The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 23, No. 6, pp.171-177, Dec. 31, 2023. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2023.23.6.171
JIIBC 2023-6-25

MDM 앱에 적용되는 위치 기반 통제 기능의 효율화 방법에 관한 연구

A Study on the Efficiency Method of Location-Based Control Function Applied to MDM Applications

오창익*, 황수길*, 손현*, 김동호**

ChangIk Oh*, SuGil Hwang*, Hyun Son*, Dongho Kim**

요 약 중앙 통제 서버 없이 앱만으로 MDM 서비스를 구성하는 경우, 보안 통제가 필요한 직장의 위치 정보를 MDM 앱에 내장하여 배포함으로써 직장의 보안 영역과 충분히 떨어진 지역에서는 GPS 신호를 기반으로 보안 통제를 해제할 수 있도록 하는 방식이 일반적으로 적용되고 있다. 본 연구에서는 직장 등 특정 구역의 위치 정보를 MDM 앱에 내장하여 배포하지 않고 배포된 앱에서 각 개인이 자신에게 필요한 보안 통제구역의 위치 정보를 직접 입력하여 설정 정보로써 유지하는 방식을 제안하였다. 본 연구에서 제안한 방법을 통해 MDM 서비스의 보편성과 호환성을 향상하여 구축 비용을 최소화할 수 있으며, 추가적인 기능 구현을 통해 보안 통제 수준 또한 향상할 수 있다.

Abstract When configuring MDM services only with applications without a central control server, a method that allows security control to be released based on GPS signals in areas sufficiently far from the security area of the workplace is generally applied by embedding and distributing location information of workplaces in MDM applications. This study proposed a method in which each individual directly enters the location information of the security control area needed for them in the distributed app and maintains it as setting information without embedding location information of a specific area such as work in the MDM applications. The method proposed in this study can improve universality, compatibility and the security control level of MDM services, and minimize deployment costs.

Key Words : MDM Applications, GPS, Location-Based Control, Security check, Information leakage

Ⅰ. 서 론

정보통신기술의 획기적인 발전으로 인해 스마트폰 사용이 보편화되었고, 스마트폰을 통한 사진 촬영과 사진 파일의 전송 · 공유 또한 일상화되었다. 직업인으로서 개인 대부분은 직장에 스마트폰을 반입하여 사용하고 있으며 직무를 수행하는 데에도 스마트폰을 사용함에 따라, 각 직장은 직무 관련 자료의 촬영 및 전송 · 공유를 통한 조직 내부의 기밀정보가 외부에 유출될 수 있는 환경에 놓여 있다[1]. 이와 더불어 외주 인력에 의한 민감 정보의 유출 위험 또한 증가하고 있다[2].

주요 기업과 공공기관, 연구소, 군부대에서는 스마트

*정회원, 숭실대학교 IT정책경영학과
**비회원, 숭실대학교 글로벌미디어학부 교수, 교신저자
접수일자 2023년 10월 30일, 수정완료 2023년 11월 30일
게재확정일자 2023년 12월 8일

Received: 30 October, 2023 / Revised: 30 November, 2023 / Accepted: 8 December, 2023
*Corresponding Author: dkim@ssu.ac.kr
Dept. Soongsil University Global School of Media. Korea

폰을 통한 직장 내부의 중요정보 유출을 방지하기 위하여 MDM(Mobile Device Management) 기술을 도입하여 운용하고 있으며, 이와 더불어 스마트폰 카메라에 보안스티커를 붙이는 방식도 보편적으로 사용되고 있다[3].

보안 통제의 대상이 되는 스마트폰 대부분은 개인 소유의 스마트폰이기 때문에 MDM 기술을 통해 스마트폰을 통제하는 데에는 한계가 있을 수밖에 없다. 임직원 중 일부와 외부인, 방문자 등 일시적으로 출입해야 하는 경우 MDM을 통한 통제 적용을 거부할 수 있으며, 이에 따라 보안스티커를 사용하는 방식도 병행하여 운영하고 있다.

본 연구에서는 보안스티커를 사용하는 보안 수준의 MDM 서비스로써 별도의 중앙 통제 서버 없이 앱 자체만으로 작동하는 MDM 구성에서, 위치 기반 보안 통제 적용 및 해제 기능을 효율화하는 방법을 제안하고자 한다. 연구에서 제안하는 방법을 구현함으로써 분산된 여러 사업장에서 동일 MDM 앱을 사용하여 스마트폰 카메라 등을 차단할 수 있으며, 이를 통해 최소비용으로 임직원 스마트폰에 대한 보안 통제가 가능하다.

