情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

# 군 통합보안시스템 구축 방안 연구

장 월 수,† 최 중 영, 임 종 인‡
고려대학교 정보보호대학원

# A study on method of setting up the defense integrated security system

Worl-Su Jang,† Jung-Young Choi, Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

군의 정보화, 과학화 추진에 따른 환경 변화에 따라 기존 수작업, 오프라인 중심의 제반 군사보안 업무도 효율적이고 체계적인 업무 수행을 지원할 수 있도록 변화와 발전이 필요하다. 이에 본 연구에서는 주요 군사보안 업무 분야에 대한 실태 및 문제점 분석과 미국, 영국 등의 사례 분석을 기반으로, 주요 군사보안 업무를 자동화, 정보화하기 위한 국방통합보안시스템 구축 표준 Model을 제시하였다. 표준 Model은 통합보안체계, 비밀관리시스템, 인원출입 시스템, 차량출입시스템, 첨단경계시스템, 테러 예방시스템 및 보안사고분석시스템 등의 단위 시스템으로 구성되며, 현재 가용한 기술 및 시스템을 기반으로 제안하였는데, 이를 각급부대에 적용할 경우 군사보안 발전에 기여할 것으로 기대된다.

ABSTRACT

A established military security tast based on existing manual and off-line needs the change and development to support effective and systematic task performance according to environment change of informational and scientific project in the military. Therefore this study suggests to set up the standard model of the defense integrated security system to automate and informationize major defense security task based on actual and problem in the area of major defense of security task and case analysis of these in America, England and other countries. The standard model consist of unit systems were made up integrated security system, security management system, man entrance system, vehicle entrance system, high-tech guard system, terror prevention system and the security accident analysis system, and this suggested model based on possible technology and system. If this model is apply to each real military unit, we will expect the development of defense security.

**Keywords**: Integrated security, Security management, Facilities security, Information and Communications security, Terrorism, Security accident

## I. 서 론

작금의 세계는 자국의 이익과 안보를 위해 최첨단 보안시스템을 구축하고 있을 뿐만 아니라 인공위성 및 인터넷 등을 통해 제반 정보를 수집하고 있다. 이와 관련해서 기술도 고도화・첨단화되어 가고 있기 때문에 군의 보안수준 향상은 필수적이고 보안요소를 통합하여 즉각 대응할 수 있는 체계를 구축해야 한다.

우리나라는 국가의 보안업무를 체계적으로 수행하기 위해 1964년 보안업무규정을 대통령령으로 제정하여 시행하고 있다. 이에 군에서도 1965년 군사보안업무 훈령을 제정하여 전군과 방산관련 업체 등에서 적용하고 창의적으로 발전시키고 있다.

접수일(2012년 1월 12일), 수정일(2012년 4월 4일), 게재확정일(2012년 4월 6일)
† 주저자, jworls@hanmail.net
‡ 교신저자, jilim@korea.ac.kr

〔표 1〕 비밀 생산·관리 문제 사례

| 구 분 | 세 부 문 제 사 례 | 비고 |
|---|---|---|
| 개 인 | - 비밀문서 후면에 비밀등급을 표시하지 않거나 평문자료에 까지 비밀 표시<br>- 대외비 문서 상단에 '대외비' 표시를 하지 않는 등 비밀 표시 규정 미 준수<br>- 비밀 관리번호 중 개인번호를 숫자로 표기해야 하나 알파벳으로 부여<br>- 비밀 수정 문을 평문으로 하달하고 접수 부서에서 접수 후 수정하지 않고 방치<br>- 비밀관리기록부 행정 부실 및 보관 기준 5년 미준수로 추적 불가<br>- 비밀이력카드에 비밀 이력 사항 14가지를 기록하도록 되어 있는데 일부 미작성 | 부대 마다 보안 수준 차이 있음 |
| 관리자 | - 접수 비밀을 결재도 하지 않고 관리번호도 부여하지 않고 방치<br>- 비밀관리기록부 갱신 후 내용을 기록하지 않았고 보관책임관 '정'의 서명 누락 | 보안 전문성 다소 부족 |
| 보안부서 | - 보안행정 시행여부 확인·감독 부실 및 비밀 분실에 대해서도 파악 불가 | " |

반면, 비밀을 생산, 관리, 사용, 이관 및 파기하는데 필요한 보안관련 대장 6종류와 비밀이력카드 14가지를 44년 前과 동일 개념으로 수작업으로 작성하고 있으며 모든 출입자 통제와 경계에 대해서도 인력에 의존하고 있어 보안취약점이 다수 발생하고 장병들이 불편해함은 물론 향후 병력감축에 따른 제반 보안취약점도 예측되고 있는 실정에 있다.

선진군의 경우 몇 십 년 전부터 보안의 첨단화 및 과학화를 수립하여 시스템에 의한 보안 관리를 수행하고 이에 따른 전담인원들의 전문화를 강화하여 자국의 비밀보호 및 핵심시설 경계에 만전을 기하고 있다. 특히, 첨단 보안기술이나 해제된 국가비밀을 해외에 수출하여 자국의 산업발전에도 이바지하고 있어 국민들로부터 신뢰를 득함과 동시에 보안시장 확대를 추진하고 있다.

