□ 研 究 論 文 □

韓國國防經營分析學會誌
제 28 권, 제 1 호, 2002. 6. 30.

WEB 환경에서 국방정보통신망 정보보호체계 구축에 관한 연구
(A Study on the Security System of the Web Based Defense Information Service Network)

신 유 찬, 남 길 현*

Abstract

The limits of current DN(Defense networks), private and closed network, become to reality; for Example, high expense of construction and maintenance of networks, restriction of new subscribers on DN. Therefore, a network using web environment that reflect fast development of IT and IS(Information Security) technology is demanded for MND.

Meeting the requirement of reliable IS system and extension and improvement of DN using common network, we can reduce the expense to extend, maintain, repair DN, form the environment that makes military business cooperate better with civil company and government agency, advance implementing Defense computing and networking service for field small size units that was a exception of Defense digitalization.

But it is essential to construct DN based on common network that there are security requisites; confidentiality, integrity, availability, efficiency, log, backup, restoration, that have to be realized at demanding level for IS.

This thesis suggested four measurements; replacement DN with common network to resolve the requirements of building new network and improvement of performance for private DN, linkage with common network for new requirement, distribution of traffic using common network, configuration of DN using Internet and proposed a refinement of IS management organization to treat security threat of common network flexibly, and LAN IS standard model of DN based on the web environment.

* 국방대학교 관리대학원

1. 서 론

현 국방전산망은 전용선 기반으로 구축되어 선로 유지/설비에 막대한 비용을 지출하고 있으며 폐쇄적 체계로 인하여 실시간 의사결정을 위한 문서결재 시스템 및 전자메일 교환 등의 능률적 사무처리가 국방전산망 개설구간으로 제한되어 국방업무의 효율적 수행에 어려움을 겪고 있다. 따라서 전용선 기반 국방정보체계에 일관된 투자보다는 비용대 효과측면에서 볼 때 상용망을 이용한 웹 기반의 국방전산망의 구축이 요구된다.

특히 웹 환경을 군 정보체계 전반에 도입하면 기존의 텍스트 기반 전산 운영환경에서 처리할 수 없었던 각종 정보제공 및 민원 서비스, 군사업무 활용과 같은 다양한 응용서비스 제공이 가능하다. 그러나 웹은 기본적으로 인터넷과 같은 개방성을 근간으로 하고 있기 때문에 인터넷의 보안취약점을 그대로 가지고 있으므로 우리 군은 웹을 통한 다양한 서비스를 제공함에 있어서 사전에 웹 서버의 접근통제와 웹 서버와 브라우저간 메시지 교환상의 보안성 확보, 네트워크 보호, 해커 바이러스 대책 수립이 요구된다.

본 연구는 웹 환경에서의 국방 정보체계 구축 및 운영을 위해 필요한 기본적인 인터넷 보안의 문제점을 분석하고 이를 바탕으로 실제 우리 군이 웹 환경 하에서 운영할 수 있는 적용업무를 도출하고 필요한 각종 위협요소 및 취약점을 파악하여 이에 대한 제도적, 기술적 대책을 제시함으로써 새로운 정보기술 환경에 적합한 저비용 고효율 국방 정보체계 건설에 이바지 하고자 한다.

2. 국방전산망의 현실태와 문제점

2.1 국방정보화 중장기 계획

국방정보화는 정보기술의 혁신적인 능력을 이용하여, 국방정보의 공유 및 적시적 유통·활용을 보장함으로써 국방구조 전반을 두뇌 집약적인 (Knowledge based) 정보시대 미래적응전력으로 전환시키는 제반 활동 및 행위이다. 이는 전쟁수행 및 국방운영, 관리기능을 전산화, 자동화, 네트워크화, 디지털화 하는 제반 활동화 행위를 총괄하는 통합적 의미를 지니고 있다.

이러한 국방정보화를 달성하기 위한 중·장기 계획은 [표 2-1]과 같이 2015년까지 정보전 수행능력을 갖춘 정예 정보화 군 육성을 기본 목표로 실시간 전장관리 및 정보 유통·공유를 통한 지휘통제와 통합된 전력을 발휘하고, 효율적인 자원관리로 작지만 강한 군을 운영하는데 있다[남길00].

[표 2-1] 국방정보화 중장기 계획

단 계	추진목표	추 진 중 점
1단계 ('99~'05)	기반 및 핵심체계 구축	· 정보화 환경여건 정비 · 정보통신기반(LAN, WAN) 구축 · 핵심 체계(C4I, CALS) 구축
2단계 ('06~'10)	기능확장 및 체계통합	· 국방초고속 정보통신망 구축 · 국방통합 C4I, CALS체계 구축
3단계 ('11~'15)	선진 정보체계 완성	· 국방초고속 정보통신망 완성 · 국방통합 C4I,CALS체계 완성 · 전자국방업무 수행체계 구축

2.2 국방전산망 현실태 및 운영현황

2.2.1 국방 네트워크의 운영현황

국방 전산망은 기존의 전용회선에 의한 일대일 통신망을 개선하여 군 전용의 단일통신망으로 통합하여 운용하고 있으며 ATM 및 패킷 교환망에 의한 교환통신을 통해 단일회선을 통한 복수의 상대와 통신이 가능하게 되었으며 통신체계도 TCP/IP에 의한 표준 통신체계를 채택함으로써 이기종간 상호통신을 가능하게 하였고, 신속한 정보 및 자료의 교환이 가능하게 되었다.

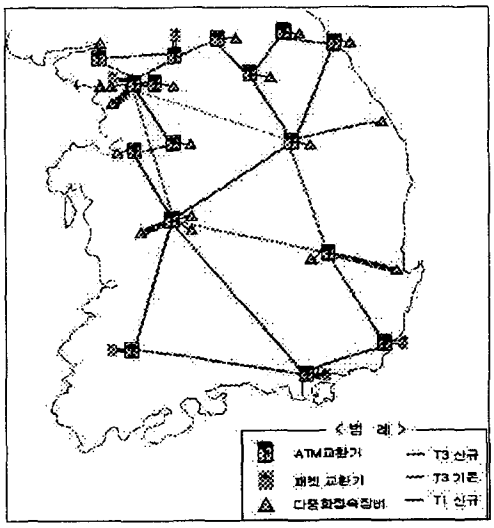
현재의 국방 전산망 활용분야는 크게 작전지휘통제 지원을 위한 전장관리 분야와 자원을 효율적으로 관리하기 위한 자원관리 분야로 구분할 수 있다[국방00a].

2.2.2 국방전산망 운영비 현황과 전망

정보통신 기술 발전에 따른 전술, 전략의 발전은 전장상황 실시간 모니터링, 지휘결심의 신속한 전달, 응용체계의 대용량화, 국방업무의 전산화 증가 등을 요구하였고 국방전산망의 데이터 전송부하가 급속하게 증가되어 고속의 국방전산망 구축이 요구되었다. 이에 따라 '99년 ATM 교환기 4기였던 것이 [그림 2-1]과 같이 '01년 현재 16개소에 설치되어 운영중이며, 간선에 대한 고속화 계획도 계속 추진될 예정이다.

국방전산망 가입부대는 국방전산망 고속화 계획에 따라 '94년 T1급 2개부대, 9.6Kbps 88개를 시작으로 '00년 9월 현재 T3급 4개부대, T1급 30개 부대, 64Kbps 165개. 9.6Kbps 141개 부대가 가입되어 있다.

또한 '94-'00년 사이에 국방전산망 구축비용은 [표 2-2]와 같으며 '00년도의 대폭 증가된 예산은 ATM 교환기 설치비용 때문이었다. 그러나 [표 2-3]과 같이 '06년 예산은 '01년의 약 2배 이상 소요되며 현재 증가추세를 감안시 2010년에는 수배의 예산소요가 전망된다[국전01].



[그림 2-1] 국방전산망 구성도

[표 2-2] '94～'00년 국방전산망 구축비용

구 분	'94년	'95년	'97년	'99년	'00년
비용 (백만원)	8,110	6,834	6,145	5,419	3,655

[표 2-3] '02～'06년 국방중기계획 (국방전산망 확장예산)

'01년 (백만원)	중 기 계 획(백만원)					합 계
	'02	'03	'04	'05	'06	
9,887	13,973	15,785	17,384	19,518	21,776	88,435

2.3 국방전산망 정보보호 현황

2.3.1 국방전산망 정보보호 체계 운영현황 및 취약성

가. 전용망 정보보호 현황

국방전산망의 대부분의 영역을 차지하는 전용망에 대한 정보보호 현황은 각 수행기관별, 사업추진 체계별 보안장비 선정 및 체계상이 등의 이유로 매우 다양하며 특히, 무결성과 가용성에 대한 대비책이 부족하다.

