안전한 모바일 오피스 도입과 운영을 위한 정보보호 수칙

2012. 12.

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

KISA 한국인터넷진흥원
Korea Internet & Security Agency

참고 사항

o 본 수칙은 모바일 오피스 도입을 준비하거나 운영하고 있는 기업들이 고려해야 할 정보보호 수칙으로서, 각 수칙은 모바일 오피스의 서비스 특성과 기업의 정책에 따라 수정하여 사용할 수 있습니다.

o 본 수칙은 기업의 보안 담당자가 모바일 오피스 “이용자” 및 “운영자”를 대상으로 활용할 수 있도록 구성했습니다.

o 본 수칙은 다양한 모바일 오피스 환경을 고려하여, 최소한으로 지켜야 하는 “기본” 사항과 보안 수준을 높이기 위해 요구되는 “권고” 사항으로 분류하였습니다.

o 본 수칙은 기술 발전에 따라 모바일 오피스 환경에 실용적으로 활용할 수 있도록, 정책 및 기술 등의 변화를 고려하여 일부 수칙이 수정될 수 있음을 알려드립니다.

목 차

제 1장. 개 요

최근 스마트폰 시장은 양적뿐만 아니라 질적으로 급속히 성장하고 있으며, 이동통신망의 속도(LTE 등) 향상은 모바일 서비스의 형태와 범위를 빠르게 변화시키고 있다. 가장 큰 변화 중 하나는 PC 기반의 업무에서 모바일까지 그 범위가 확대되는 모바일 오피스 서비스이다. 모바일 오피스는 스마트폰과 같은 모바일 단말기의 이동성, 개방성, 다양성을 기반으로 제공하는 새로운 서비스로서, 다음과 같은 이점을 제공한다.

- **이동성** : 모바일 단말기를 이용한 인터넷 서비스는 시간과 공간적인 제약 없이 업무를 수행하도록 한다.
- **개방성** : SNS, 커뮤니티 등을 통한 이용자의 자발적인 참여와 정보 공유가 이루어짐으로써, 실용적인 협업을 수행하도록 한다.
- **다양성** : 이용자는 다양한 모바일 플랫폼에서 개인에 맞춘 업무 관련 서비스를 제공받게 된다.
- **경제성** : 시간·공간적인 제약에서 벗어나 신속한 업무처리 및 효율성을 바탕으로 새로운 이익을 창출하게 된다.

이러한 이동성, 개방성, 다양성, 경제성 측면에서 긍정적인 효과가 제공되는 반면에 개인정보 유출, 불법 과금, 기업기밀 누출 등 여러 형태의 보안 사고도 발생하고 있다.

- **단말기 분실 및 도난** : 편리한 이동성과 함께 이용자의 부주의로 인한 단말기 분실과 도난은 정보(개인 및 기업정보 등) 유출 가능성을 높인다.
- **악성코드 감염** : 개방성, 다양성에 따른 악성코드 및 해킹의 위협에 대한 감염(공격) 경로는 데스크톱 영역과 유사하거나 더 증가하고 있다.
- **네트워크 위협** : 무선랜, 블루투스 등을 이용한 네트워크에서의 공격과 다양한 모바일 응용서비스에서의 도용 및 정보 유출 등이 존재한다.

따라서 모바일 오피스의 성공적인 도입과 안정적인 운영을 위해서 이용자와 운영자 모두가 제정된 정보보호 수칙을 성실히 지켜야 한다.

제 2장. 모바일 오피스 개념

□ 모바일 오피스란?

모바일 오피스(Mobile office, 이동 사무실)는 언제, 어디서나 모바일 단말기(이동통신기기)를 통해 외부에서 업무를 처리할 수 있는 업무 환경을 말한다.

최근에는 스마트폰 시장이 확대되고 처리 성능이 크게 향상됨에 따라 개인 소유의 모바일 장치가 증가하고 있으며, 이를 개인 용무(게임, 검색 등) 이외에도 업무에 활용하는 새로운 변화(BYOD: Bring Your Own Device)가 나타나고 있다.

또한 클라우드 서비스가 활성화되는 가운데, 메일, 전자 결재 등의 단순한 모바일 업무를 넘어, 다자간 협업 및 실시간 IT 자원 확장 등 보다 전문적이고, 다양한 업무를 수행할 수 있는 환경이 형성되고 있다.

이러한 IT기술의 발전과 더불어 모바일 오피스는 시·공간의 제약에서 벗어나 효율적으로 업무를 처리할 수 있는 스마트워크의 대표적인 모델로 자리 잡고 있다.

