유비쿼터스 환경에서의 국방 정보보호 발전 방안

김영화, 김정태
목원대학교
A Development Plan of Military Information Security in Ubiquitous Environment
Young-Hwa Kim, Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

정보화의 급속한 진전으로 유·무선의 통합, 광대역 통신기술 구현 및 디지털 컨버전스 등 첨단 정보통신기술이 생활에 적용되고 있으며, 유비쿼터스 사회로의 진입을 위한 환경 구축이 정부 및 자치단체, 연구소, 관련 기업 등 여러 기관 및 단체의 주관으로 순차적으로 진행되고 있다. 국방 부분에서도 첨단 정보통신기술에 대한 의존도는 점점 심화되고 있으나, 이와 더불어 해킹·바이러스 기술의 고도화를 통한 사이버테러 및 범죄 등의 침해 행위가 고도화, 전문화되고 점차 치밀한 형태로 발전하여 국가적인 차원의 대응이 필요한 형태로 급진전되고 있다. 특히 국방 에서는 이러한 위협으로부터의 정보보호가 더욱 중요하며, 이에 따라 본 논문에서는 안전하고 효율적인 유비쿼터스 국방환경을 구축하기 위한 정보보호 발전 방안에 대하여 살펴보고자 한다.

Ⅰ. 서 론

정보기술의 발전에 따른 사회 전반에 걸친 정보화 추진과 정보체계 활용도 증가는 시/공간적 제약이 없는 정보의 자유로운 공유 및 유통을 보장하는 등 많은 긍정적인 발전을 가능하게 했으나, 해킹·컴퓨터 바이러스 등의 새로운 유형의 위협이 등장하는 기반을 제공하기도 하였다. 군도 국방정보화의 추진에 따라 다양한 정보통신 기술이 활용됨으로써, 새로운 위협 및 취약성이 증가하고 있다.

과거의 전쟁은 지/해/공 이라는 3차원 공간상에서 대량살상 및 파괴로 적의 저항을 무력화시키기 위한 것이며, 이는 대부분 전쟁에 사용된 무기체계에 의존하였다. 그러나 앞으로의 미래전에서는 공간적으로는 우주를 포함하며, 차원이 다른 개념의 사이버 공간이 포함되어 5차원이라는 개념으로 이제까지와는 전혀 다른 형태의 전쟁이 치러질 것이며, 단일 무기체계에 의한 의존도는 점차 감소하고, 각종 정보수집 및 분석체계를 이용하여 적의 상황 및 전장상황을 한눈에 보고, 시·공간적으로 통합된 네트워크를 통하여 전 제대가 상황을 동시에 인지, 정밀타격/비 살상무기체계를 통하여 적의 핵심만을 무력화시켜 인명살상을 최소화시키는 방향으로 전개될 것이다.

이러한 변화는 비단 전장이라는 특수한 환경과 공간에서 뿐만 아니라 평시 인력, 군수 등 자원관리 분야와, 모병 및 병사 면회 등의 일상 군생활에도 적용되어 일반사회의 정보화 환경과 크게 다르지 않으며, 오히려 군 이라는 특수성을 이용하여 일반 사회에서는 비용 투입의 제한으로 하기 어려운 신기술 적용 등의 시험 적용이 활발히 이루어 질 수 있다.

국방부 차원의 국방정보화 추진은 크게 전장관리 정보화, 자원관리 정보화, 정보화 환경 조성의 3가지로 분류되며, 이를 위하여 지휘통제체계와 전장관리의 자동화로 군사력의 질적 변환을 도모하고, 국방자원 관리의 디지털화와 전자거래를 기반으로 저비용·고효율의 국방관리와 운영을 실천하며, 이를 위해 정보화 기반을 확충 및 국가정책과 연계된 국방정보화 정책 추진하과 정보화 교육을 주요 내용으로 하고 있다[1].

