NCW를 위한 정보보증 프레임워크

국가보안기술연구소 이철원 · 최석진
아주대학교 이철수

1. 서 론

정보통신 기술 및 네트워크 인프라의 발전으로 미래의 전장 환경은 플랫폼 중심에서 통신망과 응용체계가 통합된 네트워크 중심의 지휘통제가 이루어지는 NCW (Network Centric Warfare : 네트워크중심전)로 이동할 것이다. NCW는 현재 미 국방성의 전력변환에 있어 중요한 주제가 되고 있으며 유럽의 여러 국가는 물론 호주나 싱가폴에도 확산되어 군사발전의 중심점이 되고 있다. 우리나라도 NCW 추구의 당위성을 인식하고 한국적인 개념 정립 등 구현을 추진 중에 있어 향후 미래 국방의 중심이 될 것은 자명한 것으로 보인다.

하지만, 네트워크를 통한 정보공유가 핵심인 NCW 환경에서는 위협과 취약성이 급격히 증가하고 이에 수반되는 침해 및 공격 또한 증가할 것으로 예상되고 있어 정보보호 대책의 수립이 절실히 필요한 실정이다.

따라서, 본 논문에서는 미국 정보보증체계의 근간을 이루고 있는 정보보증기술 프레임워크(IATF : Information Assurance Technical Framework)를 모델로 하여 IATF에서 제시하는 정보보호 도메인별로 NCW 추진에 따른 환경변화 및 위협을 식별하고 이에 대한 정보보호 대책을 정책적 · 기술적 측면에서 제시하고자 한다.

2. 본 론

2.1 NCW

미 해군제독이었던 세브로스키(A. K. Cebrowski)에 의해 제시된 NCW는 전장의 여러 전투요소들을 효과적으로 연결하고 네트워킹하면, 지리적으로 분산된 여러 전투요소들이 전장의 상황을 서로 공유할 수 있고, 통합적이고 효율적인 전투력을 만들어내는 새로운 전투개념이다(그림 1).

NCW는 첨단 센서나 정보기술의 진전이라는 관점에서 기존의 전투수행효과 창출 구조를 새롭게 설명하는 하나의 이론이다. 이 이론의 핵심은 그림 2에서 보듯이 소위 센서격자망(sensor grid), 교전격자망(engagement grid), 그리고 정보격자망(information grid)이라고 불리는 3개의 격자망에 있다.

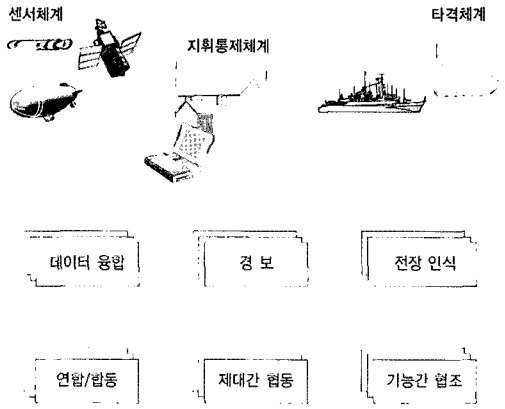

그림 1 NCW 수행 개념도

센서격자망은 여러 가지 다양한 유형의 감시센서들을 연결해서 전장상황을 폭넓게 그리고 적시에 알 수 있게 하고, 교전격자망은 여러 가지 다양한 무기체계들을 통합해서 전투력을 대폭 증가시키는 역할을 한다. 물론 정보격자망은 센서격자망과 교전격자망을 서로 밀접히 연결해서 망 안에 포함되어 있는 모든 감시장비들과 타격 무기체계들을 하나의 장치가 작동하는 것처럼 묶어 주게 된다. 결국, 흔히 플랫폼(Platform)이라 불리는 탱크나 함정, 전투기 등 하나하나의 단위 무

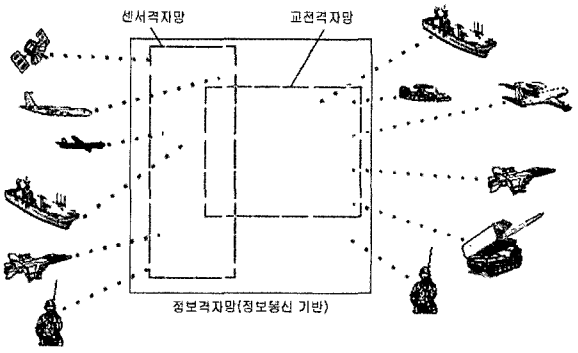

그림 2 NCW개념 구현을 위한 네트워크 구조

기체계의 효과보다 이들 간에 네트워크 연결을 통해 시너지 효과를 창출하고 이 효과를 극대화하는 것이라 할 수 있다.

