https://doi.org/10.33778/kcsa.2023.23.1.125

망분리 환경에서 민감정보를 안전하게 처리하기 위한 기술적 방안

이 주 승*, 김 일 한**, 김 현 수***

요 약

공공기관을 필두로 민감정보를 취급하는 기업들은 사이버 공격 예방을 위하여 업무망과 인터넷망을 분리 구축하고, 강한 접근통제를 바탕으로 중요 데이터를 보호하고 있다. 그렇기에 업무망과 인터넷망이 연결되는 접점을 수반하는 시스템은 관리적, 기술적으로 안전한 보안환경 구축이 필수적으로 요구되고 있다. 기관에서 사용하고자 하는 모바일 장치의 경우 기기를 통제하기 위한 MDM(Mobile Device Management) 솔루션이 그 예라 할 수 있다. 이 시스템은 모바일 장치 정보, 사용자 정보 등의 민감정보를 인터넷망에서 취급하여 동작하므로 운영 시 각별한 보안대책이 요구된다. 본 연구에서 인터넷망에서 반드시 운영되어야 하는 시스템에서의 민감정보 데이터 처리를 내부망에서 관리할 수 있도록 모델을 제시하였으며, 이를 망연동 솔루션을 기반으로 한 MDM 솔루션을 중심으로 기능 설계 및 구축하였다.

The Technological Method for Safe Processing of Sensitive Information in Network Separation Environments

Juseung Lee*, Ilhan Kim**, Hyunsoo Kim***

ABSTRACT

Companies that handle sensitive information, led by public institutions, establish separate networks for work and the Internet and protect important data through strong access control measures to prevent cyber attacks. Therefore, systems that involve the junction where the Intranet(internal LAN for work purposes only) and the Internet network are connected require the establishment of a safe security environment through both administrative and technical measures. Mobile Device Management(MDM) solutions to control mobile devices used by institutions are one such example. As this system operates by handling sensitive information such as mobile device information and user information on the Internet network, stringent security measures are required during operation. In this study, a model was proposed to manage sensitive information data processing in systems that must operate on the Internet network by managing it on the internal work network, and the function design and implementation were centered on an MDM solution based on a network interconnection solution.

Key words : Network Separation, Mobile Device Management, Personal Data, Sensitive Information

접수일(2023년 02월 22일), 수정일(2023년 03월 17일), 게재확정일(2023년 03월 27일)

* 국방과학연구소(주저자)
** 국방과학연구소(교신저자)
*** 국방과학연구소

1. 서 론

사이버위협의 고도화·지능화로 정보보안의 중요성이 고조됨에 따라 공공, 금융, 국방 등 중요정보를 처리하는 기관 및 기업들은 다양한 보안기술과 보호대책을 강구하여 시스템과 정보자산을 보호하고 있으며, 시스템과 데이터의 보안성을 보장하는 것이 사회적으로 중요한 요소가 되었다.

그중 하나로 상용 인터넷망과 업무망에 대하여 물리적 혹은 논리적인 망분리를 통해 시스템 운영을 함으로써 보안을 강화하고 있다. 그러나 단순히 별도의 네트워크를 사용하는 것만으로 사이버위협으로부터 중요 정보의 보안을 완벽하게 보장하기에는 충분하지 않다[1].

특히, 이러한 배경 속에서 MDM, 이메일 서비스 등 내부 업무망으로의 데이터 유입과 처리가 필요한 시스템이 존재하기 때문에 물리적으로 분리되어 있는 인터넷망과 업무망 간에 망연동 솔루션을 통한 망의 연결 접점을 구성하는 연계적 시스템 구성이 불가피하다고 할 수 있다. 이는 내부 업무자료, 개인정보 등의 민감한 정보에 대한 취급과 처리되는 데이터의 양, 그리고 사이버 위협이 폭발적으로 급증하는 추세에 따라 데이터 처리에 대한 관리적, 기술적, 물리적 보호조치의 필요성도 커지고 있다[2].

따라서, 본 연구에서는 업무 특수성에 따라 보다 엄격한 망분리 보호기준을 적용받는 국방기관 및 방위산업체를 중심으로 물리적 망분리 환경에서 운영되는 MDM 시스템의 민감한 정보를 관리적, 기술적, 물리적 보호조치를 강구하여 데이터를 안전하게 처리하고 운영할 수 있는 다양한 기술 적용 방법과 구축 과정, 그리고 실제 적용 결과를 분석 및 검토하는 것을 목표로 한다.

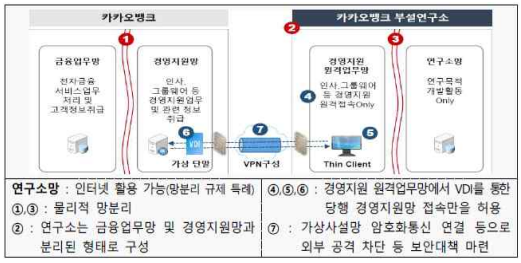
본 논문의 구성은 2장에서 망분리에 대한 규정 및 현황과 MDM 시스템에 대해 살펴보고 3장에서 망분리 환경에서 중요 데이터 처리 방안과 MDM에 적용할 기술을 검토하여 시스템 설계를 제시하였다. 4장에서는 실제 구현된 기능의 동작 형태와 성능 검증 결과 및 타 시스템과 비교분석을 통해 시사점을 제시하고 5장에서 결과에 대해 논의한다.

2. 관련 연구

2.1 망분리 규정 및 규제

인터넷망과 내부 업무망을 분리하여 운영하는 주체는 국가정보원의 「국가 정보보안 기본지침」을 따르는 공공기관과 「전자금융감독 규정」을 따르는 금융기관이 존재하며, 「국방보안업무 훈령」, 「국방사이버안보 훈령」을 따르는 국방부와 소속기관, 그리고 「방위산업기술 보호법」에 해당하는 관계기관과 방위산업체가 존재한다. 특히, 개인정보 처리에 관하여는 공공 및 민간부문의 모든 개인정보 처리자가 대상으로 「개인정보 보호법」에 따라 개인정보를 안전하게 취급하기 위한 보호조치가 요구된다.

한편, 공공기관과 금융권의 경우 엄격한 망분리 규제에 따라 디지털 신기술 도입과 활용을 위한 혁신을 저해한다는 지속적인 의견제기로 (그림 1)과 같이 망분리 규제의 특례 사례 등 개정과 보완이 이루어지고 있다. 특히, 연구·개발 분야에서 망분리 규제와 관련하여서는 금융규제 샌드박스를 통해 운영성과 및 안정성 등을 검증하여 개인정보를 처리하지 않는 것을 전제로 망분리의 예외허용 사례가 있다[3].



