기업의 핵심정보 유출방지를 위한 모바일 단말 통제방안 연구

강용석* · 김윤덕** · 신용태*** · 김종배****

*숭실대학교 대학원 IT정책경영학과, **,****숭실대학교 SW특성화대학원, ***숭실대학교 컴퓨터학부

E-mail : kjb123@ssu.ac.kr

요 약

정보기술환경이 모바일, 클라우드, BYOD 기반으로 변화함에 따라 과거 통화기능에만 머물던 모바일 단말은 인터넷을 활용한 전자상거래 및 모바일 오피스를 뒷받침하는 기반으로 전환되고 있다. 하지만, 단말의 분실과 도난, 악성코드 감염으로 인한 도청 및 정보유출 등의 위협이 발생하고 있으며 특히, 기업의 핵심정보가 유출되는 경로로서 활용되는 사례가 발생하여 이에 대한 조치가 시급하다.

기업은 핵심정보의 유출을 방지하기 위해 출입통제를 강화하고 스마트폰 카메라에 대한 스티커 부착을 통해 보안을 강화하고 있지만 원천적인 보호조치로는 미흡한 실정이다. 높은 수준의 보안을 유지하기 위하여 RFID, Beacon 등을 활용하여 위치기반서비스가 적용된 보안통제기능을 적용하고 위험평가기반의 출입자 보안정책을 수립하여 모바일 디바이스를 직접 통제할 수 있는 방안을 제시한다.

키워드

BYOD, MDM, 출입통제, 위험평가

Ⅰ. 서 론

스마트폰과 모바일오피스의 확대에 따라 단말의 분실, 도난 및 악성코드 감염으로 인해 개인정보 및 회사의 기밀이 유출될 수 있는 가능성이 높아지고 악성코드 감염으로 인한 도청, 정보유출 사례가 발생하고 있다.

이에 따라 기업은 핵심정보 보호를 위해 사업장 방문 시에는 RFID 등을 활용하여 출입증을 발급하고 등록되지 않은 단말의 네트워크 접속을 차단하거나 스마트폰 카메라에 대한 스티커 부착 등을 통해 보안을 강화하고 있지만 아직도 스마트폰 등을 활용한 정보유출의 가능성이 상존하고 있다.

높은 수준의 보안을 유지하기 위해서는 출입시스템과의 연동을 통하여 RFID, Beacon, 시간 기준 등 다양한 방식으로 업무시스템에 연계하여 사업장에 출입하는 모바일 디바이스를 직접 통제할 수 있는 방안의 적용이 필요하며 이를 위하여 모바일 출입통제 방안을 제시하고자 한다.

Ⅱ. 모바일 단말의 보안통제정책 모델

정보유출을 방지하기 위한 모바일 단말 통제 및 출입통제시스템의 고도화를 위해서는 MDM을 활용한 모바일 단말의 기능 통제 강화, 비콘기반의 실내측위를 활용한 단말인식, 위험기반의 정보접근 정책의 반영이라는 3가지 관점에서 시스템 설계가 필요하다.

모바일 단말의 보안 통제기능은 원격제어, 비밀번호 제어, 디바이스제어로 구성된다.

구성원의 불편을 최소화 하면서 일관된 보안정책을 반영하기 위한 전제조건은 다음의 3가지이다.

첫째, 회사의 업무 App을 사용하기 위해서는 보안통제를 적용해야 한다.

둘째, 평상시에는 보안 통제를 최소화한다.

셋째, 모바일 보안 통제가 삭제된 경우에는 회사의 업무 App을 사용할 수 없다.

또한, 기업 내부의 핵심정보에 대해 카메라, 녹음기, USB 등을 통하여 외부에 유출되는 것을 방지하기 위해서는 엄격한 통제를 실시하여야 하며, 이를 적용하기 위해서는 해당 모바일 단말이 사내에 들어 왔을 때 모바일 보안 통제를 실시하고 회사 외부로 나갔을 때는 기능을 자동 해제하도록 해야 한다.

