

모바일 오피스 정보보호 안내서

2013. 12



미래창조과학부
Ministry of Science, ICT and
Future Planning

KISA 한국인터넷진흥원
Korea Internet & Security Agency

제 · 개정 이력

순번	제 · 개정일	변경내용	발간팀	연락처
1	2013. 12. 30	제정	기업정보보호팀	02)405-6521

서 문	05
제 1 장 모바일 보안위협	06
제 1 절 모바일 오피스 구성	06
제 2 절 위협 유형에 따른 분류	08
1. 개인정보침해	10
2. 도청	10
3. 피싱(Phishing) 및 파밍(Pharming)	11
4. 서비스 거부(DoS/DDoS)	11
5. 권한탈취	12
6. 악성코드 · 해킹	13
7. 정보유출	14
제 3 절 보안위협 시나리오	18
1. 단말기 주요기능 조작을 통한 개인정보 및 업무정보 침해	18
2. 취약한 무선 네트워크 사용에 따른 정보유출	19
3. 스미싱을 이용한 인증정보 탈취	20
4. 권한 상승을 통한 악성코드 배포	23
5. 사용자 부주의로 인한 악성코드 감염 · 해킹	24
6. 단말기 키로거 감염 또는 관리소홀로 인한 정보 유출	26
제 2 장 모바일 오피스 보호대책	29
제 1 절 보안 유형별 모바일 오피스 보호대책	29
1. 기술적 보호대책	30
2. 관리적 보호대책	32
제 2 절 정보 유형별 모바일 오피스 보호대책	34
1. 인증정보 보호대책	34
2. 개인정보 보호대책	35
3. 업무정보 보호대책	35
4. 금융정보 보호대책	35

제 3 절 모바일 오피스 보안 점검항목	36
1. 운영자를 위한 보안 점검항목	36
2. 사용자를 위한 보안 점검항목	40
결 론	41
용어정리	42
참고문헌	44

부 록

제 1 장 모바일 오피스 현황 및 분류	46
제 1 절 모바일 오피스 시장 및 서비스 현황	46
제 2 절 모바일 오피스 유형 분류	50
제 2 장 보안위협 및 보안대책 매칭표	53

그림 목차

【그림 1-1】 모바일 오피스 구성도	06
【그림 2-1】 단말기 주요기능 조작을 통한 개인정보 및 업무정보 침해	18
【그림 2-2】 가짜(Fake) AP를 이용한 도청	19
【그림 2-3】 스미싱을 이용한 악의적인 애플리케이션 설치 유도	21
【그림 2-4】 권한 상승을 이용한 악성코드 배포	23
【그림 2-5】 웹 애플리케이션 기반에서 XSS 공격을 이용한 악성코드 감염	24
【그림 2-6】 테더링 사용에 의한 업무용 PC 공격	25
【그림 2-7】 키로거를 통한 업무정보 유출	26
【그림 2-8】 관리 소홀로 인한 업무정보 유출	28



서 문

모바일 오피스 정보보호 안내서

“모바일 오피스 정보보호 안내서”는 모바일 오피스 운영자와 사용자의 보안 인식 수준을 제고하고, 모바일 오피스의 안전한 구축 및 운영 방법을 안내하기 위해 제작되었습니다.

모바일 오피스는 스마트폰과 같은 모바일 단말기의 이동성, 개방성, 다양성을 기반으로 제공되는 새로운 형태의 업무 서비스로서 기업의 비용절감, 효율성 증대 등 다양한 측면에서 긍정적인 효과를 가져올 것으로 기대되고 있습니다. 하지만 단말기 분실 및 도난, 악성코드 감염 등의 보안위협으로 개인정보 및 기업 기밀정보 유출, 불법 과금 등 여러 형태의 보안 사고가 발생할 수 있으며, 이로 인한 피해는 더욱 커질 것으로 예상됩니다.

이에 본 안내서에서는 모바일 오피스 보안위협 분석결과를 토대로 모바일 오피스 구축 및 이용 시 고려해야할 보안문제들을 이해하기 쉽게 시나리오 형태로 다루고 있으며, 안전한 모바일 오피스 도입·운영이 이루어질 수 있도록 기술적·관리적 보호대책을 마련하였습니다. 아울러 운영자 및 이용자가 스스로 모바일 오피스 보안수준을 진단해볼 수 있도록 보안점검 항목을 제시하고 있습니다.

본 안내서의 구성은 다음과 같습니다.

1장에서는 모바일 오피스 보안위협에 대해서 설명하고, 2장에서는 모바일 오피스 보안위협에 대응하기 위한 보호대책을 제시하고 있습니다.