최근 우리의 일부 부대에서는 문서·인원·시설·정보통신 보안 분야와 테러 대비시설 등의 문제점을 진단한 데 이어 보안 Master Plan을 수립하여 미래전(NCW)에 대비하고 있다. 또한, 창군 이래 최초로 On-Off Line 비밀관리시스템을 도입할 수 있는 개념을 정립·구축하여 보안수준을 획기적으로 향상시켰다. 아울러, 인원·차량출입은 One Card로 全軍을 출입하고 미래 현역병 부족과 위민국방 구현을 위해 모든 출입문의 1차 검색은 민간청경에 의거 실시하며 핵심시설과 2차 검색에 대해서만 헌병이 임무를 수행하여 경제성과 보안성을 높이는 방향으로 보안정책을 발전시켜 나아가고 있다.

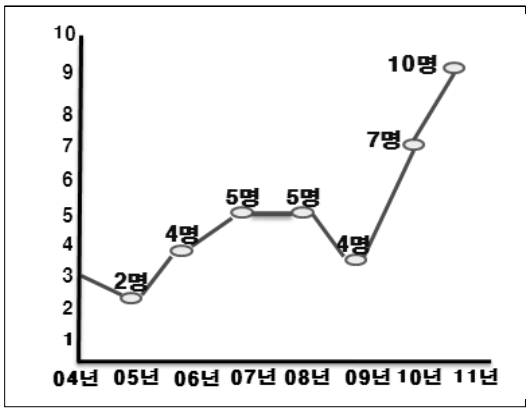
본고에서는 군의 보안실상과 문제점을 보안 분야별로 고찰하고 미국과 영국의 주요기관들이 국가의 핵심자료 및 시설 등을 보호하기 위해 수립하여 구축·운영 중인 보안정책과 국내 대기업들의 보안대책 사례를 분석하였으며 이를 근거로 군 통합보안시스템 표준 Model 및 구축 방안을 제시하였다.

## II. 군의 보안실태 및 문제점

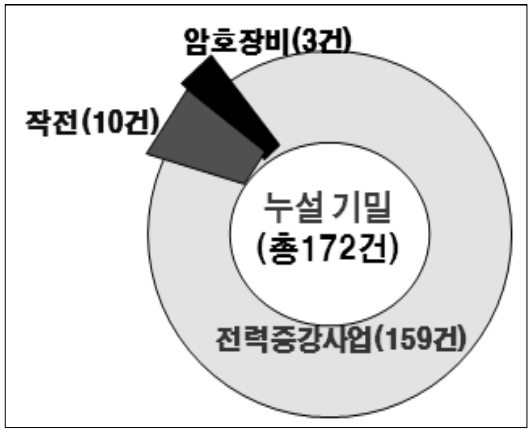
### 2.1 문서보안 측면

문서보안이란 모든 비밀을 비인가자, 외국인 및 업무상 관련 없는 인원에게 절취, 탐지, 열람 등의 방법을 통하여 누설되는 것을 미연에 방지하는 필요한 보안대책이다[1]. 군의 첨단화·과학화로 정보통신보안의 비중이 커지고 있지만 군사보안의 핵심은 비밀을 생산·관리하는 문서보안이다. 비밀을 체계적으로 관리하기 위해 군사보안업무훈령에 생산, 관리, 파기 및 이관 등의 제반 절차를 명시해 놓았는데 이에 대한 문제 사례들을 정리하면 〔표 1〕과 같다.

이러한 문서보안의 문제점이 발생하게 된 원인은 세 가지이다. 첫째, 보안행정이 비밀 생산으로부터 파기 및 존안에 이르기까지 복잡하면서 전산화가 되어 있지 않아 개인들이 준수하기 어렵기 때문이다. 둘째, 비밀분류 시 미국처럼 문장 단위로 비밀을 분류하면 쉽지만 우리군은 쪽 단위로 분류하여 판단이 곤란한 경우가 발생한다. 셋째, 개인이 보관·관리해야할 비




〔그림 1〕 年도별 군사기밀보호법 위반자 40명




〔그림 2〕 2004년 이후 누설 기밀 유형별 현황

밀을 위임하거나 절차를 준수하지 않기 때문이다.

또한, 이러한 보안 취약점으로 인해 중요 보안사고는 〔그림1〕 와 같이 계속 증가하고 있다. 군 최고위급 장성부터 영관급・위관급 장교는 물론 부사관과 사병 출신에 이르기까지 군사기밀을 빼내는 데는 지위고하가 따로 없었다. 이들이 빼돌린 Ⅱ~Ⅲ급 군사기밀 수백 건 중에는 〔그림2〕 와 같이 전력증강 사업과 이에 따라 새로 도입하려는 최신 무기들, 청와대와 군수뇌부의 군사전략 회의 내용, 암호장비는 물론 심지어 한반도 전쟁발발 시 투입 전투기와 미사일 규모도 포함돼 있었다〔2〕.

### 2.2 시설보안 측면

맥아더 장군은 "작전에 실패한 지휘관은 용서할 수 있어도 경계에 실패한 지휘관은 용서할 수 없다"라는 명언을 남길 정도로 군에서의 시설보안은 매우 중요하다. 첨단보안시스템을 구축하면서 부대별로 수십억이 소요되기 때문에 투자대 효과 및 유지보수 등이 매우 중요한 이슈로 나타나고 있다.

각급부대에서는 병영시설 Master Plan 수립 시 복지시설, 전투근무지원시설 및 작전시설 등으로 구분하고 외부인들을 통제하는 보안정책을 반영해야 하나 그렇지 못한 상태에서 병력을 투입하여 다수의 경계인력이 소요되고 이에 따른 장병들의 경계 부담과 피로도가 높아지고 있다.

또한, 기존 설치된 첨단보안시스템인 적외선 센서, CC(폐쇄회로)TV, 인원・차량출입 게이트 및 리더기 등도 대부분 노후 된 상태이며 각 軍별로 통일된 표준 보안정책 없이 구축하여 호환이 되지 않을 뿐만 아니라 시스템 구축 방법과 운영 개념도 미흡한 실정이다〔3〕.