(그림 1) 카카오뱅크 '금융기술연구소' 운영 사례[3]

국방부 및 국방 산업의 경우, 취급하는 기술 및 주된 업무 사항이 곧바로 국가 보호자료 취급에 해당되며, 방위산업기술 연구·개발 자료는 국가 안보와 직결되므로 강력한 보호가 요구됨에 따라 물리적으로 인터넷망과 업무망을 분리하는 등의 엄격한 망분리 운영 기준을 적용받고 있으며, 공공 및 방위산업체에서는 전문 컨설팅을 받고, 물리적인 망 분리를 추진하고 있다[4].

2.2 망 연동장치 관리 대책

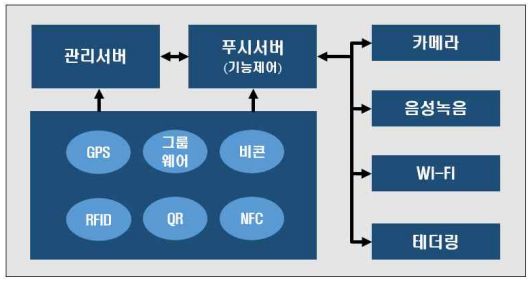
인터넷과 내부 업무망이 물리적으로 분리된 환경에서 양단 망 사이의 PC와 PC 간 및 서버와 서버 간 자료 연동이 필요하게 되었고, 정책적으로는 보안을 강화하면서 사용자의 업무 효율을 높이기 위한 기술적 해결책으로 망 연동장치의 필요성이 대두되었다[5]. 국방분야 외에도 에너지, 교통, 전기, 원전 등 국가 중요 제어시스템 운용 시에는 인터넷과 내부 업무망과는 분리하여야 하며, 국가 정보보안 기본지침 “국가·공공기관 제어시스템 보안가이드라인”을 준수하여 일방향 망 연동장치 구축·운용을 준수하도록 하고 있다[6]. 이와 같이 망 연동장치는 제어시스템으로부터 시작하였으며, 2008년도부터 국가 공공기관의 망분리 사업이 진행되면서 독립적으로 구축 운영되는 제어망을 업무망과 연결하기 위한 보안시스템으로 탄생하였다[7][8][9]. 망분리 환경 구축 후 내부망에서는 평상시 보안관제 이상징후 이벤트가 거의 탐지되지 않는다. 따라서 내부망 대상 사이버 공격에 특화된 위협 분석 및 대비를 통한 지속적인 보안관제 평가 모델이 필요하다[10]. 망 연동장치를 운영 시에는 자료연동 과정에서 외부 악성코드가 업무망으로 유입될 수 있어 보안 가이드를 준수하여 보안취약점을 제거 후 운영이 필수적이며 <표1>과 같은 주요 점검항목이 있다[11][12].

<표 1> 망 연동장치 보안점검 항목

분류	점검 항목
정책 관리	• 관리 책임자 지정
	• 초기 설정 비밀번호 변경
	• 관리자 PC IP만 접근 허용
데이터 관리	• 전송 자료 유형 정의
	• 전송 시 스토리지 내 데이터 즉시 삭제
	• 스토리지 접근권한 설정
	• 일시적 자료 저장 시 암호화하여 저장
서버 보안 관리	• 비인가 접근 차단
	• 인터넷 직접 연결 차단
	• 최신 보안 업데이트 적용
	• 불필요 서비스 사용 제한
기타	• 주기적 로그 확인

2.3 MDM 구성 요소

MDM 시스템의 일반적인 구조와 기능은 (그림 2)와 같이 MDM 관리서버, 정책·알림 푸시서버, 모바일 기기 제어 수단 및 항목으로 이루어진다.



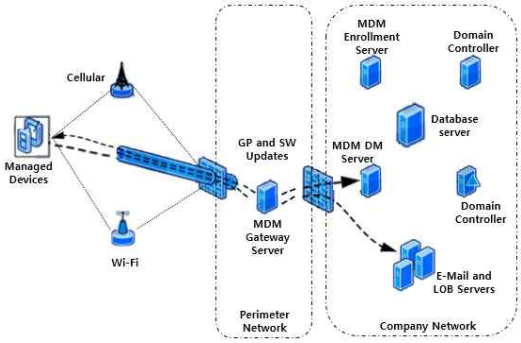
(그림 2) MDM 시스템 구성 요소

사용자와 기기 정책 구성 그리고 기기 관리를 처리하는 관리서버와 사용자 앱으로 정책 등의 명령을 전송하는 푸시서버, 그리고 모바일 기기에 설치되는 애플리케이션을 통해 정책을 송·수신하고 하드웨어(카메라, 녹음 등)를 제어하는 역할을 수행한다. 모바일 기기의 정책을 활성화 또는 비활성화하기 위한 부속환경으로는 GPS(위치정보), 그룹웨어 로그인 정보, 비콘, RFID(출입태그), QR코드, NFC 등 기관에서 운영하는 물리적 환경에 따라 다양하게 적용할 수 있다.

통신사 기지국을 통하여 상용 인터넷망으로 운영되는 모바일 기기를 제어하기 위해 기본적으로 MDM 시스템의 물리적인 네트워크 위치는 인터넷망에서 운영이 필요하다. 서버 역할에 따라 관리서버는 외부연결 접근을 통제하는 인터넷망 서버팜 영역(Private Internal Network Zone)에 설치하고, 모바일 기기로 정책전송을 위한 APNS(Apple Push Notification Service), FCM(Firebase Cloud Messaging) 통신을 처리하는 푸시서버의 경우 DMZ(Demilitarized Zone) 영역에 구축할 수 있으나, 강한 접근 통제와 보호가 요구되는 사용자 정보와 관리자 영역 등이 여전히 인터넷망에 위치함으로써 관리서버와 푸시서버가 연결되어 데이터 처리를 하므로, 고도화되는 사이버위협 공격에 노출되어 침해사고 우려가 여전히 존재한다고 볼 수 있다.