즉, 상용망과의 분리운영으로 인한 정보보호 부담감 감소로 보안정책/대책 수립 및 보안관리가 매우 취약하다. 특히 국방전산망과 같은 대규모 네트워크에서 내부의 악의의 사용자를 대비한 방화벽 설치, DB 암호화 등의 대비책 수립이 매우 빈약한 실정으로 서버, 네트워크 정보보호 측면뿐만 아니라 패스워드 수준에 머물러 있는 PC 보안장치도 생체정보나 스마트 카드를 이용한 사용자 통제 및 로그관리 등이 요구된다.

나. 상용망(인터넷) 정보보호 현황

국방업무는 아직까지는 인터넷에 크게 의존하고 있지 않으며 홈페이지 운영, 자료검색, 교육목적 등을 위해 별도의 분리된 상용망(인터넷)을 운영하고 이를 위한 정보보호 정책은 부대별/기관별로 일관성 없이 추진되어 온 것이다 현실태이다. 그러나, 사회의 정보화 추진 및 추세에 비추어 볼 때 업무추진에 있어서 인터넷을 통한 빈번한 대외접촉과 의존도가 높아질 것이 예상되므로 이에 대비한 적절한 보안대책 및 정책 수립이 반드시 요구된다.

특히, 보급률이 꾸준히 증가하고 있는 인터넷 전용PC의 경우 활성화되어 있는 이메일과 FTP, P2P를 이용한 자료유출에 대비하여 송수신자료에 대한 백업자료 작성 및 높은 수준의 통제책 마련이 필요하다.

다. 국방정보체계의 구성요소별 보안 취약점

(1) 시스템의 구성 및 관리문제

국방 전산시스템에 사용되는 대부분의 주장비가 UNIX의 운영체제를 사용함으로써 UNIX자체의 구성설정 오류로 인한 보안취약성 유발 및 시스템에 관한 로그수행 미흡으로 감사 추적 자료로 활용이 어렵다.

또한 시스템 관리절차 수립이 미흡하고, 시스템 관리요원의 보안의식이나 경험·지식 등이 부족하고 최신 버전의 운영체제 도입지연으로 구 운영체제 사용으로 인해 보안 취약점이 노출되고 추측 가능하거나, 노출된 패스워드를 지속적으로 사용하고 있어 악의의 비인가자의 시스템 접근 가능성이 상존하고 있다[기무98].

(2) 통신선로상의 취약성

국방정보통신망 구성은 물리적으로는 공중망의 선로를 사용하고 논리적으로 국방정보통신망을 구분하여 사용하고 있기 때문에 물리적 파괴와 회선 감청을 통한 정보 유출, 교란 등의 위험성이 존재한다[박만98].

또한, 불가능하게 여겨졌던 광케이블에 대한 도청방법이 연구되고 있으며 최근 케이블 굴절을 통해 도청이 가능한 것으로 알려져 매설선로에 대한 보호대책 수립에도 변화가 요구된다.

(3) 네트워크 소프트웨어 및 관리문제

파일전송 서비스(FTP,TFTP 등) 통제가 미비하여 패스워드를 통한 접근이 가능하고 네트워크를 통한 시스템 불법침입을 모니터링 할 수 있는 기능이 없어 해커나 비인가자의 불법 침입시 실시간으로 망 운영반이나 주 전산실 관리자가 불법침입 사실을 인지할 수 없으며 침입차단시스템과 침입탐지 시스템 설치는 아직 미흡하다[김유99].

그리고 네트워크 공유에 대한 통제가 미약하여 비인가자에 의한 자료 유출 가능성이 상존하며, IP 도용 등을 이용한 불법적인 시스템 접근 및 사용자 위장 등이 용이하다.

(4) 보관중인 자료와 전송자료의 무결성에 대한 취약성

현재 운영중인 대부분의 데이터 보관은 일반적인 유닉스 및 오라클의 보안정책에 의해 자료가 관리되고 있어 암호화가 이루어지지 않은 상태이다. 따라서 불법침입자의 공격으로 데이터베이스에 접속이 허락된다면 보관중인 자료에 대한 비밀성, 무결성에 영향을 미칠 수 있다. 또한 웹기반으로 운영되는 전자메일과 문서결재시스템은 송수신자의 인증과 메시지 무결성에 대한 대책이 미흡하여 부인봉쇄 기능과 책임성 한계를 명확하게 제공하기 어려운 실정이다.

2.4 미 국방망 운영현황 분석

2.4.1 미 국방망 현황

미 국방망 개선사업은 1983년 ARPANET인 국방통신망과 군사통신망을 DDN(Defense Data Network)으로 통합하면서 본격적으로 시작되었고 지금의 미국 국방망인 DISN은 1991년 사업을 시작하여 1996년부터 본격적으로 사용되었고 1997년 ATM 서비스를 시작하면서 NIPRNET, SIPRNET 서비스를 제공하였다. 특히, 미 국방망의 NIPRNET은 한국군에서는 아직까지 적용하지 않은 형태의 네트워크로써 차기 국방정보체계 구축사업에 반드시 참고해야한다.

가. NIPRNET (Non Secure Internet Protocol Network)

NIPRNET은 비문이 아닌 SBU 정보와 평문을 처리하기위해 국방성 정보체계망(DISN)내에서 운용되는 데이터 망으로 E-MAIL 서비스, NEWS, 파일전송, 전문체계 서비스가 제공되고 있다. 현재 NIPRNET은 [그림 2-2]와 같이 DISA의 인터넷 통신망으로 전용라우터를 설치하고 있으며, DISA의 광역 통신망인 DISN과도 연결되어 운영된다. 즉, NIPRNET은 DISN을 통해 인터넷 통신망고 접속하게 도며 개인 사용자는 NIPRNET을 경유하여 인터넷과 접속하여 서비스를 제공받게 된다.

나. SIPRNET(Secure Internet Protocol Network)

SIPRNET은 비밀로 분류된 정보를 국방성 정보체계망(DISN) 내에서 운용하는 데이터 통신망으로 전용 라우터를 이용하여 DISN과 연결 운용되며 상용망과는 분리되어 있고, KG, KIV 등의 보안장비를 이용한다.

다. NIPRNET/SIPRNET의 정보보호대책

방화벽은 B2급 이상 사양을 사용하며, 망 외부의 비정상적 접근과 해커 공격으로 방지하기 위해 라

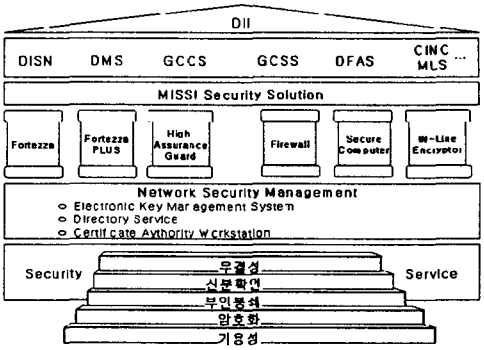
우터 전후에 방화벽을 설치하여 DMP을 구성한다. 여기서 사용자 시스템 및 데이터 전송 책임은 DIES지침에 따라 사용자가 책임을 지도록 되어 있다[연합01].

2.4.2 미 국방만 발전 방향과 보안대책(MIDIS)

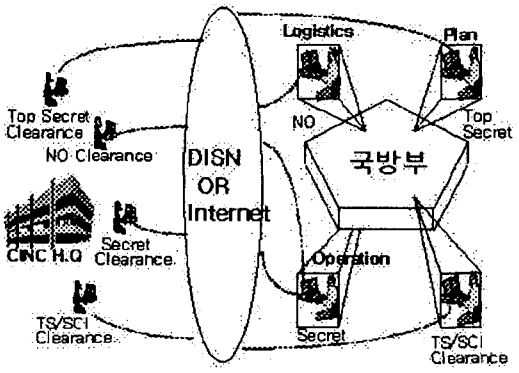
가. MIDIS (Multilineal Information System Security Initiative)

미 국방부는 각 기관이 업무 성격 및 보안등급을 이유로 각각의 전산망을 별도로 구축하여 운용하여 통신망 운용비를 고다 지출한다고 판단하여 미 국방부네의 정보 처리 시스템을 통합하여 하나의 전산망으로 구축하려는 프로젝트를 구상하게 되었다. 그러나 하나의 전산망으로 구축할 경우 통합된 전산망에서 서로 다른 등급의 정보가 처리된다는 취약점을 해결하기 위해 MIDIS라는 프로젝트 명칭 하에 NSA가 주축이 되어 다단계 정보보호 기반구조를 구축중이다.[강상99].