□ 모바일 오피스 서비스 유형

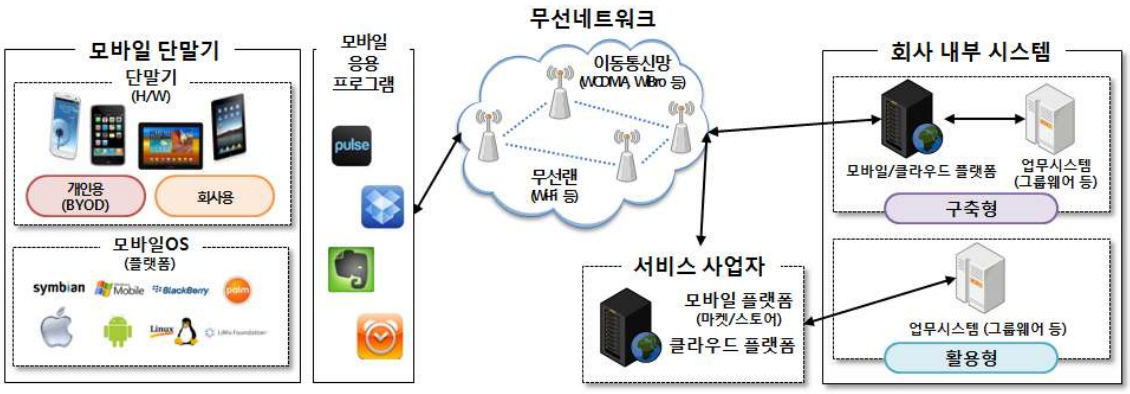
모바일 오피스는 다양한 분야에서 업무의 새로운 바람을 일으키고 있다. 특히 제조, 의료, 교육 등의 전문 분야에서 IT기술을 접목한 모바일 오피스 환경은 생산성 및 서비스 향상 등의 기대효과를 주고 있다.

모바일 오피스 서비스 유형은 크게 2가지로 구분할 수 있다.

- o **그룹웨어 서비스** : 메일, 전자결재, 회계처리 등의 일반 업무를 모바일 단말기로 제공하는 서비스
- o **현장업무 서비스** : 현장단속, 시설물관리, 보험 상담 등 기업의 현장 업무를 모바일 단말기로 제공하는 서비스

제 3장. 모바일 오피스 구성요소

모바일 오피스는 **모바일 단말기**, **모바일 응용프로그램**, **무선네트워크**, 그리고 기업 업무와 관련된 **내부 시스템**으로 구성된다.



< 모바일 오피스 서비스 구성도 >

□ 모바일 단말기

직원 개개인이 소유한 휴대용 기기로서, 스마트폰, 태블릿 PC, 노트패드 등 다양한 종류가 있다. 모바일 단말기는 단말기 하드웨어(H/W), 모바일 운영체제(OS)로 구성되어 있다. 모바일 운영체제는 모바일 단말기 내 다양한 응용프로그램들이 설치 및 실행될 수 있도록 관리하는 역할을 수행한다. 현재 많이 사용되는 모바일 운영체제는 안드로이드 OS, iPhone OS, 윈도우 모바일 등이 있다.

□ 모바일 응용프로그램

o 모바일 응용프로그램(S/W)은 모바일 운영체계 상에서 설치 및 실행되는 서비스로서, “모바일 웹(Mobile Web)”과 “모바일 앱(Mobile App)”으로 분류된다.

□ 무선 네트워크

케이블, 광케이블 등의 전송매체를 사용하지 않고 데이터를 전달하는 기술로서, 이동통신망(3G/4G, WiBro 등)과 무선랜(WiFi) 등으로 분류 할 수 있다.

제 4 장 모바일 오피스 보안 요구사항

제 1 절 모바일 오피스 보안 위협

□ 모바일 단말기 보안 위협

모바일 단말기는 개인 휴대기기의 특성상 이용자의 부주의로 인해 기기 및 메모리카드 등을 도난당하거나 분실할 위험이 존재한다. 특히, 스마트폰은 일반적으로 통화내역, 수신메시지, 전화번호부, 일정, 위치정보, 금융거래정보 등과 같은 다량의 개인정보가 저장되고, 업무용으로 사용되는 경우 회사 기밀정보 및 업무정보가 저장되기 때문에, 스마트폰이 도난 또는 분실될 경우에 개인 또는 회사의 중요 정보가 외부로 유출될 가능성이 존재한다.

악의적인 사용자는 도난 및 분실된 모바일 단말기를 습득하면, 이를 통해 회사의 업무용 서버에 불법 접속한 후, 업무 정보를 외부로 유출하거나 위변조 하는 행위가 가능하다. 또한 모바일 단말기는 그 자체가 대용량 이동식 저장매체로 사용되기 때문에, 내부자가 회사 기밀정보 또는 업무정보를 외부로 유출하는 수단으로 사용될 수 있는 위험도 존재한다.

□ 모바일 응용프로그램 보안 위협

모바일 단말기는 다양한 네트워크 인터페이스를 가진 '손안의 컴퓨터'로, 일반 PC에서 발생할 수 있는 모든 보안위협이 모바일 단말기 환경에도 동일하게 적용될 수 있다. 모바일 응용프로그램은 오픈된 개발 환경에서 자유롭게 프로그램 개발 및 설치가 가능하기 때문에, 악성코드 등의 악성 프로그램이 제작될 가능성이 높다. 또한 구글의 안드로이드 마켓은 오픈마켓으로서, 누구나 스마트폰 응용프로그램을 제작하여 등록 하는 것이 자유롭고, 손쉽게 유통될 수 있다. 응용프로그램을 등록 시 보안 검증 절차를 거치지 않아, 게임 프로그램으로 가장한 악성코드가 안드로이드 마켓에 유포된 사례가 최근에 실제로 발생하였다.

모바일 악성코드로 인한 모바일 응용프로그램 보안 위협은 정보 유출, 과금 피해, 단말기 사용 제한 및 불능, DDoS(Distributed Denial of Service) 공격 등으로 나누어볼 수 있다.

