



Received: 2022/02/07
Revised: 2022/03/04
Accepted: 2022/03/27
Published: 2022/03/31

***Corresponding Author:**

Kyung-Won Oh

Tel: +82-63-450-7724

E-mail: n.kwoh@hanmail.net

보급형 국방 모바일 통제체계 개발에 관한 연구

A Study for Development of Popular Mobile Device Management on Military

백현민¹, 오경원^{2*}

¹해군사관학교 항해운용학과 조교수

²호원대학교 항공정비공학과 교수

Hyun-Min Baek¹, Kyung-Won Oh^{2*}

¹Assistant professor, Dept. of Naval Ship Handling, ROK Naval Academy

²Professor, Dept. of Aircraft MRO Engineering, Howon University

Abstract

현대전(現代戰)에 있어 정보보호의 중요성은 아무리 강조해도 부족하지 않은 만큼 군사 분야에서의 상용 모바일 통제체계에 의한 정보 유출의 피해를 방지하기 위한 예방적 대책 마련이 시급하다. 현재 국방부 청사와 합동참모본부는 실정에 맞는 모바일 통제체계를 마련하여 시행 중이나 이를 예하 전군에 확대 적용하기에는 구조적, 경제적 문제점이 있다. 이에, 본 연구에서는 보다 쉽게 보급 가능하고 경제적 운용이 가능한 모바일 통제체계 제작을 위한 필요성을 언급하고 실제로 해군 일부 부대에서 운용 중인 NFC를 활용한 모바일 통제체계의 개발 과정을 소개한다.

We realized the importance of the information-protection issue coming from the personal mobile device. Especially, it's urgent for us to take damage prevention in military security. Now, in the buildings of Ministry of National Defense and the Joint Chief of Staff, they use the mobile security system adequate for each others. But it is impossible to extend that system to all troops in the Korean Armed forces due to the structural and financial restriction. So in this study, we introduce the process of development for the mobile security system using NFC.

Keywords

모바일 단말기 원격 통제시스템 (MDM, Mobile Device Management), 개인 통신단말기(Personal Mobile Device), 근거리무선통신(NFC, Near Field Communication), 정보보호(Information Security), 스마트 전함(Smart Battle Ship)

1. 서론

‘진보된 기능의 핸드폰’인 스마트폰은 IBM사가 1992년 개발하여 1993년 일반 대중에게 소개된 사이먼(Simon)이 최초이지만 스티브 잡스에 의해 개발되고 2007년 1월 9일 공개된 아이폰(iPhone)부터 본격적으로 대중화되었다. 이후 국내에도 기존 핸드폰 제작 업체들이 안드로이드 운영체제 기반의 스마트폰 사업을 비롯한 모바일기기 사업에 뛰어들기 시작하였고, 기존 IT 강국 이미지와 부합한 모바일기기 사업은 어플리케이션 개발 시장과 접목되어 보다 큰 시너지효과를 창출하고 있다. 그 효과는 금융, 산업, 의료, 교육 등 일일이 열거할 수 없이 많은 부분에서 우리 생활 깊숙이 파고들었으며, 2014년 4월 국내 스마트폰 전체 가입자수는 38,395,889명으로 4천만 명을 향해 가고 있다.

그러나 모바일기기의 편리성에 가려 간과되어 왔던 정보보호에 대한 문제 인식과 그 대안 제시의 필요성이 최근 점차 대두되고 있다. 특히, 정보보호의 필요성이 크게 부각되는 산업 분야에서는 막대한 예산을 투입하여 모바일기기에 의한 자료 유출 방지를 위한 MDM(mobile device management) 체계를 개발하여 적용 중이다. 그러나 이러한 산업 분야보다 더 정보보호의 필요성이 부각되는 분야는 군사분야이다. 현대전(現代戰)에 있어 정보보호의 중요성은 아무리 강조해도 부족하지 않은 만큼 군사 분야에서의 상용 모바일 통제체계에 의한 정보 유출의 피해를 방지하기 위한 예방적 대책의 마련이 시급하다. 현재 국방부 청사와 합동참모본부는 각 규모와 실정에 맞는 모바일 통제체계를 마련하여 시행 중이나 이를 예하 전군에 확대 적용하기에는 구조적, 경제적 문제점이 있다. 이에, 본 연구에서는 보다 쉽게 보급 가능하고 경제적 운용이 가능한 모

바일 통제체계 제작을 위한 필요성을 언급하고 실제로 해군 일부 부대에서 운용 중인 NFC를 활용한 모바일 통제체계의 개발 과정을 소개한다.

2. 보급형 모바일 통제체계 개발의 필요성

폐쇄성이라는 특징을 갖는 군부대는 외부인의 출입이 엄격히 통제되며 사전 인가된 인원만 출입이 가능하다. 부대 내부에서도 부대의 특성과 다루어지는 업무, 시설 등에 관한 정보에 대하여 보호등급을 구분 적용하고 있으며 인원만이 아닌 물자와 자료, 심지어 정보 또한 보안상 유해성 유무의 검토를 받아야 한다. 정보통신망 또한 별도의 전산망을 구분 구성하여 인가 인원만 사용 가능하며 인터넷망의 사용은 그 통제가 더더욱 엄격하게 이루어진다. 이러한 군의 환경에서 스마트폰, 태블릿 PC 등과 같은 모바일 기기의 군 내 등장은 군내 보안환경을 위협하고 있다. 군사보안에 위배되는 모바일 기기의 기능은 크게 인터넷 검색, 이메일 전송, 사진 및 동영상 촬영 등을 들 수 있다[1]. 현재 국방부, 합참, 각 군은 군사보안업무훈령 및 보안지침에 의거하여 등록된 개인용 모바일 기기의 반입을 허용하고 관리적·기술적 보안대책을 수립하여 시행하고 있다. 관리적 보안대책으로는 보안담당관 주관의 기기 등록, 보안서약서 작성 및 제출, 승인 스티커 발급 및 부착, 군사통제구역, 비밀작업실, 비밀회의장 반입금지, 업무용, 인터넷 PC의 모바일 기기 접속 금지, 모바일 기기를 통한 군사자료 작성, 저장, 전송 금지, 군사보호구역에서의 화상통화 금지 등을 들 수 있으며, 기술적 보안대책으로는 정보보호체계를 통한 PC와의 접속 차단, 군사자료 암호화를 들 수 있다[3]. 그러나 이러한 노력에도 불구하고 모바일 기기를 이용한 SNS 통신은 제2의 작전통신망이라고 불릴 정도로 작전, 훈련 중 음성적으로 사용되고 있으며, 심지어 그 실태를 파악하기에도 역부족이다. 실제로 2013년 10월의 매체 보도 자료에 따르면, 최전방의 육군부대에서 작전상황과 장비를 점검하는 연례적 훈련 중에 훈련 일정과 지도 좌표, 심지어 지형이 상세히 표시된 군사지도까지 SNS를 통해서 전송되었다[2]. 이러한 폐해를 예방하기 위하여 국방부 청사에는 2013년 7월부터 MDM(mobile device management)을 적용 중이며, 2013년 10월 국방위 국정감사 시 국방부장관은 국방부 청사 내에만 사용 중인 스마트폰 보안대책(MDM)을 일선 예하부대까지 확대 시행하겠다고 하였다.