2.2 IATF

IATF는 美 정부내 보안관련 부서 및 보안 산업체의 요구에 의하여 국가안보국(NSA : National Security Agency)에 의해 개발된 보안지침 문서로서 정보보증 정책, 기술, 환경 등의 내용을 담고 있다.

IATF는 보편적인 프레임워크를 적용하지 않음으로써 발생할 수 있는 정보시스템의 혼란을 해결하고자 그림 3과 같이 지역 컴퓨팅 환경(엔클레이브), 엔클레이브 경계, 네트워크 및 기반구조, 그리고 지원 기반구조의 4개 도메인으로 구분하여 정보시스템의 정보보증기술 양상을 구분하고 프레임워크를 제시하고 있다.

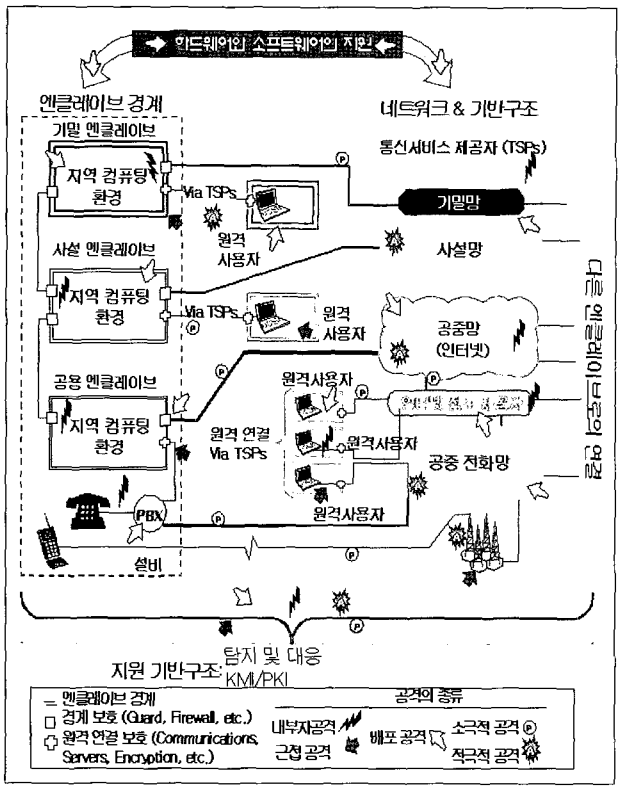

그림 3 IATF 정보보호 도메인

2.2.1 지역 컴퓨팅 환경[1](Enclave)

지역 사용자의 컴퓨팅 환경은 일반적으로 서버, 클라이언트, 서버 및 클라이언트에 설치된 응용을 말한다(그림 4). 대부분의 조직들은 그들의 임무를 수행할 수 있는 다양한 응용을 사용하고 있지만 현재의 컴퓨팅 환경 보안은 주로 운영체제 및 서버와 클라이언트 시스템에 집중되어 있다.

1) 로컬 컴퓨팅 환경 또는 엔클레이브로 지칭하기도 함.

2.2.2 엔클레이브 경계(Enclave Boundary)

엔클레이브는 일반적으로 근거리통신망(LAN)을 통하여 지역 컴퓨팅 장비들과 상호 연결할 수 있도록 묶어 놓은 하나의 지역이며 엔클레이브 경계는 엔클레이브 내부 또는 외부로부터의 정보고 나가고 들어가는 접점이다(그림 4). 각 엔클레이브들은 외부의 네트워크를 통해 다양한 연결이 이루어지기 때문에 엔클레이브 경계 보호막을 설치하여 외부정보의 유입이 조직의 시스템 운용이나 자료에 영향을 미치지 않도록 해야 한다. 엔클레이브 경계보호를 위해 가드(Guard), 방화벽 등이 이용되며, 원격접속으로부터의 보호를 위해 암호화를 사용한다.