II. 이론적 배경

1. MDM(Mobile Device Management)

MDM(Mobile Device Management)은 기업 또는 기관에서 스마트폰, 태블릿 등의 모바일 장비들을 효과적으로 관리하고, 보안을 유지하며, 기능 제한 및 사용자 권한을 제어하는 것을 목표로 하는 기술이다[4]. 주요 기능으로는 애플리케이션 이용 제한, 카메라 마이크 제한, 공유 기능 제한, 분실 시 원격 삭제, VPN 등이 있고 그 외에도 추가적인 보안 향상 기능을 포함하는 경우가 있다.

일반적인 MDM 서비스는 그림1과 같이 직장 건물의 출입 통제 시스템과 연동되어 있으며, 개인의 출입 정보를 처리하여 모바일 통신망을 통해 출입자의 앱의 차단 기능이 작동하게 하는 방식으로 구성된다. 이러한 방식은 건물 출입 시 출입자의 모바일 보안 통제가 자동으로 작동 또는 해제되어 사용자 편의성을 보장할 수 있으며, 전체적인 보안 통제 상황을 통합 관제할 수 있다는 장점이 있다. 하지만 출입 통제 시스템이 구축된 경우에만 적용할 수 있고, MDM 서버에 출입자 개인의 휴대전화 번호 등 개인정보를 일일이 등록하여 관리해야 한다는 제한 사항이 있다.

MDM 서비스를 구축하는 또 다른 방식으로 그림2와 같이 출입 통제 시스템과의 연동 없이 MDM 앱만으로 운용할 수도 있다. MDM 앱 단독 운영 방식에서는 모바일 보안 통제 작동 또는 해제를 위해 NFC와 비콘 등의 장치를 사용하는데[5], 이 중 비콘 장치는 BLE(Bluetooth Low Energy) 기술이 적용되어 50m 범위 안에서 스마트폰과 무선통신이 가능하며, 스마트폰에 설치된 MDM 앱에 보안 통제 해제 신호를 보내는 데 활용된다[6]. 직장 출입 정문에서 충분히 떨어진 지역에서는 GPS 신호를 수신하여 보안 통제를 해제할 수도 있다.

이러한 앱 단독형 서비스 구성으로 운영하기 위해서는 모바일 보안 통제 작동 여부를 보안담당자가 눈으로 직접 확인하여 출입을 허용해야 하는 제한 사항이 있다.

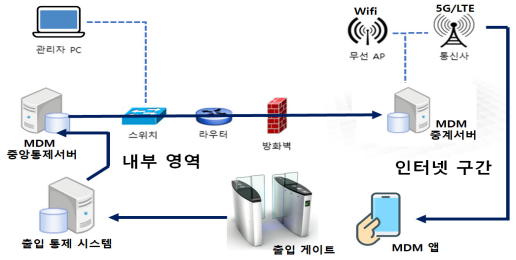

그림 1. 일반적인 MDM 구성도
Fig. 1. Typical MDM Configuration Diagram

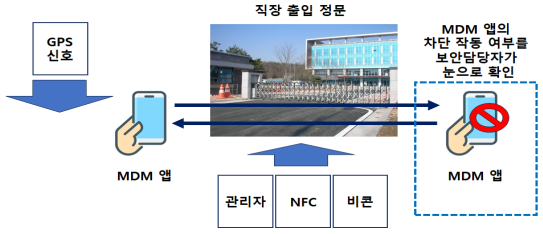

그림 2. MDM 앱 단독 운영 방식 서비스 구성도
Fig. 2. Configuration diagram of services run solely by MDM applications

2. 관련 보안 규정

국가기관 · 지방자치단체 · 교육청 및 그 소속기관, 공공기관, 국 · 공립학교, 군(軍)기관 등에 적용되는 국가 정보보안 기본지침에 MDM 적용에 대한 규정이 포함되어 있다. 국가 정보보안 기본지침 제79조(비인가 기기 통제)의 제3항에는 '개인 소유의 정보통신기기가 업무자료를 외부로 유출하는데 악용될 수 있거나 소속된 기관의 정보통신망 운영에 위해가 된다고 판단되는 경우 반출 · 입 통제, 보안소프트웨어 설치 후 반입 등 보안대책을 수립 · 시행하여야 한다'라고 명시되어있다.