① 정보 유출 : 모바일 단말기에는 USIM(Universal Subscriber Identity Module)번호, 전화번호, 일정, SMS, 통화기록, 연락처, 사진 등 기존 휴대전화에 존재하는 개인정보뿐만 아니라, 이메일, GPS, 회사 기밀 정보, 공인인증서, 인터넷 사이트 계정 등이 저장될 수 있다. 해커는 이러한 개인 정보를 유출하여, 인터넷뱅킹 해킹, 휴대전화 소액결제 유도, 불법 광고 유포, 위치 추적 등 추가적인 범죄 목적으로 악용할 수 있다.

② 과금 피해 : 최근 해커는 금전적 이득을 노리고 악성코드를 제작·유포하고 있다. 이러한 경향은 모바일 침해사고로 이어질 수 있으며, 스마트폰이 인터넷뱅킹 등 금융결제의 수단으로 활용됨에 따라 앞으로 많은 악성코드가 출현할 것으로 예상된다. 2010년 4월, 국내 최초로 발생한 모바일 악성코드(WinCE/TerDial)는 악성코드를 인기 게임으로 위장하여 윈도우모바일 스마트폰을 감염시키고, 해외 프리미엄 번호로 국제 전화를 주기적으로 발신하였다. 또한 2011년 8월, 러시아에서 발생한 안드로이드 스마트폰 동영상 플레이어로 위장하여 배포된 악성코드(TrojanSMS.AndroidOS.FakePlayer.a)는 이용자 몰래 요금을 결제하고, 특정 번호로 SMS를 전송하는 등의 금전적 피해를 발생시켰다.

③ 단말기 사용제한 : 이용자가 정상적으로 모바일 단말기를 이용하지 못하는 일종의 DoS(Denial of Service)를 의미한다. 예를 들어 휴대전화의 배경화면을 바꾸거나 메뉴의 텍스트가 보이지 않게 함으로써, 이용자의 불편함을 초래한다.

④ DDoS 공격 : 모바일 침해사고로 대표되는 공격으로서, 일반 PC에서의 대용량 데이터를 유발시키는 공격과 다량의 전화를 발신하거나 SMS 문자 메시지를 전송하는 공격이 있다. 대용량 데이터 공격은 앱을 이용하여 트래픽 용량은 작지만 많은 커넥션을 요청함으로써 특정 사이트를 공격할 수 있다. 전화·SMS 공격은 특정인의 휴대전화뿐만 아니라 콜센터 및 기업 대표전화 등으로 다수의 스마트폰이 전화를 걸거나, 다수의 SMS문자 메시지를 전송함으로써 전화를 사용할 수 없게 할 수 있다.

□ 무선 네트워크 보안 위협

모바일 단말기는 이동통신망, 무선랜 및 블루투스 기능이 기본적으로 탑재되어 있어 공중 무선랜이나 사설 무선랜의 이용 빈도가 높으며, 모바일 단말기 이용자들이 무선데이터 요금을 절약하기 위해 무작위로 검색되는 무선 접속장치(AP: Access Point)를 이용하는 사례도 늘고 있다. 만약 해커가 악의적인 의도를 가지고 악성코드를 심어놓은 무선 AP를 제공한다면, 모바일 단말기 사용자는 이러한 무선 AP에 접속하는 것만으로도 악성코드에 감염될 수 있다.

따라서 모바일 단말기의 무선인터넷 접속환경은 유해한 사이트에 방문해야 악성코드에 감염되었던 기존 PC 환경보다 악성코드 유입이나 해킹 공격 등이 용이한 환경이라 할 수 있다. 스마트폰과 PC의 개인정보와 위치정보를 무선랜의 취약점을 이용하여 수집한 사례가 있고, 가짜 무선 AP를 통한 개인정보 유출 가능성도 꾸준히 제기되고 있다.

제 2 절 모바일 오피스 보안 요구사항

모바일 오피스 “이용자” 및 “운영자” 관점에서 분석된 보안 요구사항은 다음과 같다.

보안 요구사항 분석				
이용자 보안 요구사항	단말 H/W	사용자 인증	수행 시점	o 구동 시 사용자 인증 수행 o 일정 시간 미사용 시, 자동 잠금 설정 o 잠김 해제 시 사용자 인증 수행
			인증 방법	o 추측하기 어려운 비밀번호 사용 o 비밀번호 평문 저장 금지
			실패 조치	o 일정 횟수이상 인증 실패 시 보안담당자에게 요청
		단말기 관리	분실/도난 대책	o 분실/도난 단말기에 대한 원격 삭제 요청
	모바일 S/W	SW 관리	SW 배포/설치	o 서명 또는 허가한 SW만 설치
		모바일 OS보호	보안 패치	o 모바일 OS 보안패치 최신상태 유지
			변조 방지	o 모바일 OS의 무결성을 검사하여 변조 방지
		데이터 보호	저장매체 접속 통제	o 모바일 단말기↔업무PC 접속 및 데이터 전송 자제 o 담당자 허가를 받은 저장매체만 모바일 단말기에 사용
	네트워크 보안		무선랜	o 인가된 무선 AP만 접속
운영자 보안 요구사항	관리적 보안		모바일 단말 관리	o 모바일 단말기의 수리·교체 시 기관 보안 담당자의 통제 하에 실시
			S/W취약점 분석	o 업무용 소프트웨어에 대해서 도입 전, 취약점 분석 실시 및 보안조치 수행
			보안성 검증	o 서비스, 인프라 등에 대한 주기적인 모의해킹, 취약점 점검 등 보안성 검증/보완 조치 후 서비스 실시
	업무 서비스 보안		사용자 인증 보안	o ID/PW 외 OTP 또는 인증서 등으로 복합인증 o 기기인증서 또는 단말고유정보로 단말기 인증
			서비스 보안	o (업무용 프로그램 배포) 서비스관련 응용프로그램은 공개용 앱스토어를 통하여 배포금지 o (업무 서비스 보호) - 업데이트 미수행시 서비스의 접속 제한, 무결성 점검 수행 - 비정상적인 접속 및 정보가 송신될 경우, 강제 세션 종료 및 원인분석을 위한 로그 기록
			정보자산 보안	o 중요정보의 유출, 위·변조 방지
	인프라 보안		시스템 보안	o 주기적 보안패치(patch) 실시