일부 부대의 경우 첨단보안시스템을 운영하면서 중앙통제실에서 대부분 감시할 수 없는데 다 명확한 감시 정책도 정립되어 있지 않고 시스템을 분산 설치하여 보안의 강도가 저하되는 결과를 초래하고 있다.

특히, 시설보안관련 외래인 출입대장, 신청서, 근무명령서 및 순찰일지 등을 수작업으로 작성하고 있어 경계에 치중하기보다 행정 정리 등에 많은 시간을 소비하고 있는 실정이므로 전산화가 필수적으로 이루어져야 한다.

### 2.3 정보통신보안 측면

정보통신보안은 군의 과학화와 네트워크 중심전(Network Centric Warfar)으로 발전되어 가면서 보안의 중요성은 한층 증가되고 있으며 제반 시스템 구축 시 보안대책 강구는 필수적이라 할 수 있다.

그러나, 인터넷 PC에 비인가 프로그램(한글 2002 프로그램, 네이트 온, 곰 플레이어 등)을 설치하여 사용하고 PC 화면보호용과 최초 부팅 비밀번호까지 운용하지 않은 경우가 있으며 특히, 군사자료를 다량 저장・활용하는 등의 취약점이 표출되었다.

또한, 비밀 생산 및 보조기억매체 사용 규정을 준수하지 않고 있었는데 네트워크(인트라넷 망)가 연결된 PC로 비밀을 생산하고, 비밀작업용 USB 內 비밀 및 일반용 폴더를 구분하지 않았으며, 비밀작업용 디스켓 內 평문 자료를 저장하고, 비인가 보조기억매체를 무단 반입하는가 하면, 개인 PC 하드디스크 內에 생산중인 비밀을 저장하고 있으며, 보조기억매체 內 음성비밀을 보관하는 등의 문제점이 표출되었다.

아울러, 군사보안업무 훈령에 의거 노트북에 저장된 자료는 목록을 유지하도록 되어 있으나 유지하지 않았고 노트북에 지키미 프로그램 저장된 자료에 대한 암호화와 비인가 저장매체 접속차단 기능이 있어 군에서만 사용하는 프로그램이다.

을 설치하지 않았으며 디스켓 관리자도 명시하지 않는 데다 보조기억매체가 저장된 각 파일의 비밀번호를 동일하게 설정하는 등의 보안상 취약점이 표출되었다.

## III. 국외 주요기관 보안대책 사례

외국의 군사시설 사례는 미국 국방성(Pentagon),

전시시설인 마운틴 벙커, 공군 우주사령부 및 영국 공군사령부 등 4개 부대에 대한 보안대책을 파악하였다. 4개 부대의 출입시스템, CC(폐쇄회로)TV, 방호시설 및 기타 특수 시설 등을 비교하면 〔표 2〕와 같다. 또한, 비밀원본을 다량 보관하고 있는 미국 국가기록관리청(NARA)의 보안설계 방법과 첨단보안시스템 설치 현황을 파악하였다.

### 3.1 미국의 군사시설 보안시스템 구축

미국 Pentagon, 전시시설인 마운틴 벙커 및 공군 우주사령부에 대해서 정리하였다. 먼저 Pentagon은 2차 세계대전 중 16개월 만에 완료하였으며 특징은 근무자들이 업무차 한 사무실에서 다른 곳으로 걸어서 이동하는데 7분 이내 도달할 수 있도록 설계하였다.

더욱이, 건물형태를 오각형에 5개의 링으로 설계하여 건물 폭격 시 부분 파손만 이루어지도록 방호대책을 강구함과 아울러, 링 단위로 되어 있어 독립된 부대(기관)에게 구획단위로 할당함으로서 보안통제가 용이하고 외부인들이 들어 올 수 있는 부분을 지정하여 철저히 통제하였다. 특히, 9·11테러 이후 제반 사업은 국방관련 산하기관에서 할 수 있도록 조정하여 국방성 內의 보안수준을 한층 향상시켰다〔4〕. 다음으로 全 세계 방공망 감시와 전시 지휘시설인 마운틴 벙커는 주요 출입구가 1개이고 주변이 고압선 울타리로 차단되어 있을 뿐만 아니라 출입 전에 금속탐지기로 몸을 수색하며 보안교육 후 개인 사물은 보관하도록 조치하여 사전 보안취약 요인을 차단한다. 출입자에 대해서는 카메라가 지속적으로 추적하면서 녹화하도록 되어 있고 폭격 시 충격 완화로 전산장비 보호를 위해 벙커內 시설물을 전체 스프링으로 지탱하도록 구축하였다.

또한, 미군 우주사령부도 보안을 고려하여 출입구를 1개만 설치하고 출입자는 1회 1인만 통과할 수 있는 게이트 15개를 설치하고 외부인은 안내가 없으면 절대 출입이 불가하도록 했다. 특히, 보안관련 모든 권한이 보안담당인 부사관(상사)에게 있어 지휘관이나 상급자들도 사진촬영 및 외부인을 출입시키고자 할 때에는 하급자에게 사전 승인을 받고 시행하고 있다〔5〕.