3. 선행연구

보급형 국방 모바일 통제체계 개발에 관한 연구에서는, NFC 태그 중심의 보안 통제 적용 및 해제 기능을 적용한 보급형 MDM 서비스를 제안하였는데, 연구를 통해 개발한 MDM 서비스의 운영 프로세스는 그림3과 같다[7].

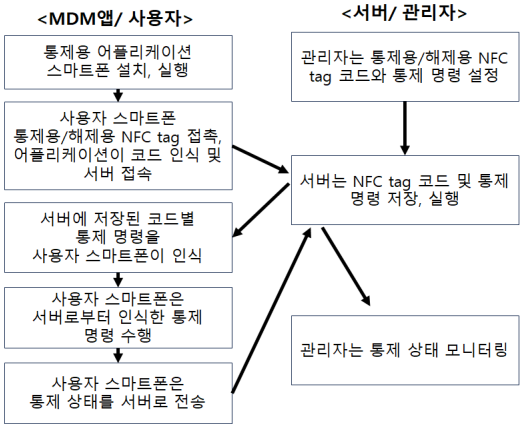

그림 3. 선행연구에서 제시한 MDM 기능의 운영 프로세스
Fig. 3. Operational processes of MDM functions presented in previous studies

해당 연구에서는, 제안한 MDM 서비스를 운용하는 데 있어 별도의 통제 서버 없이 통제 대상자들의 모바일기기 정보를 등록할 저장 공간만 필요하다는 점을 강조하고 있다. 하지만 사용자의 휴대전화 번호 등 개인정보 수집 및 저장, 사용자별 관리자 지정 및 변경 등 시스템 운용을 위한 관리 기능의 복잡성을 제대로 제시하지 않았으며 이에 따른 구축 비용 또한 제대로 산정하지 않았다. 해당 MDM 서비스는 적용 대상자가 증가함에 따라 조직의 보안 관리 업무에 새로운 과업이 추가되는 등 운용 비용이 증가할 것이라는 점 또한 쉽게 예상할 수 있다.

해당 연구에서는 소규모 조직 범위에서 운용한 사례를 제시했을 뿐, 보편적 적용을 위한 운용 및 관리 주체 또한 명확히 설정하지 못하였다. 보안 통제 해제 기능을 NFC 태그에만 의존하는 점 또한 사용자 편의성을 저해하므로 보편성 측면에서 문제가 있는 요소이다.

Ⅲ. 위치 기반 통제 기능의 효율화 방법

중앙 통제 서버 없이 앱 단독으로 MDM 서비스를 구성하는 방식에서는 직장 건물에 들어오는 사람들에 대해 모바일 보안 통제 작동 여부를 철저히 확인하는 것과는 다르게, 건물에서 나가는 사람에 대해서는 별도로 통제하지 않는다. 따라서 모바일 보안 통제를 해제하는 것 또한 출입자가 자율적으로 알아서 처리해야 하므로, 사용자의 편의성 지원을 위해 직장 외부 지역에서의 GPS 신호 기반 해제 기능은 필수적으로 제공해야 한다.

이러한 MDM 서비스 구성에서 일반적으로 적용하는 GPS 신호 기반 해제 기능은, 그림4와 같이 보안 통제가 필요한 직장의 위치 정보를 MDM 앱에 내장하여 배포함으로써 직장 보안 영역과 충분히 떨어진 통제반경 밖의 지역에서는 GPS 신호를 기반으로 보안 통제를 해제할 수 있도록 구현된다. 이때 직장 위치 정보를 노출할 수 없는 경우에는 직장 외부에 별도의 해제 가능 구역을 설정하여 운영하는 방법을 적용할 수도 있다.

하지만 해제를 요청하는 위치의 적정성을 확인하기 위해 직장 등 특정 구역의 위치 정보를 MDM 앱에 내장하여 배포함에 따라 MDM 서비스의 보편성 또는 호환성은 저하된다. 따라서 MDM 서비스의 보편성 또는 호환성을 향상하기 위해 위치 기반 차단 및 해제 기능을 효율화하는 방법이 필요하다.