본 논문에서는 IT 환경변화에 따른 국방 환경의 변화와 유비쿼터스 환경에서의 국방 정보보호 기술 적용 및 발전에 관하여 살펴보고자 한다.

Ⅱ. 유비쿼터스 환경 변화 및 위협 양상

1. 유비쿼터스 사회로의 변화

현재 우리사회는 광대역 네트워크 인프라(BcN)를 기반으로 사람, 컴퓨터, 사물이 연결되는 유비쿼터스 환경으로 급격히 전환 중이다.

표 1. IT 환경 변화 특성[2]

구 분	전산화	정보화	유비쿼터스
시기	1980년대~1990년대 중반	1990년대 중반~2000년대 중반	2000년대 중반 이후
Keyword	자동화	온라인화	컨버전스(융합)
주요 구성	H/W, S/W	H/W, S/W, N/W	H/W, S/W, N/W, Sensing
서비스 특징	개별서비스	Seamless 서비스	자율서비스
정보의 유용성	정보축적	정보공유/확산	사물의 지능화
주 거래 방식	오프라인	온라인, 오프라인 병행	온라인-오프라인 연계

향후 5년간 네트워크에 연결되는 광의의 단말(Network Appliance)은 현재보다 100배, 10년 후에는 수만 배 규모로 증가하면서 총체적인 네트워크 연결시대(Network of All)로 변화할 것임. 사람과 사람(P to P) 간의 의사소통에 통신도구를 활용하던 것을, 사람과 기계(P to M), 사물과 사물(T to T)간에도 연결되어 통신이 이루어지는 유비쿼터스 환경으로 변화될 것임.

2. 최근 사이버위협의 특징

1) 다기능 악성코드 출현 및 전파속도 고도화

최근의 악성코드는 바이러스+자기복제+트로이목마+발신지제거 기능이 포함된 형태로 나타나며 기존 웜과 바이러스간의 경계가 파괴됨. 주로 TCP를 이용한 단일 프로토콜 이용 전파방식에서 다양한 전파방식(TCP, UDP, P2P, e-mail 등)을 사용하며, 취약점을 공격하여 유포하는 전파방식이 자동화됨.[3]

2) 탐지를 회피하기 위한 웜·바이러스 출현

탐지를 피하기 위해 잠복기를 갖거나 고의로 느리게 전파하는 웜도 출현하였으며, 정상 프로토콜이나 사용자 행위를 모사하여 탐지를 회피하는 기술을 보유하는 등 날로 지능화됨.

3) 공격도구의 지능화

개별적인 침입시도에서 자동화된 공격으로 전환되어 공격의 신속하여 졌으며, 침입차단 시스템의 기능을 무력화 하고 IDS를 우회하여 게시판을 공격 하는 등 날로 다양화, 지능화됨.

4) 시스템의 취약점을 이용한 공격 증가

매년 2배 이상씩 증가되는 취약점을 이용하며, 0-day attackd이 증가됨.

표 2. 최근 침해사고 동향의 변화[2]

구 분	과 거	최근(2004-2005)
유형	웜, 바이러스, 서버 크래킹	홈페이지 변조, 악성 Bot, 피싱, 악성코드(트로잔)
목적	흥미, 과시	경제적, 정치적 목적, 과시
공격기법	주요시스템 취약점, 웜/바이러스 전파, 이메일 웜 등	응용프로그램/시스템 취약점(SQL Injection, PHP Injection 등)
특징	네트워크 서비스 이용(RPC 등)	주로 웹서비스 이용 (홈페이지 이용, 악성코드 유포, 피싱 등)
대상	모든 인터넷 사용자	특정 대상 (일단 불특정 다수에게 → 이후 가치있는 대상 선별)

5) 기간망에 대한 공격 증가

과거 컴퓨터에 대한 공격에서 네트워크에 대한 공격으로 대상이 변경되고 있으며, 서비스 거부 공격, 웜 공격, DNS 공격, 라우터 공격이 주를 이룸.

