유비쿼터스 시대의 정보보호 추진동향 : 국방 분야를 중심으로

최인수

한국국방연구원
130-012 서울특별시 동대문구 청량리2동 산5-7번지
Tel: +82-2-961-1779, E-mail:ischoi@kida.re.kr

Abstract

정보기술 발전과 활용 확대에 따라 정보보호의 개념과 범위는 지속적으로 확대, 발전하여 왔다. 최근 우리나라 및 주요 선진국은 유비쿼터스 사회 건설을 위해 다양한 노력을 기울이고 있는데 이의 일환으로 정보보호 강화를 위한 다양한 노력도 병행되고 있다. 이러한 추세는 국방 분야 또한 마찬가지이다. 현재 미국방부 등 주요 군사선진국들은 미래전 환경을 대비하여 네트워크중심전 개념의 전력변환을 추진 중인데, 이에 따른 정보보호 문제 대비를 위해 다양한 노력을 추진 중에 있다. 이에 본 고에서는 정보화 환경 변화와 유비쿼터스 시대의 미래전 환경을 대비한 주요 군사선진국들의 정보보호 추진 동향을 살펴보았는데, 주요 시사점으로는 공통 정보보호 추진 전략 정립 및 세부 기준/지침 강화, 미래전 환경에 부합하는 정보보호체계 개발 및 성능개량, 정보시스템의 보안성 평가/검증 및 관리체제 강화 등과 같이 실질적인 정보보호 추진을 위해 기반을 강화하고, 기존 정보보호 대응수단을 더욱 체계화, 고도화하기 위한 노력을 적극적으로 추진하고 있다고 분석된다.

Keywords:

정보보호; 정보보증; 사이버전

1. 서론

정보보호의 기본적인 목적은 조직의 중요한 정보자산을 다양한 보안 위협으로부터 보호, 방어하는 것이라고 할 수 있다. 그런데, 이러한 목적을 달성하기 위한 수단은 항상 고정된 것이 아니다. 조직의 전략 및 목표, 기술 환경 등의 변화에 따라 조직의 정보자산과 이를 구축, 운영하는 환경은 지속적으로 변화하고 있으며, 이에 따라 조직의 정보자산에 대한 보안 위협 또한 변화하고 있기 때문이다.

정보보호의 고려 요소는 단순히 기술적 측면으로 제한되지 않는다. 하지만 정보기술의 급속한 발전과 이를 기반으로 한 정보통신 환경의 변화는 새로운 정보보호 문제점 및 역기능을 발생시켰으며, 이에 대응하기 위해 정보보호의 개념 및 범위를 지속적으로 확대, 발전하여 왔다. 과거 컴퓨터 및 네트워크 활용이 제한적이고 독립적이었던 정보화 초기 단계의 정보보호는 중요 정보의 불법적인 노출을 방지하기 위한 기밀성 (confidentiality) 보호에 중점을 두고 주로 국가나 국방 조직에서 활용되었지만, 컴퓨터의 활용이 일상화되고 인터넷 등을 통해 상호 연결되는 오늘날의 정보화 환경에서는 새로운 보안 위협에 대처하기 위해 기밀성 뿐만 아니라 무결성 (integrity), 가용성(availability), 인증(authentication), 부인봉쇄(non-repudiation) 등과 같은 정보보호 서비스도 중요해지고 있으며 사이버공격의 탐지/차단/대응과 같은 역량도 필수적인 요소로서 인식되고 있다.

이와 같은 변화는 첨단 정보기술의 지속적인 발전과 활용 확대에 따라 계속될 것이다. 최근 우리나라 및 주요 정보화 선진국은 그간의 정보화 추진 성과를 더욱 고도화한 유비쿼터스 사회의 건설을 위해 다양한 노력을 기울이고 있다. 이와 같은 변화는 언제, 어디서나 정보화 서비스를 편리하게 이용할 수 있는 환경을 구축한다는 긍정적인 효과가 예상되지만, 이에 대한 역기능으로 해킹, 컴퓨터 바이러스, 웜 등과 같은 악성코드, 서비스거부공격, 개인정보침해 등과 같은 사이버 위협이 더욱 증가하고, 사이버 공격 기법 또한 지능화, 고속화, 다양화될 것으로 예상되고 있다. 따라서 유비쿼터스 사회 건설을 위한 노력의 일환으로 정보보호의 중요성에 대한 인식은 확산되고 있으며, 이를 사전에 대비하기 위해 국가적 차원에서는 다양한 정보보호 대비 노력들을 수행하고 있다.