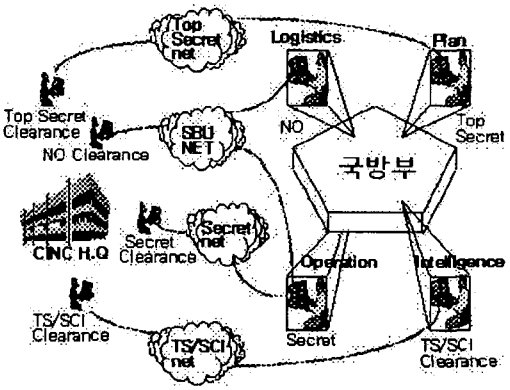
MISSIS는 [그림 2-2]에서 보는 바와 같이 보안서비스를 제공하기위해 상업 벤더들과 공동 연구를 통해 획득한 Fortezza, firewall, Secure OS. IN-LINE Encryptor 등을 이용하여 인증, 통합보안관리, 다단계보안과 같은 서비스를 제공하며 미 국방망에서 운용중인 DISN, GCCS, DMS에 대한 정보보호 역할을 수행한다. 이러한 MISSI의 보안서비스는 [그림 2-5,6]에서와 같이 단일 전산망을 통해 다중 등급의 정보 교환이 가능해진 미래의 네트워크와 다중 보안등급 정보 처리를 위해 다수의 망을 운용해야하는 현재의 네트워크를 비교할 수 있다.



[그림 2-1] MISSI 기술구조



[그림 2-3] 현재 미국의 네트워크



[그림 2-4] 향후 미국의 네트워크

2.5 현행 보안관련 법·규정 분석

2.5.1 국방전산망 내에서의 비밀 소통시 관계규정 분석

전시 상황 등 국가 위급 상황에서 전산망을 통한 비밀 소통은 가장 신속한 정보전달을 가능하게 함으로써 장차전 상황에서 가장 필수적인 사항이 될 것이다. 그러나 현규정에 의하면 전용선을 통한 비밀 소통도 수비지 않은 실정이다. 즉, 전산망을 이용한 비밀소통 제반 절차가 하드웨어 기반으로 까다롭고, 정보보호 S/W 및 H/W에 관한 업무주관도 모호한 실정이다.

2.5.2 국방전산망과 대외 전산망 연동에 관한 규정 분석

군사보안업무시행규칙 및 국가 정보통신보안기본지침에 의하면 현재의 국방전산망은 대외 전산망과의 연동이 불가능하다고 규정되었다. 그러나, 현재의 국방전산망은 간선구간에 있어서 한국통신으로부터 전송대역을 할당받아 논리적으로 분리된 전용선으로 쓰고 있는 것에 불과하므로 진정한 의미의 전용망이라고 하기엔 어렵다. 따라서, 군사보안업무시행규칙 제 41조 외부망 연동 및 제42조 상용망 연동규정을 적절한 보안대책 수립을 전제로 완화시켜 대외 전산망을 이용한 자료전송 및 전산망의 연동을 가능토록 함으로써 군 전산망의 생존성 및 경제적이 장점을 살릴 필요가 있다. 이를 위해서는 대외전산망과 관련한 정보보호체계에 대한 주관부서 지정과 정보보호체계 기술 표준 마련, 정보보호 전반에 걸친 주요 업무에 대한 주관부서 지정이 선행되어야 한다. [국방00b][국정00]

3. 웹 환경에서 관리적·기술적 정보보호 대책

3.1 컴퓨터 시스템 보안

3.1.1 보안 운영체제(Secure OS)

보안운영체제(Secure Operating System)란 컴퓨터 운영체제에 내재된 보안상의 결함으로 인하여 발생 가능한 각종 해킹으로부터 시스템을 보호하기 위하여 보안 커널(Security Kernel)을 추가한 운영체제로서 컴퓨터 사용자에 대한 식별 및 인증, 강제적 접근통제, 임의적 접근통제, 재사용방지, 침입탐지 등의 보안기능을 갖고 있다.

보안 OS를 구현하는 방법은 Add-On 방식과 커널 구현 방식으로 분류 할 수 있다. Add-On 방식은 기존 운영체제의 커널을 수정없이 그대로 이용하므로 구현은 쉬우나 추가된 보안 기능을 우회하는 침입, 내부자의 조작, 시스템 성능의 저하 등에는 취약하고, 커널구현 방식은 컴퓨터 시스템에서의 여러 가지 보안 취약성을 원천적으로 차단하여 외부 침입자로부터의 노출이나 수정을 근본적으로 차단 할 수 있으며 보안기능의 부가적 처리로 인한 성능 저하 현상을 최소화 할 수는 있으나 Add-On 방식에 비해 구현이 어렵고 새로운 버전에 융통성이 부족하다.

그러나, 국방전산 시스템과 같이 높은 보안성을 요구하는 시스템에서는 커널 수준에서 보안기능을 구현하는 방법이 요구된다.[홍기98].

군사적으로 보안 OS를 이용하기위해서는 보안 OS의 일반적인 기능이외에도 DB를 이용한 실시간 감사·추적, 커널 모드의 암호화, 비밀표시 강제 출

력 등이 추가로 요구된다.

3.1.2 인증대책

가 . 사용자 인증대책

사용자 신분에 대한 인증(Authentication)은 다음의 세 가지 방법을 독립적으로 또는 조합하여 사용할 수 있다[CA98].

첫째, 사용자가 알고 있는 것을 기반으로 한 식별 및 인증방법으로써 비밀 패스워드, 개인식별번호(PIN), 도는 암호키 등의 비밀 정보 등을 이용한다.

둘째, 사용자가 소유하고 있는 것을 기반으로 하는 식별 및 인증 방법으로써 ATM 카드, 스마트카드 등의 보안 토큰을 이용한다.

셋째, 사용자의 생체학적 특성을 기반으로 하는 사용자 식별 및 인증 방법으로써 생체의 특성을 이용한 인증기술은 그 사람의 신분을 인증하기 위해서 개인의 독특한 특성 즉, 지문, 홍채 등을 사용한다.

나. 공개키 기반구조(PKI : Public Key Infrastructure)

공개키 기반구조(PKI)는 전자결재·전자메일등 전자거래의 안전성·신뢰성을 보장하기 위해 암호기술이나 전자서명 시스템을 이용하여 당사자의 신분확인, 전자업무 내용의 정보보호 및 무결성, 전자행위에 대한 부인 봉쇄 기능 등을 신뢰할 만한 제3자(인증기관)가 확인 및 증명 할 수 있도록 하는 기반 시스템을 말하며 사용자 인증 이외에도 다음과 같은 서비스를 제공한다.

(1) 전자결재 시스템

전자결재 사용자들이 늘어나게 되면 아무리 훌륭한 방화벽이나 시스템 보안 툴을 사용한다 할지라도 사용자가 추후에 송 · 수신 사실을 부인하거나 내·외부의 적이나 불순분자들에게 중요한 정보가 도청되거나 위 · 변조될 가능성도 커지게 된다. 따라서, 이러한 위협으로부터 정보보호를 위해 공개키 기반구조는 데이터 기밀성, 무결성, 부인봉쇄, 사용자 인증, 접근통제와 같은 인증서비스를 제공한다.

(2) E-mail 송수신

국방전산망을 통한 E-mail의 사용은 국방인트라넷의 구축 및 확장과 함께 계속 증가하고 있다. E-mail은 국방부나 각 군의 E-mail ID를 가진 사용자간에 정보교환을 가능하게 한다. 그러나, 이러한 과정에서 snipper등 각종 해킹 프로그램을 이용한 불순분자나 적에 의하여 불법 도청 및 위·변조의 가능성은 상존하며, 상용망과 국방망을 연동시킬 경우 이러한 문제점은 더욱 커질 수밖에 없다. 따라서 이러한 위험에 대비하기 위해 공개키 기반구조는 기밀성, 무결성, 부인봉쇄와 같은 인증서비스를 제공한다[안혜99].

3.1.3 컴퓨터 바이러스 및 악성소프트웨어 대책

최근 인터넷 확산과 더불어 통신망을 통한 컴퓨터 바이러스 및 악성소프트웨어의 전염과 피해정도가 급속도로 증가하는 추세이며 폐쇄망을 운영하는 국방전산망에서도 이로인한 피해가 속출하고 있다. 이것은 사용자가 명확한 인식 없이 사용한 것도 분명한 이유가 되겠으나, 적절한 대처를 하지 못한 시스템 및 네트워크 관리상 허점도 커다란 문제인 것이다.