제 5장. 모바일 오피스 도입 · 운영을 위한 보안 수칙

모바일 오피스 이용자 보안 수칙

1. 회사에 개인 단말기·사용자 정보를 안전하게 등록하고 인증받기
2. 회사가 지정·권고하는 프로그램을 확인하고 설치하기
3. 비정상적인 모바일 단말기로 모바일 오피스에 접속하지 않기
4. 회사 중요 정보는 개인 모바일 단말기 내 보관하지 않기
5. 안전한 무선 환경에서 모바일 오피스 접속하기

모바일 오피스 운영자 보안 수칙

6. 이용자의 단말기 정보 및 인증 정보를 안전하게 관리하기
7. 이용자에게 프로그램 제공 시 안전하게 배포하기
8. 프로그램의 업데이트 정보를 이용자에게 수시로 알려주기
9. 모바일 단말기 도난 · 분실 시, 원격으로 정보를 삭제하기

※ 본 수칙은 모바일 오피스 환경을 위한 보안 수칙이며, 스마트폰, 무선랜을 위한 기본적인 수칙은 다음의 수칙을 기본적으로 준수하길 권고한다.

- 스마트폰 이용자 10대 안전수칙 (방송통신위원회, 2010년 2월)
- 안전한 무선랜 이용 7대 수칙 (방송통신위원회, 2011년 5월)

제 1 절 모바일 오피스 이용자 보안 수칙

1. 회사에 개인 단말기 사용자 정보를 안전하게 등록하고 인증받기

기 본

o 이용자는 개인 모바일 단말기를 통해 모바일 오피스를 이용하기 위해서 회사에 단말기 및 사용자 정보를 등록하고, 운영자로부터 사용 승인을 받아야 합니다.

- 이용자는 개인 모바일 단말기 및 사용자 정보 등록 후, 운영자로부터 받은 사용자 인증(ID/패스워드 등) 정보를 안전하게 관리하고, 주기적으로 변경해야 합니다.

- 이용자는 모바일 오피스를 고려하여 개인 모바일 단말기를 구입할 경우, 모바일 오피스에 이용 가능한 단말기 모델을 참고하여 선택해야 합니다.

o 이용자는 모바일 오피스에 접속 시 사용자 인증을 반드시 받아야 하며, 자동 잠금 기능, 자동 로그인 기능 등을 주의해서 설정해야 합니다.

-「자동 로그인」기능은 개인 모바일 단말기의 분실 및 도난 시 허가받지 않은 사용자가 서비스에 접속할 수 있기 때문에 주의해서 설정해야 합니다.

-「자동 잠금」기능은 훔쳐보기 등 사용자 인증 정보의 유출이 우려됨에 따라 일정시간 미사용 시 자동 잠금이 되도록 반드시 설정해야 합니다.

권 고

o 회사가 원격단말관리(MDM) 기능을 도입할 경우, 이용자는 단말관리용 프로그램(Agent, Profile 등)을 설치 후 최초 실행하면 자동으로 개인 모바일 단말기를 등록할 수 있습니다.

o 이용자는 개인 모바일 단말기 분실 및 도난에 의한 정보 유출을 막기 위해서 이중인증방식을 통한 단말기 보안을 강화할 수 있습니다.

- 개인 모바일 단말기를 부팅 시 단말기 OS 플랫폼(안드로이드 OS, iOS 등)에 따라 패턴 인증, PIN번호 인증, 비밀번호 인증 등을 병행하여 사용할 수 있습니다.

※ PIN(Personal Identification Number) : 모바일 단말기의 USIM카드를 잠그는 개인 비밀번호

2. 회사가 지정·권고하는 프로그램을 확인하고 설치하기

기 본

o 이용자는 개인 모바일 단말기에 응용프로그램을 설치할 경우, 회사가 안전성을 검증한 프로그램인지 확인해야 합니다.

- 이용자는 모바일 오픈 마켓/스토어를 통해 다양한 응용프로그램을 다운로드 및 설치할 수 있기 때문에 이용자도 모르는 사이 악성코드에 감염될 수 있으며, 이에 대한 주의가 필요합니다.

  ※ 이용자는 응용프로그램을 실행할 경우, 악성코드 감염 여부를 확인하기 위해서 모바일 백신 프로그램을 이용하여 실시간 검사를 할 수 있습니다.