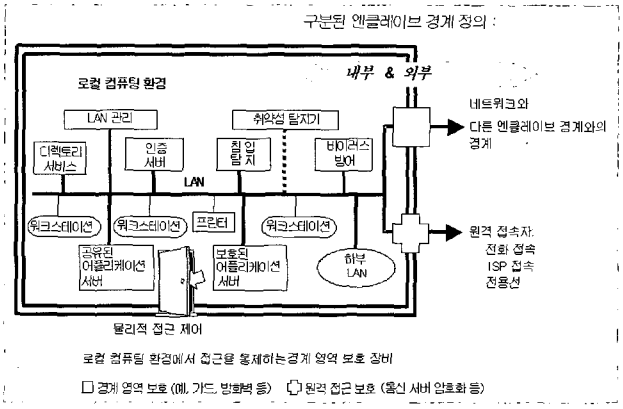

그림 4 엔클레이브와 엔클레이브 경계 도메인

2.2.3 네트워크와 기반구조 (Network and Infrastructure)

네트워크와 기반구조는 엔클레이브로 둘러싸인 지역들 사이에 상호 통신 능력을 제공한다(그림 5). 기반구조에는 운영지역 통신망(OAN : Operational Area Network), 도시권 통신망(MAN : Metropolitan Area Network), 캠퍼스 통신망(Campus Network), WAN, LAN 등이 있다. 네트워크는 또 다른 중요 요소로서 네트워크 관리, 도메인네임서버(DNS), 네트워크 침입탐지시스템(IDS) 및 디렉토리 서비스를 포함한다.

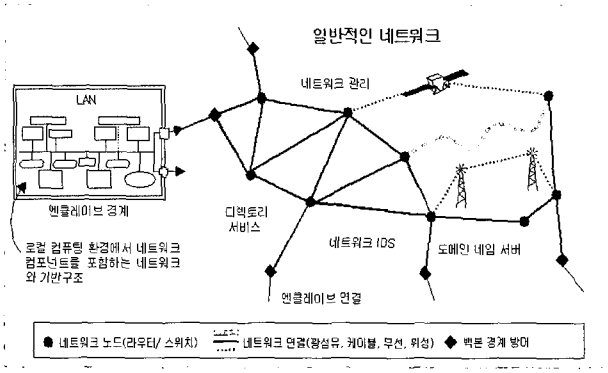

그림 5 네트워크 및 기반구조 도메인

2.2.4 지원 기반구조(Supporting Infrastructure)

지원 기반구조의 역할은 시스템 보안관리와 보안서비스를 위해 네트워크, 엔클레이브 및 컴퓨팅 환경에서 정보보증 메커니즘의 기초를 마련하는 것이다. 즉, 지원기반구조는 네트워크서비스, 컴퓨터 사용자, 웹서비스, 응용, 파일, 도메인네임서버와 디렉토리서비스 등에 보안서비스를 제공한다. 정보보증기술 프레임워크가 제시하는 지원 기반구조는 공개키기반구조(PKI : Public Key Infrastructure)를 포함하는 키관리기반구조(KMI : Key Management Infrastructure)와 탐지 및 대응 기반구조의 두 가지이다.

2.3 환경변화 및 정보보호 위협

NCW 이론은 현재는 물론 미래의 정보통신 기술 발전을 기반으로 하고 있어 적절한 정보보호 대책의 수립을 위해서는 정보통신 환경의 변화 및 이에 따른 취약성·위협의 식별이 선행되어야 한다.

2.3.1 환경 변화

NCW 환경은 현재 뿐만 아니라 미래의 정보통신 기술을 고려하여야 한다. 기존의 정적인 네트워크 환경은 동적인 환경으로 변화할 것이며 M/W망, 위성망 뿐만 아니라 유비쿼터스 환경에서의 센서 네트워크가 통합화 또는 연동되는 환경으로 발전할 것이다. 이처럼 NCW 추진에 따라 예상되는 환경변화를 살펴보면 표 1과 같다.

그림 6에서는 표 1에서 식별된 환경변화 요소들이 IATF에서 제시하는 정보보호 도메인과 어떻게 연결되는지를 도식화 하였다.