그러나 U-실험사업의 일환으로 진행된 국방부의 MDM

은 초기 구축 비용이 3.4억원으로 일선 예하부대에 모두 적용하기에는 경제적 한계가 있다. 실제로 민간의 유사 모바일 기기 통제체계를 전군의 일선 예하부대에 적용할 경우의 설치 비용과 10년간의 유지비용을 계산한 결과, 최초 설치 비용은 최소 27억원, 10년 운용 시 사용되는 프로그램의 라이선스 비용이 추가되어 108억원이 소모되는 것으로 계산되었다. 계산에서 적용한 부대는 약 300개 부대로, 사령부, 본부, 각 단 등 국직부대 25개 부대, 합참을 포함한 육·해·공군 부대 275개 부대 총 30만명을 통제할 경우를 가정하였다. 그러나 이 가정 또한 MDM의 설치 가능한 건물 형태의 부대에만 국한하였으며, 야전에서의 체계 적용 가능성을 고려한다면 그 비용은 더 증가할 것으로 판단된다.

이러한 경제적 한계성과 더불어 고려해야 할 것이 구조적 한계성이다. 기업과 국방부에서 적용하고 있는 MDM의 공통점은 출입통제체계와 연동되어 운용된다는 것이다. 즉, 통제구역 내로 입장 시 통제되고 퇴장 시 통제가 해제되는 개념인데 이러한 체계를 가능케 하기 위해서 필요한 것이 제한된 출입구에서의 하드웨어와 출입자 정보를 확인하기 위한 별도의 서버 및 소프트웨어이다. 그리고 이러한 체계가 적용 가능한 부대 유형(건물, 경제지, 함정 등)은 건물 형태의 부대이다. 그러나 해군만 하여도 대부분의 부대는 함정의 부대 유형을 띄고 있으며, 육군의 경우, 다수의 건물과 야지를 포함하는 경제지로 구성되어 있으며 경제지 내부는 모두 군사보호구역이다. 즉, 국방부 청사의 MDM은 건물 형태의 부대에만 적용 가능한 구조적 한계성에 의해 확대 적용에 어려움이 있다.

통제체계의 손쉬운 이동 및 이동형 통제가 불가능하다는 문제점 또한 있다. 한 건물 내에 설치된 모바일 통제체계는 그 건물에 고정되어 건물 내의 모바일 기기 통제만을 담당한다. 그러나 야전에서의 작전과 훈련이 항상 존재하는 우리 군의 특성상, 통제하에 있는 건물 외부에서의 모바일 기기 통제 필요성 또한 절실하다. 즉, 군사보호구역이 아닌 일반 구역에서 유사시 작전, 훈련을 수행할 경우, 참가자의 모바일 기기를 현지에서 통제 가능하거나 건물 내에서의 통제가 지속적으로 유지될 수 있는 기능이 보완되어야 비로소 일선 예하부대에 확대 적용 가능한 통제체계를 할 수 있다.

또 다른 문제점은 상용 MDM은 사전에 등록된 통제 대상자에 대해서만 통제가 가능하다는 점이다. 즉, 통제 서버에 통제 대상으로 등록된 인원이 아닌 비상근자, 외부인에 대한 통제가 필요하다면 대상자에 대한 별도의 등록절

차를 거쳐야 하는 과정상의 복잡함이 존재한다. 특히, 상시 비상근자와 외부인이 출입하는 사령부, 본부급 이상의 부대에서 해당 인원에 대하여 MDM을 적용하기에는 지나친 행정 소요가 발생한다는 것이다.

따라서 이러한 한계성을 극복할 수 있도록 부대 유형(건물, 경계지, 함정 등) 및 부대 임무(작전, 훈련, 교육 등), 통제 대상(상근자, 비상근자, 외부인 등)에 대한 구분 없이 군사보호구역 내에서 손쉽게 보급 가능하고 효과적인 모바일기기의 통제가 가능한 저비용의 통제체계 개발이 필요하다.

3. NFC를 활용한 모바일 통제체계 개발

3.1 통제 필요 기능의 검토

모바일기기를 이용하여 정보를 생산할 수 있는 방법은 크게 사진 및 동영상촬영, 음성 녹음, 문서 생산, 위치 정보 저장 등을 들 수 있다. 사진 및 동영상 촬영은 일반적인 모바일기기의 카메라 기능을 이용하여 생산되고, 음성 녹음은 녹음기, 문서 생산은 메모장 등 기타 워드프로세서 프로그램에서 이뤄진다. 위치 정보의 경우, 사용자가 인지하지 못하는 과정 중에 카메라, 녹음기, 워드프로세서 프로그램에서 생산되는 위치기반 정보도 함께 포함된다.

군사보호구역 내에서 카메라 및 녹음기에 의해 생산되는 정보는 모두 허가되지 않은 정보에 해당하기 때문에 카메라, 녹음기를 이용하는 정보 생산은 모바일기기의 하드웨어 장치를 제어하는 방식으로 통제 가능하다. 그러나 문서 생산을 통제하기 위하여 하드웨어 장치(키보드 기능)를 통제할 경우, 통제 대상자들이 군사보호구역 내에서 사용할 수 있는 제반 기능들 또한 함께 사용 불가능하여 사용자의 편의성을 제약하기 때문에 하드웨어 제어 방식으로 통제할 수 없다.