### 3.2 영국의 군사시설 보안시스템 구축

영국 공군 사령부 벙커의 경우도 〔표 2〕와 같이 보안을 고려하고 출입자들을 완벽히 통제하기 위해 출입구는 1개이며 모든 출입자에게 금속탐지기로 몸을 수색하고 소지품은 소지할 수 없도록 보안조치 후 안내자와 함께 1회 1人만 출입할 수 있는 철재 게이트로 통제한다. 승인을 받은 출입자라도 이동하는 경로를 추적용 카메라가 지속 녹화하며 출입 불가지역에 도달하면 경고와 함께 근무자가 조사·확인하는 개념으로 운영되고 있었다. 중앙통제실에서는 근무자 3명이 24시간 모니터링을 실시하고 영상장비, 각종센서, 화재수신반, 화생방 경보시스템 및 기타 보안시스템을 통합하여 구축·운영 중에 있었다〔6〕.

### 3.3 미국 국가기록관리청(National Archives Ⅱ)

Archive Ⅱ는 종이 기록물, 지도, 그림, 사진, 필름 및 전자기록물 등을 광범위하게 보존하고 있으며,

〔표 2〕 美·英 군사시설 보안대책 비교

| 구 분 | 출입시스템 | CCTV | 방호시설 | 기타 특수시설 |
|---|---|---|---|---|
| 美 국방성 Pentagon | ●금속 탐지기 몸수색<br>●사무실 카드 설치<br>●출입인원 최소화 | ●통로 코너<br>●주요 사무실<br>●건물 외곽 | ●오각형 5개 링<br>●신속한 대피<br>●폭격 대비 | ●도청예방(템페스트 설치)<br>●화생방 설비<br>●대피위해 동선 단축 |
| 美마운틴벙커 (전시 지휘소) | ●금속 탐지기 몸수색<br>●사무실 카드 설치 | ●통로 코너<br>●주요 사무실 | ●산7부 능선에 지하로 건립 | ●건물하부 충격완화용 스프링 설치<br>●울타리에 고압선 설치<br>●화생방 방호 설비 |
| 美 공군우주 사령부 | ●카드키 설치<br>●1회1인 통과 15개 문 | ●건물 외곽 | ●상황실만 지하<br>●기타 지상위치<br>●방호시설 無 | ●건물의 主 출입구외 외부 연결문 無 |
| 영국 공군 사령부 벙커 | ●금속탐지기로 몸수색<br>●카드키 설치<br>●1회1인 통과 문 | ●지하통로 (이동 추적)<br>●주요 사무실 | ●벙커<br>●1,000B/L폭격 대비 설계 | ●화생방 방호 설비<br>●자료 유출 방지문 설치 |

이들 기록물 중에는 민감하고 기밀이 유지되어야 할 뿐만 아니라 역사적으로 중요한 가치를 갖는 유물이기 때문에 절도, 외부 공개, 스파이 활동, 파괴 행위 등과 같은 위협으로부터 보호해야 한다[7].

이러한 중요성을 감안하여 건물을 신축할 때부터 4단계로 구분하는 보안설계(Security Design)를 별도로 실시하였다. 먼저, 1단계지역인 공공영역(Public Area)은 모든 방문자가 보안체크 없이 쉽게 접근할 수 있는 강당, 회의실, 식당, 편의점, 연구자 라커룸 등이 해당된다. 2단계지역으로 업무영역(Offices)은 반드시 보안체크 지점을 통과해야하는 구역이다. 3단계지역으로 비공공영역(Non-Public Areas)은 기록물 보존영역, 기록물 처리실 및 연구실 등 리더기가 설치된 구역이다. 4단계지역으로 연구센터(Research Center)은 기록물의 보호를 위해 연구과정 동안 직원이 지속적인 통제(감시)가 요구되는 지역이다.

또한, 최첨단보안시스템을 아래 [그림3] 과 같이 중앙통제실을 중심으로 물리적 보안, 전자보안, 접근조절시스템 및 CCTV시스템을 통합 구축하여 24시간 모니터링 하도록 되어 있다. 특히, 미국인의 신고 정신을 감안하여 보안취약점 및 기록물 유출자 등을 신고할 수 있도록 서고 입구, 업무처리실 및 계단, 통로에 전화기를 비치하였다.

## IV. 군 통합보안시스템 구축 방안 제시

통합보안시스템 구축 방안은 군의 낙후된 보안시스템 현실을 보완하기 위해 선진군의 군사시설 보안대책 사례와 상용화된 첨단 보안장비를 융합하여 MP (Master Plan)를 제시한다. 이러한 구축으로 인해, 군의 보안수준 향상은 물론 인원·예산 절감에 기여하고 보안관계관들의 업무의 편리성을 도모하는데 있다.

### 4.1 시스템 구성

통합보안시스템 구성은 국방부(사이버방호정책과)에서 전군 보안활동 분야를 조정·통제할 수 있어야 한다. 보안사고 분석시스템을 통하여 비밀 유출 사항을 실시간으로 전파·대책을 강구한다. 보안업무 분야별로 담당자들이 모니터링 해야 한다. 각급부대 차원에서는 보안담당관이 인원차량출입통제, 경계시스템 관리, 저장매체관리, 비밀관리 및 기타 보안행정 등을 수행한다. 이러한 모든 보안업무를 제대별로 통합하여 상호 공유하고 대처하도록 하는 것이 통합시스템의 목표이다. 또한, 통합보안시스템 구축을 위한 몇 가지 전제 조건이 있다. 첫째, 관리적인 보안측면에서 순수 보안업무 부서, 정보보호 부서, 경비팀 및 보안지원기관 등의 협조가 있어야 한다. 둘째 기술적인 보안측면에서 각군의 보안시스템, 서버이중화, 정보보호시스템, 암호장비 및 인사정보체계 등이 호환되도록 구축되어야 한다. 셋째, 제도적인 측면에서 주둔 지역內에 있는 전 기관의 규정 및 제도가 일원화되어야 한다는 것이다.