2.4 MDM 동작 절차

MDM 시스템 구축 후 조직의 구성원들이 소유하고 있는 모바일 기기에 설치를 안내하고, 애플리케이션을 유지관리하는 절차로 등록단계, 배포단계, 설치유도단계, 설치 후 관리 단계로 나눌 수 있으며, 등록단계는 관리자가 사내 배포 서버 또는 앱스토어를 통해 설치파일을 업로드하여 배포 목록에 등록하는 단계라고 할 수 있다. 배포단계는 배포할 애플리케이션을 배포할 대상을 선정하고, 배포기간을 설정하여 스케줄러에 등록하는 단계이다. 설치유도단계는 MDM 배포서버의 스케줄러에 의해 배포 대상 모바일 기기에 통신사의 Push Server를 통해 배포 신호를 전송하고, 신호를 수신한 모바일 기기는 다운로드 서버로부터 애플리케이션 다운로드 및 설치를 진행하고, 화이트리스트에 추가한다. 마지막으로 설치 후 관리 단계는 사용자의 모바일 기기에서 설치 유무 정보를 전송받아 설치된 디바이스를 정기적으로 모니터링하는 단계이다[13]. 각 과정별 MDM 서비스 구성은 (그림 3)과 같다.



(그림 3) MDM 서비스 구성도[14]

2.5 MDM 시스템 연구 동향

MDM 시스템과 출입 시스템을 연계하여 사내 모바일 기기 보안강화를 위해 회사 외부에서는 사내 메일 등 내부 컨텐츠 접근을 차단하여 모바일 기기의 보안을 강화하고 있다. 모바일 기기의 정책 제어를 위해 직원들이 출입증을 태깅하고, 게이트를 통과하여 사내로 진입 시 출입정보를 MDM 서버로 전송하고, MDM 서버는 통신사 Push 서비스와 연동하여 직원의 모바일 기기로 사전에 정의된 보안 정책을 적용하여 단말기 분실, 단말기 I/O 통제, 컨텐츠 보호, 사내 메일 실행 등의 기능을 통제할 수 있다[14]. 군에서는 모바일 기기의 영내 반입 사용으로 인한 군사자료 유출을 차단하기 위해 통제구역 출입 시에는 스마트폰 회수 등의 조치를 취하지만, 군 내 전 구성원을 대상으로 포괄적인 통제를 위해 MDM 시스템은 기술적으로 유효한 방안으로 대두되고 있다. 서경진[15]의 연구에서는 모바일 기기의 기능별 5가지 군사보안침해 가상 시나리오를 제시하며, 군에서 MDM 시스템의 성공적인 도입을 위해 예상되는 한계점 해결방안으로 모바일 기기의 NFC 기능과 RFID 출입시스템을 연계하여 작동하게 하는 기술적 해결방안과, MDM 관련 보안위반 규정과 같은 MDM 시스템에 대한 관리규정 필요성의 제도적 해결방안을 제시하고 있다. 배희성 외[16]의 연구에서는 OS 커널 수준에서 카메라 및 녹음 기능을 제어 가능한 프로토타입을 구현하여 일반적인 솔루션과 달리 커널 수준에서 모바일 기기의 제어 가능함을 확인하고, 커널 모듈을 적재 전과 후를 AnTuTu 벤치마크 도구를 활용하여 성능 상의 오버헤드로 인한 영향이 무시할 정도로 미미함을 증명하였다. 프로토타입 모델인 만큼 모바일 기기의 NFC 인증과 출입정보를 활용한 보안정책 적용 등의 확대가 필요하고, 통제할 대상 장치의 추가 연구 필요성을 제시하고 있다.

3. MDM 시스템 설계

3.1 운영관리를 위한 주요 기능

휴대용 상용정보통신장비로 분류되는 모바일 기기를 기관 내로 반입하는 경우 보안담당 부서를 통해 등록절차를 거쳐 등록번호를 부여받는 관리적 행정처리가 필요하다. 또한, 사용자 모바일 기기에 MDM 애플리케이션을 설치하고 사용자 등록(가입) 시 인가된 장비 여부를 확인하는 절차 또한 필요하다. 그러나 사용자 정보가 사전에 존재하지 않고 모바일 기기 등록여부를 판단할 수 없는 단기 방문객의 경우 개인정보 수집 최소화를 위해 소속기관 및 이름을 수집하여 처리한다.

시스템 관리·운영 부서에서는 MDM 애플리케이션이 설치되어 운영되고 있는 모바일 기기의 현황관리, 이에 따른 사용자 정보 및 부서 정보의 데이터 최신화가 필요하며, 관리대상의 모바일 기기에 정책이 적용된 이력관리가 요구된다. 그 밖의 MDM 시스템의 관리적 요소와 애플리케이션 정책 통제 등 보호조치가 요구

되는 기능은 <표 2>와 같다.

<표 2> MDM 시스템 요구 기능

분류	요구 기능
관리 요소	• 개인정보 보호조치 요구 기능
	• 인가된 장비 여부 확인 및 등록 처리
	• MDM 애플리케이션 설치 내역
	• MDM 보안정책 적용 내역
	• 앱 변경 방지(App Defense)
	• 앱 버전 관리
	• 임직원 / 방문객 이원화 관리
	• 민감 정보 암호화
보안 정책	• 통제 정책적용 및 서버 전송
	• 정책 제어 시작시간 노출
	• MDM 통신 불능 탐색 로직
	• 애플리케이션 삭제 방지 / 로그 전송

3.2 제어를 위한 주요 기술

MDM 애플리케이션을 통한 모바일 기기 제어 정책을 적용하기 위한 기술은 크게 상용 인터넷망 환경에서 적용 가능한 기술과 내부 업무망에서 적용 가능한 기술로 <표 3>과 같이 분류할 수 있다.

<표 3> 정책제어 기술 분류

구 분	정책제어 기술
상용 인터넷망	GPS(위치정보), NFC태그, 비콘(Beacon), 무선AP
내부 업무망	출입시스템(출입정보), QR코드, 그룹웨어(로그인 정보)

상용 인터넷망에서 처리가 가능한 기술로는 GPS(위치정보), NFC태그, 비콘(Beacon), 무선AP(Wireless Access Point) 등을 통해 제어가 가능하다.

GPS로 정책제어를 하는 경우 정책이 적용되어야 하는 구역을 지정하고 모바일 기기가 지정된 구역 내에 존재하는 경우 보안정책 활성화, 구역 외에 존재하는 경우 보안정책 비활성화되도록 처리한다. 이의 경우 보호가 필요한 대상 구역이 넓은 지형이 아닌 단일 건물 형태의 사무실인 경우 MDM 애플리케이션에서 사용자의 현재 위치정보가 정확하게 판단되지 않을 수 있어 실내에서 MDM 보안정책 적용이 제한될 수 있다.