또한 통제 대상자가 고의로 위치 정보를 생산할 경우는 문서 생산과 동일하고, 인지하지 못한 과정에서 모바일 기기 내에서 자동적으로 생산되는 정보 내에 위치정보가 함께 기록되는 경우, 해당 정보만을 필터링하기에는 체계가 복잡해지는 단점이 발생하게 된다. 따라서 문서나 위치 정보의 생산은 보다 강화된 보안 수준이 필요한 구역에서 모바일 기기의 사용 자체를 차단하는 방식으로 통제하고 그보다 낮은 수준의 보안 수준에서는 모바일 기기의 사용은 허가하되 위치 정보를 수집할 가능성이 있는 어플리케이션의 실행을 차단함으로써 위치정보를 이용하는 어플리케이션에 의한 생산 정보의 전송을 차단할 수 있도록 구현하여야 한다. 본문에서 언급된 위치 정보는 GPS뿐만 아니라 Wi-Fi를 이용한 위치 정보 수집을 포함한다.

따라서 보급형 모바일 통제체계에 요구되는 기능은 크게 촬영 차단 기능, 녹음 차단 기능, 위치 정보 이용 어플리케이션 사용 차단 기능, 모바일 기기 사용 차단 기능으로 구분하였다. 이러한 각각의 기능은 독립적으로 수행 가능하여 부대의 실정에 맞도록 관리자의 손쉬운 설정과 조작이 가능하여야 하고 보안 수준이 강화될수록 각 기능들의 조합을 통해, 필요시 보다 강화된 통제 방식이 구현 가능하도록 개발하여야 한다.

또한 관리자와 통제 대상자 간의 통신을 통해 통제 모바일 통제체계에 필요한 프로그램이 설치된 대상자가 소유한 모바일기기의 통제 가능 상태, 현 통제 상태 및 통제 수준을 확인할 수 있어야 하며, 필요시 허가되지 않는 통제 수준으로 하향하거나 통제를 거부할 경우, 관리자에 의한 강력한 통제가 가능토록 원격 통제 기능을 부여하여야 한다. 위 기능은 rooting, 탈옥 등, 시스템 core 부분을 수정하지 않은 사용자 권한 상태에서 구현되어야 한다.

또한 관리자와 통제 대상자 간의 통신을 통해 통제 모바일 통제체계에 필요한 프로그램이 설치된 대상자가 소유한 모바일기기의 통제 가능 상태, 현 통제 상태 및 통제 수준을 확인할 수 있어야 하며, 필요시 허가되지 않는 통제 수준으로 하향하거나 통제를 거부할 경우, 관리자에 의한 강력한 통제가 가능토록 원격 통제 기능을 부여하여야 한다. 위 기능은 rooting, 탈옥 등, 시스템 core 부분을 수정하지 않은 사용자 권한 상태에서 구현되어야 한다.

3.2 적용 가능한 기술의 검토

보급형 모바일 통제체계를 구현하기 위하여 우선적으로 검토해야 할 요소는 사용성과 계속성, 경제성이다. 즉, 복잡한 등록 절차나 통제 절차 없이 통제 대상자들의 편의성을 최대한 확보하여 통제 과정 자체에 대한 복잡성을 줄여야 하며, 지속 사용 가능한 기술을 적용하여 향후 개발되는 신종 모바일기기에 대한 통제 가능성을 확보하여야 한다. 또한 예하 부대 확대 적용에 필요한 비용이 최소가 되어야 하며, 별도의 유지비용 또한 없거나 매우 적어야 한다. 이러한 사용성과 계속성, 경제성을 확보하기 위해 가장 필요한 검토 과정은 통제 신호를 감응시키는 방식에 대한 검토이며, 연구 과정에서는 GPS 방식과 NFC, 수동 통제 신호 입력 방식을 검토하였다.

3.1.1 GPS 기반의 통제 신호 인식

처음 검토한 기술은 GPS(global positioning system) 기반의 통제 신호 인식 방식이다. 즉, 통제 대상자가 정해진 좌표 구역에 진입하고 통제 대상자의 모바일기기가 인식하는 좌표 신호가 통제 구역 내에서 인식될 경우, 통제가 되도록 하는 방식이다. 모바일기기의 GPS 신호 수신기

능은 필수적으로 내장되어 있으며 GPS를 이용하는 상용 어플리케이션 또한 지속 개발되고 있는 추세이기 때문에 이 기능을 이용한 모바일 통제체계는 충분한 계속성이 보장된다. 그러나 이 방식은 경계지 형태의 부대 유형에만 적용 가능하며 건물이나 함정 형태의 경우에는 적용이 어렵다. 또한 이동 통제를 실시할 경우, 모바일기기의 통제를 위한 작전, 훈련 구역의 좌표 입력 자체가 곧 정보의 유출로 이어질 여지를 남기므로 가능성과 사용성이 제고된다. 추가적으로 GPS를 사용할 경우, GPS의 실행과 종료를 어플리케이션에서 임의로 할 수 있어야 하나 일반 어플리케이션의 경우, 권한과 보안의 이유로 해당 기능을 수행할 수 없다. 이를 해결하기 위해선 모바일기기 제조사의 협력을 받아야할 뿐 아니라 모바일 OS 제공 업체의 정책에 위배되지 않아야 하기 때문에 이는 결국 개발 비용 상승으로 이어질 수 있다.

3.1.2 NFC 기반의 통제 신호 인식

다음 검토한 기술은 NFC(near field communication) 방식으로, 통제 대상자가 특정 NFC tag에 모바일기기를 접촉시키게 되면 통제가 되고 다른 NFC tag에 접촉하면 통제가 해제되게 된다. 근거리무선통신의 약자인 NFC는 근접거리(proximity) 무선 기술로서 다양한 모드에서의 서비스를 지원한다. 특히, MFC 기술은 유사한 RFID 기술에서의 단순한 태그 인식 서비스보다 복잡하고 상호 연결 가능한 기술지원으로 소액결제서비스, 티켓팅과 같은 금융서비스 지원 또한 가능하다. 그 결과 NFC를 활용한 보안 기술은 보다 강력한 보안기술로 정의된다[4]. Fig. 1은 NFC 이용 단말기와 NFC tag, 사용 예를 나타낸다.