6) 해킹의 범죄화

과거의 지적 호기심 충족과 도전정신의 실현을 위한 해킹에서 근래에는 중요 정보 절도, 개인정보 절도를 통한 금전전 이익 추구, 적국 또는 공격 대상에 대한 스파이 행위 및 테러에 악용되는 등 날로 그 심각성이 더해감.

Ⅲ. 유비쿼터스 기반기술의 국방 정보화 적용

1. 전장관리 분야

21세기의 전쟁에서는 무기 및 정보획득기기의 무인 시스템화와 자율시스템화가 보편화될 것이다. 이는 언제, 어디서든, 어떤 수단을 통해서든지 목표물에 대한 정보를 획득하고 추적하며, 정확한 타격을 가하기 위해서이다.

유비쿼터스 컴퓨팅은 산재해있는 작전공간에서 시사각각 변하는 아군과 적군의 전술적 상황정보(병력, 장비, 무기, 군수물자, 지형, 기상, 생태 등)를 실시간으로 수집하고 이를 지휘통제에 활용하며, 작전활동의 결과에 대한 정보를 다시 센싱, 추적하는 순환과정을 통합하여 적용될 것이다. 전술정보의 순환과정은 언제, 어디서, 누구나 유선, 무선, 위성 등의 모든 네트워크와 단말기기 간의 상호운용성과 상호접속성이 이음매 없이(seamless) 확보된 유비쿼터스 네트워크를 기반으로 이루어진다.

1) 전투원 개개인의 전투력 향상

개개인의 전투원들이 디지털화되어 전장에서 실시간에 지휘통제체계에 의해 전투를 수행하기 위해 전장 정보의 제공, 위장 능력의 향상, 신체 상황 통제 등의 기능이 제공되며 이는, 더욱 더 소형, 경량화되는 컴퓨터 기술과 WLAN, 블루투스, Nueron Micro Chip 등 쌍방향 통신이 가능한 무선 송·수신 장치 및 이를 종합한 웨어러블 컴퓨터 기술에 의해 제공될 것이다.

2) 전장의 상황정보 파악

완전한 자율센싱이 가능한 1mm^3 크기의 초소형 스마트 먼지를 이용하여 사방 100m 크기의 공간상 무선 송수신 능력을 이용하여 작전공간에 수천~수만개의 센서로 기상/지형/ 생화학적 오염 상태 등의 자료를 수집하고, 또한 적의 이동현황 등에 관한 정찰을 수행한다.

3) 전투원의 무인 대체

현대전 특성상 이제는 더 이상 많은 희생을 수반하는 전쟁은 국민들로부터 지지를 받지 못한다. 자국 전투원의 희생을 줄일 수 있는 무인 전투체계가 전 차원에서 구비될 것이다. 마이크로 머신, 지능형 전술구동체시스템(smart actuator system), 개별 통제 가능한 IPv6 주소부여, 센서 네트워크 등의 기술로 무인경비, 적지역 침투 탐지, 무인 정찰/전투 비행체UAV/ACAV) 등 전 분야에 대한 전투수단의 무인 대체가 빠르게 진행 될 것이다.

2. 자원관리 분야

통합전투관리체계에서 군수지원은 동맥과 같은 역할을 한다. 무기체계의 개발/획득/운영/정비/도태에 이르는 전 과정은 빠르고 효율적이며,

정확하게 관리하는 것은 전쟁에서의 승리는 물론이고 평상시의 부대유지관리에도 매우 중요하다.

유비쿼터스 컴퓨팅과 네트워크 기술을 활용한 '유비쿼터트 군수지원(u-Logistics)'은 지금까지의 군수지원 역량을 획기적으로 개선해 줄 것이다.