NFC 태그는 태깅 시 처리할 애플리케이션의 Activity 호출 코드를 내장시켜 모바일 기기의 정책을 제어할 수 있다. 이에 따라 다양한 구성을 할 수 있으며 본 연구에서는 고정형 NFC 태그와 이동형 NFC 태그로 분류하여 구성하였다. 보호 구역 내에서 사용할 목적의 고정형 NFC는 모바일 기기 접촉 시 보안정책을 활성화되도록 설계하고, 이동형 NFC는 GPS(위치정보)로 처리하는 API를 호출하여 보안정책 동작을 연계 한다. NFC 안에 내장된 코드는 공개될 수 있는 데이터로, 해킹 수단으로 이용될 수 있는 가능성이 존재하여 보안정책을 비활성화하는 API는 설계하지 않았으며, 모바일 기기가 NFC 처리를 지원해야 적용가능하다.

비콘은 근거리에 있는 모바일 기기에 저전력으로 필요한 데이터를 전송할 수 있는 무선 통신 장치로 근거리 무선 통신인 NFC는 10cm 이내의 근거리에서만 작동하는 반면, 비콘은 최대 50m 거리에서 작동할 수 있다[17]. 비콘을 고정된 위치에 설치하여 모바일 기기가 비콘의 일정거리 이내에 존재하는 경우, MDM 애플리케이션에 적절한 보안 정책을 적용할 수 있도록 신호를 전송한다.

내부 업무망에서 처리 가능한 기술로는 사용자가 소지하고 있는 RFID 신분증(사원증) 카드로 건물에 출입한 정보를 바탕으로 건물에 들어갈 때 MDM 보안 정책을 활성화하고, 건물을 나갈 때 비활성화 정책을 전송하도록 설계할 수 있다. 이 경우 출입을 위한 단말기(RFID카드 리더)가 존재하지 않는 건물이거나 건물 밖 보안구역에서는 보안정책이 비활성화될 수 있다. 또한, 각 건물에 설치된 출입 단말기의 네트워크 오류 등에 의해 출입시스템 서버로의 데이터 전송이 지연되거나 전송 불능 상태의 경우 모바일 기기로 보안정책이 실시간으로 전송되지 않을 가능성 있다.

QR코드 기술의 경우 코드 내에 대상 기기정보, 보안정책 활성화·비활성화 등 처리할 데이터를 구성하여 MDM 보안 정책을 제어한다. QR코드 생성 모듈을 외부 개체로 구성하거나 MDM 애플리케이션에서

생성되도록 구성하는 양방향의 두 가지 처리 방법이 있으나, 전자의 경우 모바일 기기 내 카메라로 처리해야 하고 보안 활성화 정책 적용 시 카메라가 제어되어 사용이 불가하므로 후자의 방법으로 기술 적용이 요구된다. 이때, 생성된 QR코드를 재사용하거나, 타인에게 제공하는 등의 부정사용 방지를 위해 QR코드 사용 시간제한, QR코드 변경 등의 보안 기능이 구현되어야 한다. 내부 업무망에서 추가로 MDM 보안 정책을 제어 할 수 있는 방법은 그룹웨어 로그인 정보를 활용하는 방법이 있다. 사용자의 계정으로 그룹웨어 로그인에 성공하는 경우 MDM 보안정책을 활성화하는 명령을 전송하며, 그룹웨어를 로그오프 하는 경우는 사용자가 보안지역을 이탈하였다고 보장할 수 없으므로 보안정책 비활성화 명령 전송에 대한 기능은 별도로 구현하지 않는다.

3.3 민감정보 처리를 위한 모듈

3.3.1 처리대상 민감정보 식별

MDM 시스템에서 활용되는 데이터 중 민감정보로 취급되어야 하는 대상을 <표 4>와 같이 식별하였다.

<표 4> 민감정보 분류

정보생성 구분	민감정보 대상
기관내부 생성정보	• 사용자 정보(이름, ID 등)
	• 부서 정보
	• 기기 등록 번호
MDM 생성정보	• 전화번호
	• 기기 식별 값(Unique Key)
	• 방문객 이름 및 회사명
	• 정책 제어기술 정보
	• 각종 로그

외부로 유출되는 경우 민감하게 작용할 수 있는 임직원에 대한 인사정보와 그룹웨어에서 관리하는 인가된 모바일 기기에 대한 정보는 보호대책이 필요하다. 또한, MDM 애플리케이션 등록 시 수집되는 전화번호, 모바일 기기 정보, 방문객 이름 및 회사명을 개인정보 처리 데이터로 식별하였으며, MDM 운영을 위한 보안 정책제어 기술(GPS 등록정보, 출입시스템 단말기 관리정보, 비콘/무선AP 관리정보 등)의 경우 노출되었을 경우 시스템 운영에 치명적인 영향이 우려되어 민감정보로 분류하였으며, 시스템 운영 중 발생하는 설치 이력, 정책적용 이력 등 관리 대상이 되는 로그 자료 전체를 보호대상으로 식별하였다.

3.3.2 관리적, 기술적 보호조치

식별된 민감정보는 <표 5>와 같이 내부 업무망에만 존재하는 데이터와 인터넷망에도 반드시 존재해야 하는 데이터로 구분할 수 있다.

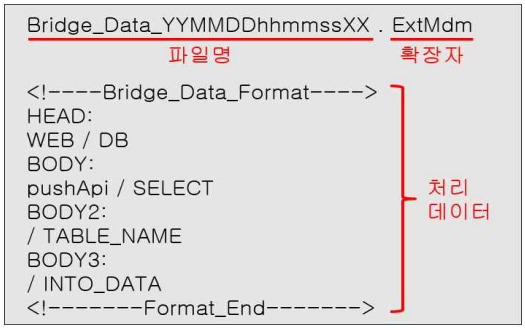
<표 5> 민감정보 별 처리 위치 구성

민감정보 대상	처리 위치
• 사용자 정보(이름, ID 등)	업무망 / 인터넷망
• 부서 정보	업무망
• 기기 등록번호	업무망 / 인터넷망
• 전화번호	업무망
• 기기 식별 값(Unique Key)	업무망
• 방문객 이름 및 회사명	업무망
• 정책제어 기술정보	업무망 / 인터넷망
• 각종 로그	업무망

MDM 시스템 운영을 위하여 반드시 인터넷망에 존재해야 하는 데이터의 경우 암호화 처리하여 사이버 위협으로부터 보호조치가 필요하다.