- 이용자는 응용프로그램 설치 전, 운영자로부터 제공되는 응용프로그램 목록(블랙리스트, 화이트리스트)을 통해 안전 여부를 확인하고, 해당 응용프로그램의 정보가 없는 경우는 설치 가능 여부를 반드시 확인해야 합니다.

o 이용자는 응용프로그램의 최신 업데이트 버전을 확인하고 설치해야 합니다.

- 응용프로그램은 최신 버전으로 업데이트 하지 않을 경우 소프트웨어 취약점에 노출되어 악성코드에 감염될 수 있기 때문에, 주기적인 응용프로그램 업데이트를 위한「자동 업데이트」기능을 설정해야 합니다.

- 이용자는 모바일 악성코드 감염을 막기 위해 안티바이러스(Anti-Virus) 프로그램을 최신 버전으로 업데이트해야 합니다.

권 고

o 이용자는 모바일 오피스를 통해 회사의 중요(기밀) 정보를 다룰 경우, 회사에서 개발한 전용 응용프로그램을 위주로 사용해야 합니다.

- 이용자는 회사가 중요(기밀) 정보의 반·출입 관리, 문서 암호화 저장 등을 실시간 관리할 수 있도록 전용 프로그램을 설치해야 합니다.

- 이용자는 전용 프로그램 다운로드 시, 회사에서 배포·관리하는 전용 마켓 또는 사이트 주소를 확인하고 다운로드 받아야 합니다.

3. 비정상적인 모바일 단말기로 모바일 오피스에 접속하지 않기

기 본

o 이용자는 개인 모바일 단말기의 모바일 운영체제(이하 "운영체제")를 임의로 변경하지 않으며, 변경 시 모바일 오피스에 접속하지 않아야 합니다.

- 운영체제가 변경될 경우 운영체제가 제공하는 보안 기능이 일부 제거되어 새로운 보안 취약점이 발생할 수 있기 때문에, 운영체제를 임의로 변경하지 말아야 합니다.

※ 비정상적인 모바일 단말기 유형

▶ 안드로이드 OS "**루팅(rooting)**" : 안드로이드의 오픈소스를 이용해 최고 관리자(Super User) 권한을 획득한 후, 다양한 시도를 할 수 있는 행위

▶ iOS "**탈옥(Jailbreaking)**" : iOS 안전성을 위해 애플사가 막아둔 시스템 영역을 이용자가 사용할 수 있도록 시스템을 임의로 변경하는 행위

- 이용자는 개인 모바일 단말기의 정상적인 운영체제를 유지하기 위해서, 필수 응용프로그램에 문제가 없는 상태에서 운영체제를 최신 버전으로 업그레이드해야 합니다.

권 고

o 이용자는 모바일 오피스 접속 시 개인 모바일 단말기의 자원 상태를 확인하고, 모바일 오피스와 관련 없는 부가 기능의 사용을 자제해야 합니다.

- 이용자는 모바일 오피스에 접속하기 전에, 모바일 단말기의 실행프로그램 및 메모리 사용량, 저장 공간, 배터리 사용량 등의 자원을 확인하고, 카메라, GPS 등 자원 소모량이 많은 부가 기능의 사용을 자제해야 합니다.

※ 모바일 단말기는 일반 PC보다 제한된 자원(CPU속도, 메모리, 배터리 등)에서 작동하기 때문에, 개인용과 업무용으로 동시에 사용할 경우에 모바일 단말기의 비정상적인 상태(프로그램 오류 발생, 통신 장애 등)를 유발할 수 있기 때문에 주의해야 합니다.

4. 회사 중요 정보는 개인 모바일 단말기 내 보관하지 않기

기 본

o 이용자는 모바일 오피스를 통해 사용한 회사 중요 정보를 개인 모바일 단말기 내 별도 저장하지 않고, 반드시 삭제해야 합니다.

- 이용자는 중요 정보를 개인 모바일 단말기 이외에도 별도 모바일 데이터 관리 프로그램을 통해 다른 매체에 전송하거나 저장하지 않습니다.

- 이용자는 개인 모바일 단말기의 카메라 기능, 화면 캡처 기능 등 다양한 인터페이스를 통해 중요 정보를 저장하거나 전송하지 않습니다.

o 업무 특성상 부득이하게 개인 모바일 단말기나 외부 매체에 저장할 경우, 이용자는 운영자에게 반·출입 승인을 받은 저장 공간에 암호화하여 저장해야 합니다.

- 이용자는 모바일 오피스를 통해 사용되는 중요 정보, 주소록, 통화기록, SMS 내역 등을 암호화하여 저장해야 합니다.

- 이용자는 반·출입 승인을 받은 메모리, USB 등의 시큐어 스토리지(secure storage)나 개인 모바일 단말기 내 시큐어 폴더(secure folder)에 암호화하여 저장해야 합니다.

권 고

o 회사가 클라우드 서비스를 도입할 경우, 이용자는 모바일 오피스에서 업무를 수행한 후, 관련 정보를 클라우드 서버에 실시간으로 전송하여 백업하도록 설정할 수 있습니다.

- 이용자는 중요 정보를 개인 모바일 단말기에서 클라우드 서버로 전송할 경우, 데이터 압축 및 암호화 전송의 가능 여부를 확인하고, 기능이 활성화되도록 설정할 수 있습니다.

5. 안전한 무선 환경에서 모바일 오피스 접속하기

기 본

o 이용자는 암호 설정이 되지 않은 공공 무선랜(WiFi 등)의 사용을 자제하며, 이동통신망을 사용해야 합니다.