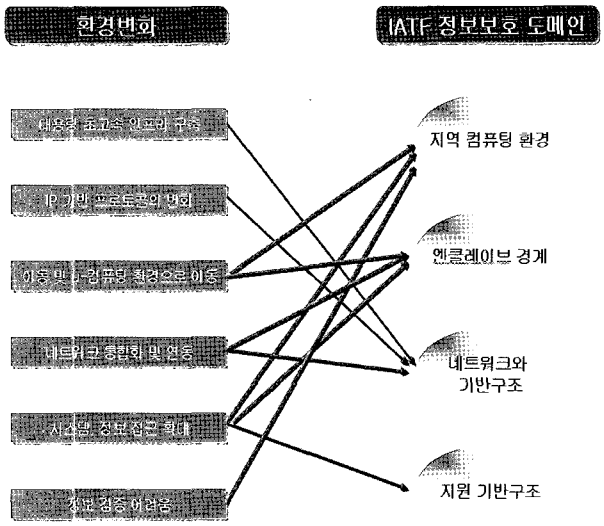

그림 6 환경변화와 IATF 정보보호 도메인과의 상관성

2.3.2 정보보호 도메인별 정보보호 위협 식별

정보보호 대책을 수립하기 위해서 앞에서 식별된 환경변화에 따른 정보보호 위협 및 취약성을 식별이 선행되어야 한다. 다음은 그림 6에서 구분한 정보보호 도메인별 환경변화에 따른 위협·취약성을 살펴보고자 한다.

표 1 NCW 구현에 따른 환경변화

환경 변화	내 용
대용량·초고속 인프라 구축	· 다양한 형태의 정보 제공 및 공유증가 · 정확한 전장상황인식을 위한 영상이나 사진과 같이 대용량 정보 유통 증가 - 유선 인터넷, 유선 통신망, 이동 통신망 및 무선랜 환경이 융합되는 국방 BcN(Broadband Convergence Network) 환경으로의 발전 및 트래픽의 폭발적인 증가를 수반할 것으로 예상됨
IP기반 프로토콜 변화	· 전장 환경에서의 네트워크 가용성, 생존성 및 이동성 보장 요구 증가 - 현재의 IPv4에서 IPv6로의 전이 및 궁극적으로 All IP로의 기반 프로토콜의 전이 예상
이동 및 u-컴퓨팅 환경으로의 이동	· 이동성이 강조되는 전장 환경에서의 정보 공유를 위한 무선 네트워크 기반 및 서비스 구축 필요성 증가 - WiBro, 위치확인서비스, 텔레매틱스 등 · 분산 전장 환경에서의 다양한 정보수집 및 공유를 위해 첨단 센서 네트워크(USN : Ubiquitous Sensir Network) 구축 필요성 증가 - ad-hoc 네트워크와 같은 동적인 네트워크 환경으로 발전 - 센서 전송 정보수집 및 처리를 위한 통신 플랫폼의 다양화 - 다양한 수집정보 처리를 위한 응용 서비스 확대
다양한 네트워크들의 통합화 또는 연동 수준의 혁신적 증가	· 다양한 정보공유를 위한 이기종 망간 연동 및 체계의 상호운용성 보장 필요 - M/W망, 위성망 및 센서 격자망 등의 사용 활성화 및 통합 운용으로 발전 - 비밀 등급별 또는 체계 용도별로 분리·운용하고 있는 다양한 네트워크의 통합화(전략-전술 망간 연동 등)
시스템, 정보에 대한 접근 및 활용 범위 확대	· 전장상황인식 정보와 전력의 통합화를 위해 많은 정보들의 공유 및 유통 체계 개선 필요 - 시스템, 정보에 대한 접근 및 활용 범위가 통합적·광역적으로 확대
정보의 정확성, 신뢰성 검증의 어려움	· 정보 생산 및 트래픽의 폭발적 증가로 인해 정보를 처리하는 사용자(생산자 또는 소비자)에 대한 명확한 예측이 어렵고 단일 시스템을 이용한 모든 정보의 획일적 통제도 어려워 짐

□ 지역 컴퓨팅 환경

표 2 지역 컴퓨팅 환경에서의 위협 및 취약성

환경변화	위협 · 취약성
이동 및 u-컴퓨팅 환경으로의 이동	· 통신 플랫폼의 다양화로 웜·바이러스 등의 악성코드 전파 경로 확산 - 단말에 대한 제어 신호의 위/변조 위협 증가 · 무선 환경 플랫폼의 기술적 제한으로 인한 공유 · 유통 정보의 기밀성, 무결성 침해 가능성 증가 - 동적으로 변화하는 네트워크 환경에서의 보안성 유지 및 관리기반 미비로 인한 정보 침해 가능성 증가 - 공격자 위치의 다양성으로 역추적 어려움
시스템 및 정보 접근 확대	· 인가되지 않은 사용자에 의한 불법적인 시스템 · 정보 접근, 활용 가능성 증가 - 언제 어디서든 정보의 접근이 가능한 환경으로 변화함에 따라 사용자가 비약적으로 증가하는 반면 단위 시스템, 정보 수준에서 사전에 명확히 수많은 사용자들을 정확히 식별하고 인증하기 힘듦 · 대용량 정보의 처리 및 적시 유통을 위한 요구로 인해 적절한 정보보호 대책 적용의 어려움 - 낮은 수준의 정보보호 대책 적용으로 중요 정보 유출 위험 증가 · 다양한 응용으로 인한 트래픽의 폭발적 증가 - 가용성 침해 가능성 증가
정보검증의 어려움	· 폭발적인 정보 유통 및 공유의 증가로 인한 단위 정보의 신뢰성 및 무결성 검증의 어려움 증가 - 잘못된 정보 공유로 인한 사고 가능성 증가