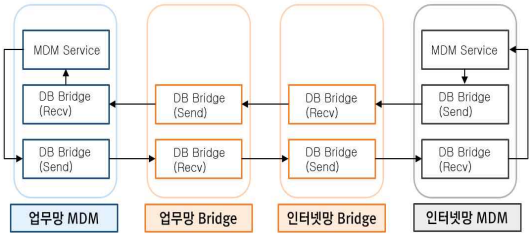
업무망에서 생성된 데이터가 인터넷망으로 전달되어야 하는 경우나 인터넷망에서 생성된 데이터가 업무망으로 전송되어야 하는 경우 망연동 솔루션을 통해 데이터가 전달되어야 한다. 이 경우 Command Injection, SQL Injection 등의 해킹 위협에 대비할 수 있도록 데이터 전송 모듈(Bridge)에서 사전에 정의된 데이터 형식인 경우에만 전송될 수 있도록 설계가 필요하다.

사전 정의되어 처리되는 형식에는 (그림 4)와 같이 파일명, 확장자 그리고 처리할 데이터의 내용을 세분화하여 처리할 수 있다. 정의된 데이터 형식이 아닌 경우 해당 데이터는 파기하며 처리하지 않는다.



(그림 4) Bridge 송·수신 사전정의 형식 예시

사전 정의된 데이터 처리 규약에 따라 업무망과 인터넷망 MDM 데이터베이스 간의 동기화 처리를 위해 Data Sync Bridge의 동작 과정은 (그림 5)와 같이 출입시스템 등 내부망에서 발생한 이벤트 정보와 외부에서 보안정책을 갱신하거나, 비콘, GPS 신호에 의한 보안정책 갱신 이벤트 정보를 DB Bridge 모듈을 통해 실시간으로 Sync 처리된다. Sync는 부하분산을 위하여 내부망에서 발생한 직원들의 이벤트 정보와 모바일 기기 상태값 데이터, 외부망에서 발생한 이벤트 처리가 별도의 Bridge를 통해 병렬로 이루어진다.



(그림 5) Data Sync Bridge 동작 과정

3.3.3 민감정보 가명코드 처리

인터넷망에서 운영 목적 상 반드시 존재해야 하는 데이터는 유출되어도 제대로 활용되기 어렵도록 가명코드를 별도로 생성하여 처리한다. (그림 6) 왼쪽 테이블에서 사용자 고유 식별자인 User_ID를 가명코드 처리하고 두 필드가 양쪽 네트워크의 각 서버 데이터베이스에 존재하지만 업무망에서는 실 데이터와 가명코드, 두 필드의 데이터를 저장하고 인터넷망에서는 가명코드 필드의 데이터만 저장 및 처리한다.

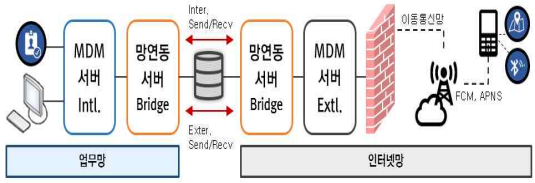
(그림 6) 가명코드 변경 적용 예시

내부망에서 대상 사용자의 실데이터를 참조하여 인터넷망에 전송 후 처리하고, 인터넷망에서는 오직 가명코드로만 데이터를 취급한다.

오른쪽 테이블의 경우 업무망에서 인가된 기기 등록 정보인 실데이터(Device_ID)가 MDM 에이전트에 출력되어 활용되어야 하므로 암호화하여 인터넷망에서 처리하고, Own_Dv_ID를 활용해 가입처리를 진행한다. 이는 보안강화 효과 외에 시스템 운영 처리 과정에서 데이터 암·복호화에 대한 시간을 감소시켜 가용성 측면에서 처리 효율을 증가시킨다.

3.4 MDM 시스템 구성도

MDM 운영을 위한 주 관리서버는 내부 업무망에 설치되고 인사DB가 연동되어 사용자 정보가 자동 업데이트되며 등록된 모바일 기기에 대한 현황관리, 정책적용 내역 등의 데이터 처리를 담당한다. 인터넷망에서는 MDM 정책 적용을 위한 최소한의 데이터만 저장 및 활용하여 모바일 기기를 제어하며, 시스템 구성은 (그림 7)과 같다.