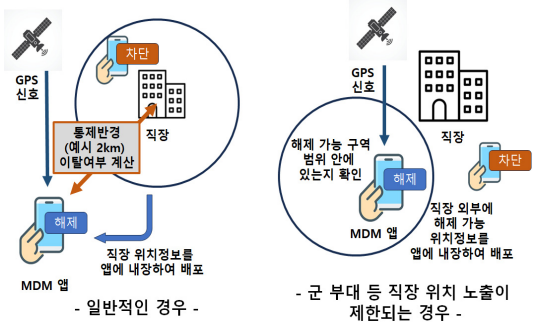

그림 4. 일반적인 MDM 앱 단독 운영 방식에서의 GPS 신호 기반 해제 기능
Fig. 4. GPS signal-based release function in a typical services run solely by MDM applications

1. 개인별 통제구역 설정

본 연구에서 제안하는 위치 기반 통제 기능의 효율화 방법은 직장 등 특정 구역의 위치 정보를 MDM 앱에 내장하여 배포하지 않고, 배포된 앱에서 각 개인이 자신에게 필요한 보안 통제구역의 위치 정보를 직접 입력하여 설정 정보로써 유지하는 방식으로 작동한다.

보안 통제구역의 위치 정보 입력은 사용자 개인이

자율적으로 수행하는데, 보안 통제가 해제된 상태에서만 활성화되며, GPS 또한 활성화되어 있어야 한다. 사용자가 편리하게 위치 정보 설정을 진행할 수 있도록 앱 화면에 현재 위치와 반경을 표시하고 현 위치 선택 시 해당 정보가 앱에 저장되도록 입력 기능을 구현할 필요가 있다.

보안 통제구역의 위치 정보 설정이 완료되면, 그림5와 같이 해당 정보를 가지고 GPS 기반 해제 기능이 지원된다. 또한, 직장 출입 시 사용자가 MDM 앱의 모바일 보안 통제를 작동하는데, MDM 앱에서는 직장 출입문에서 수신되는 GPS 위치 정보와 개인이 설정한 위치 정보를 비교하여 위치 정보 간 일치 정도를 확인하여 적정한 경우 모바일 보안 통제가 작동하게 한다. 이후 보안담당자는 모바일 보안 통제 작동 여부를 눈으로 확인하여 출입을 통제한다.

개인이 설정한 위치 정보가 직장 출입문에서 수신되는 현장 GPS 위치를 기준으로 하는 비교반경 외부에 있는 경우나 통제반경 밖 원거리로 떨어져 있는 경우에는 보안 통제 미작동 상태가 유지되고 보안담당자는 이를 확인하여 출입을 불허하게 된다. 이때, 사용자는 직장 출입문에서 수신되는 GPS 위치 정보를 보안 통제구역의 위치 정보로 다시 설정하여야 한다.

이와 같이 설정한 위치 정보와 원거리로 떨어져 있는 지역에서 보안 통제 미작동 상태가 유지되는 방식은, 직장 외부의 자택 등에서 MDM 앱 보안 통제가 잘못 작동하는 상황을 방지하는 기능으로도 활용될 수 있다.

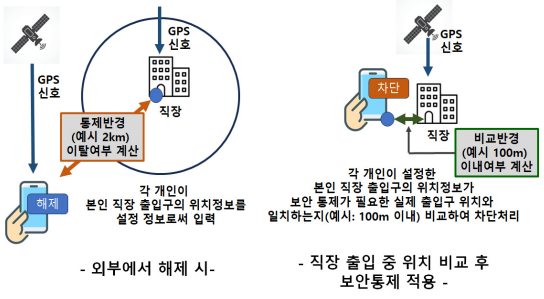

그림 5. 위치 기반 통제 기능 효율화 방법의 개념도
Fig. 5. Conceptual diagram of location-based control function efficiency methods

2. 3가지 운영 상태

보안 통제구역의 위치 정보를 사용자가 직접 입력하여 설정 정보로써 유지하는 방식으로 운용하기 위해서는, 모바일 보안 통제 해제 상태와 더불어 모바일 보안 통제가 작동하는 상태를 두 가지로 구분할 필요가 있다. 그림6과 같이 모바일 보안 통제가 작동하는 상태는 직장 출입문에서 수신되는 현장 GPS 위치 정보로 검증한 상태와 모바일 보안 통제가 계속 작동하고 있는 상태 두 가지로 구분한다.