가. 컴퓨터 바이러스와 악성 소프트웨어

컴퓨터 바이러스나 악성 소프트웨어는 대부분이 다른 시스템이나 소프트웨어를 감염시키기 위해 자신을 복제 할 수 있는 코드를 가지고 있으며, 주로 어셈블러와 C 언어로 작성되어 있고 새로운 바이러스나 악성소프트웨어가 나오게 되면 그것을 모방한 변형 바이러스가 나오게 된다. 이러한 컴퓨터 바이러스 및 악성 소프트웨어 종류로는 부트 · 파일 · 트로이목마 · 웜 · 논리폭탄이 있다.

컴퓨터 바이러스와 악성소프트웨어의 감염 경로 중 주로 이용되는 것은 E-mail, 불법 소프트웨어가 많이 이용되며 과거의 독립 · 단독 PC 개념과는 달리 웹 환경에서는 파일서버를 이용하여 바이러스를 감염시킴으로써 LAN에 연결된 모든 PC에 동시 다발적으로 감염 시키고, 그 전파 속도도 매우 빠르다. 또한 수많은 바이러스가 매일매일 탄생하고, 변조됨에 따라 그에 대한 탐색, 치료도 점점 어려워지고 있는 실정이다.

나. 예방대책

컴퓨터 바이러스와 악성소프트웨어로부터 정보체계를 보호하기 위해서는 컴퓨터 관리적 대책과 기술적 대책이 동시에 수립되어야 한다.

관리적 대책은 효율적 컴퓨터 관리를 위해 장비의 도입단계에서 운영단계까지 수시/정기 바이러스 검사를 수행하고, 바이러스에 대한 적절한 대응을 위해 시스템의 하드웨어 및 소프트웨어에 대한 상세 정보를 남겨두어 만일의 사태에 대비하고, 인가되지 않은 접근을 통한 컴퓨터 바이러스 감염 확산을 막기 위해 시스템 접근 사용자나 관리자의 수를 최소화 하여야 한다.

그리고, 네트워크 관리 측면에서 감염 확산 범위를 확인하기 위해 네트워크에 연결되어 사용한 사용자 목록을 관리하고 컴퓨터 바이러스 감염 손상에 적절히 대응하기위해 긴급 사태 경보시스템을 설치하여 사용하여야 한다.

기술적 대책으로는 사용자와 관리자 양 측면에서 강구되어야 한다. 사용자 측면에서는 최신버전의 백신을 주기적으로 다운 받아 사용하고, 중요자료 및 프로그램에 대해서 반드시 백업을 받아야 한다. 관리자 측면에서는 사용자들에 대한 최신 버전의 백신 프로그램 배포와 위험 바이러스에 대한 경고도 지속적으로 병행하여 사용자가 쉽게 바이러스 검색, 치료가 가능토록 해야 한다. 그러나 기존의 백신 프로그램의 경우 종류가 너무 많고 종류별로 설치, 유지 보수하게에 비용과 시간이 너무 많이 소요되고, 업데이트 시기를 놓치는 경우가 많이 발생하므로 백신 프로그램이 탑재된 바이러스 월(Virus Wall)과 같은 전용서버를 설치하여 네트워크를 보호하는 것도 바람직하다.

3.2 네트워크 보안

3.2.1 웹 보안 프로토콜

HTTP는 특정 정보에 대한 접근 프로토콜(Access Protocol)과 메시지교환을 위한 구문(Syntax) 제공이라는 두가지 특성을 가지고있다. 즉, SMTP(Simple Mail Transfer Protocol), Telnet, RPC(Remote Procedure Call)등과 같이 정보에 대한 접근 프로토콜이라는 측면에서는 세션에 대한 채널보호가 요구되며. MIME(Multi-purpose Internet Mail Extensions)이나 WAIS/Z39.50과 같은 구문(Syntax) 측면에서는 메시지 중심의 보안이

필요하다.

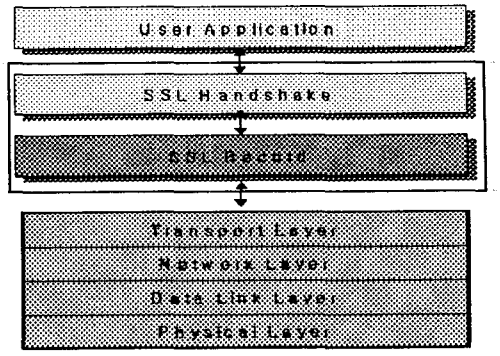
가. 내용기반 보안 (Content-Based Security)

HTTP상에서 외부 응용인 PGP 도는 PEM(Privacy Enhanced Mail)에 의해 암호화된 문서 형태로 안전하게 데이터를 전송하는 방법으로, 이 기술은 보통 MIME 표시기로 구현된다. 또한 전자우편에서 암호화 및 전자서명에 많이 쓰이고 있는 PGP와 모자익 웹의 CCI(Common Client Interface) 기능을 이용한 방법, PEM과 넷스케이프 클라이언트 API 또는 플러그-인(Plug-In) 기술을 이용한 방법이 있다.

나. 채널기반 보안(Channel-Based Security) : SSL

SSL(Secure Sockets Layer)은 Application 계층과 TCP/IP 계층 사이에 존재하는 프로토콜로서 웹을 위한 HTTP 뿐만 아니라 Telnet, FTP(File Transfer Protocol) 등 다른 프로토콜에도 적용될 수 있다. SSL의 구조는 <그림 3-1>에서 보는 바와 같이 SSL 동작에 대한 관리를 위해 사용되는 SSL Handshake와 실질적인 보안 서비스를 제공하는 SSL Record Protocol 두 부분(계층)으로 나누어져 있다.

클라이언트와 서버가 SSL을 이용해 연결을 할 경우 먼저 SSL Handshake Protocol을 수행하여 한 세션동안 보안 서비스 제공에 사용되는 세션키, 암호 알고리즘, 인증서와 같은 암호 매개변수를 서로 공유하고 여기에서 생성된 세션정보를 SSL Record Protocol에서 이용한다.



[그림 3-1] SSL 프로토콜의 구성

다. 메시지기반 보안 (Message-Based Security)

채널기반 방식은 HTTP, NNTP(Network News Transfer Protocol) 등과 같은 응용 프로토콜의 하위에서 독립적으로 동작하는 것에 반해, 메시지 기반 방식은 동등 응용 프로토콜로서 다른 응용 프로토콜에 의해 생성되는 메시지를 암호화한다. 하지만 이 두가지 방식은 서로 배타적인 구조를 가지고 있지 않으므로 서로 보완하여 새로운 웹 보안 메커니즘을 개발할 수 있다.

3.2.2 침입차단 및 탐지시스템

가. 침입차단시스템(Firewall)

침입차단시스템의 사용목적은 외부 네트워크로부터 내부 네트워크를 보호하는 것으로써 허가되지 않은 외부 네트워크를 통한 내부 네트워크에 접근을 방지하고 허가된 사용자들이 방해를 받지 않고 네트워크 자원에 접근할 수 있도록 하는 것이다.[임차97].

[표 3-1] 침입차단시스템의 장·단점

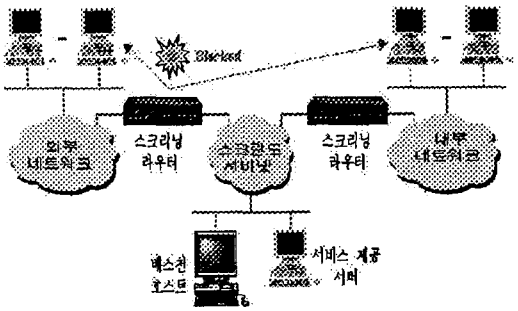
장 점	단 점
· 취약한 서비스에 대한 보호 가능 · 호스트 시스템에 대한 접근 제어 가능 · 로그와 통계자료 유지 · 내부 네트워크 상의 모든 자원들에 일관된 보안정책 적용 가능	· 제한된 서비스 제공 · 침입차단시스템을 통과하지 않는 트래픽은 제어 불가 · 내부자들에 대한 시스템 보호 곤란

침입차단시스템의 분류는 구현방식에 따라 패킷 필터링과 프락시를 이용한 응용게이트웨이 방식이 있으며 구축형태에 따라 듀얼-홈드 게이트웨이, 스크린드 호스트 게이트웨이, 스크린드 서브넷 게이트웨이로 분류할 수 있다.