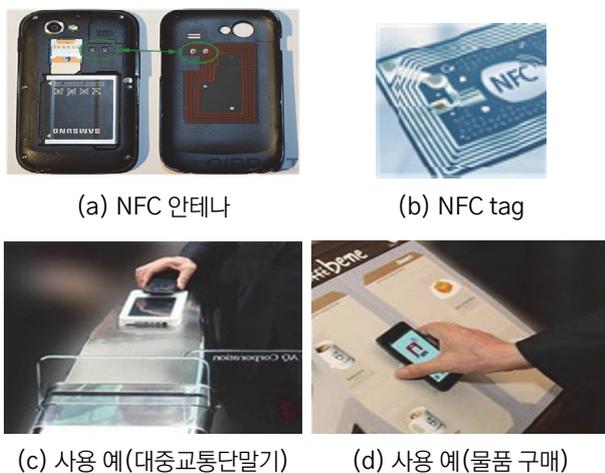


Fig. 1. NFC 단말기, NFC tag, 사용 예

NFC를 이용한 방식은 요즘 대중교통을 이용할 때, 휴대폰을 결제 단말기에 갖다대면 결제되는 것과 유사한 방식이다. 정부는 2011년 6월 ‘코리아 NFC 포럼’을 출범하여 민·관 협력하에 이동통신사(3사)와 협의하여 모바일 결제, 교육, 보안 등에 대한 NFC 활용의 확대를 추진 중이다. 이러한 추세를 바탕으로 2010년 이후 개발되는 스마트폰에 탑재되고 있는 NFC 기능은 모바일 통제체계 계속성 보장을 위한 기술적 대안으로 충분히 고려될 수 있다.

또한, NFC 기능 구현을 위하여 필요한 NFC tag의 기능은 일반 사용자도 손쉽게 설정이 가능하며 구매 비용 또한 저렴하여 사용성과 경제성이 보장된다.

3.1.3 수동 방식의 통제 신호 입력

통제 신호의 전송 및 인식에 별도의 기술을 적용하지 않고 관리자가 원격으로 신호를 송신할 경우, 신호를 받은 통제 대상자의 모바일기기가 통제되도록 하는 수동 방식은 기존의 MDM이나 기타 모바일기기 통제체계에서 사용된 방식이다. 그러나 이러한 방식은 관리자에 의한 임의적·무작위적 통제가 가능하다는 이유로 통제 대상자들의 사전 동의가 전제되어야 하기 때문에 사용성을 보장하기 어렵다. 그러나 항상 엄격한 규율과 통제 속에서 보다 완벽히 모바일기기를 통제하여야 하는 군의 실정상, 수동 방식의 통제 신호 입력은 필요시 사용할 수 있는 기술적 실현 가능성, 보다 강력한 통제라는 이점에서 오는 계속성, 또한 기타 부수적 비용이 들지 않는다는 점은 개발하고자 하는 모바일 통제체계에 적용 가능한 여지를 남겨준다.

이러한 검토 과정을 바탕으로 체계에 적용하기 위한 평가 요소를 가능성, 계속성, 사용성, 경제성으로 구분하여 평가한 결과를 Table 1에 나타낸다.

Table 1. 체계 적용 기술에 대한 검토 결과

기술	가능성	계속성	사용성	경제성
GPS	下	上	下	上
수동	上	中	下	上
NFC	上	上	中	上

GPS 기반의 통제 신호 인식의 경우, GPS 신호를 수신 가능한 경계지 유형의 부대에 적용 가능하나 건물, 함정 등 밀폐된 구역에 대한 적용과, 보다 제한된 구역(사무실, 함정 격실 등)에 대한 정확한 구역 구분이 어렵다는 점에서

군의 보급형 모바일 통제체계에 적용하기는 어려울 것으로 판단된다. 그러나 모바일 통제체계가 통제하고자 하는 일반적인 SNS 및 인터넷 어플리케이션이 GPS 신호를 필요로 하기 때문에 어플리케이션이 GPS 정보를 가져오는 기능을 차단할 경우, 해당 어플리케이션을 사용치 못하도록 할 수 있다는 점과 군사 정보인 군부대의 위치 정보를 통제할 수 있다는 점에서 통제 신호의 인식 방식이 아닌 생산 정보의 전송이 가능한 SNS 어플리케이션이나 인터넷 어플리케이션의 통제 방식으로 검토 가능하다.

수동 방식의 경우, 앞에서 설명한 바와 같이 기존 MDM에서 사용되었기 때문에 기술적인 적용 가능성은 높게 평가할 수 있다. 그러나 매번 관리자가 통제를 해야 하는 조작의 불편함을 보완하기 위하여 수동 방식은 통제를 거부하는 인원에 대한 경고 및 원격통제 방식으로 사용 가능하거나 관리자의 조작을 최소화하기 위하여 시간표와 알람 기능을 추가하여 보다 강화된 관리 대책을 위한 기술로 적용 가능하다.

NFC는 통제 대상자들이 직접 개인 모바일기기를 NFC tag에 접촉함으로써 스스로 통제 상태로 설정하여야 한다는 점에서 사용성은 일부 부족하나 관리자 입장에서 지속적인 확인과 조작이 불필요하다는 점, 통제 대상자가 필요시 손쉽게 통제 및 해제가 가능하다는 점, 건물이나 함정의 격실과 같은 세부적인 통제 및 제한구역에 대한 보안수준의 설정이 가능하다는 점에서 개발하고자 하는 보급형 모바일 통제체계의 주요 적용 기술로 선정하였다. 기존의 RFID가 수동적 통신 기능만 제공하였기 때문에 충분한 안전 인증 및 권한 검증 방법을 제시하지 못한 반면, NFC는 보다 안전한 인증 방식을 제공하여 다양한 응용에서 요구하는 보안 요구사항을 만족시킬 수 있기 때문에 출입 통제 시스템에 대한 활용 사례가 보다 증가하고 있으며[5], 보급형 군 모바일 통제체계 개발에 대한 적용은 이러한 추세를 반영한다.

3.2 모바일 통제체계의 개발

일선 예하부대에 보급 가능한 국방 모바일 통제체계 개발을 위해선 군의 정보보호 특성을 정확히 반영할 필요가 있다. 이에, 연구를 진행하면서 해군 함정인 해군 53전대 고준봉의 승조원들과 해군 교육사령부 기술행정학교의 실무 장병과 교육생들을 통제 대상으로 지정하였다. 또한 기술의 적용 가능성을 검토하고 실제 프로그래밍을 위하여 LG 모바일 연구원과 함께 연구가 진행되었다.