이러한 추세는 국방 분야도 마찬가지이다. 오늘날 정보기술의 발전은 일반적인 국방 업무 영역뿐만 아니라 군 고유의 임무 영역인 전쟁 수행에 있어서도 커다란 영향을 끼치고 있다. 우세한 정보수집 및 분석능력, 정밀타격능력을 기반으로 적의 핵심 전력과 지휘통제체계의 무력화에 초점을 두는 최근의 현대전 양상에서 정보기술의 영향력은 점차 증가하고 있는데, 이러한 추세는 예견되는 미래전 환경에서 더욱 심화될 것으로 전망되고 있다. 네트워크중심전(Network Centric Warfare)으로 대변되는 미래전 개념은 기술적 측면에서 첨단 정보통신 및 유비쿼터스 기술의 적극적인 활용을 통해 제 전력 요소들을 네

트워크로 연결한다는 개념을 기반으로 하는데, 이러한 변화는 정보보호 측면에서 새로운 문제점 및 위협을 발생시킬 수 있다. 따라서, 이에 대한 대비로 미국방부 등 주요 군사선진국들은 미래 국방정보통신 환경의 보안성, 안전성을 보장하기 위해 기존의 정보보호 추진 방식을 새롭게 정비하고 발전시키기 위한 다양한 노력을 기울이고 있는 상황이다.

이에 본고에서는 유비쿼터스 시대의 미래전 개념과 정보보호 측면에서의 영향을 살펴보고, 이를 대비한 미국방부 등 주요 선진국들의 정보보호 추진 동향을 살펴보고 그 시사점을 분석하고자 한다.

2. 미래전 개념과 정보보호

2.1 미래전 개념 : NCW

최근 정보화 시대의 전쟁 개념, 작전수행 개념으로 네트워크중심전(NCW: Network Centric Warfare) 이론이 주목 받고 있다. 이 이론은 현재 미래전 환경을 대비하여 미국방부 등 주요 군사선진국에서 추진중인 전력변환(force transformation)이나 군사력 발전의 중심 지향점이 되고 있으며, 우리나라 또한 국방개혁 추진의 핵심 방향으로 인식되고 있다. 네트워크중심전의 기본 사고는 전장에 참여하는 제 전력 요소에 관해 정보통신 기술의 발전을 이용한 네트워크를 구축하면, 전장상황인식의 공유와 전력의 통합화가 가능해지고, 이에 따라 작전임무의 수행 효과를 획기적으로 높일 수 있다는 것이다.

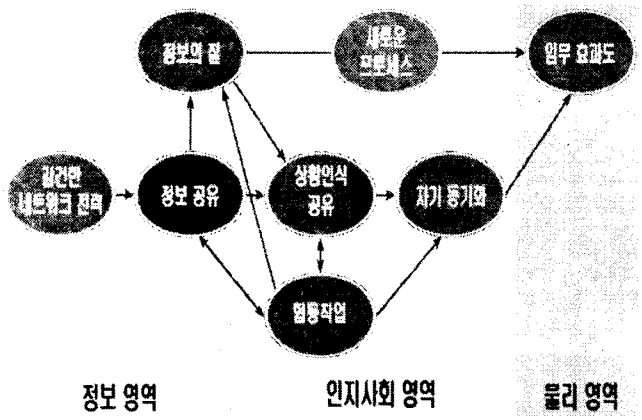

그림 1 - NCW의 기본 사고

네트워크중심전은 기본적으로 작전 이론으로 이를 구현하는 것은 단순히 기술 영역으로만 제한되지 않는다. 하지만, 다양한 전력 요소들이 유기적으로 네트워킹하기 위한 기술적 환경의 구축은 네트워크중심전 이론을 구현하는데 핵심적인 요소이다.