1) u-Logistics

모든 무기, 차량, 장비, 군사시설, 물자, 부품, 탄약 등에 생산단계부터 무선인식 태그(RFID 또는 AUTO-ID)를 부여하며, 생산, 운용 등 각 단계마다 센싱되고 데이터베이스화되어 관리된다. 또한 웹 현실화시스템(Web Presence System)과 연계되어 가상의 공간과 현실의 공간을 일치시켜 상황을 예측 가능하게 한다.

2) 군사 사물의 식별 및 위치/이동경로 추적

모든 사물은 RFID 라벨에 고유의 식별정보를 가지고 수량, 정보, 특성을 관리하며, 단계별 이동에 대한 추적을 통하여 관리케 한다.

3) 수요과 공급관리 및 유지보수

물자의 수량관리로 수요를 예측하며 공급수량을 조절하여 생산단계에서부터 낭비요소를 제거하고, 장비의 내부 모듈의 자가 고장진단을 통하여 신속한 정비로 운영율을 향상시킨다.

Ⅳ. U-국방환경에서 정보보호 기술 적용 방향

1. 유비쿼터스 국방환경에서 주요 정보보호 이슈

1) 네트워크를 통한 대량 정보 공유

네트워크 통합 및 연동이 증가하여 과거 국방 전용망, 체계별/목적별 통신망 이용 환경에서 seamless한 정보 유통을 보장하는 통신망 구조로 변경됨. 또한 정보의 생성, 소비, 유통의 수준 및 범위가 확장되어 유통 정보량이 급격히 증가하여 기반 네트워크 속도 및 대역폭 확장이 불가피함. 전장 환경변화에 따라 신속한 재구성/확장이 가능한 네트워크 구조의 동적인 변화/발전이 필요.

2) 정보에 대한 통제 및 검증 제한

정보통제 요구는 네트워크 수준에서 단위시스템/데이터 수준으로 확장되며, 정보 생산자/소비자의 사전 예측이 제한됨.

3) 상용기술의 의존도, 활용도 심화

기반 기술의 발전은 민간 영역에서 주도되어 군에 적용하여 활용되나, 보안의 요소는 군 요구를 전량 수용하지 못함.

4) 지역적인 공격/침해가 전체로 쉽게 확산

네트워크/시스템 연동이 확대되어 공격/침입 경로 또한 증가됨. 핵심 노드/연관체계 공격시 목표체계 마비/방해가 발생.

5) 동적 네트워크 환경의 보안성 유지/관리 제한

NCW(Network Centric Warfare : 네트워크 중심전) 작전 환경의 네트워크는 무선기술 활용이 확대되며, 무선 환경 정보보호기술의 미성숙으로 동적 네트워크 환경의 보안관리 기반 및 기술이 미비함.

6) 불법적 체계 접근 및 활용 가능성 증가

NCW 환경에서 통제 대상은 비약적으로 증가되며, 사용자의 사전 정의가 제한. 한 네트워크/체계 중심 식별/인증 기술의 확대 적용이 제한됨.

2. 정보보호 기술 적용

1) 침입대응 시스템

새로운 악성 코드 및 공격들을 탐지하고 방지하기 위한 시스템은 침입 종류와 대응방식에 따라 크게 침입차단시스템(Firewall), 침입탐지시스템(IDS), 침입방지시스템(IPS)으로 분류한다.

- **침입차단시스템(Firewall)**

침입차단시스템은 라우터, 컴퓨터, 호스트 또는 호스트들의 집합이 될 수 있으며, 서브넷 밖의 호스트에서 남용될 수 있는 프로토콜과 서비스로부터 사이트나 서브넷을 특별히 보호하도록 구성된다. 개인방화벽은 차후 널리 확산될 PDA나 스마트폰 등과 같은 모바일 기기를 위하여 필수적이며, 스마트 방화벽, 인텔리전트 방화벽, 능동형 방화벽 등의 웹 방화벽의 적용이 필요하다.