□ 엔클레이브 경계

표 3 엔클레이브 경계에서의 위협 및 취약성

환경변화	위협 · 취약성
이동 및 u-컴퓨팅 환경으로의 이동	· WiBro 서비스 도입 등 상용 서비스 사용 증가 - 상용 표준 보안 서비스(프로토콜) 사용으로 인한 취약성 공개 및 이를 이용한 공격 가능성 증가
네트워크 통합화 및 연동	· 공격 · 침해의 확산 범위 및 속도 증가 - 유기적인 네트워킹 보장을 위한 시스템 연동, 연결의 확대로 인해 공격 및 침입 경로 증가 - 경계 영역 외부의 공격 및 침해가 엔클레이브 내부 시스템으로 쉽게 확산 가능 - 개별 지역보안관제체계로 인한 통합 및 연동망에서의 신속하고 능동적인 위협 대응 미흡 · 망 통합에 따른 연동 노드 지점 자료 유출 증가 · 비화망, 일반망 연동에 따른 비밀통신망 침해 공격 가능
시스템 및 정보 접근 확대	· 인가되지 않은 사용자에 의한 불법적인 시스템 · 정보 접근, 활용 가능성 증가 - 언제 어디서든 정보의 접근이 가능한 환경으로 변화함에 따라 사용자가 비약적으로 증가하는 반면 단위 시스템, 정보 수준에서 사전에 명확히 수많은 사용자들을 정확히 식별하고 인증하기 힘듦 · 다양한 응용으로 인한 트래픽의 폭발적 증가 - 가용성 침해 가능성 증가

□ 네트워크와 기반구조

표 4 네트워크와 기반구조에서의 위협 및 취약성

환경변화	위협 · 취약성
대용량 초고속 인프라 구축	· 네트워크 보안과 관련된 상황 정보의 분석 및 공유 제한 - 정보량의 폭발적인 증가로 트래픽 분석 및 위험요소 판단이 어렵고 필요한 개체에게 필요한 수준에 맞는 분석 정보 배포가 힘듦
IP기반 프로토콜 변화	· IPv6 신규기능의 취약점을 이용한 새로운 공격 발생 가능 - IPv4에서 IPv6로의 전이 과정에서 발생하는 보안 취약점을 이용한 공격 증가 - IPv6 환경에서의 DNS에 대한 의존도 증가 등으로 인한 신규 위험 증대 - 상용 표준 보안 프로토콜의 오버헤드로 인해 전송되는 패킷 크기(수) 증가로 인한 네트워크 트래픽 증가로 네트워크 효율성 침해 및 가용성 위협 증대
이동 및 u-컴퓨팅 환경으로의 이동	· 통신 플랫폼의 다양화로 웜·바이러스 등의 악성코드 전파 경로 확산 - 각 노드에 대한 제어 신호의 위/변조 위협 증가
네트워크 통합화 및 연동	· 네트워크 일부분에 대한 공격 · 침해가 전체 네트워크로 쉽게 확산 - 체계 전체의 보안성은 체계를 구성하는 다양한 구성 요소 중 가장 취약한 요소의 보안성 수준만큼만 안전 - 상대적으로 보안이 취약한 개별망을 통한 침입 위협이 BcN을 통해 통신망 및 USN까지 확산 가능 · 상용 보호 장비 도입 증가 및 다양한 암호장비 적용에 따라 일관된 보안정책 관리의 어려움으로 보안 관리상의 취약점 증가

□ 지원 기반구조

표 5 지원 기반구조에서의 위협 및 취약성

환경변화	위협 · 취약성
시스템 및 정보 접근 확대	· 인가되지 않은 사용자에 의한 불법적인 시스템 · 정보 접근, 활용 가능성 증가 - 인가되지 않은 사용자에 의한 시스템 주요 정보 훼손 및 도용 가능성 증가 · 다양한 응용 체계에서의 서비스 요구 증가 - 정보보호에 대한 지원 기반구조 의존성이 심화됨으로 인해 서비스 요구가 증가하고 이로 인한 가용성 침해 가능성 증가

2.4 정보보호 대책

과거 정보보호의 주요 관심 영역은 정보가 적에게 노출되는 것을 방지하기 위한 기밀성에 중점을 두어 왔다. 하지만 네트워크 기반의 NCW 환경에서는 무결성, 가용성 및 인증 등이 중요한 정보보호 서비스 요소로서 대두되었으며, 최근에는 사이버전과 같은 새로운 위협이 대두됨에 따라 해킹, 바이러스 등과 같은 사이버 공격에 대한 탐지, 차단, 대응 등의 중요성이 강조되고 있다.