네트워크중심전 구현을 위한 기술적 환경은 상위적 수준에서 <그림-2>와 같이 센서격자망(sensor grid), 교전 격자망(engagement grid), 정보격자망(information grid)으로 불리는 3개의 격자망을 통해 설명된다. 센서격자망은 여러가지 다양한 유형의 감시센서들을 연결해서 고차원의 전장 상황 정보를 생성하고 적시에 알 수 있게 하는 기능을 수행하고, 교전격자망은 다양한 무기체계들이 상호 유기적으로 연계하여 전투력을 증가시키는 기능을 수행한다. 정보격자망은 제 전력 요소들의 컴퓨팅과 네트워킹의 기반이 되는 환경으로 센서격자망과 교전격자망이 구성, 운영되는 기반을 제공한다.

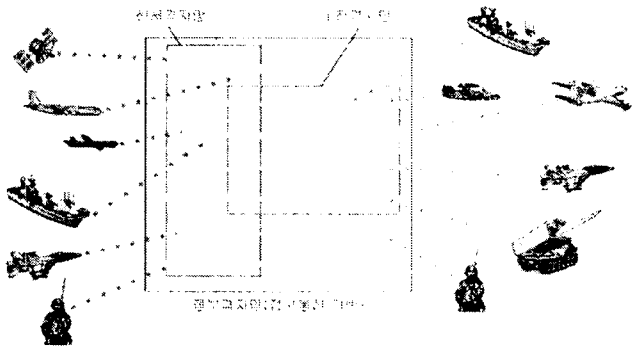

그림 2 - NCW의 논리적 구현 모델

이와 같은 기술적 환경 구축을 위해서는 다양한 첨단 정보기술 및 유비쿼터스 기술의 적용 확대가 요구되는데, 이와 관련하여 검토 또는 적용을 추진중인 기술들로는 국방BcN, IPv6, RFID, UsN, 데이터링크, 무선/이동 네트워킹, 웹서비스, SoA, 통신망/시스템 연동 기술 등이 있다.

2.2 미래전 환경과 정보보호

네트워크중심전은 오늘날의 첨단 기술이 제공하는 다양한 능력을 전투력 향상으로 연결시키는 개념을 설명하는 이론으로, 이를 실제적으로 구현하는 구체적인 방안까지 제공하지는 않는다. 이러한 측면에서 네트워크중심전 구현은 각 나라가 직면한 국가안보 및 군사환경 등에 따라 달라질 수 있으며 경제적, 기술적 기반 역량 또한 구현의 수준이나 범위를 결정하는데 커다란 영향을 줄 수 있다. 즉, 현재 시작 단계인 네트워크중심전 구현에 따른 정보통신 환경의 변화를 정확히 예단하는 것은 매우 어려운 일이며 따라서 이에 따른 정보보호 위협 및 추진 방향을 정확히 도출하는 것은 제한된다.

하지만, 네트워크중심전 이론의 기본적인 추구 방향만으로도 미래 국방정보통신 환경의 변화와 발전 모습은 어느 정도 예상 가능하다. 유기적인 네트워킹 보장을 위해서는 우선 언제 어디서나 정보의 유통이 가능한 통로의 구축이 필요한데, 이를 위해서는 어떠한 전장 환경에서도 정보를 유통시킬 수 있는 네트워크가 지원되어야 하며, 중단없는 정보의 유통을 위해 상호 분리되어 운영 중인 다양한 네트

워크 및 시스템들의 연동이나 통합이 확대되어야 한다. 또한, 제 전력 요소들이 적시에 정확한 전장상황 정보를 공유하기 위해서는 정보를 생성, 저장, 유통, 활용, 관리하는 방식이 현재와는 다르거나 더욱 진보한 방식으로 변화할 것이다.

이와 같은 미래 국방정보통신 환경의 변화는 정보보호 측면에서 볼 때 많은 문제점을 내포하고 있다. 다양한 네트워크 및 시스템들의 연동이나 통합 확대는 사이버공격의 경로가 확대되고 공격을 인한 지역적인 피해가 전체 정보통신 환경으로 쉽게 확산될 수 있는 환경을 제공할 수 있다. 또한, 정보의 저장, 유통, 활용, 관리 방식의 변화는 기존 정보보호 수단의 적용 범위나 수준이 비약적으로 확장되거나 새로운 접근방식을 필요로 하여 이전에 고려할 필요가 없던 새로운 위협과 취약성을 발생시킬 수 있다.