### 4.2 통합보안시스템 구축을 위한 우선 조치사항

선진국 사례에서도 살펴보았듯이 첨단보안시스템을 구축하기 前에 최우선적으로 물리적 및 방호적인 측면


[그림 3] Archive II통합보안체계 구성도

〔표 3〕 주요시설별 보안정책 개념

| 구 분 | 출입통제 및 장치설치 개념 |
|---|---|
| 1 단계<br>(핵심시설 지역) | o 통제구역(정책 입안지역, Ⅰ급비밀 생산/회의실, 암호실, SCIF, C4I실 등)<br>o 첨단보안SYSTEM+인원에 의한 출입통제, 인가자만 출입 |
| 2 단계<br>(중요시설 지역) | o 제한구역(비밀 보관함이 위치한 건물지역 등)<br>o 첨단보안SYSTEM+외래인의 비밀보관 사무실 출입 불가 |
| 3 단계<br>(지원시설 지역) | o 통제구역 및 제한구역 업무를 지원하는 시설물<br>o 출입증을 교부받은 자는 출입허용 |
| 4 단계<br>(복지시설 지역) | o 민원실, 편의시설, 종교시설, 안내실, 체력단련장 등<br>o 일반인은 신분증만 제시 후 자유롭게 출입 |

에서 보안설계를 〔표 3〕과 같이 4단계로 구분하여 실시해야 한다. 이러한 보안설계가 이루어진 이후 첨단 보안시스템을 주요 '목'지점에 구축했을 때에 인력·예산 절감 효과뿐 아니라 보안수준을 높일 수 있다〔8〕.

### 4.3 보안사고 분석System

군에서는 매년 고질적인 보안사고가 발생하는데 이는 대부분 장병들이 군사업무 수행 및 각종훈련 등으로 인해 유발되는 일반적인 사항으로 보안관계자와 지휘관의 관심 여하에 따라 부대별 보안사고 건수가 많은 차이를 보이고 있다.

아울러, 철도청에서는 사고 유형별로 사고예방 분석시스템을 개발하여 각 역과 건널목 신호등에 경고방송을 지속적으로 송출하고 있고 사고 빈도가 높은 시기, 계절, 기후 및 장소 등에 대해서는 별도 예방 대책을 강구하도록 알려주고 있어 사고 예방에 기여하고 있다.

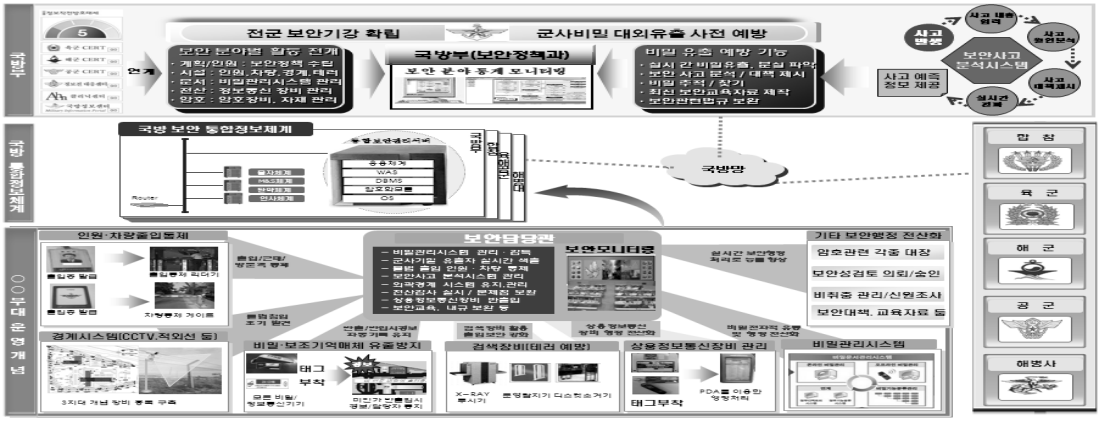
이와 같이, 군에서도 보안사고 유형을 부대별, 임무별, 계절별, 시기별 및 보안유형별 등으로 분석하고 각급부대 지휘관과 보안관계자들에게 신속히 전파한다. 사전 주의사항과 함께 사례 중심의 정신교육을 할 수 있도록 지원하며 부대별 통계를 지속 확인하여 소속부대원들의 보안의식 고취에 기여할 수 있도록 구축되어 한다.

보안사고 분석 System 작동은 사고가 발생되면 사고발생 부대 보안담당관이 사고 내용을 입력하고 System에서 자동으로 과거 유사사례 등과 함께 분석됨과 아울러, 전군에 자동 전파되며 사고가 발생되지 않더라도 보안강조 사항이 자동 전파되도록 구축되어야 한다.

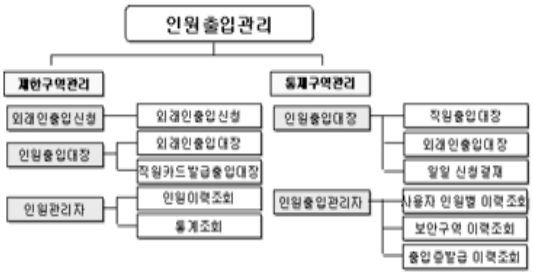
### 4.4 인원출입System

행정안전부에서는「공무원증규칙 개정('08.7.10)」에 따라 전자공무원증(13.56MHz) 발급을 2010년 전반기에 전면 시행하였고 이러한 전자공무원증을 이용하여 출입증으로도 활용 중에 있다.