- 해커는 위장 무선 AP 통해 접속을 유도하고, 스니핑(sniffing) 등 공격을 할 수 있기 때문에, 이용자는 공공/거주 환경에서 모바일 오피스 접속 시 상대적으로 안전한 이동통신망을 이용해야 합니다.

- 부득이하게 공공 무선랜을 이용하는 경우, 이용자는 개인 모바일 단말기와 무선인터넷 공유기 사이의 WPA2 이상 보안 수준의 사용자 인증 및 데이터 암호화를 수행해야 합니다.

※ **WPA2**(Wi-Fi Protected Access 2) : Wi-Fi 사용자를 위해 개발된 보안 표준으로서, AES(Advanced Encryption Standard) 암호화 알고리즘을 사용한 강한 보안을 제공

o 이용자는 회사에서 제공하는 보안 설정이 된 무선랜만 사용해야 합니다.

- 이용자는 회사에서 설치한 무선인터넷만 사용하고, 무선랜 인증 정보를 유출하거나 공유하지 말아야 합니다.

※ 회사는 입·출입 통제 시스템과 연계하여 외부 공공 무선랜, 이동통신망 등 외부 통신망과의 접속을 차단할 수 있습니다.

권 고

o 이용자는 개인 모바일 단말기의 테더링(Tethering) 기능을 통한 인터넷 사용을 자제해야 합니다.

- 이용자는 테더링 기능을 사용할 경우, 반드시 암호 설정을 통해 외부와의 접속을 최대한 제한해야 합니다.

※ 테더링 기능을 악용한 해킹

무선랜 지역 등에서 해커는 테더링 기능을 이용해 모바일 단말기를 정상 무선AP로 위장시킨 뒤 이용자를 끌어들여 악성코드를 설치하거나, 우회 네트워크를 만들어 개인정보 및 기업정보를 유출할 수 있습니다.

제 2 절 모바일 오피스 운용자 보안 수칙

6. 이용자의 단말기 정보 및 인증 정보를 안전하게 관리하기

기 본

o 운영자는 수집된 이용자의 모바일 단말기 정보를 암호화하여 안전하게 관리해야 합니다.

- 운영자는 이용자가 개인 모바일 단말기를 등록 시 수집되는 단말기 정보를 암호화하여 안전하게 보관해야 합니다.

- 이용자가 모바일 운영체제를 패치하거나 단말기를 교체하는 경우, 운영자는 이용자의 변경된 단말기 정보를 최신으로 업데이트해야 합니다.

o 이용자가 모바일 오피스 접속 시, 운영자는 일정 수준 이상의 사용자 인증을 통과하도록 보안을 강화해야 하며, 수집된 이용자의 인증 정보는 암호화하여 안전하게 관리해야 합니다.

- 운영자는 사용자 인증을 강화하기 위해서 이중 인증 방식을 활용하거나, 필요에 따라 별도 인증 프로그램을 통해 보안을 강화할 수 있습니다.

- 운영자는 이용자가 사용자 인증을 위해 입력하는 개인 정보를 암호화하여 안전하게 보관해야 합니다.

권 고

o 외부 서비스 사업자의 인증 서버를 활용할 경우, 운영자는 내부 관리자로 인하여 단말기 및 인증 정보가 유출되는 사고를 막기 위한 별도의 보안 대책을 마련해야 합니다.

- 운영자는 단말기 및 인증 정보에 대한 외부 서비스 관리자의 접근을 통제하기 위하여, 관리자 비밀번호를 별도 관리하고, 수시로 변경해야 합니다.

7. 이용자에게 프로그램을 제공 시 안전하게 배포하기

기 본

o 운영자는 이용자의 모바일 단말기에 정상적인 응용프로그램이 설치되도록 통제해야 합니다.

- 운영자는 이용자가 개인 모바일 단말기에 설치하는 응용프로그램의 안전 여부를 확인할 수 있는 목록(예:블랙리스트, 화이트리스트)을 만들고, 프로그램의 최신 버전 및 보안패치 등을 주기적으로 관리해야 합니다.

- 운영자는 응용프로그램이 이용자의 개인 모바일 단말기로 안전하게 전송될 수 있도록 별도 배포 방안(앱 마켓, 게시판 사이트)을 수립해야 합니다.

권 고

o 운영자는 이용자가 중요(기밀) 정보를 다루는 업무를 수행할 경우, 회사에서 제공하는 전용 응용프로그램만 이용하도록 통제할 수 있습니다.

- 운영자는 중요(기밀) 정보의 유출을 막기 위해서, 이용자에게 보안이 강화된 전용 프로그램을 회사가 운영하는 전용 마켓 또는 게시판 사이트를 통해서만 다운로드 받아 설치하도록 안내해야 합니다.

o 외부 서비스 사업자를 활용하여 클라우드 서비스를 이용할 경우, 운영자는 서비스에 대한 보안 적합성을 철저히 검토해야 합니다.

- 운영자는 외부 서비스 사업자가 보유한 서버의 안정성, 보안 기술 등이 회사가 요구하는 모바일 오피스 환경에 적합한지 철저히 검토해야 합니다. 특히, 외부 서비스 사업자가 운영하는 서버와 이용자의 모바일 단말기 간 암호통신 여부도 반드시 확인해야 합니다.

