 구조 제안

본장 "가~다"절의 내용을 기반으로 국방주요정보통신기반시설의 정보보호기술구조를 그림 3과 같이



[그림 3] 국방주요정보통신기반시설에 대한 정보보호 기술구조

제안한다. 이때 기준축은 앞에서 전개한 핵심 사항을 모두 포괄할 수 있도록, "다"에서 분석한 취약점과 그에 대한 종심방어전략을 기반으로, 4개 보호영역을 가로축으로, 보안기술범주를 세로축으로 하였으며, 도출된 세부보안기술들은 공통항목과 개별항목을 구분하여 해당 영역에 배치하였다. 또한, 영역별 특성을 분석하여 주요 공격유형을 표시하였다. 정보보호기술구조에 대한 연구는 신기술 및 위협요소의 변화, 경제성, 보안성 등을 고려하여 지속적 수정 및 보완이 필요하다.

4. 결 론

본 논문은 국방주요정보통신기반시설의 전용네트워크 분야에 대해, 보안대상 영역을 구분하고 각 영역별 취약점과 종심방어전략을 제안하였으며, 이를 바탕으로 국방주요정보통신기반시설에 대한 정보보호기술구조를 도식하였다. 이 과정에서 시퀀스 다이어그램을 활용하여 보안대상 영역별로 도출한 종심방어전략의 가독성을 높이는 방법을 적용하였다.

본 논문의 내용은 보안대상 영역별로 구체적인 정보보호 기술을 제시하여, 국방 정보보호 업무의 지침서로 활용될 수 있을 것이며, 차후 정보보호 정책수립 및 정보보호기술 연구개발시 방향 설정의 참고자료로 활용될 수 있을 것이다.

향후 연구과제로는 국방 환경 및 정보보호 위협의 변화와 정보보호 신기술의 발전에 따라, 정보보호기술구조의 지속적인 수정 및 보완이 필요하며 또한, 전체 정보기술아키텍처(ITA) 내에서 타 분야 기술과의 통합과 조정을 고려한 정보보호 기술의 자리매김이 이루어져야할 것이다. IATF의 정보보호 대상영역의 구분이나 종심방어전략의 개념은 국방 환경에 접목하기에 적합한 내용으로서, 국방정보화시스템 전반에의 확대 적용이 가능할 것으로 판단된다.

참 고 문 헌

[1] 국방부, 국방정보체계표준(DITA) 버전3.1, 2003. 1.
[2] 최인수 · 임재혁, 국방정보보호기술구조 연구, 한국국방연구원, 2004. 12.
[3] 한국전자통신연구원, 차세대 국방정보통신망 최적화 설계 연구, 국방부, 2004. 12.
[4] 정통부 정보화기획실, 정보통신기반보호법, 정보통신부, 2003.
[5] 국정원 · 정통부, 2005 국가정보보호백서, 2005. 6.
[6] 국방부, 국방정보통신기반보호규정(국방부 훈령 제752호), 2004. 7.
[7] 국방부 정보화기획실, 국방정보화 e-Defense Vision 2015, 국방부, 2003. 1.
[8] 남길현, 정보시스템보안론, 국방대학교, 2003.
[9] IATF, IATF Release 3.1, Department of Defense, September, 2002.
[10] 국방부, 군사보안업무시행규칙(국방부훈령 제757호), 2004. 9.
[11] 손태종외 3명, 국방정보화 정책 방향 연구, 한국국방연구원, 2004. 10.
[12] 정재민외 2명, 차세대 국방정보통신망에서의 접근 통제향상방안, WISC2004논문집, pp.386~407, 2004.