모바일 보안 통제가 계속 작동하고 있는 차단유지 상태는, 카메라 등이 차단은 되어있으나 직장 출입문에서 수신되는 현장 GPS 위치 정보를 검증한 뒤 시간이 흘러 위치 확인이 제한되는 상태를 나타낸다. 개인이 자신에게 필요한 보안 통제구역의 위치 정보를 직접 입력하는 방식에서는 직장 출입문에서 매번 직장 출입문의 GPS 위치 정보 검증을 시행해야 하며, 검증된 상태는 시간이 지남에 따라 검증 불가 상태가 되므로 그러한 상태를 표시하기 위해 차단유지 상태임을 앱 화면에서 보여줄 필요가 있다.

직장 외부에서 보안 통제를 해제하지 않고 차단유지 상태에서 다시 직장에 출근하는 경우를 고려하여, 차단유지상태 화면에 출입 점검 버튼을 제공한다. 출입 점검 버튼을 누르면 개인이 설정한 위치 정보를 검증하여 비교반경 내부에 있는 경우, 차단 확인 상태로 변경되어 보안담당자가 보안 통제 작동 여부를 확인할 수 있게 되고 이후 다시 차단유지상태로 전이된다.

차단유지상태에서 출입 점검 버튼을 누르더라도 개인이 설정한 위치 정보가 적정하지 않은 경우, 차단 확인 상태로 변경되지 않는데, 이때는 비콘 등을 활용하여 보안 통제를 해제한 후 위치 정보를 수정하여야 한다.

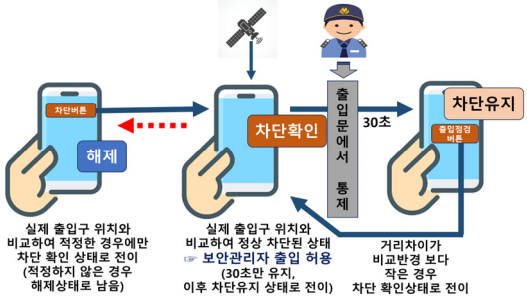

그림 6. 모바일 보안 통제가 작동하는 3가지 상태
Fig. 6. 3 states where mobile security controls work

차단유지 상태에서 사용자가 직장 외부로 나가 직장과 충분히 떨어진 지역으로 이동한 때에는 그림7과 같이 GPS 기반 해제가 가능하다.

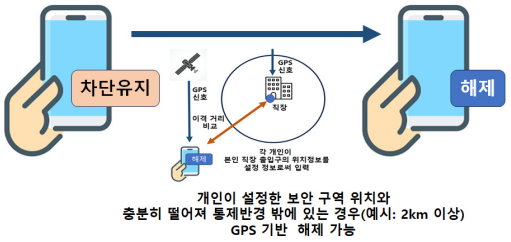

그림 7. 직장 외부에서의 GPS 기반 해제
Fig. 7. GPS-based release security controls outside the workplace

3. 효율화 방법의 적정성과 한계

본 연구에서 제안한 효율화 방법을 통한 보안 통제 기능의 적정성은 표1을 통해 확인할 수 있는데, 직장 출입문에서 개인이 설정한 위치의 적절성을 확인하여 보안 통제를 적용하기 때문에 직장 내부에서는 항상 적절한 보안 통제가 이루어진다.

표 1. 위치 기반 통제 기능 효율화 방법의 적정성 검토
Table 1. Appropriateness of location-based control function efficiency methods

직장 외부에서 예상할 수 있는 상태	직장 출입문에서의 보안조치	직장 내부에서 예상되는 상태
해제 상태 - 위치설정 적정	통제 적용	차단유지상태 - 위치설정 적정
해제 상태 - 위치설정 부적정	위치 재설정 후 통제 적용	
차단유지상태 - 위치설정 적정	통제 적용 (출입 점검 버튼)	
차단유지상태 - 위치설정 부적정	해제 및 위치 재설정 후 통제 적용	

표 2. 위치 기반 통제 기능 효율화 방법의 한계
Table 2. Limitations of location-based control function efficiency methods

직장 외부에서 예상할 수 있는 상태	직장 출입문에서의 보안조치	직장 내부에서 예상되는 상태	비 고
해제 상태 - 위치설정 적정	미조치, 누락	해제 상태 - 위치설정 적정	보안 위험
해제 상태 - 위치설정 부적정		해제 상태 - 위치설정 부적정	보안 위험
차단유지상태 - 위치설정 적정		차단유지상태 - 위치설정 적정	통제됨
차단유지상태 - 위치설정 부적정		차단유지상태 - 위치설정 부적정	보안 위험

추가로, 직장 출입문에서 개인이 설정한 위치의 적절성을 확인하지 못한 경우를 가정해 볼 필요가 있으며, 가정에 따른 보안 통제 상태는 표2와 같이 예상할 수 있다. 따라서 본 연구에서 제안한 효율화 방법은 직장 출입문에서 적절한 보안 통제가 수반되는 경우에만 유효하다.