3.2.1 모바일 통제체계의 통제 구현 단계 설정

모바일 통제체계의 통제 구현 단계는 총 4단계로 설정하였다. 1단계는 모바일기기 내 통제체계의 기능을 구현시키기 위한 통제 프로그램을 저장시키고 활성화시키는 단계이다. 2단계는 모바일기기에 구비된 NFC tag 인식부가 통제 구역의 출입 장치에 구비된 NFC tag 또는 휴대 가능한 NFC tag와 전기적으로 접촉하여 모바일 통제체계가 실행되게 하는 단계이다. 3단계는 통제 프로그램이 설치된 모바일기기의 정보를 저장 서버로 전송시키는 단계이며, 4단계는 서버에 저장되어 있는 NFC code와 통제 대상자의 모바일기기가 인식한 NFC code를 비교하여 일치 시 해당되는 code 명령을 실행시켜 통제되도록 하는 단계이다. 이 과정은 서로 다른 통제 수준을 갖는 중첩된 통제 구역 내에서의 영역과 시간의 제약에 관계 없이 서로 다른 복수개의 NFC 명령을 자유롭게 인식하고 그에 따른 통제 수준을 설정하고 통제 명령에 반응할 수 있도록 실현되어야 한다.

특히 4단계는 모바일기기 및 사용자의 정보 중 적어도 하나 이상을 바탕으로 보안 수준을 설정하는 단계, 시기에 따라 보안수준에 새 정보를 부여하여 보안 수준을 자동 업데이트하는 단계, 업데이트된 통제 수준을 모바일기기의 하드웨어에 부여하여 통제하도록 하는 세부 단계와 기능을 포함한다.

3.2.2 통제 구현을 위한 구성요소 설정

모바일 통제체계의 통제 구현을 위해서는 통제구역(군사보호구역, 군사제한구역, 군사통제구역)과 모바일기기, 통제구역마다 설치될 입구용 통제 장치와 출구용 해제장치, 통제장치와 해제장치에 반응하여 하드웨어를 통제할 모바일기기 어플리케이션, 통제대상자들의 모바일기기 정보(개인정보는 저장하지 않는다), 통제 및 해제 장치의 정보를 저장할 저장서버, 서버와 모바일기기 간 통신을 담당하는 기지국이 필요하다.

통제구역 중 군사보호구역, 군사제한구역, 군사통제구역은 요구되는 보안 수준이 상이한 구역으로 군사보호구역의 경우, 카메라 및 음성 녹음 기능의 제한이 필요한 영역이라면 제한구역은 추가적으로 인터넷 전송을 제한하고 통제구역은 모바일기기의 사용 자체를 차단하는 구역이라고 할 수 있겠다.

모바일기기는 기기의 고유 명칭에 구애받지 않고 컴퓨터

터 지원기능을 추가한 지능형 핸드폰(스마트폰), 태블릿 PC 등을 말한다. 통제구역 입구에 설치될 통제 장치는 통제 명령 코드가 부여된 NFC tag이며 출구에 부착될 해제 장치는 통제 상태를 해제하여 모바일기기의 기능을 일부 또는 전체 복구시키는 명령 코드가 부여된 NFC tag이다.

서버는 별도 통제용 서버가 아닌 기존 각 군에 구비되고 운용 중인 인터넷 서버를 활용하며 서버는 통제구역 내부 또는 외부에 설치될 수 있다. 기지국은 일반 상용 통신 기지국을 활용한다.

3.2.3 구성요소 간의 연결

Fig. 2는 모바일 통제체계 구성요소 간의 연결방식을 나타낸다.

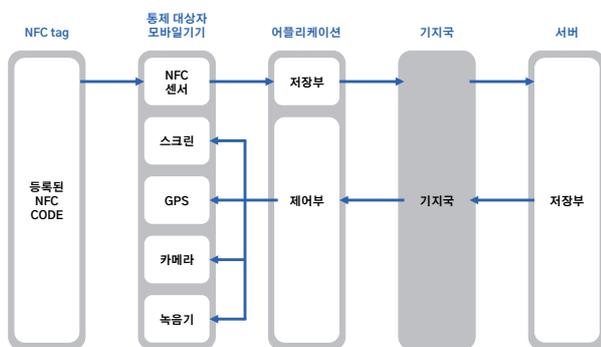


Fig. 2. 보급형 국방 모바일 통제체계의 구성요소 간의 연결방식

먼저 통제대상자의 모바일기기 내에 설치된 NFC 입력부가 NFC tag의 code를 인식하게 되면 해당 정보는 어플리케이션을 통해 기지국을 거쳐 서버로 전송되고, 어플리케이션은 사전에 서버에 등록되어 있는 NFC code 데이터 정보와 비교하여 일치하는 code의 명령을 가져와 통제 대상자의 모바일기기 내에서 해당 명령을 수행한다. 즉, 통제 구역 내에 설치된 NFC tag에 등록된 NFC code에 해당하는 명령으로, “카메라를 작동치 못하게 하라”가 서버에 저장되어 있다면, 그 명령을 통제 대상자의 모바일기기 내에서 실행하는 개념이다.

기존의 모바일 통제체계의 경우, 통제 대상자의 모바일기기와 통제용 서버 간의 인터페이스에 중점을 두어 구현되도록 설계되었으나 보급형 모바일 통제체계는 서버의 역할을 정보의 저장만으로 최소화시키고 통제 대상자의 모바일기기 자체에 통제와 관련한 핵심기능을 탑재함으로써 보다 저비용으로 간편한 통제의 구현이 가능토록 만들 필요가 있다. 따라서 개발하고자 하는 모바일 통제체계

가 통제하는 모바일기기는 기기 자체가 가지고 있는 모든 하드웨어적 기능을 최대한 활용하여야 하며, 이에 보급형 모바일 통제체계의 모바일기기는 메모리, 제어부, 입력부, 통신부, 저장부, 태그부를 전부 포함한다.