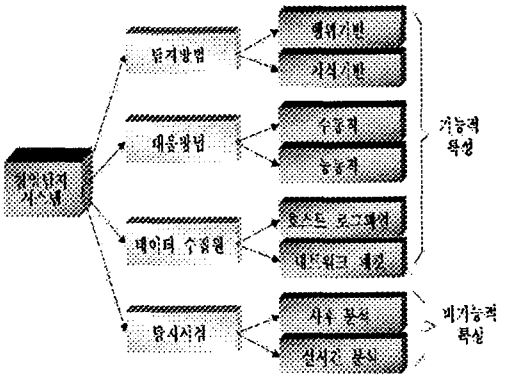
특히, 이 세가지 구축형태 중 미 국방망에서 운용중인 스크린드 서브넷은 보안성이 가장 높은 구성방식으로 우리 군에 가장 적합한 방식이다. 흔히 De-Militarized Zone(DMZ)이라고 불리는 서브넷 게이트웨이는 [그림 3-2]와 같이 내부 네트워크와 외부 네트워크 사이에 설치되며 서브넷에 진입하는 지점은 보통 배스천호스트이고, 스크리닝 필터는 외부 네트워크와 서브넷 사이, 서브넷과 내부 네트워크 사이에 위치한다. 이 방식에서 DMZ는 내부 네트워크를 보호하기 위한 쿠션 역할을 한다.

나. 침입탐지시스템(Intrusion Detection System)

침입탐지시스템은 내부 사용자 및 외부 침입자가 컴퓨터시스템 또는 네트워크 자원을 정당한 권한없이 불법적인 사용을 하기위한 시도나 주어진 권한 밖의 자원을 사용하기 위한 시도를 사전에 탐지하여 그 피해를 예방하는 시스템으로 가장 보편적으로 쓰이는 IBM Zurich Research Lab의 분류는 [그림 3-3]과 같다.[조규00]



[그림 3-2] 스크린드 서브넷 게이트웨이

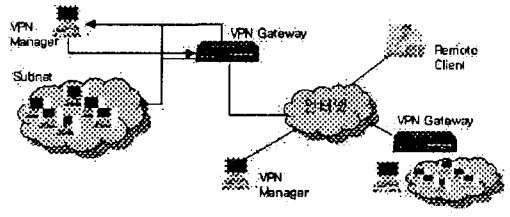


[그림 3-3] 침입탐지시스템 분류

침입탐지 시스템은 크게 데이터 수집, 데이터 가공 및 축약, 침입분석 및 탐지, 보고 및 대응의 4단계 구성 단계를 갖고 있으며 장·단점은 [표3-2]와 같다.

3.2.3 가상사설망
(VPN : Virtual Private Network)

가상사설망(VPN)이란 [그림3-4]와 같이 인터넷



[그림 3-4] VPN 개념도

과 같은 공중망을 이용하면서 사설망(전용망)을 이용하는 것과 같은 효과를 내는 네트워크를 말한다.

[표 3-2] 침입탐지시스템의 장·단점

장 점	단 점
· 해킹에 대하여 침입차단 시스템 보다 적극적인 방어 가능 · 내부 사용자의 오·남용 탐지 및 방어 가능 · 해킹사고 발생시 어느 정도의 추적 가능	· 대규모 네트워크 상에서는 사용곤란 · 잘못된 침입탐지(False Positive)의 가능성 존재 · 관리 및 운영의 어려움 존재 · 새로운 침입기법에 대한 즉각적인 대응 곤란 · 보안사고에 대한 근본적인 해결대책이 되지 못함

즉 인터넷과 같은 공중망 사용자간에 터널링(tunneling) 기술을 이용하여 터널을 형성함으로써 사용자들에게 공중망을 이용하면서도 사설망을 이용하는 것과 같은 효과를 만들어 낼 수 있는 네트워크이다.

VPN은 보안을 목적으로 하지 않지만 인터넷 응용분야에 직접 적용하기 위해서 보안서비스는 기본적인 요구사항이다. 특히, 전자상거래나 전자경매, 사이버 주식거래 등의 민감한 정보들을 교환해야 하는 기업분야와 부대간의 정보교류, 정보공유 및 재택근무자나 이동 근무자들의 안전한 원격 사설망 접속을 요구하는 국방전산망 분야에 있어서 강력한 보안성 제공은 필수적인 요구사항이 된다. 따라서 강력한 보안성을 제공하고 사용자가 원하는 서비스 품질을 제공하기 위해서 요구되는 VPN 요소기술은 키관리 기술, 터널링 기술, VPN 관리기술 등이 있다.

3.3 응용체계 보안

인터넷을 통해 제공되는 기존의 메일시스템은 보안에 대한 고려가 없으며 송/수신의 안전성이 보장되지 않는다.

따라서 개인이나 기업의 정보가 이메일을 통해서 교환될 경우 타인의 공격에 의해 쉽게 내용이 노출되거나 위/변조될 수도 있다.

그러나 미군의 NIPRNET에서 운용중인 이메일의 경우 비밀성, 무결성, 부인봉쇄 등의 기능을 추가시켜 간단한 업무연락부터 중요도가 있는 지시/명령, 업무협조까지도 이메일을 통해 업무가 이루어지고 있으며 그에 대한 법적 효력도 보장된 상태이다. 따라서 우리 군에서도 보안메일의 조기도입을 통해 국방업무의 간편화, 효율화를 추구해야할 필요가 있다.

현재까지 개발된 보안메일의 구현방식은 대칭키 방식, PKI 방식, PGP 방식 등이 있으며 우리 군에서는 국방인증체계 구축이후에야 보안메일 서비스가 가능할 것으로 예상된다.

4. 웹 환경에서의 정보보호체계 구축방안

4.1 웹 환경에서 국방 정보보호체계 보안 요구사항

국방전산망 정보보호체계의 기본적인 목표는 내부 또는 외부의 침입자에 의해 행해지는 각종 정보의 파괴, 변조 및 유출 등과 같은 침해사고로부터 중요한 정보를 보호하는 것으로서 특히, 웹 환경에서 정보보호체계 구축시 해결되어야 할 과제는 크게 비밀성, 무결성, 가용성의 세가지로 구분할 수 있다. 특히 웹 환경에서는 외부 네트워크를 통한 악의의 접속자에 대한 정보보호 측면이 가장 중요하다. 웹 환경에서 국방 정보보호체계의 보안 요구사항은 [표 4-1]과 같다.

[표 4-1] 웹 환경에서 보안 요구사항

전산시스템	네트워크	응용체계
비밀성 보장 무결성 보장 가용성 보장 효율성 제고 기록 유지 백업 및 복구	비밀성 보장 무결성 보장 데이터 발신처 확인 통신사실 부인방지 사용자 확인 및 인증 인가된 접근만 허용 가용성 향상	위조 불가 사용자 인증 재사용 불가 변경 불가 부인 불가

4.2 상용망 기반 국방전산망 구성방안

4.2.1 웹 환경에서 국방전산망 구축방안

본 논문에서는 상용망을 이용한 국방전산망 구성방안 3개안과 현재의 폐쇄망 기반의 국방망은 그대로 두고 인터넷을 이용하여 별도의 망을 구성하는 1개안을 국방전산망 네트워크 구축방안으로 제안하겠다.

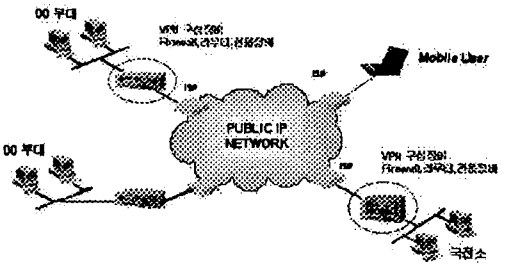
국방전산망 구축방안의 주요 고려사항으로는 국방전산망에 소요되는 엄청난 망 운용비 절감과 상용망 이용에 따른 정보보호에 초점을 맞추었다.

가. 제 1안 : 국방전산망(전용선) 전구간 상용망 대체 방안

(1) VPN(Virtual Private Network) 기반 국방전산망

공개키 기반 솔루션의 지원이 불가능한 경우 VPN을 이용하여 각 부대 LAN을 연결하고 각 LAN에 대한 기술적 정보보호대책을 강구한다.

[그림 4-1]은 기존의 국방전산망을 VPN으로 대체한 구성도로서 ISP에서 제공하는 상용망을 이용하여 각 LAN간의 가상사설망이 구성된다.