Ⅳ. 보안 통제 수준 향상 방법

1. 직장 내부에서의 통제

직장 출입문에서 개인이 설정한 위치의 적절성을 확인하지 못한 경우를 고려하여, 직장 내부에서 추가로 통제하는 방법을 생각해 볼 필요가 있다. 이를 위해서는 출입문에서 보안담당자는 모바일 보안 통제 작동 여부를 눈으로 확인하는 것과 마찬가지로, 직장 내부에서 보안담당자가 임의로 모바일 보안 통제 작동 상태를 확인하는 절차가 필요하다. 보안담당자가 모바일 보안 통제 작동 상태를 점검할 수 있도록 지원하기 위해, 앞서 제안한 방안 중 차단유지 상태에 보안 점검 기능을 추가한다.

보안 점검 기능은 그림8과 같이 작동한다. 보안 점검 당시의 GPS 정보를 기준으로 개인이 설정한 위치가 통제반경 밖에 있는 경우에는 원거리 경고상태로 전이하게 된다. 원거리 경고상태는 직장 외부 원거리에 있는 구역을 개인의 보안 통제 위치로 설정하고 MDM 앱에서 보안 적용을 실행한 후, 직장 출입문에서의 보안 통제 없이 업무공간에 들어오게 되는 상태를 적발하기 위한 것이다. 보안 점검 상태에서는 차단 후 경과시간과 개인 설정 위치와의 거리 정보를 보여주게 되는데, 보안담당자는 해당 정보를 가지고 보안 위반 여부를 유추할 수 있다. 개인 설정 위치와의 거리 정보가 매우 작은 경우, 보안 해제 상태에서 직장 출입문에서의 보안 통제 없이 업무공간에 들어온 후, 보안 점검 시행에 따라 업무공간 구역을 개인의 보안 통제 위치로 설정하여 차단을 실행한 것으로 추정해볼 수 있다.

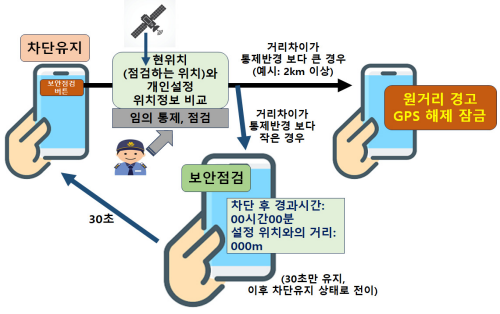

그림 8. 보안 점검 기능 작동 방식
Fig. 8. How the security check function works

2. 보안 통제 수준 향상 방법의 적정성

직장 출입문에서 개인 스마트폰에 대한 통제가 미흡한 경우 직장 내부에서의 스마트폰의 보안 적용 상태는 다양할 수 있는데, 이번 장에서 추가로 제안한 보안 통제 수준 향상 방법의 보안 점검 기능을 사용하여 보안 점검을 수행하면 표3과 같은 결과를 예상할 수 있다. 이와 같이 본 연구에서 제안한 통제 효율화 방법 및 보안 통제 수준 향상 방법은 스마트폰 보안 통제 방법으로서 적정하다고 볼 수 있다.

표 3. 보안 통제 수준 향상 방법의 적정성 검토
Table 3. Appropriateness of methods for improving security control

직장 내부에서 예상되는 상태	직장 내 보안점검 시 예상되는 상태	비 고
해제 상태 - 위치설정 적정	해제 상태	적발
	차단 → 차단유지상태 → 보안점검	적발가능 (경과시간 =짧음)
해제 상태 - 위치설정 부적정	해제 상태	적발
	위치 재설정 → 차단 → 차단유지상태 → 보안점검	적발가능 (경과시간 =짧음, 위치설정=초근접)
차단유지상태 - 위치설정 적정	→ 보안점검	통제됨 (차단확인 상태)
차단유지상태 - 위치설정 부적정	→ 원거리 경고 (GPS해제 잠금)	적발
	해제 → 위치 재설정 → 차단 → 차단유지상태 → 보안점검	적발가능 (경과시간 =짧음, 위치설정=초근접)