- **침입탐지시스템(Intrusion Detection System)**

침입탐지시스템은 자원의 무결성(Integrity), 비밀성(Confidentiality), 가용성(Availability)을 저해하는 행위를 실시간 감지하는 것으로, 방화벽이 해킹되었을 경우는 물론 서브넷의 시스템 해킹시 이를 인지하도록 하며 해킹의 구체적인 내용을 관리자에게 알려주어 그에 따른 대응을 할 수 있도록 한다.

표 2. IDS와 Firewall의 비교[4]

구 분	IDS	F/W
주요역할	탐지(Detection)	방어(Prevention)
물리적위치	내부에서 불법사용자 감시	외부와 내부 경계에서 외부출입자 방어
설계정책	명백하게 금지하는 것만 금지	명백하게 허용하는 것만 허용
시스템 장애시 네트워크상태	네트워크가 오픈됨	네트워크 사용불능
네트워크 부하	적음	병목현상 발생

- **침입방지시스템(Intrusion Prevention System)**

침입방지시스템은 공격을 찾아내 네트워크에 연결된 기기에서 수상한 활동이 이루어질 경우 자동으로 대응작업을 수행하여 행위를 중지시키는 시스템으로, 침입탐지시스템의 갈수록 복잡하고 지능화되는 보안침해 방법과 기술에 대처에 한계로 침입방지시스템으로 대체가 이루어지는 추세다.

- **보안운영체제(Secure Operating System)**

보안운영체제란 컴퓨터 운영체제의 커널(Kernel)에 부가적인 보안 기능을 추가한 운영체제를 말하며, 서버의 보호, 시스템 접근 제한, 관

리자에 의한 권한 남용 제한, 응용프로그램 버그를 이용한 공격으로부터의 보호 등 네트워크 중심 보안제품의 한계를 보완하는 것이다.

2) 악성코드 대응

악성코드는 크게 바이러스, 웜, 트로이목마, 스파이웨어, 스팸 메일, 피싱으로 구분할 수 있으며 이에 대한 예방 시스템 운영이 요구된다.

- **바이러스 · 웜 · 트로이목마 탐지 및 예방**

바이러스, 웜, 트로이목마를 탐지하고 차단하는 방역체계의 사용 및 주기적인 업데이트가 필수적이다. 최근에는 모바일 기기를 대상으로 한 악성프로그램이 발견되고 있으며, 복잡하고 고도화된 다양한 형태의 무선 단말기들이 네트워크상에서 다양한 파일 및 정보교환의 목적으로 사용될 것이 예상되어 이에 대한 대응이 요구된다.

표 3. 바이러스, 웜, 트로이목마 특성 비교

구 분	바이러스	웜	트로이목마
자기복제	O	O	x
숙주필요여부	O	x	x
전파방법	감염파일실행 감염디스크통한부팅	감염대상을 자동 검색하여 전파	전파되지 않음
전파대상	파일 및 부트 섹터	네트워크 전체	전파되지 않음
악성행위	데이터 파괴 네트워크 마비	데이터 파괴 네트워크 마비	정보유출 컴퓨터 제어

- **스파이웨어 탐지 및 예방**

스파이웨어는 웹서버나 개인 컴퓨터에 설치되어 정보들을 유출시키는 악성코드로, 사용자의 동의하에 또는 호스트의 취약점을 이용하여 설치된다. 스파이웨어는 차단 프로그램이나 통합 보안 시스템을 이용한다.

3) 인식 및 인증

PKI(Public Key Infrastructure)와 같은 인증서 기반의 전자서명과 SSO(Single Sign On)과 같은 다양한 인증 메커니즘을 단일 로그인 서비스하는 방식에서 AC(Attribute Certificate)를 이용한 사용자 권한 관리 기법인 PMI(Privilege Management Infrastructure)로의 전환이 예상며, 유/무선의 다양한 네트워크 환경을 고려할 때 네트워크 연동시의 문제와 다양한 체계의 통합 인증, 소형 무선 환경에서 적합한 암호 관련 기술의 개발이 요구된다.