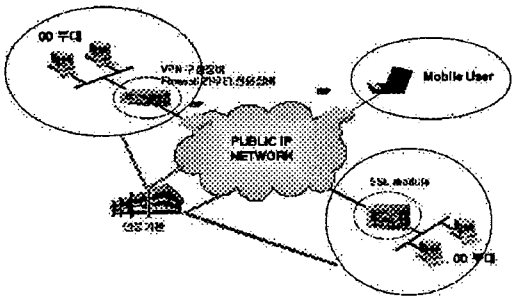
[그림 4-1] VPN 기반 국방전산망

VPN을 기반으로 별도의 국방전산망을 구축시 기존의 망 운영/유지비가 절감되고, 개방성, 확장성이 높아 차세대 정보체계 구축의 기반이 될 수 있으며 망내 가입자의 인터넷 사용이 가능하게 되어 기존의 인터넷 상용망과 전용망을 분리운영 할 때보다 비용절감의 효과가 있다.

또한, ISP가 망 운용, 증설, UP-Grade를 담당하여 망 신설 및 증설, Performance 개선을 위한 국방비 비용 지출이 불필요하다. 그러나 해킹의 위험이 높고, ISP에 종속되어 국방전산망의 생존성이 ISP에 의존하게 된다. 그리고 VPN을 구축하기 위해 별도의 VPN 전용 시스템을 설치해야 하므로 그에 따른 추가 비용 지출이 요구되며 현재까지 대규모 네트워크를 위한 VPN 기술이 완전히 활성화되어 있지 않아 보안성이 완전히 입증되지 않았다는 문제점을 안고 있다.

(2) PKI 기반 국방전산망

PKI를 기반으로한 보안 솔루션을 사용했을시 [그림 4-2]에서와 같이PKI 기반 VPN 전용장비를 쓰거나 SSL과 같은 보안프로토콜을 이용하여 상용망을 이용한 국방전산망 구축이 가능하다. 여기서 PKI기반 VPN은 단지 PKI 기반의 인증, 암호화를 이용한다는 것이 일반 VPN과의 차이점이며, SSL은 VPN이 LAN 단위로 터널링하여 Session하는 반면 각 클라이언트가 개별적으로 국방 웹서버에 접속하여 Session하므로 불필요한 Session 유지가 필요 없다는 특성을 갖고 있다.

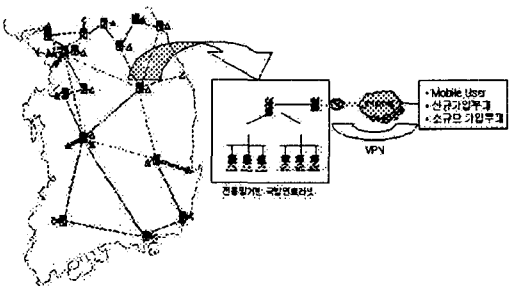


[그림 4-2] PKI 기반 국방전산망

PKI 기반 국방전산망 구축시 공인 인증기관 구축은 선행조건으로서 국방부 자체의 공인 인증기관을 구축하거나 기 구축된 인증기관을 이용할 수 있다.

나. 제 2 안 : 국방전산망(전용선)의 일부구간 상용망 대체 방안

부분적 사용망 대체방안은 기존의 전용망 기반 국방전산망을 백본으로 그대로 두고, 신규가입부대 및 소규모 부대, 이동사용자에 대해 상용망을 통해 접속토록 하는 것이다. 이 방식의 구성은 [그림 4-3]과 같다.



[그림 4-3] 전용선 기반 국방전산망

이 방식은 국방전산망 미설치 부대가 상용망을 통해 국방전산망에 접속이 가능토록 하고 이때 주소변환 서비스(NAT) 등을 사용하여 내/외부망 접속이 가능토록 한다.

이 방식의 장점은 전 국방전산망을 상용망으로 대체한 방안에 비해 상용 접속점에 대한 집중적인 보안대책을 수립하여 외부망에 대한 집중적인 보안관리가 가능하고, 기존의 망 구성체제에 비해 큰 차이가 없어서 대대적인 망 구축공사, 네트워크 환경변화에 따른 사용자 혼란, 서비스 일시 중단 등의 피해는 없다. 그러나 기존의 전용선 운영/유지

비를 그대로 지불해야 하며, 새로운 국방정보체계 적용 위해 전용선 성능 향상 등이 지속적으로 이루어져야 하는 단점이 있다.

다. 제 3 안 : 전용망·상용망 트래픽 분산처리 방안

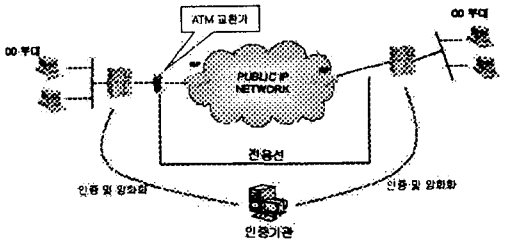
제3안은 국방전산망에서 유통되는 데이터에 대한 트래픽을 분산 처리하는데 있다. 트래픽 분산은 단순히 선로의 전송상태를 판단하여 전용망과 상용망 중 가장 좋은 전송속도를 낼 수 있는 망을 선택하여 데이터를 전송하는 방법과 전송자료에 대한 중요도를 판단, 망을 선택하여 데이터 전송 및 접속할 수 있도록 하는 두 가지 방법으로 구현이 가능하다.

이 트래픽 분산처리 방안은 전송선로를 두 개 갖고 폭주하는 데이터 소통의 분할이 가능하고 가입자가 인터넷을 활용할 수 있다는 장점을 가지고 있으며 전산망 성능 향상을 위해 소요되는 예산에 대한 절감효과를 가질 수 있다.

(1) 제 3-1 안 : ATM 교환기 수준에서의 트래픽 분산

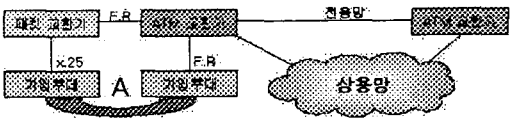
이 방안은 [그림4-4]에서와 같이 ATM 교환기 구간에서 상용망을 이용하여 간선을 구성하는 방안이다. 이때, ATM 교환기간에 전송되는 데이터에 대한 정보보호는 SSL과 같은 PKI 솔루션이나 VPN을 이용할 수 있으며, 사용자 인증은 ATM 교환기 도달 전에 완료되어 교환기 라우터가 전송망을 선택하게 된다.

현재 ATM 간선 구간은 T3급으로 현재 한국통신 등 ISP에서 시험 제공하는 기가 이더넷 등에 비해 처리속도가 늦으므로 상용망을 이용하면 간선의



[그림 4-4] ATM 교환기간 데이터 전송 분할 방식

성능향상 비용지출 없이 ISP 주관의 망 개선이 이루어져 경제적 효과와 우수한 망 성능을 기반으로 한 멀티미디어 국방전산서비스가 가능하다. 그러나 [그림 4-5]에서와 같이 가입부대간(A구간)에는 상용망을 이용한 데이터 전송은 이루어지지 않는다는 단점을 가지고 있다.

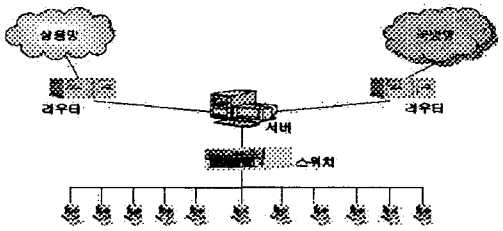


[그림 4-5] ATM 교환기 수준의 트래픽 분산

(2) 제 3-2 안 : 가입부대 수준의 트래픽 분산

ATM 교환기 수준의 트래픽 분산과는 달리 지선 구간에서의 상용망을 이용한 데이터 전송을 위해 가입부대 LAN에 사용망을 연결하여 트래픽을 분산하는 방식이다. 가입부대 수준의 트래픽 분산 방식은 [그림 4-6]과 같이 라우팅 기능을 가진 서버에서 트래픽을 제어하여 전송속도 또는 보안등급에 따라 망을 선택하여 전송하게 된다.

이 방식의 경우 현재의 국방전산망 확장계획에 따라 전용망을 확장한다고 하여도 대대급까지 가설되어 있는 인터넷망을 이용하여 트래픽을 분산 처리할 수 있으며, 국방전산망을 통한 트래픽 감소



[그림 4-6] 가입부대 수준의 트래픽 분산

효과가 예상된다.

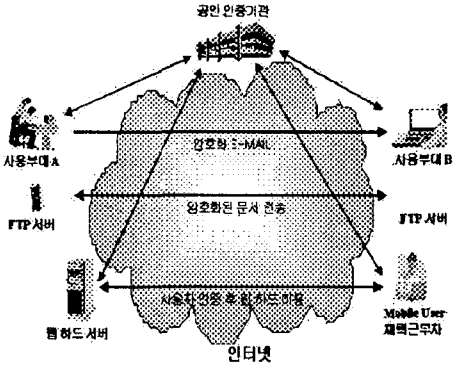
특히, 자료 소통량이 가장 많은 지선 구간의 데이터 소통에 대해 트래픽을 분산시킴으로써 제3-1안에 비해 비용절감 및 성능향상의 효과가 크다.