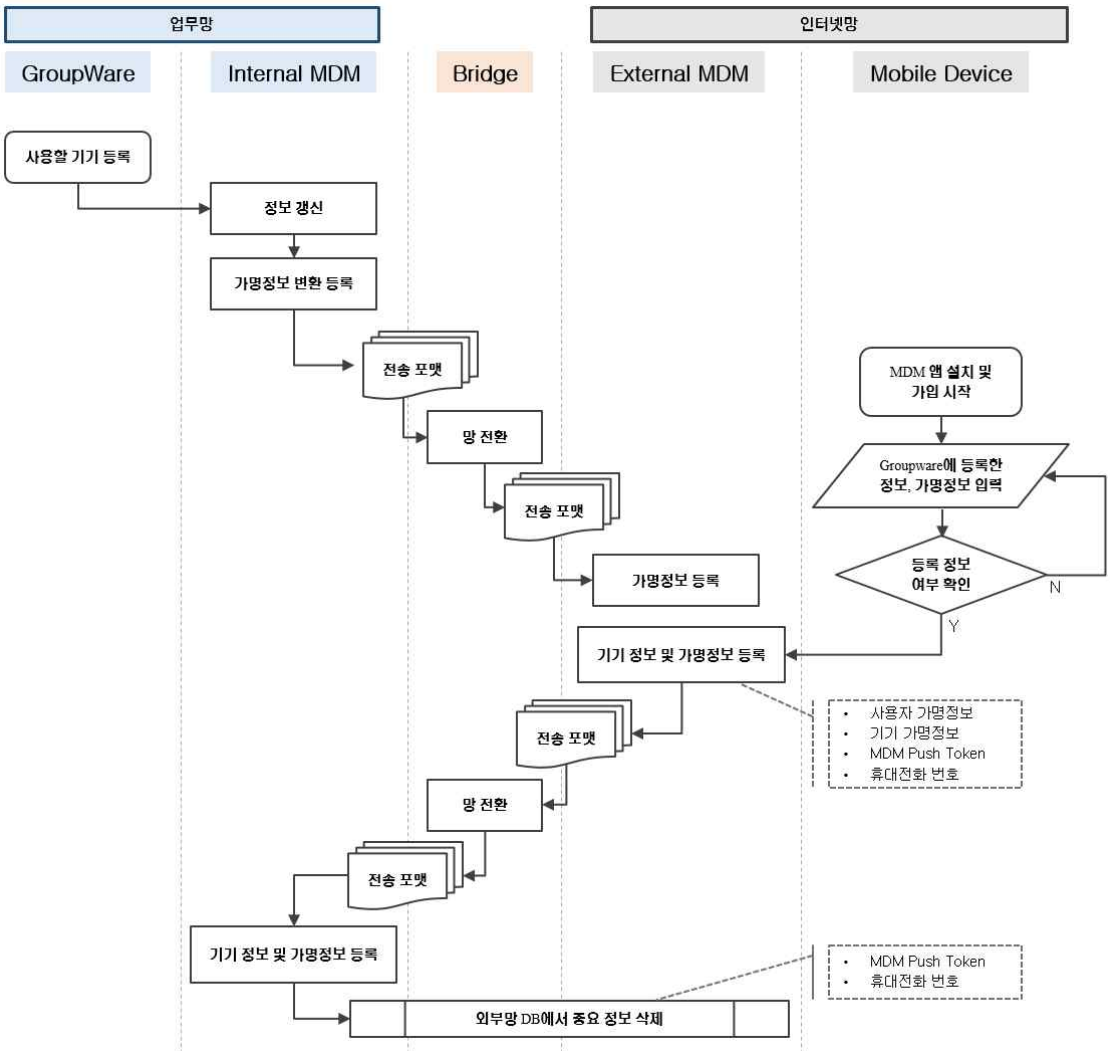


(그림 7) MDM 시스템 구성도

업무망 관리서버에서는 사용자 정보와 모바일 기기 관리 부서로부터 생성 및 인가된 모바일 기기 등록 번호에 대하여 가명코드를 생성하여 저장하고, 인터넷망의 관리DB에 전송·보관한다. 이후 사용자는 MDM 애플리케이션을 다운받아 설치하고 가입정보를 확인한 뒤 로그인할 수 있다.

업무망에 존재하는 정책제어 기술을 통해 정책이 적용된 경우, 대상 기기의 가명정보 만을 이용하여 정책 명령을 인터넷망으로 전송하여 처리하고 이후 처리 결과를 모바일 기기로부터 수신한 뒤 업무망에 전송 후 인터넷망에서는 데이터를 삭제한다.

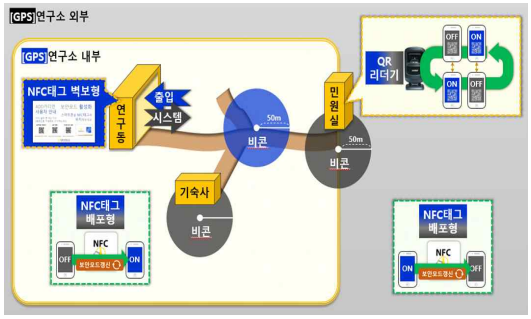
인터넷망에 존재하는 정책제어 기술을 통해 정책이 적용된 경우, 관리DB와 정책변경 요청을 Sync하여 정책을 처리하고 처리 결과를 기기로부터 수신한 뒤 업무망에 전송 후 인터넷망에서는 데이터를 삭제한다. 업무망과 인터넷망 간의 업무흐름 과정을 살펴보면 (그림 8)과 같다.



(그림 8) MDM 시스템 업무 흐름

4. MDM 시스템 구현

정책 처리 기술이 적용된 환경은 (그림 9)와 같으며, 보안 정책이 활성화되는 보호 구역과 비활성화되는 외부 구역으로 구분되어 정책이 동작하며, 건물 형태의 사무실, 실험을 위한 야외 환경 또는 네트워크가 존재하지 않는 구역 등의 각각 다른 특수한 환경에 맞게 유연한 보안정책 처리를 할 수 있도록 구현하였다.



(그림 9) 보안정책 처리기술 적용환경

4.1 외부망 처리 모듈

MDM 애플리케이션은 사용자 정보와 인가된 등록 기기를 갖추고 있는 임직원, 정보가 존재하지 않는 방문객을 구분하여 (그림 10)과 같이 두 가지 버전이 존재한다. 임직원의 경우 로그인 정보가 없거나 사용자 정보와 모바일 기기의 정보가 일치하지 않으면 로그인 처리 및 등록처리가 되지 않는다.

(그림 10) 사용자 및 기기 인증 등록 처리부

인터넷망에서 활용할 수 있는 정책처리 기술은 (그림 11)과 같이 위치정보, 비콘 그리고 NFC를 적용하였다. 위치정보는 설정된 보호구역 내에서 MDM 애플리케이션 안의 보안모드 갱신 버튼을 누르는 경우 보안 정책이 활성화되며, 보호구역 외에서 버튼을 누르는 경우 보안 정책이 비활성화된다.

비콘은 보안정책 활성화 비콘과 비활성화 비콘으로 구분되며, 비콘으로부터 근거리 내에 기기가 위치하면 정책이 적용된다.

NFC태그는 고정형의 경우 보안 정책을 활성화하고 이동형의 경우 위치정보 API를 참조하여 동작한다.

(그림 11) 인터넷망 정책처리 적용 기술

4.2 내부망 처리 모듈

내부망에서 활용할 수 있는 정책처리 기술은 (그림 12)와 같이 RFID 출입 태깅, QR코드 인식 그리고 그룹웨어 로그인 정보를 통한 처리 방식을 적용하였다.

출입시스템을 통해 보안정책 적용 시 각 건물별 출입단말기 정보를 목록화하여 단일 건물의 사무실 같은 GPS 위치정보로 정책 적용이 적절하지 않은 곳을 별도 관리하고, 해당 출입 단말기를 통해 출입한 경우 GPS 위치정보를 통해 비활성화 정책 적용이 불가하다.

(그림 12) 내부망 정책처리 적용 기술

보안 위협에 대한 요소와 출입에 대한 무분별한 보안 정책 갱신의 데이터 통신이 발생하지 않도록 지정된 시간 내에서는 활성화 보안정책만 전송하며, 출입시스템을 통한 비활성화 보안 정책은 처리하지 않는다.

QR코드는 MDM 애플리케이션 내의 기능을 통해 생성 가능하고 생성된 QR코드를 QR리더기에 인식시킴으로써 보안 정책이 동작한다. MDM 정책이 활성화

상태에서 QR코드를 처리하는 경우 비활성화 정책 명령이 처리되고, 현재 MDM 정책이 비활성화 상태라면 활성화 정책 명령이 처리된다. 그룹웨어 로그인은 업무망에서 그룹웨어에 로그인 시 보안정책 활성화 옵션 선택 후 로그인에 성공하는 경우 대상 사용자가 보유한 모바일 기기 전체로 활성화 보안정책 명령을 전송한다.