군에 근무하는 현역과 군무원의 신분증도 전자공무원증과 동일하게 교체하였기 때문에 全軍이 「One




〔그림 4〕 군 통합보안시스템 구축 방안 구성도




〔그림 5〕 인원출입관리 프로그램 구성도

Card 체계」로 구축한다. 이러한 시스템이 구축되면 장병들이 각급부대 출입 시 근무자가 휴대용 PDA를 가지고 신분 확인과 동시에 출입이 가능하고 대장에 자동 기록되어 출입보안의 신속·정확·편리성을 충족하도록 한다.

또한, 직원 출입과 외래인 출입을 구분하여 출입통제시스템을 구축하며 직원 출입도 전자공무원증으로 각자 출입이 가능한 지역(부서)과 제한 지역 등의 보안등급을 설정하여 관련부서만 통행할 수 있도록 하고 외래인의 경우 Dual Card(13.56MHz : 출입 + 900MHz : 추적)로 제작하여 추적이 되도록 한다.

방문하고자 하는 외래인은 출입신청서를 민원실에 와서 작성하는 것이 아니라 국방망 및 인터넷(홈페이지) 등으로 접수받아 등록하도록 다양하게 구축한다. 보안담당자는 등록된 데이터를 근거로 출입 가능 여부를 승인한 후 민원실에 통보하면 외래인은 방문증을 발급받아 방문 목적이 있는 부서에만 출입한다.

보다 높은 수준의 보안을 요구하는 통제구역 등의 주출입구에는 다수의 인원이 동시에 출입할 수 있고 보안성과 신속한 출입을 보장하도록 Anti-Tailing 기능을 탑재한 Speed Gate 시스템을 구축해야 한다. 아울러, 인원출입관련 외래인 출입대장, 통제구역 출입대장 및 출입증 발급대장 등을 관리하는데 어려움이 있기 때문에 반드시 〔그림5〕와 같이 전산화를 해야 한다. 특히, 출입신청에 대한 보안담당관 결재도 전산화하여 근무자들이 보다 효율적이고 신속하게 행정처리 업무를 수행하여 초병들이 검문검색에 전념하도록 구축해야 한다.

### 4.5 차량출입System

차량 출입증은 RFID(Passive 900MHz)와 번호인식시스템을 혼합한 全軍 동일 체계 개념으로 구축하여 각급부대에서 시스템으로 자동 통제되고 근무자는


〔그림 6〕 차량출입관리 프로그램 구성도

승차 인원 확인 및 검문검색에 집중할 수 있도록 구축해야 한다.

차량 인식용 RFID Reader기는 軍 차량의 특성을 고려하여 인식률 향상을 위해 안테나 2개(소형용, 대형용)를 특수제작·설치한다. 차량 출입 신청도 「인원출입 신청서」에 포함하여 구축해야 하고 차량등록, 예약승인, 출입허가, 외래인 차량출입대장, 출입증 발급대장, TAG 관리 및 각종 조회 기능 등이 〔그림 6〕과 같이 구현되도록 설계해야 한다.

일반적인 차량관리시스템과 같이 리더기가 인식하고 게이트가 올라가는 형태는 Peak Time 시 차량 정체를 유발하기 때문에 역발상으로 전환하면 신속·정확히 출입조치가 가능하고 출입자 입장에서도 악천우 시 태그를 접촉할 필요가 없어 편리하게 된다.

정부에서 2부제 및 5부제 등을 시행할 경우 시스템에 입력하면 자동적으로 기계가 통제하여 간부들과 근무자 간에 마찰이 생기지 않고 출입근거가 명확히 남기 때문에 제반 교육자료 등으로 활용한다.

특히, 차량 및 인원관리시스템은 병영시설 현대화 설계 단계에서 미군 우주사령부와 같이 인원과 차량 이동량을 고려하여 건물 출입구와 부지 출입문 수량을 결정하여 첨단보안시스템을 구축해야 효과가 있다.

### 4.6 첨단경계 System

각급부대 경계시스템은 〔그림7〕와 같이 外柔內剛형 개념으로 외부에서는 주변과 어울리면서 부드러운 분위기를 띠게 하고 내부로 들어오면 최첨단시스템으로 다중 설치하는 3지대 개념의 보안정책이 요구된다.

울타리 침입감지 시스템은 외곽 울타리(블록담장, 휀스 등)로 침입을 시도하는 불순분자를 조기에 발견하고 경보할 수 있는 장치로 불순분자 침입 차단은 물론 경계 인원 감소 및 침입 위치 확인 등 효율적인 외곽 경계가 가능하도록 구축한다.

이를 위해서 울타리의 종류와 지형에 따라 장비별


〔그림 7〕 첨단경계System 구성도

시뮬레이션을 통해 최적의 장비 위치를 선정해야 한다. 일부 장비는 지형, 기상, 인원·동물왕래 등 주변 여건에 영향을 받으므로 충분한 현장 환경 분석이 필요하다. 고가 및 최초 설치 후 변경이 곤란한 장비에 대해서는 설치 前에 충분히 검토한 후 설치여부를 결정한다. 수입, 군내생산 등 다양한 제품이 있음을 감안해서 가격, 오작동률, 운영, 유지보수 등을 검토하여 장비를 선정한다. 대부분의 장비들이 낙뇌에 취약하므로 접지대책을 강구한다.

특히, 외부 침입상황을 조기에 발견하고 신속히 대응하기 위해서는 울타리 시스템과 연계하여 고정형 적외선카메라(야간 40M까지 식별)를 설치하고 중앙통제실에서 통제할 수 있도록 해야 한다.