8. 프로그램의 업데이트 정보를 이용자에게 수시로 알려주기

기 본

o 운영자는 모바일 단말기의 운영체제 및 응용프로그램에서 취약점이 발견될 경우, 이에 대한 정보를 신속히 확보해야 합니다.

- 이용자가 개인 모바일 단말기의 운영체제 및 응용프로그램 보안 패치 및 업데이트를 수행하지 않을 경우, 취약점을 악용하는 해커의 공격이 가능하기 때문에, 운영자는 이용자가 적시에 업데이트를 할 수 있도록 관련 정보 및 교육을 제공하고 지원해야 합니다.

o 운영자는 모바일 단말기와 업무용 서버에 대한 보안패치 및 업데이트가 적시에 이루어질 수 있도록, 아래 사항을 잘 고려해야 합니다.

- 운영자는 보안패치 및 업데이트를 적용하기 전에 반드시 현재 모바일 오피스에서 안정적으로 동작하는지 검증해야 합니다.

- 운영자는 보안패치 및 업데이트를 적용한 후, 이용자에게 보안패치 및 업데이트에 대한 정보를 제공해야 합니다.

권 고

o 운영자는 신속한 보안패치를 적용하기 위하여, 백신 및 보안 솔루션 사업자, 이동통신사, 단말기 제조사, 정부기관과의 긴밀한 관계를 유지하며, 모바일오피스 운영과 관련된 정보를 수집·공유하는데 협력해야 합니다.

9. 모바일 단말기 도난 · 분실 시, 원격으로 정보를 삭제하기

권 고

o 운영자는 이용자로부터 도난 · 분실 신고 접수를 받을 경우, 원격으로 도난 · 분실된 모바일 단말기의 기능을 통제하고, 저장된 정보를 신속히 삭제해야 합니다.

- 회사는 이용자의 부주의로 인한 정보유출 등의 사고를 사전에 막기 위해 원격단말관리(MDM) 기능을 사용할 수 있습니다.

o 원격단말관리(MDM) 기능을 도입할 경우, 원격 잠금 및 삭제 기능 이외에도 다음의 통제 기능을 활용할 수 있습니다.

- 운영자는 이용자의 모바일 단말기를 이용한 P2P와 웹하드 접속, 일반 PC 접속 등 허가받지 않은 접속 등을 통제할 수 있습니다.

- 운영자는 이용자가 개인 모바일 단말기를 이용하여 기업의 중요(기밀) 문서를 열람, 다운로드, 외부 출력 등을 하는지 감시할 수 있습니다.

[참고 ①] 스마트폰 이용자 10대 안전수칙

① 의심스러운 애플리케이션 다운로드하지 않기

- 스마트폰용 악성코드는 위·변조된 애플리케이션에 의해 유포 될 가능성이 있으므로 의심스러운 애플리케이션의 다운로드를 자제해야 합니다.

② 신뢰할 수 없는 사이트 방문하지 않기

- 의심스럽거나 알려지지 않은 사이트를 방문할 경우 정상 프로그램으로 가장한 악성프로그램이 사용자 몰래 설치될 수 있으므로. 신뢰할 수 없는 사이트 방문을 자제해야 합니다.

③ 발신인이 불명확하거나 의심스러운 메시지 및 메일 삭제하기

- 멀티미디어메세지(MMS)와 이메일의 첨부파일 기능은 악성코드 유포 수단으로 사용되는 경우가 많으므로 발신인이 불명확하거나 의심스러운 메시지 및 메일은 열어보지 말고 즉시 삭제해야 합니다.

④ 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기

- 단말기를 분실 혹은 도난당했을 경우 개인정보 유출 및 악성코드 설치 방지를 위하여 단말기 비밀번호를 설정해야 합니다.

⑤ 블루투스 기능 등 무선 인터페이스는 사용 시에만 켜놓기

- 악성코드 감염 가능성을 줄일 뿐만 아니라 단말기의 불필요한 배터리 소모를 막기 위해서는 블루투스 등 무선 인터페이스는 사용 시에만 활성화해야 합니다.

⑥ 이상증상이 지속될 경우 악성코드 감염여부 확인하기

- 이상증상 발생 시 스마트폰 매뉴얼에 따라 조치하며 조치 후에도 이상증상이 지속될 경우 악성코드에 의한 감염 가능성이 있으므로 백신 프로그램을 통한 단말기 진단 및 치료해야 합니다.

⑦ **다운로드한 파일은 바이러스 유무를 검사한 후 사용하기**

- 스마트폰용 악성프로그램은 특정 프로그램이나 파일에 숨겨져 유포될 수 있으므로, 프로그램 및 파일 다운로드·실행 시 스마트폰용 백신프로그램으로 바이러스 유무 검사 후 사용해야 합니다.

⑧ **PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기**

- 스마트폰과 PC간 데이터 백업, 복사, 전송 등의 작업수행 과정에서 PC에 숨어있는 악성코드가 스마트폰으로 옮겨질 수 있으므로 PC에 대한 백신프로그램 설치 및 정기 점검을 해야 합니다.

⑨ **스마트폰 플랫폼의 구조를 임의로 변경하지 않기**

- 스마트폰 플랫폼 구조를 변경(예: Jailbreak) 사용할 경우, 기본적인 보안기능 등에 영향을 주어 문제가 발생할 수 있으므로 이용자 스스로 구조 변경을 자제해야 합니다.