3. 국외 국방정보보호 추진 동향

3.1 미국

세계 최고 수준의 군사력을 갖추고 있으며 네트워크중심전 이론의 고안 및 발전을 주도하고 있는 미국방부는 정보보호 역량의 강화 및 확보를 미래전 대비를 위한 전력변환의 핵심 성공 요소로 인식하고 있으며, 이를 위해 다양한 노력들을 추진 중에 있다. 다음은 정보통신 환경 변화 및 미래전 환경 대비를 위해 미국방부에서 추진 중인 주요 정보보호 정책 및 활동들이다.

미국방정보보증전략계획[1]

미국방정보보증전략계획(DoD Information Assurance Strategic Plan)은 미국방부 최상위 수준의 정보보호 추진전략 및 계획을 기술한 문서로 '03년 10월 v1.0이 만들어졌으며, '04년 1월 v1.1이 발표되었다. 이 문서에서는 네트워크중심전 개념으로의 전력변환을 지원하고 군의 정보통신환경을 보호, 방어하는 것을 임무로 설정하고 있으며, 미국방부 네트워크중심전 구현의 기술적 기반인 범세계정보격자(Global Information Grid)를 동적으로 보호하는 것을 비전으로 삼고 있다. 또한, 이러한 비전을 구현하기 위해 정보의 보호(protect information), 시스템 및 네트워크 방어(defend systems and networks), 통합적인 IA 상황인식정보 제공 및 IA 지휘통제(provide integrated IA situational awareness/IA command and control), IA 역량의 변환 및 강화(transform and enable IA capabilities), IA 인력의 양성(create IA empowered workforce)의 5가지를 목표로 설정하고 각 목표를 달성하기 위한 세부 목표를 기술하고 있다.

[1] '정보보증(information Assurance)'은 정보통신환경 변화에 따른 정보보호 개념의 변화를 반영하고자 '90년대 중반 이후부터 사용되기 시작하여 현재 미국방부에서 공식적으로 사용되는 용어이다.

미국방정보보증 정책/제도 정비 및 발전

미국방부는 '90년대 후반부터 국방환경 변화와 네트워크중심전 구현을 지원하기 위한 정보보호 기반 발전을 위해, 공통 구현전략을 정립하고 기존 정보보호 관련 정책/제도를 정비하거나 신규 제정하는 작업을 지속적으로 추진 중에 있다. 미 국방부의 정보보호 구현전략은 '종심방어(Defense-in-Depth)'으로 불리우는데, 이 전략은 인력(people), 기술(technology), 운영 (operation)의 3가지 요소가 상호 병행적인 발전을 강조하며, 기술적 측면에서는 계층적 방어 개념의 정보보호체계 구축을 요구하고 있다. 미 국방부의 정보보호 정책/제도는 <표 1>과 같이 통상 8500시리즈로 불리는 분류체계 하에 9개의 범주로 구분되어 있다.

표 1 – 미국방부 정보보호 정책/제도 현황

범주/범위	훈령/규정
8500 일반사항	DoDD 8500.1, "Information Assurance (IA)," `03. DoDI 8500.2, "IA Implementation", `03.
8510 인증 및 인가	DoD 8510.1-M, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document.", `01. DoDI 8510.bb, DoD IA Certification and Accreditation Process, `06.
8520 보안관리 (SMI/KMI)	DoDD 8520.1, "Protection of Sensitive Compartmented Information," `01. DoDI 8520.2, "Public Key Infrastructure (PKI) and PK-Enabling," `04.
8530 CND/취약성 관리	DoDD O-8530.1 "Computer Network Defense," `01. DoDI O-8530.2 "Support to Computer Network Defense(CND)," `01.
8540 상호연결/ 다수준보안	DODI 8540.aa, Draft, ""Interconnection and Data Transfer Between Security Domains""
8550 네트워크/ 웹	DoDI 8551.1, "Ports, Protocols, and Services Management," `04.
8560 평가	-
8570 교육/훈련	DoDD 8570.1, "IA Training, Certification, and Workforce Management," `04. DoD 8570.01-M, "IA Workforce Improvement Program", `05.
8580 기타	DoDI 8580.1, "IA in Defense Acquisition System," `04. DoDD 8581.1e, "IA Policy for Space Systems Used by DoD," `05.