위협 및 취약성에 대한 정보보호 대책은 크게 정책적인 측면과 기술적인 측면으로 고려할 수 있다. 본 절에서는 식별된 위협 및 취약성에 대한 정보보호 대책을 정책적인 측면과 IATF 정보보호 도메인별로 요구되는 기술적 측면에서 살펴보고자 한다.

2.4.1 정보보호 정책

표 6 NCW환경에서의 정보보호 정책

정책	내용
체계적인 국방 정보보호 추진 전략 수립	· 네트워크와 시스템을 안정적으로 보호 및 방어하기 위해서는 제반 정보보호 역량과 기능을 중앙 집중적으로 관리하고 지속적으로 그 성능을 개량해야 함 - 공통 네트워크, 시스템 방어 아키텍처 정립 및 이를 기반으로 하는 일관성 있는 국방 정보보호 체계 구축 필요 · 효율적 · 체계적인 정보보호 정책과 추진 전략 수립 필요 - 단위 시스템, 데이터 수준에 이르기까지의 정교한 통제가 가능한 지침과 가이드라인의 개발 · 보급이 필요
미래 정보보호 체계 구축과 현재 정보보호 대책의 동시적 진행	· 단기적으로 표준 프로세스 개발과 병행하여 현재의 제반 보안성관리 활동들의 내실화를 위한 노력 필요 - 체계적인 보안대책 수립 지원을 위한 기준 정립 - 체계 개발 과정 중의 보호 기능 구현과 검증 활동 강화 · 중 · 장기적으로 표준 프로세스를 국방정보체계의 보안성관리를 위한 기본적인 업무 활동 요구사항으로 시행 - 체계 보안성의 지속적 유지, 관리를 위해 표준 프로세스를 공식적인 인증·인가 프로세스로 발전시켜야 함
사이버 공격의 예방 및 대응 역량 강화	· 사이버 공격과 침해 행위를 적시에 탐지, 차단하고 적절히 대응하는 예방 및 대응 역량의 강화가 중요 · 기술적 측면 - 현재 국방전산망 환경에 국한되어 있는 국방통합보안관제체계를 전략·전술망 환경과 인터넷망 환경까지 확장 필요 - 네트워크 중심의 관제 범위를 주요 시스템, 단말까지 확대하고 향후 NCW 추진에 따른 국방정보통신망 환경 변화에 따라 조정 및 발전 필요 - 현재의 초보적인 관제체계의 탐지, 분석 기능을 실질적 대응 활동 지원이 가능한 심화수준으로 향상시킬 필요 있음 · 조직 · 절차적 - 사이버 공격 탐지, 대응 활동을 군사작전 지원을 중심으로 한 통합적인 프로세스로 발전 - 정보작전(IO : Information Operation), 사이버전 대응, 컴퓨터네트워크방어(CND : Computer Network Defense) 등과 같은 사이버 공격 탐지·대응과 관련된 개념들 및 유관 업무 프로세스의 재정립 및 국내 환경에의 적용 필요
탄력적인(flexible) 암호기술 · 장비 개발 및 활용 확대	· H/W 암호기술·장비 위주의 정책을 S/W 기술이 병행적으로 활용 가능하도록 정비 필요 - 유기적으로 변화하는 동적인 네트워크 환경에서는 비용적 측면과 암호기술·장비들을 설정, 관리적 측면의 어려움으로 H/W 위주의 현 국방정보보호 체계로는 지원이 제한 됨 - 미국의 경우도 NCW 환경에서 요구하는 요구사항을 만족시키기 위해, 기존 H/W 위주의 장비, 시스템에서 S/W 기술을 적극적으로 활용하고 있음 - 이를 위해 프로그램밍 가능하고, 내장가능한 암호기술·장비의 개발을 추진 중에 있음