입력부는 터치 인터페이스를 구비한 입력부가 될 수 있으며, 사용자의 터치 입력에 따른 실행화면을 표시할 수 있는 디스플레이부를 일체로 구비한 구성이 될 수 있다. 또한 이 입력부는 터치 인터페이스에 한정되지 않고 버튼식으로 사용자의 명령을 받아 그에 따른 실행화면을 표시할 수 있는 디스플레이부를 일체로 구비할 수 있다. 통신부는 기지국 또는 통신망을 매개로 하여 서버와 데이터를 송수신할 수 있고, 서버로부터 제공받은 데이터를 제어부로 제공한다. 저장부는 모바일기기의 제조 번호와 사용자의 전화번호를 저장하고, 통신부는 저장부에 저장된 모바일기기 자체의 시스템 정보 및 사용자의 정보 중 적어도 하나 이상을 읽어들이 이를 서버에 제공한다. 태그부는 출입 장치에 구비된 NFC tag를 전기적으로 접촉하는 구성으로, 태그부가 NFC tag와 전기적으로 접촉한 경우, 이를 제어부로 전송하는 기능을 수행한다. 메모리부는 비휘발성 메모리(NVM)로써 전원이 공급되지 않아도 저장된 데이터를 계속 유지하며 삭제되지 않으며, 플래시메모리, MRAM(마그네틱 RAM), PRAM(상변화 RAM), FRAM(강유전체 RAM) 등과 같이 다양한 형태로 구성될 수 있고 랜덤액세스 메모리(RAM)와 같은 비휘발 메모리로 구성할 수 있다. 또한 메모리부는 적어도 하나 이상의 통제용 어플리케이션을 저장할 수 있고 제어부의 제어 신호를 기초하여 어플리케이션을 실행하거나 해제할 수 있다.

3.2.4 통제용 어플리케이션의 개발

통제용 어플리케이션은 보급형 국방 모바일 통제체계 구축을 위한 핵심 구성요소이며, 모바일 통제체계의 전부라고 할 수 있다. 이 어플리케이션은 모바일기기의 프로그램 중에서 정보를 저장하거나 전송할 수 있는 기능, 즉, 통제 구역 내에서 보안상의 이유로 통제가 필요한 프로그램을 관리하는 어플리케이션이 되거나 통제 대상자에게 경고 메시지 송출이나 서버로 모바일기기의 상태를 제공하는 기능을 가질 수 있다. Table 2는 통제용 어플리케이션에 요구되는 주요 기능을 나타낸다.

통제용 어플리케이션이 갖는 주요 기능을 설명하면 다음과 같다. 통제용 어플리케이션이 모바일기기에 설치됨과 동시에 어플리케이션은 모바일기기의 정보를 서버로

전송하여 서버에 기존에 저장된 새로운 정보를 가진 기기 종류가 인지될 경우, 기기 정보 목록을 업데이트시킨다. 또한 어플리케이션은 통제 대상자의 모바일기기의 기능 통제 상태를 서버로 전송하고 관리자는 서버의 정보를 읽어어드리는 기능을 수행하여 개인의 모바일기기를 이용, 모니터링을 수행한다.

Table 2. 통제용 어플리케이션에 요구되는 주요 기능

기능	설명
필수 기능	· 모바일기기의 정보를 저장하거나 전송
	· 통제 명령의 제어부 전달 및 실행
	· 제어부를 통한 하드웨어 제어 기능
	· 하드웨어의 통제 상태를 서버로 전송 및 감시
	· 설치 후 임의 삭제 방지 기능
	· 임의 삭제 시 삭제 내용 인지 및 서버로 전송
	· 관리자와 통제 대상자의 사용 모드 구분
	· 통제 대상자의 허가되지 않은 관리자 권한 접근 방지
	· 관리자의 통제 대상자 모바일기기 통제 상태 모니터링
	· 통제 상태 전환 후 통신 단절 시 통제 상태 유지 기능
부가 기능	· 관리자의 NFC code 등록, 변경, 삭제 기능
	· 통제 대상자의 그룹 관리 기능
	· 통신 연결 상태 확인 기능
	· 관리자의 통제 대상자에 대한 원격 통제 기능
	· 삭제 필요시 관리자 인증 후 삭제 가능 기능
	· 어플리케이션 설치를 위한 메시지 전송, 초대
	· 통제 대상자에 대한 경고 송신 기능
	· 시간 설정을 통한 자동 통제 기능
	· 스크린 터치 방식을 통한 통제 상태 전환 기능 (NFC tag 부재 시 통제 대상자가 직접 수행)

모니터링 화면에는 통제 대상자의 통제 상태와 어플리케이션 삭제여부, 통신 연결 여부가 확인되며 필요시 경고를 송신하거나 원격으로 통제 가능하도록 한다. 통제용 어플리케이션은 통제 대상자가 임의로 삭제할 수 없도록 서로 상호 감시하는 두 개의 어플리케이션이 설치되거나 삭제 시 모니터링되도록 한다. 부가적으로 통제용 어플리케이션 자체 내에서 통제하고자 하는 신규 대상자들에게 쉽고 간편하게 어플리케이션 설치를 요구할 수 있도록 하고, 시간 설정을 통해 특정 시간 범위에 이르면 자동으로 정해진 통제 상태로 전환되도록 하는 편의 기능도 고려된다. 또한, NFC tag가 없을 시, 통제 대상자들에게 스스로 스크

린 터치 방식을 통하여 개인의 모바일기기를 통제 상태로 전화시킬 수 있는 기능 또한 고려된다.

상기 주요 기능을 구현 가능한 통제용 어플리케이션은 2013년 9월부터 2014년 5월까지 총 8개월에 걸쳐 개발되었고 다수의 모바일기기와 인원에 대한 시범적용을 통해 지속 보완되었다. Fig. 3는 개발된 어플리케이션의 기능의 실제 시연을 나타낸다.



Fig. 3. 개발된 보급형 국방 모바일 통제체계 어플리케이션의 실제 시연 화면

3.2.5 통제 및 해제용 NFC tag 등록과 설치

개발된 통제용 어플리케이션이 설치된 모바일기기가 서버에 코드가 등록된 NFC tag에 접촉될 경우, 서버에 등록된 명령을 수행한다. 따라서 어플리케이션을 수행시켜 모바일기기를 통제 상태로 전환하기 위해서 코드가 등록

되어 있지 않은 NFC tag를 관리자의 모바일기기로 인식하여 관리자가 원하는 명령을 부여하여야 하며, 명령이 부여된 NFC tag를 최종적으로 통제하고자 하는 통제구역의 출입구에 설치하여야 한다. NFC tag는 시중에서 구매 가능하며 종류에 따라 가격은 1~2천 원 가량이다. Fig. 4는 서버에 등록되어 있지 않은 NFC tag를 관리자 스마트폰에서 인식 후 코드에 해당하는 명령을 입력하는 과정과 서버에 등록된 NFC tag 목록을 나타낸다.