또한 미국방부는 정책/제도를 실질적으로 구현하는데 참조할 수 있는 지침이나 세부기준들의 개발하

는 작업도 지속적으로 추진 중에 있는데, 대표적으로 '정보보증기술프레임워크(IA Technical Framework)' 와 '정보보증기술구현가이드(IA technology implementation guides' 등이 있다.정보보증기술프레임워크는 종심방어 전략의 기술적 구현에 참조하도록 만든 공통 참조문서로 국방정보통신 환경을 지역컴퓨팅환경(local computing environment), 경계(boundaries), 네트워크 및 기반구조(network and infrastructure), 지원기반구조(supporting infrastructure)의 4계층으로 구분하고 각 계층별로 적용할 정보보호 기술과 체계, 적용 고려사항들의 정보를 제공하고 있다. 정보보증기술구현가이드는 다양한 운영체제, S/W, 시스템/네트워크 장비 등에 대한 보안 체크리스트, 정보보호기술의 구현, 구성설정 및 운영가이드 들을 제공하고 있다.

암호 현대화 프로그램

암호 현대화 프로그램(crypto modernization program)은 핵심적인 정보보호 수단인 암호기술/장비를 정보화 발전 추세와 미래전 환경에 부합하도록 개량하는 사업이다. 미국방부는 '02년도에 이에 대한 추진 정책을 수립하고 향후 10~15년에 걸친 중장기적인 사업으로 이를 추진 중에 있다. 이 프로그램에서는 통신망 대역폭 확장, 음성/데이터 통합, All-IP 환경, IPv6 전환 등과 같은 기반 환경 고도화에 따른 암호장비/기술의 성능개량뿐만 아니라 종대종(end-to-end) 네트워킹, 다양한 전력요소들의 합동작전 등을 지원하기 위해 상호운용성을 지원하고 보다 탄력적으로 적용가능한 암호장비/기술의 개발도 적극적으로 추진 중에 있다.

미국방정보보증 인증 및 인가 프로세스

미국방정보보증인증및인가프로세스(DoD IA Certification and accreditation Process)는 정보시스템 수명주기 전반에 걸쳐 체계의 보안성을 검증, 확인, 유지하기 위한 표준 절차, 업무, 활동을 정의한 프로세스이다. 이 프로세스는 과거 단위 정보자산의 보안성 인증/인가 개념을 정보체계 전반으로 확장한 개념으로, 미국방부는 '97년 이를 위한 표준 프로세스를 정립하고 지속적으로 발전시키고 있는데, 현재 모든 국방정보시스템의 획득 및 운영관리 업무 전반에 강제적 요구사항을 적용토록 하고 있다.

3.2 영국

영국은 NEC(Network Enabled Capability)라는 명칭의 네트워크중심전 개념을 정립하고 전력변환을 추진 중에 있는데, 국방정보통신 환경 변화에 대비한 정보보호 노력도 강화하고 있다.

먼저 영국 국방부는 '03년에 국방정보시스템의 보안관리에 대한 BS7799 인증을 받았으며, 이후 이 방법론을 모든 정보보호 및 정보관리 정책 및 문서에 통합시키는 작업을 수행하였다. 또한, 국방정보통신 환경 변화와 전력 변환 추진을 위해 정보보호 정책/제도의 정비 및 발전도 지속적으로 추진 중인데, 현재 <표 2>와 같은 정보보호 정책/제도, 기준, 가이드들을 개발, 발전시키고 있다.