아울러, 각급부대는 부지가 넓기 때문에 울타리로 침투 후 건물로 진입하기 위해 인원 이동이 적은 조경지역, 연병장 옆, 산림지역 등의 침투로 분석이 필요하며 침투로에 병력으로 매복한다는 것은 현실적으로 어려움이 있다. 따라서 침투 예상지역에 대한 감시System은 USN(열감지 센서)과 적외선 카메라를 혼합시켜 설치(무인 매복 장비)하고 중앙통제실에서 실시간으로 상황을 모니터링하여 상황발생 시 비대기 병력을 집중 투입하여 대응하는 것이 바람직 하다.

### 4.7 비밀관리System

통일부에 구축하여 운영 중인「정부 비밀관리시스템」을 기본 개념으로 하고 군사보안업무훈령을 준수하는 가운데 국방부에 적합한 시스템을 구상해야 한다. 비밀관리시스템은 평시뿐만 아니라 전시에도 생존성이 보장되고 원활하게 활용할 수 있도록 부가적인 제반 운영개념 및 보안대책이 뒷받침되어야 하고 전시 군사보안업무훈령 개정과 준용이 필요하다.

군의 미래전(NCW)을 고려할 경우 비밀관리스시템은 5대 전술망과 호환이 되어야 자원 및 인사 등의 비밀이 적시에 제공되어 임무 수행이 가능하고 시너지 효과를 달성할 수 있다.

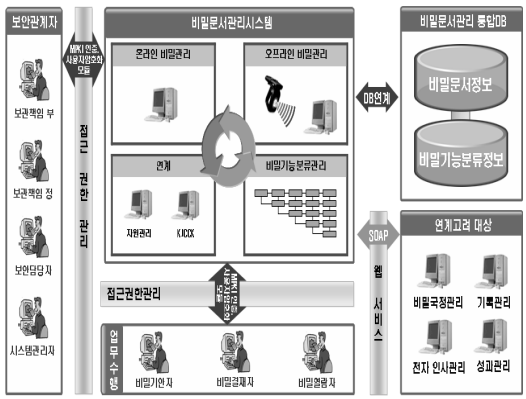
군사비밀의 분류, 관리, 이관 및 파기 등의 일련의 보안행정 절차가 동일 한데, 현재 전술망에서의 보안행정과 비밀관리시스템의 보안행정이 상이하고 향후 전군이 동시에 비밀관리시스템을 구축하지 않을 경우 보안규정을 적용받은 인원들이 혼란스러울 수 있으므로 현재의 군사보안업무훈령의 보안행정 절차를 준수하는 것이 바람직하다.

군에서 보유하고 있는 비밀은 대외비를 포함하여 약 120여만 件이며 다양한 임무 수행을 위해 보안행정도 복잡하고 비밀 외의 보안행정도 수십 件에 해당하기 때문에 통합화·전산화로 현실적이면서 편리성 중점을 주고 구축해야 한다.

특히, 군사용 비밀관리시스템 목표는 〔그림8〕에서와 같이 온·오프라인 비밀관리 및 비밀기능분류시스템의 기능을 제공하고 KJCCS 등 5대 전술망과 8대 자원관리망을 연계하여 운영되도록 하는 데 있고 보안관계자 및 비밀업무수행자는 MPKI 인증과 휴대용 암호모듈을 이용하여 비밀생산, 관리, 이관, 파기 업무를 수행한다.

비밀취급 인가자는 SBC 서버를 통한 WEB/WAS 시스템에 접근하고 비밀작성 시에는 SBC 서버를 이용하여 문서를 작성한다. 시스템 통합 모니터링이 가능하도록 SMS를 통해 시스템별 Health 체크, 서비스/네트워크별 사용량 체크를 실시하고 또한 시스템 모니터링 통합화면을 제공함으로써 즉각적인 대응체계를 확보한다[9].

On-Line 비밀관리시스템은 비밀의 생성·등록,




〔그림 8〕 비밀관리시스템 개념도

시행·유통, 사용에서 파기까지 비밀의 모든 처리프로세스를 시스템화하여 오프라인 중심의 비밀처리를 온라인 비밀처리로 전환하며, 또한 기존의 오프라인 비밀의 전자적 처리를 수용한다.

Off-Line 비밀관리시스템은 보안행정(접수용 비밀관리기록부 등 대장 6종, 비밀이력카드의 이력처리 14종)을 On-Line과 통합하여 구현한다.

아울러, 비밀도 업무수행에 필요 자료이므로 관련된 인원들이 수시 활용하여 정책 수립에 참고할 수 있도록 되어야 하고 군의 경우 정보, 작전, 인사, 군수 및 기타 업무들이 통합되어야 하는 것은 필요충분조건이기 때문에 반드시 비밀검색 기능이 잘되어 있어야 한다.

비밀 행정을 전산화하는 것은 업무의 효율성 및 정확성 등을 기하는 데 목적이 있으나 그보다 중요한 것은 각 개인별로 보안행정을 하기 때문에 명확히 하는지 보안담당관이 수시 감독할 수 있는 기능이 있어야 한다.

Off-Line시스템에서 RFID 태그를 부착하는 이유 중 가장 중요한 것은 현품과 데이터가 일치하는지 수시 확인할 수 있다는 것이고, 둘째 다량의 비밀을 단시간에 파악할 수 있으며, 셋째 분실했을 때에 체계적으로 찾아 신상필벌을 명확히 할 수 있다는 것이다. 만약 이러한 특징이 없다면 고가의 RFID 태그를 부착할 것이 아니라 바코드를 부착하는 것이 바람직할 것이다.