모바일 단말 반입 반출에 대한 제어는 출입통제시스템을 통과하는 시점을 기점으로 하며 모바일 단말의 이동 경로에 따라 동선에 따른 보안 정책을 반영할 수 있다. 특히, 대형 생산시설이나 군

부대의 경우 통신회사의 기지국이나 WiFi AP를 활용하고 실내에 진입할 경우 Beacon에 기반한 실내 측위를 활용할 수 있다.

위치기반 실내측위시스템은 무선신호센싱장치, 측위를 위한 RM 생성 알고리즘, 측위 알고리즘, 표출시스템으로 구성된다. 무선신호센싱장치는 무선주파수, 적외선, 초음파 등의 센싱기술을 수행하고 센싱기술은 시간, 각도, 주파수, 신호강도를 센싱하며 아래와 같은 요소기술을 필요로 한다[1].

효과적인 시설물에 대한 출입통제와 모바일 단말의 사용을 위해서 접근구역에 대한 분류에 따라서 역할기반접근통제 모델을 적용하여 계층적 출입과 사용통제를 수행한다. 출입자의 역할, 직책, 직위뿐 만아니라 시설물의 보호정도와 출입자의 보안등급을 연관 지어 출입과 모바일 단말의 통제기능 사용권한을 부여한다. 보안성을 높인 계층적 출입통제와 모바일 단말 기능 통제가 요구하는 사항은 다음과 같다.

첫째, 접근제어 모델의 구성요소를 반영하고 시설물의 보호정도와 출입자 개인의 보안등급간 보안연관성을 따라야 한다. 출입자가 시설물에 대한 출입을 요청할 때 역할기반접근통제 모델의 구성요소인 주체(출입자), 객체(시설물), 권한, 보안등급이 활성화 되어야 하며, 권한에 따라 시설물에 대한 출입과 모바일 단말의 보안통제기능을 허가해야 한다.

둘째, 출입자들의 무분별한 시설물 출입을 방지하기 위해서 출입자들의 직위, 직책, 역할에 권한을 할당하되 최종적으로 보안등급을 확인한 후 시설물에 대한 출입과 모바일 단말의 보안통제기능 사용을 허가해야 한다. 만약, 직위나 역할 등 하나의 구성요소에 의해서 시설물 출입과 모바일 단말의 보안통제기능 사용을 허가한다면 출입자가 모든 시설에 필요 이상으로, 업무에 무관하게, 무분별하게 시설물과 핵심정보에 접근할 수 있다.

마지막으로 출입자의 보안 위반을 예방해야 한다. 우선 출입자에게 역할, 직책과 직위 수준보다 높은 보안등급의 시설물의 출입과 모바일 단말의 보안통제기능 사용을 불허해야 한다.

출입통제시스템을 통과하는 시점을 기점으로 모바일 단말에 대한 제어는 모바일 단말의 이동 경로에 따라 동선에 따른 보안 정책을 반영해야 한다. 이때 중요한 점은 통제정책이 위험평가에 기반하여 정책이 수립되고 반영되어야 하며 이를 위해서는 Whitelist 기반의 모바일 단말 기능 허용, Blacklist기반의 기능 차단, 그리고 이상행위에 대한 정책의 3가지 관점에서 정책을 수립하고 반영하여야 한다.

위험평가를 위해 사용자의 정보를 수집하고 등록하여야 하며 사용자의 접근에 있어 적정한 접근임을 판단하기 위한 정책을 수립하여야 한다. 또한, 위험평가 결과에 따라 Score를 결정하고 그 결과값을 통하여 접근을 승인하거나 추가 인증을 요구하고 때에 따라서는 접속을 차단하여야 한다.

가장 먼저 Blacklist기반의 차단 정책에 반영되어 있는 사용자는 모바일 단말의 보안통제기능을 적용하여야 하고, 사용자의 ID, Password, 등록 또는 과거의 접속하였던 이력정보와 일치하는 경우에 신뢰할 수 있는 사용자로 간주하여 보안통제기능을 적용한다.