라. 제 4 안 : 인터넷을 이용한 새로운 국방망 구성

앞에서 기술한 방안과는 달리 기존의 국방전산망은 그대로 두고 군사상 민감하거나 비밀자료가 아닌 평문자료의 전송 및 정보교환을 위한 전산서비스를 식별하여 인터넷에 구현하는 방식으로 가장 단시간 내에 구현이 가능한 방안이다. 특히 이 방안은 [그림 4-7]에서와 같이 국방전산망이 가설되지 않은 소규모 부대까지 국방전산서비스 제공이 가능하고 현재 대대급까지 설치된 인터넷망을 이용하여 서비스를 제공하므로 별도의 망 가설비 및 운영비가 들지 않는다는 장점이 있다.

그러나 국방전산망이 폐쇄망과 개방망을 모두 이용함에 따라 관리범위가 커져 더 많은 비용지출이 요구되며, 별도의 정보보호 대책이 요구되는 단점이 있다.

지금까지 제안한 4가지 방안 중 가장 단시간에 구축 가능한 것은 제4안 인터넷을 이용하여 새로운 국방전산망을 구축하는 것이다. 그러나 진정한 의미의 웹 환경을 국방전산망에 도입하여 비용절감 및 성능향상을 도모하고자 한다면 제3-2안 가입부대 수준의 트래픽 분산 방안을 채택하여 추진함이 바람직할 것으로 예상된다



[그림 4-7] 인터넷 국방전산망 개념

4.2.2 단계별 구축 절차

가. 시범체계 선정

아무리 이론적으로 완벽한 정보보호 대책일지라도 반드시 예측하기 어려운 약점이 있을 수 있으며, 그로 인해 전체 시스템에 영향을 입어 국방업무 자체가 중단된다면 그 피해는 돈의 가치로 헤아릴 수 없다. 따라서 상용망을 이용한 웹 환경에서의 국방전산망을 구축하기 위해서는 먼저 시범체계를 선정하여 성능을 평가하는 것이 반드시 필요하다. 즉, 적당한 국방서비스를 선택하여 일정기간 시험을 거쳐 안전성을 확인한 후 국방전산서비스 전반에 확대해야 한다.

시범체계 선정은 국방정보체계 서비스 중 가장 활용빈도가 높고, 비밀자료 소통이 거의 없는 정보체계가 타당하다. 따라서 전자메일, 전자결재, 게시

판(BBS), 문서DB 등 각각 다른 성격의 보안대책이 필요하고 비밀자료 유통의 거의 없는 사무자동화체계를 시범체계로 지정하여 시험평가를 하는 것이 타당하다. 이 외에 시범체계는 대용량 파일전송, 멀티미디어 서비스 등을 추가하여 미래의 국방전산망 구축에 필요한 서비스와 다방면의 정보보호대책을 도출해야 한다.

나. 서비스 분리

현재 국방전산망도 대역폭은 나누어져 있으나 비밀자료가 소통되고 있는 지휘소 자동화망과 SBU(Sensitive But Unclassified) 자료가 소통되는 국방자원관리체계 등은 상용망과 연동하기 전에 충분한 시험기간을 거쳐야 하므로 일정기간동안은 상용망과 연동되는 '가칭' 국방행정망과 망을 구분하여 운용하여야 한다.

다. 서비스 분리이후 구축절차

첫 번째, 단계는 일정기간 시험평가 기간을 가진 후 약점을 보완하고 통합보안관제센터, CERT 팀 등 관련 조직을 정비하여 인력양성 및 관련 규정을 완비한다.

두 번째 단계는 적용 운영 단계로 네트워크 개선계획을 수립, 중장기계획에 반영하여 적용부대를 확장하고, 국방전술망에 대해서도 보안강도를 높여 상용망 이용방안을 모색한다.

세 번째 단계는 국방정보체계 전 범위에서 상용망을 이용하여 성능개선이 완료된 국방전산서비스를 제공한다.

4.3 웹 환경에서 국방정보보호체계 구축

웹 환경에서 국방정보보호체계 구축을 위해서는 기술적 대책 수립과 병행하여 개방환경에 걸맞도록 관련제도/규정 정비, 정보보호 조직 보완 등이 이루어져야 한다.

4.3.1 제도/규정/조직 정비

가. 제도/규정 보완

현재 군사보안업무시행규칙과 국가 정보통신보안기본지침에 따르면 대외전산망과 연결된 전산기는 군에 설치된 타 전산기 및 전산망과 연결할 수 없다고 규정하고 있다. 이는 앞에서 설명한 바와 같이 매우 폐쇄적인 사고로서 국방부 장관이 승인하는 적절한 보안조치가 취해졌다면 상용망과의 연동이 가능하다고 개정되어야 한다.

그리고 국방전산망에서 유통되는 자료들의 보안등급, 중요도에 따라 암호화 프로그램 및 장비 사용에 대해 다양화 시켜야 한다. 예를 들어 평문의 경우 상용 암호화 프로그램으로 암호화하고, 민감한 자료에 대해서는 군 전용 암호화 프로그램으로 암호화하며, 비밀자료는 군 전용 암호화 프로그램과 등급별 보안장비를 개발하여 이용하는 등의 차별이 있어야 한다. 이는 불필요한 암호화 S/W, H/W의 사용을 억제하여 효율성 향상에 이득을 줄 수도 있다.

나. 정보보호 관리조직 보완

웹 환경에서 국방전산망을 운영하고 그에 따른 정보보호체계를 구축하여 운영하기 위해서는 공인인증기관과 일관성 있는 정보보호 정책 수립·집행이 가능하고 지속적인 정보기술 환경에 유연하게 적응할 수 있는 관리조직이 반드시 필요하다. 특히,

개방환경인 인터넷 기반 국방전산망은 수많은 해커, 유해집단의 표적이 될 가능성이 높으므로 강력한 정보보호 대책 수립과 추진이 가능한 전문관리 조직 구성이 필수적으로 요구된다.

(1) 정보보호 관리조직의 재정비 필요성 인식

현재 국방정보체계에 대한 정보보호 업무는 국방부 정보화기획관실 주관 하에 여러 군 기관에 나누어져 각자 업무를 수행하고 있으나, 조직구성이 체계적이지 못하고, 개방환경을 도입하여 다양한 해커공격에 유연하게 대처하기에는 너무나 작은 조직이다. 즉, 과거 폐쇄망 기반의 정보보호 조직 형태를 그대로 가지고 있어 급속한 정보기술 변화 속에서 다양한 해커공격에 대해 능동적인 대처와 신기술 도입, 연구개발에 어려움이 있을 것으로 예상된다. 따라서 웹 환경에서의 국방정보보호체계 구축을 위해서는 과거의 폐쇄망에서의 위협 대처 수준을 벗어나 체계적이고 발전 지향적인 조직으로 재정비해야 할 필요가 있다.

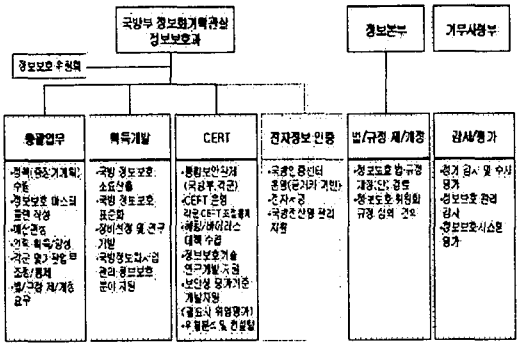
(2) 정보보호 업무 분류

국방 정보체계 정보보호 관련 조직으로는 현재 국방부 정보화기획관실, 정보본부, 기무사령부가 있으나 이들 기관에 대한 업무분담은 모호한 실정이다. 따라서 정보보호 업무의 전반적인 업무분담 및 조직 정비가 필요하다. 본 논문에서 제안하는 정보보호 관리조직과 그에 대한 업무분류는 [그림 4-8]과 같다.