2.4.2 정보보호 요소 기술

□ **지역 컴퓨팅 환경**

표 7 지역 컴퓨팅 환경에서의 정보보호 기술

위협 · 취약성	정보보호 기술
통신 플랫폼의 다양화로 웜·바이러스 등의 악성 코드 전파 경로 확산	· 모바일 운영체제 보안 기술 · 모바일 악성코드 분석 기술
무선 환경 플랫폼의 기술적 제한으로 인한 공유·유통 정보의 기밀성, 무결성 침해 가능성 증가	· 소형 저전력 암호칩 설계 기술 · 디지털 증거 획득·분석 및 소프트웨어 역공학 기술 적용 · 공격 근원지 추적 기술 · 네트워크 전송 프로토콜 분석 기술 · 스캐닝 공격 대응 기술 · 네트워크 트래픽 정형화 기술
인가되지 않은 사용자에 의한 불법적인 시스템·정보 접근, 활용 가능성 증가	· 국방 전사적 차원에서의 신원 및 권한 관리 기반체계 구축 - 공개키 기반의 국방 인증체계와 연동 - 무선 및 이동 환경 지원 역량 강화
대용량 정보의 처리 및 적시 유통을 위한 요구로 인해 적절한 정보보호 대책 적용의 어려움	· 고속 암호처리 기술
다양한 응용으로 인한 트래픽의 폭발적 증가	· 사이버공격 탐지 기술 · 대용량 트래픽 분석 및 정형화 기술 - 하드웨어 기반 고속 패킷 처리 기술 - 대용량 네트워크 패킷의 백업 및 분석 기술
폭발적인 정보 유통 및 공유의 증가로 인한 단위 정보의 신뢰성 및 무결성 검증의 어려움 증가	· 사이버공격 탐지 기술· 대용량 트래픽 분석 및 정형화 기술 · 국방 KMI 체계 구축 - 안전한 암호키 관리 체계 구축 - KMI 시스템 안전성 확보를 위한 암호장비 연동 - 초고속·대용량 네트워크 환경을 수용할 수 있는 성능 확보가 관건 · 암호장비 연동 보안 게이트웨이 기술· 이종 암호체계 변환 기술

□ **엔클레이브 경계**

표 8 엔클레이브 경계에서의 정보보호 기술

위협 · 취약성	정보보호 기술
WiBro 서비스 도입 등 상용 서비스 사용 증가	· 국방 전용 프로토콜 개발 · TICN 무선 통신 계층 보안 기술·휴대 인터넷 데이터 채널 보안 기술 - 위성 통신 채널 보안 기술 - 광대역 무선 채널 보안 기술 - 이동 단말/노드 보안 터널 관리 기술 · 상용암호시스템 안전성 검증 기술 · USN을 위한 ad-hoc 네트워크 보안 기술· 통신 보안 프로토콜 기술 - 센서 노드 인증 기술 - 미들웨어 보안 기술
공격·침해의 확산 범위 및 속도 증가	· 사이버공격 탐지 기술· 대용량 트래픽 분석 및 정형화 기술
인가되지 않은 사용자에 의한 불법적인 시스템·정보 접근, 활용 가능성 증가	· 국방 전사적 차원에서의 신원 및 권한 관리 기반체계 구축 - 권한 기반 데이터/시스템 접근 제어 기술 · 비화/非비화 망간 연동을 위한 보안 가드·응용 체계 간 프로토콜 변환 기술
다양한 응용으로 인한 트래픽의 폭발적 증가	· 공격 근원지 추적 기술 · 네트워크 전송 프로토콜 분석 기술