표 2 - 영국 국방부 정보보호 정책/제도 현황

범주/범위	정책/기준/참조문서
JSP (Joint Service Publication)	JSP 525-Corporate Governance and Risk Management JSP 503-Business Continuity Management JSP 541-Information Security Alert Warning and Response Policy and Procedures Manual JSP 440-The Defence Manual of Security JSP 602: 1001-Application Architecture JSP 602: 1003 -Authentication Services JSP 602: 1004 -Certificate Services JSP 602: 1032 -Crypto. and Key mgt. JSP 602: 1034 -Network Mapping and Configuration Management JSP 602: 1036 - Security Architecture 등
HMG InfoSec Standard	No1-Residual Risk Assessment Method No2-Risk Mgt. and Accreditation of Information Systems No 3-Connecting Business Domains No 4 - Communications and Cryptography
INFOSEC MEMO	IM4-Catalogue of High-Grade Communications Security Equipment IM13 - Protecting Government Connections to the Internet IM21 - Risk Management of Mobile Code IM24 - Use of Passwords, Tokens & Biometrics for I& A IM26 - Passwords for I&A IM29 - Secure Video Conferencing IM31 - The use of COTS Keyboard Video Mouse switches IM39-Cryptographic Algorithm Suites 등
Manual	Manual N-Vulnerabilities of the TCP/IP Protocol Suite Manual V-Use of IPSec in Gov. Systems Manual W-Secure Info. Sharing 등

그리고, 영국 국방정보통신 환경의 구축, 운영을 총괄적으로 서비스하는 DCSA(Defense Communication Service Agency)에서는 '04년 이후 NEC 추진을 위한 핵심 사업의 일환으로 사이버공격에 대응하기 위한 CND(Computer Network Defense) 프로젝트와 미래 전장 환경에서의 암호장비 개량을 위한 FCP(Future Crypto Programme) 프로젝트, 암호키 분배와 관리 체제의 개선을 위한 IEKD(interoperable Electronic key Distribution) 프로젝트를 등을 추진 중에 있다.

3.3 프랑스

프랑스는 아직 특별한 명칭을 사용하고 있지는 않

지만 다른 군사 선진국과 같이 네트워크중심전 개념의 군사력 강화를 추진 중인 것으로 알려져 있다.

미래전을 대비한 프랑스 국방부의 정보보호 노력에 대한 정보는 상대적으로 많이 공개되어 있지는 않지만, 공개된 정보를 기반으로 볼 때 프랑스 국방부 또한 '00년 이후 국방정보통신 환경 발전에 따른 정보보호 강화를 위해 다양한 업무를 추진 중인 것으로 추정된다. 현재 프랑스 국방부에서 정보시스템의 보호를 위해 적용 중인 주요 전략 및 방법들은 다음과 같다

- 'In Depth Defense' 전략 : 미국의 종심방어 전략과 유사한 정보보호 추진 전략으로, '04년 7월 이 전략의 적용을 위한 참조 문서를 공표
- EBIOS (Expression of Needs and Identification of Security Objectives) : 정보시스템의 보안 위협을 식별/평가하고 처리하기 위한 방법론을 제공
- PSSI (Information Systems Security Policy) : 정보시스템의 정보보호 수립을 지원하기 위한 절차 및 기준을 제공
- TDBSSI (Information Systems Security Trend Chart) : 의사결정, 관리, 운영 등 다양한 수준에서 활용될 정보보호 상황정보 제공을 위한 관리도구

3.3 분석 및 시사점

네트워크중심전 개념의 미래전 환경은 국가나 민간 영역에서 추진 중인 유비쿼터스 환경과 유사하다. 이러한 측면에서 주요 군사선진국들의 정보보호 추진 동향은 상위적 수준에서 안전한 미래 유비쿼터스 사회 건설을 위한 국가나 민간 영역의 정보보호 대응 및 강화 노력과 맥락을 같이 한다. 하지만, 실질적인 전력 변환 및 발전을 지원한다는 측면에서, 주요 군사선진국들의 정보보호 강화 노력은 보다 구체성을 띄고 있으며, 기존의 정보보호 대응 수단을 더욱 체계화하고 고도화하는 방향으로 추진되고 있다. 주요 군사선진국들의 정보보호 추진 동향의 시사점을 정리하면 다음과 같다.

첫째, 전사적인 공통 정보보호 추진 전략을 정립하고, 세부적인 구현 기준 및 지침 개발을 강화하고 있다. 제 전력 요소들의 네트워크화가 확대되는 미래전 환경에서는 단일 체계 중심의 보호 대책은 효율적으로 동작하기 어려우며, 정보시스템의 보호 수단들은 과거 독립적인 운영 개념의 정보보호체계를 적용 위주에서 시스템에 내장되거나 통합되는 방식으로 발전하고 있기 때문이다.