4.3.2 상용망 연동 시 정보보호 대책

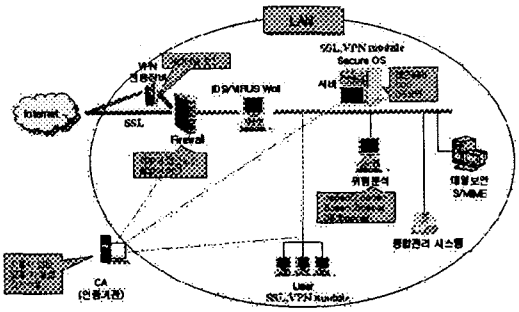
가. 국방전산망 LAN 정보보호 모델

웹 환경에서의 국방전산망에 대한 기술적 대책으로 본 논문에서는 국방전산망 LAN 정보보호체계 표준모델을 제시하겠다.



[그림 4-8] 국방 정보보호 조직

국방전산망 LAN 정보보호 표준모델은 [그림 4-9]와 같다.



[그림 4-9] 국방전산망 LAN 정보보호 표준모델

외부와 송·수신되는 패킷은 VPN 전용장비에 의해 목표가 되는 호스트에까지 터널링하거나 국방전산망의 인증서비스를 제공받아 서버와 각 클라이언트에 탑재된 SSL 모듈을 이용하여 패킷을 공개키 기반 암호화하여 전송한다. 이 때 전송되는 패킷은 외부의 적이나 불순분자가 가로채기를 하여도 복호화 시킬 수 없어 전송패킷에 대해서는 정보보

호를 보장할 수 있다.

또한, 내부망 정보보호체계 전반에 대해서도 인증기관의 서비스를 제공함으로써 강력한 보안능력을 갖도록 해야 한다. 즉, 외부해커의 침입에 대응하기 위해서 Firewall은 반드시 인증기관을 통해 사용자 인증 후 LAN 접속을 허가함으로써 IP 도용 등을 통해 내부망에 접속하려는 해커에 대한 접속을 방지한다. 그리고 Firewall 구축방식을 스크린드 서브넷 게이트웨이 방식으로 구축하여 DMZ를 가짐으로써 좀 더 우수한 성능을 발휘할 수 있도록 해야 한다.

서버는 탑재된 Secure OS가 인증기관의 인증정보를 이용하여 DB와 시스템관리의 접근통제 및 사용권한 부여가 가능하도록 구축되어야 하며 저장된 정보 암호화를 통해 해커가 정보를 탈취하더라도 이용이 불가능하도록 사전조치를 해야한다.

LAN 내의 사용자는 S/MIME과 같이 인증기관으로부터 비밀성 및 무결성 등을 보장받아 군 업무에 적극 활용할 수 있는 메일 프로토콜을 이용하여 이메일을 공식적인 업무처리 방안으로 이용해야 하며 가급적 상업적인 벤더의 이메일 서비스 이용을 억제하여 송·수신한 메일의 로그와 내용이 저장되어 법적 근거로써 사용이 가능해야 한다.

침입탐지시스템은 비정상적인 시스템 접근 및 침입을 탐지하여 침입으로 판정되면 즉시 관리자에게 통보하여 신속한 대응이 이루어 질 수 있도록 실시간 탐지와 능동적인 대처가 가능하도록 하고 컴퓨터 바이러스 및 악성소프트웨어의 망내 잠입을 방지하기 위해 바이러스 월을 이용하거나 시스템 사용자에 대한 지속적인 교육도 필요하다. 그러나 군내 시스템 사용자 대부분이 컴퓨터 바이러스 및 악성소프트웨어 대응능력이 낮은 점을 감안할 때 네트워크 관리자가 일괄적으로 방역작업이 가능한 바이러스 월 설치가 필요할 것으로 예상된다.

끝으로 이렇게 다양한 정보보호 대책에 대한 상호 운용성을 보장과 지속적인 진화를 위해서는 지속적인 위험분석을 통해 보안시스템의 위협에 대처하고, 통합보안관리시스템을 도입하여 각각의 보안시스템의 상호연동을 보장해야 한다.

나. 통합보안관리시스템

통합보안관리시스템은 이기종의 다양한 보안시스템을 통하여 침입행위를 실시간으로 탐지하고 신속한 대응을 수행하며, 침입관련 정보를 수집·분석하여 적절한 구성정보를 유지하여 주는 시스템이다. [장종00]

우리 군의 통합보안관리 시스템에 대한 필요성은 분명하나 현재까지 출시된 상용제품조차도 표준화, 보안제품간의 상호연동 등에 대해 정해진 바가 없으므로 연구개발 및 도입에 신중을 기해야 한다. 그러나 우리 군에 도입되는 통합보안시스템의 다음과 같은 특성은 기본적으로 가지고 있어야 한다.

- o 중앙집중형 원격방역 서비스 제공으로 관리자 업무 최소화
- o 24시간 원격 감시 서비스
- o 최신 해킹기술에 대한 방지책 갱신
- o 백신 프로그램 설치현황·자동버전관리 및 백신 자동실행 및 복구 기능
- o 보안시스템 상태 자동보고
- o 신종 바이러스 발견시 확산방지 및 백신 제품/프로그램 자동 배포
- o 다양한 경보 서비스와 신속한 원격 방역 서비스

○ 시스템 백업 및 복구 기능

5. 결 론

본 논문에서는 전용망 기반의 국방전산망의 문제점에 대해 분석하고, 망 운영비 절감과 개방환경의 국방전산망 도입을 위해 상용망을 이용한 국방정보체계 구축방안과 이와 관련된 정보보호 대책을 기술하였다.

우리 군이 저비용 고효율의 국방정보체계 건설을 위해서는 먼저 전용망에 연연하는 보수적 사고에서 탈피하여 좀더 개방적인 컴퓨터 네트워크 환경을 도입해야 한다. 또한 이로 인해 절감된 비용과 연구결과를 군 정보화 기술 연구 및 미래전의 핵심인 정보전에 투자하고 국가 정보화에도 기여함으로써 선진 정예군으로 거듭나기 위한 노력을 한층 더 해야 한다.

따라서, 본 논문에서 기술한 바와 같이 웹 환경에서의 국방정보체계 건설은 국방비 절감과 최신의 멀티서비스를 전용망의 성능에 의해 제한 받지않고 제공함으로써 군 전투력 향상에 도움을 줄 것이다.

그러나 웹 환경에서의 국방정보체계 건설을 위해서는 현재 폐쇄망을 기반으로 발전되어 온 정보보호 관리조직과 법령 등이 재정비 되어 최신기술에 유연하게 대처하고, 수용하여 국방정보보체계를 보호할 수 있도록 해야 하며 정보보호 표준 모델 등을 개발함으로써 일관성 있는 보안 정책 수립 및 집행이 이루어 질 수 있도록 해야 한다.

참고문헌

[국전01] 국방전산소, 국방정보화 기획문서, 국방전산소, 2001.

[기무98] 국군기무사령부, '98 정기 중앙보안감사 결과 통보, 국군기무사령부, 1998.

[김유99] 김유재, 정보전에 대비한 군 정보통신망 정보보호대책 연구, 국방대학원 석사논문, 1999.

[연합01] 한미연합사, NIPRNET & SIPRNET 개념, 한미연합사, 2001.

[강상99] 강상구 외 2인, "효율적 국방망 구축을 위한 MISSI 분석," 한국정보보호학회지 제9권 제2호, 1999.

[남길00] 남길현, "국방전산망의 정보보호체계 구축방안," 국방대학교 안보연구시리즈 제1집 3호, 2000.

[국방00a] 국방부 정보화기획관실, 국방정보화 기획문서, 국방부, 2000.

[국방00b] 국방부, 군사보안업무 시행규칙, 국방부,2000.

[국정00] 국가정보원, 국가정보통신보안 기본지침, 국가정보원, 2000.

[홍기98] 홍기융, "운영체제 보안기술 동향," 한국정보보호학회지 제8권 제2호, 1998.

[한국98] 한국전산원, CALS/EC 인증기술 개발, 한국정보보호센터, 1998.

[안혜99] 안혜연, "전자상거래 사업과 인증거래 이용방안," 제4회 정보보호 심포지움, 1999.

[박명01] 박명국, 국방전산망에 적합한 인증서 기반 해킹 역추적 시스템 제안, 국방대학교 석사논문, 2001.

[임차97] 임차식 외 5인, 정보보호 실무기술서, 한국정보보호센터, 1997.

[조규00] 조규민 외, "침입탐지시스템 보안기능 요

구사항 분석," 국가보안기술연구소 제12회 정보보호와 암호에 대한 학술대회 논문집, 2000.

[장종00] 장종수, "사이버 순찰 및 침입방어를 위한 네트워크 보안제어 기술," 한국정보보호학회 제7회 정보통신망 정보보호 워크숍, 2000.

[시큐00] (주)시큐어소프트, 바이러스 월(Virus Wall) 제안서, (주)시큐어소프트, 2000.