비밀 원본과 존안 비밀을 자료관이 보관·관리하고 있는데 이를 대출해 주면서 수작업으로 하고 있어 어려움이 있으므로 비밀 대출 및 반입 리더기를 구축하여 보다 정확하고 신속히 처리할 수 있도록 해야 한다.

### 4.8 테러 예방 System

국가보안목표 및 국가중요시설에 대해서는 X-Ray 검색기, 문형 탐지기, 휴대용 금속 탐지기 및 폭발물 탐지기 등을 설치하도록 규정되어 있고 국가보안목표 '가'급의 경우 100% 설치하여야 한다.

군의 경우 일부 부대만 최근부터 설치하였는데 이제는 국가보안목표 및 국가중요시설 '가'급에 대해서는 의무적으로 설치하여 외래인과 직원들의 휴대품을 철저히 검색함으로써 노트북 및 보조기억매체 불법 반출을 예방함과 동시에 폭발물 및 총기류 등에 대한 불법 반입을 근본적으로 차단해야 한다.

장비선정 시 고려사항으로 건물의 주요 '목' 지점을 분석하여 설치해야 최소의 비용으로 전 인원을 일제히 검색할 수 있다. 검색장비의 가장 중요한 기능이 투과력인데 최소 24mm 이상의 강철을 투사하도록 해야 한다. 해상도 또한 중요하므로 AWG 24이상의 구리선을 식별해야 한다. 검색영상의 의심스러운 부분에 대하여 64배까지 가능해야 한다. 물질 구분을 위해 영상표시 색상은 무기물(청색), 유기물(오렌지색), 혼합물(녹색), 탐지 불가 물질(흑색)을 구분할 수 있어야 한다.

## V. 결 론

군에서는 8대 자원관리체계 및 5대 전술체계를 구축하여 운영함에 따라 업무의 효율성을 높이고 있다. 반면, 보안분야는 표준이 없고 부대별로 자체 개념으로 구축하여 운영하고 있어 예산 낭비는 물론 보안수준 향상에도 도움이 되지 않는 실정이다.

이러한 보안취약점이 있는 현실에서 본 연구에서 제시한 「군 통합보안시스템 구축 방안」을 잘 적용할 경우 보안발전에 기여할 뿐만 아니라 예산 절감 및 업무효율적인 측면에서 기대가 되므로 적용을 위한 다음 몇 가지를 제언하고자 한다. 첫째, 국방부 보안정책부서에서 관련 부서와 협의를 통해 공감대 형성을 하는 것이 매우 중요하다. 둘째, 부대 마다 특성이 있기 때문에 해 부대에 적합한 통합보안시스템에 대한 종합적인 그림(Master Plan)을 작성해야 한다. 셋째, 전군 시행을 위한 예산 확보를 어떻게 할 것이며 단계별 시행을 어느 제대급 단위로 할 것인지 등에 대해 정립을 해야 한다. 마지막으로 보안관련 수사권을 갖고 있는 기무사령부에서는 보안사고 분석시스템을 개발하여 모든 사고에 대해 신속히 전파하고 미연에 예방할 수 있도록 조치해야 한다.

따라서 군에서의 보안업무는 안보와 직결되고 전쟁의 승패에도 결정적인 역할을 하는 매우 중요한 업무이기 때문에 보안 관련부서만이 시행하는 것이 아니고 전 장병이 동참해야 한다. 특히, 각급부대의 지휘관은 보안시스템을 구축할 때에는 반드시 계획수립 단계에서 부터 국방부와 각군의 구축 표준을 확인하고 호환 및 증설이 되도록 반영해야 한다.

## 참고문헌

〔1〕 장월수, 보안총론, KIDA Press, pp.122, 2011.1

〔2〕 조선일보 1면, 군기밀 빼돌린 40명, 다 풀려났다, 2011.8.5.
〔3〕 장월수, 국방부 통합보안체계 구축 방안 연구, 국방연구원, pp.23-26, 2008.12
〔4〕 http//kbank.nate.com/qna/kno
〔5〕 장월수, 국가기록원 보안체계 구축 방안 연구, pp.57, 2006.8
〔6〕 장월수, 국가기록원 보안체계 구축 방안 연구, pp.48-51, 2006.8
〔7〕 장월수, 해외 보안시설 견학 결과 보고서, 기무사령부, pp.6, 2002.10
〔8〕 장월수, 보안총론, KIDA Press, pp.154, 2011.1
〔9〕 장월수, 국방 비밀관리스템 개선방안 연구, 국방대학교, pp.15-37, 2010.12.13

## 〈著者紹介〉

장 월 수 (Worl-Su Jang) 정회원
1990년 2월: 3사관학교 졸업
2002년 2월: 연세대학교 건축공학 석사
2006년 8월: 국방대학교 정보관리 석사
2010년 2월: 고려대학교 정보보호대학원 박사수료
現 한국국방연구원 보안과장, 세종시 보안자문위원 등
〈관심분야〉 국가보안, 군사보안, 비밀관리, 통합보안, 정보보호, 클라우드 등

최 중 영 (Jung-Young Choi) 정회원
2005년 2월: 중앙대학교 산업정보학과 졸업
2011년 8월: 고려대학교 정보보호대학원 석사
現 한국국방연구원 국방정보체계관리단 선임연구원
〈관심분야〉 국방정보체계, 정보보호정책, 개인정보보호, 디지털포렌식, 융복합보안 등

임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
現 고려대학교 정보보호대학원 원장 , 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 한국저작권위원회 위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등