둘째, 미래전 환경에 부합하는 정보보호체계의 개발 및 성능개량을 적극적으로 추진 중에 있다. 통신망 대역폭 확장, IPv6, Ad-hoc/무선 네트워킹, UsN 등의 기술들은 네트워크중심전 구현을 위해 적용이 요구되는 기술들인 반면에 이를 적용하기 위해서는 기존 정보보호체계들의 성능개량이나 새로운 시스템의 개발이 필요한데, 주요 군사 선진국들은 이러한 문제점을 사전에 식별하고 대응하기 위한 노력을 체계적으로 추진 중에 있다.

셋째, 정보시스템의 보안성 평가, 검증 및 관리체제를 강화하고 있다. 대부분의 나라에서 정보시스템 보안성의 평가, 검증 및 관리 업무는 새로운 업무는 아니다. 하지만, 정보기술의 활용 범위가 급격히 증가하는 반면 정보기술 연구개발의 민간 의존성이 커지는 상황에서, 안전한 정보시스템의 획득 및 연구개발은 점차 중요해지고 있는데, 주요 군사선진국들은 정보체계 수명주기 전반의 활동과 밀접하게 연계되는 보안성 평가, 검증 및 관리체계를 발전시키고 있다.

4. 결론

현재 많은 군사선진국들은 네트워크중심전 개념의 미래전 환경을 대비하여 기존 전력의 강화와 변환을 위한 다양한 노력을 기울이고 있다. 이러한 변화와 발전은 향후 국방정보통신 환경의 많은 부분을 변화시키고, 군의 임무 수행에 있어 정보기술에 대한 의존성을 더욱 심화시킬 것으로 예상되는데, 이는 정보보호 분야에서도 보다 체계적인 강화 노력을 필요로 한다.

본고에서는 유비쿼터스 시대의 미래전 환경을 대비한 주요 군사선진국들의 정보보호 추진 동향을 살펴보았다. 현재 주요 군사선진국들은 네트워크중심전 구현의 지원을 위한 보다 실질적인 정보보호 추진을 위해 기반을 강화하기 위한 노력을 기울이고 있으며, 기존 정보보호 대응 수단을 더욱 체계화, 고도화하고 있다.

우리 군 또한 미래전 환경을 대비한 국방정보통신 환경의 변화를 고려한 국방정보보호 발전 방안을 계획하고 있는데, 이러한 노력은 한국적 네트워크중심전 개념이 구체화됨에 따라 지속적으로 개선, 발전하여야 한다. 또한, 국방정보보호 발전을 위한 기술을 대부분 민간 영역에서 의존하여야 하는 상황에서 안전한 유비쿼터스 사회 건설을 위해 국가, 민간 차원에서 추진 중인 정보보호 노력과도 유기적인 연계체제를 마련할 필요가 있다.

참고문헌

[1] 정보통신부(2005). *안전한 u-Korea 구현을 위한 중장기 정보보호 로드맵.*

[2] 손태종 외 (2005), *네트워크중심전(NCW) 연구*, 한국국방연구원

[3] Jacques .S. Gansler and Hans Binnendijk(2004), *Information Assurance : Trends in vulnerabilities, threats, and technologies*. National Defense University CTNSP.

[4] Scot Miller(2005), "EVALUATION OF INFORMATION ASSURANCE REQUIREMENTS IN A NET-CENTRIC ARMY", research paper, U.S. Army War College

[5] N. Coleman(2004), *Information Assurance : A review of UK Government and industry initiatives*, UK Cabinet Office
[6] UK DCSA(2006), *Defence through Information : DCSA corporate plan*
[7] DCSSI advisory office(2004), *Memo on the concept of In Depth Defense applied to Information System.*
[8] D.G .Wolf(2006), Leveraging Cybersecurity, http://www.military.information-technology.com/article.cfm?DocID=389
[9] US CJCSI 6510.02B(2002), Cryptographic modernization plan.
[10] US DoD(2004), DoD Information Assuran- ce Strategic Plan
[11] http://www.jsp600.ia.mod.uk/jsp/index_html
[12] http://www.ssi.gouv.fr/fr/dcssi/
[13] http://www.disa.mil/