Fig. 4. NFC 등록 과정과 등록된 NFC 목록

NFC tag 등록 후 등록된 tag를 통제 구역의 출입구 또는 관리상 용이한 위치에 설치하거나 이동형 통제로 관리하고자 할 경우, 관리자가 보관한다. Fig. 5는 해군 기술행정학교에서 부착 운용 중인 NFC tag를 이용한 모바일 통제체계의 활용 예를 나타낸다.



Fig. 5. 개발된 모바일 통제체계의 실제 활용 예

3.2.6 개발된 모바일 통제체계의 통제 세부 과정

통제용 어플리케이션을 이용하여 통제 대상자들의 모바일기기를 통제 상태로 전환하고 해제하는 과정은 Fig. 6의 과정을 따른다. 이 과정을 통해 통제 대상자의 모바일기기는 정상적으로 통제된다.



Fig. 6. 보급형 국방 모바일 통제체계의 통제 상태 전환 과정

4. 보급형 국방 모바일 통제체계 개발 효과

4.1 모바일 통제체계의 시범 적용

개발된 보급형 국방 모바일 통제체계는 해군 함정 1개 부대와 육상 1개 부대에 시범적용되었다. 함정은 해군 53전대 고준봉함, 육상부대는 해군 기술행정학교를 선정하였다. 고준봉함에는 함정이 육상에 정박 시 유일한 출입문인 현문과 전투상황실, 사관실, 함장, 부장 집무실, 장교 집

무실, 비밀보관소 등 총 10개소에 각 격실에 맞는 보안수준으로 설정된 NFC tag를 설치하였고, 현문에는 함정의 태세에 따라 보안 수준을 설정할 수 있도록 여러 종류의 NFC tag를 설치하여 당직자로 하여금 관리될 수 있도록 하였다. 기술행정학교에는 교육생들이 출입하는 출입구와 장교 회의실, 시험자료를 관리하는 평가실 등 총 5개소에 설치하였다.

통제 대상자에 해당하는 승조원들과 교육생, 실무장병들은 관리자들이 배포한 URL 및 일반 어플리케이션 다운로드 방법을 통해 모바일기에 통제용 어플리케이션을 다운로드 및 설치하였다. 이후, 관리자가 통제 가능하도록 그룹을 형성하여 조직을 구성하였으며, 2014년 2월부터 5월까지 총 4개월 동안 Fig. 7과 같이 시범적용을 실시하였다.

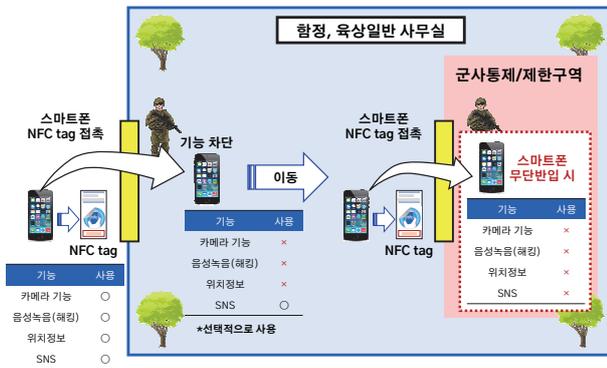


Fig. 7. 스마트폰 보안통제(NFC+원격) 체계도

4.2 시범 적용 결과

4.2.1 무형적 효과

Table 3는 시범 적용 전, 무작위로 추출한 익명의 통제 대상자들에 대한 모바일기기 사용 실태 조사 내용 중 일부를 나타낸다.

Table 3. 모바일기기 사용 실태 조사 내용(통제 전)

조사 내용	그렇다	아니다
부대 내에서 모바일기기를 이용하여 사진촬영을 한 적이 있다.	00 %	00 %
모바일기기 내 개인 자료를 SNS를 통하여 부대 내에서 타인에게 전송한 적이 있다.	00 %	00 %
군사 통제-제한구역에 모바일기기를 무단 반입 후 사용한 적이 있다.	00 %	00 %

이러한 조사 내용이 내포하는 의미는 모바일기기에 의해 보안위규 및 사고 사항에 해당하는 수준으로 악화될 수 있는 보안 유해 요소가 현재 군 내 상존하고 있다는 것이다. 이러한 유해 요소의 상존 환경하에서 모바일 통제체계를 시범 적용 후 통제기간 동안의 모바일기기 사용 실태 조사 결과를 Table 4에 나타냈다.

Table 4. 모바일기기 사용 실태 조사 내용(통제 후)

조사 내용	그렇다	아니다
부대 내에서 모바일기기를 이용하여 사진촬영을 한 적이 있다.	-	99 %
모바일기기 내 개인 자료를 SNS를 통하여 부대 내에서 타인에게 전송한 적이 있다.	-	99 %
군사 통제-제한구역에 모바일기기를 무단 반입 후 사용한 적이 있다.	-	99 %

통제체계의 시범 적용 기간 동안, 통제 대상자들은 통제 전에 비하여 부대 내 사진촬영이나 자료의 전송, 통제 구역, 제한구역 내 모바일기기의 무단반입 사용 등이 거의 완벽한 수준으로 통제되었다.

Table 5는 시범 적용 기간 동안, 관리자들이 주로 사용한 모바일 통제체계의 기능에 대한 만족도를 나타낸다. 이는 체계의 편리성을 나타내는 빈도로 해석 가능하다.

Table 5. 통제체계 기능에 대한 만족도(관리자)

조사 내용	만족도
시간 설정 기능(과업 시작 시 통제, 종료 시 해제)	99 %
그룹 관리 기능	90 %
원격 모니터링 및 원격 통제 기능	90 %
이동형 통제 기능	95 %
어플리케이션 내 초대 기능	99 %

개발된 모바일 통제체계의 효용성을 나타내는 이러한 결과 외에도 눈에 띄는 것은 군사통제, 제한구역이 아닌, 통제 자체가 불가능했던 군사보호구역 내에서의 모바일기기 사용이 효과적으로 통제된다는 점이다. 즉, 결론적으로 군의 인원, 시설, 정보의 유무에 관계없이, 군에 영향을 미치는 모든 지역과 시기에 무방하게 모바일기기의 통제가 가능하게 됨으로써 군사보안에 대한 신뢰성 구축이 가능해졌다.