또한, 정책명령 발송, 관리자 콘솔 등의 관리업무 시스템을 내부 업무망에 설치하여 업무 처리와 민감정보에 대한 관리 편의성 증가 및 보안위협으로부터 물리적으로 격리시킬 수 있으며, 내부망에서 관리할 경우 인터넷망 전용 접속 단말기가 불필요하여 보안취약 요소를 감소시킬 수 있다.

4.3 망연동 구성 성능 테스트

보안정책 갱신 과정을 살펴보면 출입 태깅과 같은 보안정책 갱신 이벤트 발생 시 태그 리더기로부터 내부망 MDM 서버를 거쳐 인터넷망 MDM 서버까지 망 연동시스템을 통해 데이터가 전송되고, 사용자 모바일 기기로 보안정책 갱신 Push 신호가 발송된다. 성능 측정은 인터넷망 관리서버 DB로 이벤트가 수신되고 보안정책이 갱신되기까지의 처리시간과 처리량을 측정하여 본 연구에서 제안하는 모델에 대한 성능의 적정성을 검증하였다. 본 연구에서 제안하는 모델은 1회 망연동 시스템으로 이벤트 전송 시 파일 I/O 효율성을 극대화하기 위해 500개의 트렌젝션을 한 세트로 묶어 전송한다. (그림 13)은 임의의 500개 트렌젝션 한 세트의 처리시간 일부 자료이며, 한 세트 처리의 평균시간은 8초 정도 소요되었으며 실시간 이벤트 처리 성능을 확보하였다.

sync_db_no	create_time	recv_time
523,001	2023-03-20 15:15:41	2023-03-20 15:15:48
523,002	2023-03-20 15:15:41	2023-03-20 15:15:48
523,003	2023-03-20 15:15:41	2023-03-20 15:15:48
523,004	2023-03-20 15:15:41	2023-03-20 15:15:48
523,005	2023-03-20 15:15:41	2023-03-20 15:15:48
523,006	2023-03-20 15:15:41	2023-03-20 15:15:48
523,007	2023-03-20 15:15:41	2023-03-20 15:15:48
523,008	2023-03-20 15:15:41	2023-03-20 15:15:48
523,009	2023-03-20 15:15:41	2023-03-20 15:15:48
523,010	2023-03-20 15:15:41	2023-03-20 15:15:48

이하생략

(그림 13) 보안정책 갱신 이벤트 처리시간 발췌

4.3.1 성능 테스트 시나리오

발생하는 이벤트 별 처리에 대한 성능을 테스트하기 위하여 <표 6>의 시나리오로 진행하였다. 첫 번째는 범위의 시간(1H) 동안 인터넷망 MDM 서버에서 발생한 이벤트를 측정한다. 두 번째로 대상 이벤트에 대해 초당 처리된 레코드의 양(TPS)을 측정하고 Data Sync에 소요된 평균 시간을 측정한다.

<표 6> 성능 테스트 시나리오

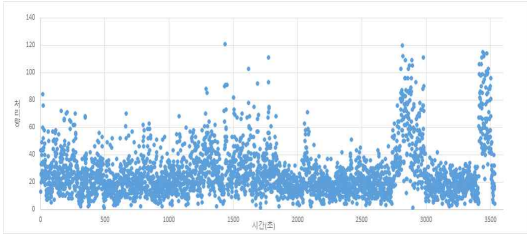
구분	주요 내용	비고
1차	• 1H 동안 이벤트 발생량 측정 • TPS 측정	
2차	• Bridge 전송 포맷 별 이벤트량 측정 • 전송 포맷 별 평균 처리시간 측정	max(500)

4.3.2 성능 테스트 결과

최대 퍼포먼스의 측정을 위하여 레코드 발생량이 가장 많은 퇴근시간(17:30~18:30, 1H) 동안의 데이터를 분석하였으며, 1차 시나리오의 성능 측정 결과는 <표 7>, (그림 14)와 같다.

<표 7> 트렌젝션 발생량 및 TPS

시간(초)		발생량	TPS(avg.)
~600		14,623	24.3717
~1200		13,570	22.6167
~1800		18,801	31.335
~2400		11,905	19.8417
~3000		19,835	33.0583
~3600		14,651	24.4183
합계	평균	93,385	25.9403

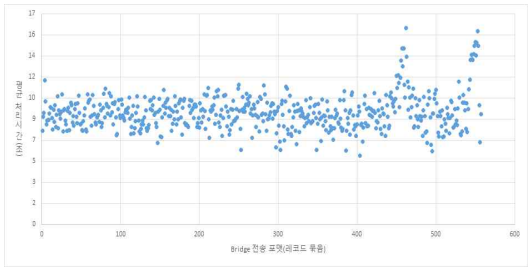


(그림 14) 트렌젝션 발생량

18시, 18시 20분과 18시 30분에 중점으로 트렌젝션이 많이 발생하였고 그에 따른 시간당 처리량이 높아졌음을 확인하였다. 2차 측정 시나리오는 Data Sync를 위하여 다량의 트렌젝션을 1개 세트(최대 500개 트렌젝션)로 처리하여 각 세트 별 평균 처리 시간은 <표 8>, (그림 15)와 같다.

<표 8> 세트(묶음) 별 처리 시간

세트(묶음) (개)	평균 처리 시간 (초)
~100	9
~200	9
~300	9
~400	9
~500	10
~557	10



(그림 15) 세트(묶음) 별 처리 시간

측정 시간 동안 557개의 세트(묶음)가 처리되었으며, 트렌젝션 발생량이 증가한 약 450번, 550번 구간에서 약간의 처리 속도 지연이 발생하였음을 확인하였으며, 각 묶음 별 처리할 트렌젝션 수의 차이가 있었으나, 처리 시간 차로 인한 운영상의 영향은 무시할 정도로 미미하였다.

4.4 선행 연구와의 비교

본 연구에서 제안하는 물리적 망분리 환경과 민감정보 보호를 위해 관리자 시스템을 내부 업무망에 구축하고 양 서버 간 Data Sync 구조의 MDM 구축사례는 많지 않다. <표 9>는 운영 환경에 따른 본 연구 모델의 효과를 나타내고 있으며, 일반적인 MDM 시스템 선행 연구와 비교하여 시사점을 요약하면 다음과 같다.