- **PKI(Public Key Infrastructure)**

PKI는 공개키 기반 구조로써, 네트워크 환경에서 보안 요구사항을 만족시키기 위해 공개키 인증서 사용을 가능하게 해준다. 암호화된 메시지 송신시는 수신자의 공개키를 사용하며, 암호화된 서명 송신 시에는 송신자의 개인키를 사용한다. 암호화된 메시지 해독 시에는 수신자의 개인키를 사용하여 복화하며, 암호화된 서명을 해독하고 송신자를 인증하기 위하여 송신자의 공개키를 사용한다.

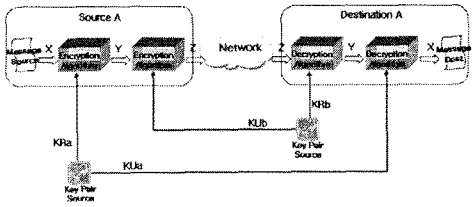

그림 1. 공개키 암호시스템(기밀과 인증)

- **SSO(Single Sign On)**

SSO는 단 한번의 사용자 인증 및 권한 부여로 사용자가 가진 권한 범위 내에서 모든 컴퓨터와 시스템에 접근이 가능하도록 하는 메커니즘이다. 다양한 체계에 사용되는 로그인 정보를 별도로 관리할 필요가 없어 사용자의 개인 정보유출 등의 문제를 효율적으로 개선할 수 있다.

- PMI(Privilege Management Infrastructure)

PMI는 다양한 응용 환경에서 특정 리소스에 접근할 수 있는 권한을 차등적으로 부여하여 보안 관리를 하는 메커니즘이다. 사용자 인증만으로 한정된 PKI와 달리 PMI는 인증뿐만 아니라 접근 권한까지 체계적으로 관리한다.

- **스마트카드**

스마트카드는 인증을 목적으로 사용되는 칩 기반 카드로 단말기와 직접적으로 통신하며, 자체전력을 가지고 있지 않고 단말기 등의 외부 장치로부터 전력을 공급받는다.

- **바이오인식 시스템**

사람마다 가지고 있는 고유한 생체정보는 보안성과 더불어 편리성을 제공한다. 접근제어 부문에서 여러 가지 활용이 가능하며, 특히 전장 환경을 고려하여 볼 때 신체의 일부분의 손상으로 인하여 사용이 불가할 경우 및 복제의 위험성을 줄이기 위하여 타 인증기술의 중복사용이 요구된다. 대표적인 활용 기술로는 음성, 지문, 망막, 홍채, 정맥인식 등이 있다.

- **일회용 패스워드(OTP : One Time Password)**

시스템이나 네트워크 접근에 대한 인증은 주로 비밀번호에 의존되어 노출시 악의적인 접근이 가능하다. OTP 인증은 비밀번호가 노출되더라도 다음 번 접근시는 다른 패스워드를 사용하는 일회용 암호 방식 인증으로 보다 안전하다.

4) 무선환경 보안

앞으로 일상생활 및 전장 환경을 고려하여 볼 때 기존 통신망 운영의 이동상의 제한을 극복하여 뛰어난 성능과 편리성을 모두 갖춘 무선 네트워크가 차지하는 비중은 점차 커질 것이 분명하며 이를 활용하기 위해서는, 무선환경에 적합한 보안기술 개발이 요구된다.