⑩ **운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하기**

- 해커들은 보안 취약점을 이용하고 다양한 공격기법을 사용하고 있으므로 이용자는 자신이 사용하는 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하여 사용해야 합니다.

※ 출처 : 스마트폰 이용자 10대 안전수칙 (방송통신위원회, 2010년 2월)

[참고 ②] 안전한 무선랜 이용 7대 수칙

① 무선공유기 사용시 보안기능 설정하기

- 무선 AP에서 제공하는 인증/암호 기술은 보안 강도에 따라 WEP, WPA, WPA2가 있으며, 안전한 이용을 위해 WPA2 설정을 권고합니다.

② 무선공유기 패스워드 안전하게 관리하기

- 무선공유기에 설치된 초기 패스워드는 공개되어 있어 타인이 쉽게 접속할 수 있으므로 반드시 변경 후 사용해야 합니다. 또한, 설정한 패스워드는 주기적으로 변경하고 추측하기 쉽거나 7자리 이하의 짧은 패스워드는 사용하지 않아야 합니다.

③ 사용하지 않는 무선공유기는 꺼놓기

- 사용하지 않는 무선공유기를 켜 놓을 경우 외부인이 불법다운로드, 해킹등에 악용할 수 있고 전력이 낭비될 수 있으므로, 사용하지 않는 무선공유기는 꺼놓아야 합니다.

④ 제공자가 불분명한 무선랜 이용하지 않기

- 개인정보 유출 등을 위해 악의적인 목적으로 설치한 무선공유기를 이용할 경우 개인정보가 쉽게 유출될 수 있습니다. 부득이 외부에서 무선랜 이용이 필요할 경우 본인이 잘 알고 있거나, 무선랜 이용 장소에서 제공자가 확인된 무선랜 만을 이용해야 합니다.

⑤ 보안설정 없는 무선랜으로 민감한 서비스 이용하지 않기

- 보안설정이 없는 무선랜의 경우 이용자의 접속행위, 개인정보 등이 유출될 수 있습니다. 부득이 무선랜 이용이 필요할 경우 금융거래, 기업업무, 로그인이 필요한 서비스, 개인정보를 입력하는 서비스 등 민감한 서비스는 가급적 사용하지 않아야 합니다.

⑥ **무선랜에 자동 접속 기능 사용하지 않기**

- 무선단말기에는 한번 접속한 무선랜에 자동으로 접속하는 기능이 있습니다. 무선랜 이름은 관리자가 임의로 변경가능하기 때문에, 해커가 잘 알려진 무선랜을 가장하여 자동접속 기능을 통해 이용자의 접속을 유도할 경우 개인정보 유출 등의 위험에 노출될 수 있습니다. 따라서, 무선랜의 자동접속기능은 끄고, 기존 접속한 무선랜 리스트는 주기적으로 지워야 합니다.

⑦ **무선공유기의 SSID를 변경하고 숨김 기능 설정하기**

- SSID(Service Set IDentification)란 무선랜을 구분하기 위한 이름입니다. SSID 숨김은 SSID 보안설정과 함께 사용 되어 보안성을 높이는 기능입니다. SSID를 숨김으로 할 경우 외부인은 해당 무선랜이 존재하는 지 알 수 없으므로 무선랜을 이용할 수 없어 해킹, 정보유출을 예방할 수 있습니다.

※ 출처 : '알기쉬운 무선랜 보안 안내서' (방송통신위원회-한국인터넷진흥원, 2010.8월)

[참고 ③] BYOD (Bring Your Own Device) 정의

많은 기업들은 모바일 오피스를 도입하는 과정에서 비용은 줄이면서 직원의 만족도 및 생산성을 높이기 위해서, 직원 소유의 모바일 단말기를 업무에 사용하는 방안을 고려하고 있다.

BYOD는 사용자의 개인 단말기를 개인 용무 이외에 회사 업무에도 사용하는 정책으로서, 전세계 기업들 중 약 3분의 2가 BYOD 정책을 갖고 있으며, 이들 중 20~22%의 기업들은 직원들이 소유한 노트북, 태블릿, 스마트폰 등을 지원할 정도로 BYOD 기반의 모바일 오피스로 변화하고 있다.
※ 출처: 포레스터 컨설팅이 전세계 546개 기업을 대상으로 조사

하지만 모바일 오피스 도입하려는 회사들은 우선적으로 BYOD 환경을 고려하면서도, 분실·도난의 위험, 취약한 네트워크 이용 등의 심각한 보안 위협도 우려하는 것이 현실이다.

BYOD 보안은 네트워크 접근 제어(NAC)와 모바일 기기 관리(MDM) 기능을 통해 개인 소유의 모바일 단말기가 관리됨으로써 보안이 강화될 수 있다.

BYOD 보안 = 네트워크 접근 제어(NAC) + 모바일 기기 관리(MDM)

「네트워크 접근 제어(NAC : Network Access & Control)」는 누가, 무엇을, 어디에서, 언제, 어떻게 네트워크에 접근하고, 어느 곳에서 나가는지 결정하는 기능이며,「모바일 기기 관리(MDM : Mobile Device Management)」는 루팅, 탈옥 등 비정상적인 단말기 사용 금지, 분실 또는 도난 단말기의 원격 데이터 삭제 실행 등 모바일 기기의 중요한 자산 관리 및 단말기를 관리하는 기능이다.