또한 기술행정학교에서 시범 적용한 결과, 개발된 모바일

일 통제체계의 정부 부처 및 방산업체, 일반 산업체, 학교에까지 확대 적용 가능성을 엿볼 수 있었다. 수업 중 모바일기기를 사용할 수 없도록 일괄 수거하여 관리하던 기존의 관리적 대책은 지나친 인권 침해와 도난 및 분실에 대한 우려가 상존하고 있었다. 그러나 개발된 모바일 통제체계를 사용함으로써, 교육생들을 수업 시작 전 스스로 모바일기기를 통제 상태로 전환하였으며, 관리자인 교관들은 교육생들에게 자율성을 보장하면서 자신의 모바일기기로 수업 시간 중 사용 여부를 통제함으로써 보다 효율적인 관리가 가능해졌다고 평가하였다. 이러한 결과는 군부대 뿐만 아니라 모바일기기의 지나친 사용에 의해 생산성에 대한 문제점이 발생하는 일반 산업 시설, 교육 시 모바일기기의 통제가 필요한 학교 등에서도 효과적인 활용이 가능함을 의미한다.

4.2.2 유형적 효과

개발된 모바일 통제체계에는 통제 및 관리의 기능을 다수의 관리자 모바일기기로 분산하여 운용되도록 구성하였기 때문에 통제를 위한 별도 서버가 불필요하며 통제용 어플리케이션과 통제 대상자들의 모바일기기 정보를 등록할 저장 공간만 요구된다. 통제용 어플리케이션의 용량은 약 4 MB에 해당하고 통제체계에서 요구되는 모바일기기의 정보는 1인당 최대 1 MB 이하로, 50만명 기준 50 GB의 용량이면 충분하며, 이는 시중에서 시판 중인 1TB(6~7만원) 하드디스크의 1/20의 용량에 해당한다. 이처럼 통제용 서버가 불필요하고 요구되는 저장 공간이 적다는 점은 모바일 통제체계를 구축하는데 드는 비용을 크게 절감시켰다. 또한 시중에서 1~2천원으로 구매 가능한 NFC tag와 군 내 근무자에게 모두 지급되는 군 신분증을 활용할 수 있는 체계로 만듦으로써 구현 비용을 획기적으로 절감시킬 수 있었다.

개발된 모바일 통제체계를 해군 내 125개 부대에 적용하고, 각 부대마다 충분한 수량인 총 20개소의 통제구역을 운용하는 경우를 가정할 때, 체계 구현에 요구되는 비용은 총 500만원에 불과하다. 이는 민간 상용 통제체계를 운용 시 요구되는 최초 설치비용 8.1억원에 비하여 8.05억원을 절감한 셈이며 10년 운용을 가정할 경우, 통제체계의 라이선스 비용을 고려하여 총 13.43억원을 절감할 수 있을 것으로 계산되었다.

또한 개발된 모바일 통제체계를 전군에 확대 적용 시 소요되는 비용은 최초 설치 비용 0.12억원, 10년 운용 시 소

요비용 0.17억원으로 이는 각급 부대에서 운용하는 수용비로 총당 가능한 금액이며, 상용 통제체계 운용 시에 비해 최초 설치 비용을 26.9억원, 10년간 107.8억원을 절감시킬 수 있을 것으로 계산되었다.

5. 결론

현대전(現代戰)에 있어 정보보호의 중요성은 아무리 강조해도 부족하지 않은 만큼 군사 분야에서의 상용 모바일 통제체계에 의한 정보 유출의 피해를 방지하기 위한 예방적 대책 마련이 시급하다. 본 연구에서는 그 예방적 대책의 한 가지 대안으로 대두되고 있는 모바일 통제체계를 군의 실정에 맞도록 보급형으로 개발하는 과정을 연구하였다. 일선 예하부대에서 운용 가능한 국방 모바일 통제체계에 요구되는 특징은 손쉬운 체계의 설치와 사용, 통제 구역과 시기, 통제 대상에 대한 제약이 없는 통제 가능성, 전군에 적용 시 소요비용을 고려한 경제성이다.

개발된 모바일 통제체계는 이러한 특징을 모두 만족한다. 개발된 모바일 통제체계가 갖는 주요 기능은 모바일기기를 이용한 촬영과 녹음, SNS 통제 및 GPS 위치 정보 사용 제한이며, 이러한 기능들은 부가 기능인 시간 설정 기능, 원격 감시 및 통제 기능, 그룹 관리 기능 등에 의해 사용성에 대한 저해 없이 효과적으로 발휘된다. 또한 향후 지속 발전 기술인 NFC를 체계의 기반 기술로 적용하여 체계 사용에 대한 계속성을 보장하였으며, 체계의 구현 비용 또한 획기적으로 절감이 가능하였다.

개발된 모바일 통제체계의 시범 적용 기간 중, 그 효과는 충분히 입증되었으며, 체계의 정부부처, 일반 산업 시설, 학교에까지의 확대 적용 가능성 또한 엿볼 수 있었다. 현재 본 통제체계는 해군작전사 예하 함정 및 육상부대에 확대적용 결정되어 해군 5전단 주관으로 준비 중이다.

참고문헌

- [1] 김영철, "스마트폰 활성화 전망에 따른 군사보안 대응방안 연구", 송실대학교 정보통신학과 학위논문, 2011년.
- [2] 이만수, "군사지도에 좌표까지...카톡 유출 심각", YTN, 2013년 10월.
- [3] 해군보안업무규정, 제5장 시설보안, 제6장 정보통신보안, 2012년 12월.
- [4] 임선희, 전재우, 정임진, 이옥연, "NFC 보안기술분석 및 UICC 적용 효과 연구" 한국통신학회논문지 제36권, pp. 29-36, 2011년 1월
- [5] 이민규, 김동완, 손진수, "NFC를 활용한 능동형 인증 방법", 한국통신학회논문지 제37권, pp 140-156, 2012년 2월.