표 3. RFID의 보안 위협[6]

종 류	내 용
물리적공격	태그를 획득하여 내용을 다른 태그로 복사하여 위장 공격
도청	RF통신 중 정보가 암호화되지 않은 채 전달되면 근거리에서 리더기로부터 정보 탈취 가능
스누핑	휴대용 리더기로 태그의 내용을 읽거나 위치 추적
스푸핑	태그의 내용을 변조하거나 정상 리더기로 위장 가능
서비스 거부 공격	강한 전파 송·수신을 통해 리더기와 RFID간 정상적인 통신 방해
세션 가로채기	인증된 세션을 가로채거나 프로토콜 일부를 다시 실행하여 세션을 얻음

- **RFID(Radio Frequency Identification)**

저렴한 가격 및 이용의 편의성으로 인하여 군수 물류 관리, 출입자 관리 등의 부분에서 주로 활용지만, RFID 센서의 기능이 아주 단순하기 때문에 높은 보안기술을 접목시키기 어려운 단점이 있으며, 동시에 연산이나 저장 능력이 다른 매체에 비해 약하다. 정보보호에 활용할 수 있는 공간이 적으므로 기존의 표준 암호 알고리즘 대신 물리적인 보안 대책이 제안된다.

- **USN(Ubiquitous Sensor Network)**

USN의 구조는 센서영역, 게이트웨이, 외부 네트워크로 구분되며, 센서들이 인증하는 절차가 필요하다. 인증절차가 없을 시에는 인증되지 않은 침입자에 의해서 센서들이 제어되어 정보가 훼손되거나, 정보의 유출이 발생할 수 있다. 이와 같은 보안위협을 차단 및 대응할 수 있는 센서노드용 경량 보안 칩 및 보안 OS, 키 분배 및 관리, 경량 인증 메커니즘 등 USN 환경에 최적화된 센서노드 보안 구조 기술 및 USN 침입탐지/대응기술이 요구된다.

- **휴대인터넷(WiBro)**

휴대인터넷 서비스는 휴대형 단말기(휴대폰, PDA, 노트북 등)를 이용하여 정지 및 이동중에도 빠른 전송속도를 제공한다. 휴대인터넷 구축시 각 네트워크 간의 연동은 필수적이기 때문에 기존의 개별 네트워크를 넘어 연동되는 네트워크상세서의 인증, 키 교환 및 데이터 암호화 등을 가능하게 하는 연동 보안기술이 요구된다.

V. 결 론

본 논문에서는 정보통신 기술의 발전에 기인한 유비쿼터스 환경에서의 국방 정보보호 발전에 관하여 살펴보았다. 우리 사회의 유비쿼터스 사회로 진입하는 과정에서 나타나는 현상을 예상하여 볼 때 군대라는 영역에 적용시 일반적으로 취해야 할 정보보호에 관한 사항은 충분히 유추 가능하며 최초 소요제기 단계부터 준비가 가능한 사항이므로 실 체계 개발시는 반드시 고려되어야 할 요소이다. 또한 국방정보기술표준(DITA) 및 상호운용성 측면에서 실제 군 작전환경에 맞는 다양한 조건에서의 정보보호 요구사항이 이루어지도록 정책/제도 및 사이버전 역량 강화, 기반기술/체계의 고도화, 교육 등의 부분에서 다양한 환경 변화와 연계하여, 지속적인 변화와 발전을 위한 연구가 필요하다.

참고문헌

[1] 2006 DEFENSE WHITE PAPER, Ministry of National Defense
[2] 유비쿼터스 정보보호 기본전략 연구, KISA
[3] 박응기, "유비쿼터스 환경에서의 정보보호기술 발전추세", DISC 2007 논문지 pp.44-46
[4] 김종필, 박동섭, 이성중, "정보보호 핵심지식", 정일, pp. 324
[5] William Stallings, "Cryptography and Network Security" 3rd edition, Pearson Prentice Hall, pp. 296
[6] 2007 국가 정보보호 백서, National Information Security
[7] 김배현, 나원식, 유인태, 권문택, "국방 정보보호 기술 발전동향", 정보보호학회지 제12권 제6호
[8] 남길현, "국방정보보호와 PKI 응용", 정보보호 심포지엄 2003