□ **네트워크와 기반구조**

표 9 네트워크와 기반구조에서의 정보보호 기술

위협 · 취약성	정보보호 기술
네트워크 보안성 상황 정보의 분석 및 공유 제한	· 광대역통합망(BcN) 정보보호 기술 - BcN 생존성 보장 기술 · 암호장비 통합 보안 관제 기술· 다중 플랫폼 보안 에이전트 기술 - 다중 에이전트 관리 기술 - 보안관제 통신 프로토콜 기술 - 종합 분석/대응 플랫폼 기술 · 사이버위협 예측 기술 - 데이터 마이닝 기술 - 데이터 연관성 분석 기술 - 트래픽 정보 시각화 기술
IPv6 신규기능의 취약점을 이용한 새로운 공격 발생 가능	· IPv6 환경의 침해 차단 기술 · IPv6 트래픽 제어 기술 - IPv6 확장헤더 처리 기술 - IPv6 공격 차단 기술 - DNS 보안 관리 기술 · IPv6 보안 프로토콜 기술· IP 계층 보안 프로토콜 기술 - 보안 터널 이동성 보장 기술 - IPv4/IPv6 연동 보안 터널 관리 기술
네트워크 일부분에 대한 공격·침해가 전체 네트워크로 쉽게 확산	· 이기종 망 관리 및 분리 기술 - 이기종망 연동 게이트웨이 침해 대응 기술 · 암호장비 연동 보안 게이트웨이 기술· 이종 암호체계 변환 기술 · 비화/非비화 망간 연동을 위한 보안 가드 · 응용 체계 간 프로토콜 변환 기술 · 이종 네트워크 분리 기술
상용 보호 장비 도입 증가 및 다양한 암호장비 적용에 따라 일관된 보안정책 관리의 어려움으로 보안 관리상의 취약점 증가	· 상용암호시스템 안전성 검증 기술

□ **지원 기반구조**

표 10 지원 기반구조에서의 정보보호 기술

위협 · 취약성	정보보호 기술
인가되지 않은 사용자에 의한 불법적인 시스템 · 정보 접근, 활용 가능성 증가	· 국방 KMI 체계 구축
다양한 응용 체계에서의 서비스 요구 증가	· 국방 KMI 체계 구축

3. 결 론

국방 정보보호의 미래 전략인 NCW의 핵심은 초고속 · 대용량 백본망을 기반으로 한 유비쿼터스 환경에서의 이동 · 분산 컴퓨팅 및 통합화 · 융합화를 통한 정보공유이다. 이러한 환경의 변화는 정보의 유통 및 공유에 대한 신뢰성 및 가용성을 보장하는 한편 침해의 광범위화 및 고속화를 가속화 시킬 것이다.

NCW가 미래 국방의 중심이 되리라는 것은 분명하지만 충분한 안전성, 보안성을 전제할 수 있어야만 의미가 있다. 따라서, 본 논문에서는 NCW가 가져올 수 있는 미래 환경변화 및 위협요소를 식별하고 이에 대한 정보보호 대책을 정책적인 측면과 기술적인 측면에서 제시하였다.

아직까지 NCW는 다분히 이론적이며 한국적 NCW 추진 방향도 명확히 정립되지 않은 실정이다. 미래를 예상하여 대응책을 마련하는 것이 정책의 기본 목적임을 고려할 때 본 논문은 미래 국방 정보보호를 위한 초석으로 활용될 수 있을 것이라 판단된다. 하지만 향후 NCW의 개념이 명확히 정립되고 정보기반구조의 실체가 명확해지는 시점에서 좀 더 체계적인 정보보증 프레임워크 연구가 필요할 것으로 본다.

참고문헌

[1] "IATF : Information Assurance Technical Framework, Release 3.1", National Security Agency, Sep. 2002.

[2] Arthur K. Cebrowski & John J. Garstka, "Network-Centric Warfare : Its Origin and Future", U.S. Naval Institute Proceedings, Jan. 1998.

이 철 원

1987년 충남대학교 수학과(이학사)
1989년 중앙대학교 전자계산학과 (이학석사)
2001년 아주대학교 컴퓨터공학과 박사과정 수료
1989년~1996년 한국전자통신연구원 선임연구원
1996년~2000년 한국정보보호진흥원 선임연구원, 과제책임자
2000년~현재 ETRI부설 국가보안기술연구소 실장, 책임연구원
관심분야 : 컴퓨터 및 네트워크 보안, 정보통신기반보호, 정보보호시스템 평가
E-mail : cheolee@etri.re.kr

최 석 진

1995년 경북대학교 전자공학과(공학사)
1998년 한국과학기술원 전기전자공학과 (공학석사)
1998년~2000년 하이닉스 반도체 메모리사업부 연구원
2000년~현재 ETRI부설 국가보안기술연구소 선임연구원
관심분야 : 컴퓨터 및 네트워크 보안, DRM
E-mail : choisj@etri.re.kr

이 철 수

1973년 서울대학교 공과대학 응용수학과 (학사)
1979년 서울대학교 자연과학대학원 전자계산학과(석사)
1984년 미국 Kansas State University 전자계산학과(박사)
1986년~현재 IEEE : 802.4.802.6, 802.10 Working Group Member, Asiacrypt '96 조직위원회 위원장, 건설교통부 항공교통관제소 신항공 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국통신정보보호학회 부회장 역임
1979년~현재 아주대학교 정보 및 컴퓨터공학부 교수
관심분야 : 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링