<표 9> 운영 환경에 따른 효과

구분 \ 운영 환경	내부망 처리	인터넷망 처리
보안성(기밀성)	High	Low
가용성	High	Middle
효율성	High	Middle
편의성	High	Middle

첫째, 기존 MDM 시스템 구조와 달리 개인정보와 같은 엄격하게 보호가 필요한 민감한 데이터를 물리적으로 분리된 내부 업무망에서 처리함으로써 시스템 운영 간 데이터 암·복호화에 필요한 소요시간 및 과정을 단축시킬 수 있다. 둘째, 인터넷망에서 발생하는 사이버 공격으로부터 관리자 시스템을 물리적으로 분리시켜 안전한 환경에서 시스템을 운영할 수 있다. 셋째, 안전한 민감정보 처리와 동시에 NFC, 비콘, 그룹웨어 로그인 정보, GPS 등 다양한 정책제어 수단을 적용하여 MDM의 주요 기능인 카메라, 녹음기, 테더링, WiFi 등 모바일 기기의 기능을 효과적으로 제어할 수 있다. 넷째, 보안정책 해제 전용 NFC 태그를 사용자들에게 배포하여 외부에서 정책 해제 시 간단한 태깅만으로 정책 갱신이 가능하여 사용 편리성과 만족을 증가시켰다.

5. 결론

방위산업 관련기관 및 기업이 처리하는 업무의 영역은 국가 안보와 직결되는 만큼 보안에 대해서는 강도 높은 수준이 요구되고 있다. 그중 하나가 모바일 기기의 사용으로 자료유출에 대한 위협을 해소하기 위하여 MDM 솔루션을 도입하여 운영하는 것이다. 그러나 단순히 보안을 위한 통제의 범위를 넘어 민감한 정보를 처리하기 위한 기술적, 관리적 보호가 요구되고, 무기체계 실험 장소와 같이 특수한 물리적 환경과 네트워크 환경을 고려하여 정책을 적용하기에는 기존 MDM 시스템 구조로는 한계점이 존재한다. 이를 위해 망분리 환경을 활용하여 관리자 시스템을 인터넷으로부터 분리하고,

민감 데이터를 보다 안전하게 처리할 수 있는 가능성을 본 연구를 통해 실증하였다. 다만, 시스템 구조상 내·외부망 데이터베이스 간 모바일 기기의 실시간 상태정보 등 동기화 작업이 수반되며, 망분리 환경 구축을 위한 서버, 스토리지, 망연동 장치 등이 추가적으로 소요되어, 구축비용과 관리 포인트 증가로 이어질 수 있다.

향후 연구로는 망분리 환경에서 내·외부망 데이터베이스 동기화 모듈의 안정성과 효율성을 높이기 위해 최소한의 필수 데이터만 Sync 될 수 있도록 최적화가 필요하다.

참고문헌

[1] 조병주, 윤장호, 이경호, “금융회사 망분리 정책의 효과성 연구,” 정보보호학회논문지, 제25권, 제1호, pp.181-195, 2015.

[2] 이선재, 이일구, 안예린, 박소영, 윤지희, 정유진, 최유림, 윤선우, 정다은, “사이버보안 위협 분석 및 개선 방안에 대한 연구,” 한국산업보안연구, 제9권, 제1호, pp.69-97, 2019.

[3] 금융감독원, “[보도자료] 클라우드 이용절차 합리화 및 망분리 규제 완화를 위한 「전자금융감독규정」 일부개정고시안 금융위 의결,” 2022.

[4] 장경준, “방산업체 망 분리 사업 성공을 위한 제언,” 한국방위산업진흥회, 국방과 기술, 제459호, pp.100-105, 2017.

[5] 이현정, 조대일, 고갑승, “망분리 환경에서 안전한 서비스 연계를 위한 단방향 망간자료전송 시스템 보안 모델 연구,” 융합멀티미디어논문지, 제5권, 제6호, pp.539-547, 2015.

[6] 김경호, 장엽, 김희민, 윤정한, 김우년, “제어망 특성을 반영한 물리적 일방향 자료전달 시스템 설계,” 정보과학회논문지, 제40권, 제2호, pp.126-130, 2013.

[7] 지정은, 이상지, 이성렬, 배병철, 신용태, “사이버 해킹 및 테러 공격 대응을 위한 논리적 망분리 기법,” 정보과학회논문지, 제39권, 제1호, pp.95-101, 2012.

[8] 장문수, 김신규, 민병길, 서정택, “제어시스템 보안제품 기술동향 분석을 통한 기술 요구사항 도출에 관한 연구,” 보안공학연구논문지, 제5권, 제4호, pp.35-45, 2008.

[9] 김민수, 박기태, 김종민, “국가·공공기관 전산망 특성에 따른 사이버 위협 분석 및 분류에 관한 연구,” 융합보안논문지, 제20권, 제4호, pp.197-208, 2020.

[10] 이동휘, 김홍기, “망분리 네트워크 상황에서 사이버보안 취약점 실시간 보안관제 평가모델,” 융합보안논문지, 제21권, 제1호, pp.45-53, 2021.

[11] 국방부, 국방사이버안보 훈령, 2019.

[12] 국방부, 국방 정보체계 망 연동 보안 가이드라인, 2017.

[13] 임준호, “MDM 시스템에서 모바일 애플리케이션의 보안 위협 요소 최소화 방법,” 아주대학교 석사학위논문, 2014.

[14] 한송훈, “MDM과 출입 시스템을 연계한 모바일 보안 시스템 구축 사례 연구,” 단국대학교 석사학위논문, 2012.

[15] 서경진, “軍내 이동전화 통제에 관한 연구 - 모바일단말관리 시스템을 중심으로-,” 한성대학교 석사학위논문, 2013.

[16] 배희성, 김소연, 박태규, “리눅스 보안 모듈을 이용한 모바일 장치 통제 시스템,” 정보보호학회논문지, 제27권, 제1호, pp.49-57, 2017.

[17] 위키백과, “ko.wikipedia.org/wiki/블루투스_비콘,” 2023.

〔저자소개〕

이 주 승 (Juseung Lee)
2012년 12월 Shepherd University B.S.
2018년 8월 아주대학교 석사
현 재 국방과학연구소 선임기술원

email : ljs-1212@hanmail.net

김 일 한 (Ilhan Kim)
2008년 8월 충남대학교 석사
2021년 2월 충북대학교 박사
현 재 국방과학연구소 선임기술원
정보보호팀장

email : ilhan2676@hanmail.net

김 현 수 (Hyunsoo Kim)
2010년 5월 Carnegie Mellon University B.S.
2013년 2월 연세대학교 석사
현 재 국방과학연구소 선임연구원

email : rmffpd@gmail.com