보안정책에 따른 위험평가의 결과는 항시 다면적 결과를 보이기 때문에 완벽할 수 없고 매번 추가적인 인증 등의 요구를 실시하는 것은 위험평가를 통해 신뢰할 수 있는 사용자에 대해 편리성을 제공하는 것에 위배가 된다. 그러므로 병합된 형태의 비즈니스 Rule을 생성하여 그에 따른 종합적인 판단을 하여야 한다.

기존에 등록된 사용자와 모바일 단말의 기본정보가 100% 일치하지 않거나 기본정보가 일치한다고 하더라도 이상행위에 대한 정책에 적용되는 범위의 사용자라면 추가적인 2차 검증을 요구하여 보안통제기능을 승인하거나 차단하여야 한다. 만일 2차 검증에 실패한 사용자나 모바일 단말의 경우는 유형관리에 등록하여야 하고 재사용을 시도할 경우 횟수를 제한하여 Blacklist로 등록하여 사용을 차단하여야 한다[5].

Ⅲ. 모바일 단말의 보안통제 구현

기업 내부의 핵심정보에 대해 카메라, 녹음기, USB 등을 통하여 외부에 유출되는 것을 방지하기 위해서는 역할기반의 접근통제와 위험평가기반의 모바일 단말 보안통제정책을 적용하여야 한다.

이를 실행하기 위해서는 먼저 모바일 단말의 보안통제기능을 구체화하여야 한다.

모바일 단말의 보안정책으로 회사의 업무 App을 사용하기 위해서는 위와 같은 세부적인 보안통제를 적용해야 하며, 평상시에는 모바일 단말의 보안 통제를 최소화하고 모바일 보안 통제가 삭제된 경우에는 회사의 업무 App을 사용할 수 없으며 회사의 보호구역에 출입할 수 없다.

이를 적용하기 위해서는 첫째 RFID기반의 SpeedGate를 통해 출입을 통제하며 시설에 대한 출입이 시작됨과 동시에 모바일 단말에 대한 보안통제기능이 활성화되어야 한다.

둘째는 Whitelist로 등록된 사용자인 임직원은 Beacon 인식된 후 보호구역에서는 카메라 등의 보안통제기능이 활성화되어야 하고 보호구역을 벗어났을 때는 보안정책에 따라 일부 기능을 사용할 수 있도록 조치해야 한다.

셋째는 신규 방문자 등 Blacklist로 등록된 사용자의 경우 Beacon 인식 된 후 MDM Agent의 설치를 유도한 후 Agent가 설치된 이후 SpeedGate를 통과할 수 있도록 구성이 되어야 한다.

넷째는 업무시간 등의 경우에 모바일 단말의 보안통제기능을 활성화할 수 있어야 한다.

Ⅳ. 결론 및 향후 연구 과제

현재 모바일 단말관리 산업은 MDM시장에서 MAM시장으로 급속하게 진화되고 있으며 경쟁력 있는 공장 자동화 및 생산 자동화를 위한 기반인 프라로 활용이 시작되고 있다. 이러한 과정에서 보안 문제는 더욱 중요성이 강조될 것이므로 공장 및 생산자동화를 위한 MDM과 MAM 측면의 기술 연구는 미흡한 실정이다. 이미 모바일 단말의 취약성이 확인되었고 모바일 단말의 특성에 따라 상호운용성 측면에서 애플리케이션의 위변조 예방 및 메시지 보안 등의 핵심기술에 대한 연구를 통해 BYOD기반의 공장 및 생산자동화를 뒷받침하기 위한 방안을 연구하고자 한다.

참고문헌

[1] Jung Jong In, “A High-Precision and Low-Search-Cost Nomadic-Device-Based Indoor Positioning System”, Department of Electronic and Computer Engineering The Graduate School Hanyang University, (2013)
[2] KANG, YONG SUK, “A Study on the Risk Analysis Based Access Control Model of IT Services through the airport security inspection process review”, Department of IT policy and Management Graduate School of Soongsil University, (2015)