V. 결 론

중앙 통제 서버 없이 앱만으로 MDM 서비스를 구성하는 경우 MDM 서비스의 보편성 또는 호환성 확보는 구축 비용과 연계되는 중요한 요소이다. 본 연구에서는 배포된 앱에서 각 개인이 자신에게 필요한 보안 통제구역의 위치 정보를 직접 입력하여 설정 정보로써 유지하는 방식을 제안하였고, 이를 통해 MDM 서비스의 보편성과 호환성을 향상하여 구축 비용을 최소화할 수 있다.

또한 추가로 제안한 보안 점검 기능을 구현하여 직장 내부에서 활용하는 경우, 조직의 보안 통제 수준을 한층 더 향상할 수 있다.

본 연구에서 제안한 보안 점검 기능 등을 실제 MDM 서비스에 적용하기 위해서는 각 직장의 실내 환경에서의 GPS 수신 가능 여부를 고려해야 하며, 보안담당자 또는 사용자의 요구 사항을 추가로 검토할 필요가 있다.

향후 연구에서는, 본 연구에서 제안한 스마트폰 보안 통제 적용 점검 기능을 개선, 영지식증명 기술을 적용하여 개인정보 유출 없이 스마트폰 보안 통제 적용 상태를 확인 · 점검하는 방법을 연구해 보고자 한다.

References

[1] Yong-Sik Kang, Sun-Dong Kwon, Kang-Hyun Lee, "A Case Study on Implementation of Mobile Information Security", Information Systems Review, Vol. 15, No. 2, pp. 1-19, 2013.

[2] Eun-Sub Lee, Sin-Ryeong Kim, Young-Kon Kim, "A Study on Enhancing Security Management of IT Outsourcing for Information System Establishment and Operation", The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 17, No. 4, pp. 27-34, 2017.
DOI: https://doi.org/10.7236/JIIBC.2017.17.4.27

[3] Hyon-Woo Seung, "A Study on Mobile Device Security Control Policy for the Enterprise Business Service", Jounal of The Korea Society of Information Technology Policy & Management, Vol. 7 No. 6, pp. 25-41, 2015.

[4] Kanghyun Lee, Doo-sik Yoon, "Effective Approach of MDM for Mobile Security", Journal of The Korea Institute of Information Security & Cryptology, Vol. 23 No. 2, pp. 29-34, 2013.

[5] Min-Jeong Woo, Jae-Hun Jeong, Jeong-Hun Choi, Eun-Ki Lim, Deuk-Hwan O, "Development of Specialized Smartphone Function Control Application Using Beacon", Proceedings of the 2017 Summer Joint Conference of the Korean Institute of Information Technology and Digital Contents Society, pp 270-271, 2017

[6] Sang-Min Park, Chul-Jin Kim, "A Dual Security Technique based on Beacon", Journal of the Korea Academia-Industrial cooperation Society, Vol. 17, No. 8, pp. 311-317, 2016.
DOI: https://doi.org/10.5762/KAIS.2016.17.8.311

[7] Hyun-Min Baek, Kyung-Won Oh, "A Study for Development of Popular Mobile Device Management on Military", Journal of the KNST, Vol. 5, No. 1, pp. 47-56, 2022.
DOI: https://doi.org/10.31818/JKNST.2022.03.5.1.47

저 자 소 개

오 창 익(정회원)

- 성균관대학교 정보통신대학원 정보통신공학과(석사)
- 숭실대학교 IT정책경영학과(박사과정)
- 현재 국방부 전산사무관

황 수 길(정회원)

- 인하대학교 공학대학원 인공지능융합학과(석사)
- 숭실대학교 IT정책경영학과(박사과정)
- 현재 아와소프트 스마트금융사업부 상무이사, 위드펫 대표이사

손 현(정회원)

- 숭실대학교 정보과학대학원 IT경영학과(석사)
- 숭실대학교 IT정책경영학과(박사과정)
- 현재 ㈜아이웨이 대표

김 동 호(비회원)

- 서울대학교 전자공학과(학사)
- KAIST 전기및전자공학과(석사)
- George Washington University 전산학과(박사)
- 숭실대학교 글로벌미디어학부 교수