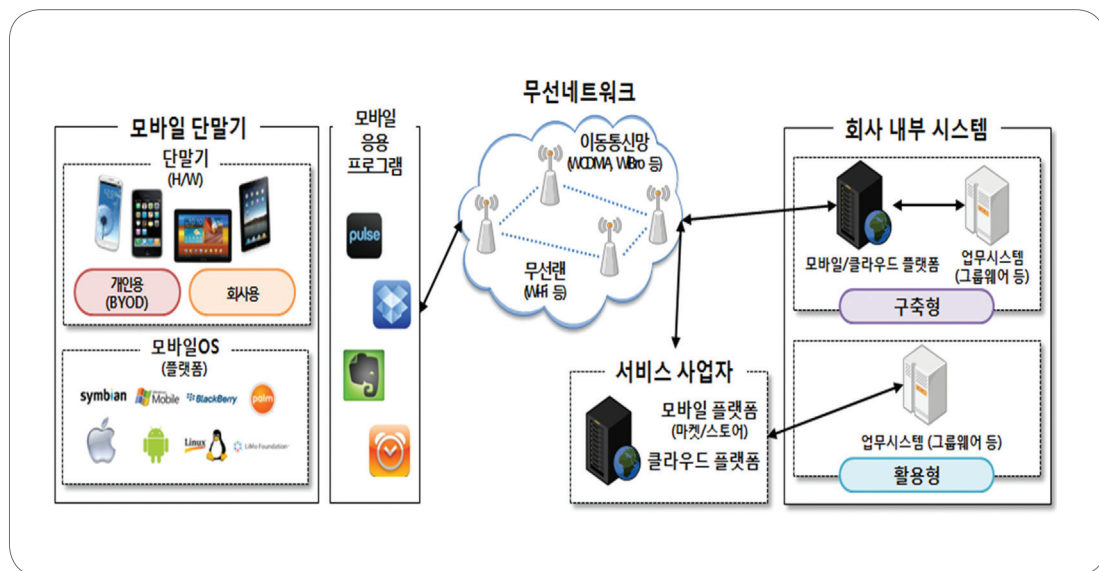


제 1 장 모바일 오피스 보안위협

제 1 절 모바일 오피스 구성

모바일 오피스(Mobile office, 이동 사무실)는 언제, 어디서나 모바일 단말기(이동통신기기)를 이용하여 외부에서 사내업무를 처리할 수 있는 업무 환경을 말한다.¹⁾

모바일 오피스는 별도의 단말기나 네트워크를 구성할 필요 없이 사용자가 보유하고 있는 모바일 단말기와 무선인터넷(이동통신망, Wi-Fi, WiBro 등)을 사용하여 서비스되며, 모바일 단말기, 모바일 응용프로그램, 무선 네트워크, 그리고 기업 업무와 관련된 내부 시스템으로 구성된다.



【그림 1-1】 모바일 오피스 구성도

● 모바일 단말기

모바일 단말기는 직원 개개인이 소유한 휴대용 기기로서, 스마트폰, 태블릿 PC 등 그 종류가 다양하다. 모바일 단말기는 하드웨어(H/W), 운영체제(OS)로 구성되어 있다. 운영체제는 모바일 단말기

1) 방송통신위원회, 한국인터넷진흥원, “안전한 모바일 오피스 도입과 운영을 위한 정보보호 수칙”, 2012.

내 다양한 응용프로그램들의 설치 및 실행을 관리하는 역할을 수행한다. 현재 많이 사용되는 모바일 운영체제는 구글의 안드로이드, 애플의 iOS, 마이크로소프트의 윈도우/윈도우폰 등이 있다.

● 모바일 응용프로그램

모바일 응용프로그램은 모바일 운영체제 상에서 설치 및 실행되는 서비스 프로그램으로서, 개발 방식에 따라 “모바일 웹(Mobile Web)”과 “모바일 앱(Mobile App)”으로 분류된다.

● 무선 네트워크

케이블, 광케이블 등의 유선 전송매체를 사용하지 않고 무선 네트워크를 활용하여 데이터를 전달하는 기술로서, 이동통신망(3G/4G, WiBro 등)과 무선랜(WiFi) 등이 활용되고 있다.

● 내부 시스템

모바일 오피스 업무가 실제로 처리되는 내부 시스템 영역으로, 인증 서버, 데이터베이스(DB) 등으로 구성된다.

제 2 절 위협 유형에 따른 분류

모바일 오피스 보안위협은 단말기 자체에 내재된 취약점 또는 단말기 사용 부주의로 발생할 수 있다. 모바일 오피스 보안위협의 유형은 크게 개인정보침해, 도청, 피싱 및 파밍, 서비스거부(DoS/DDoS), 권한 탈취, 악성코드 및 해킹, 정보유출과 같이 분류할 수 있다.

위협	내 용	위협코드(MTE)
개인정보침해	- 위치정보 탈취를 통한 개인정보 침해	MTE-101
	- 카메라, 마이크 등 단말기의 하드웨어 자원을 이용한 개인정보 침해	MTE-102
도청	- 네트워크로 전송되는 데이터 패킷 도청	MTE-201
	- mVoIP 사용 시 음성 및 영상 통화 도청	MTE-202
피싱 및 파밍	- 악의적인 사이트를 이용한 사용자 정보 입력 유도	MTE-301
	- 문자 메시지, 이메일 등을 이용하여 악성 애플리케이션 설치 유도	MTE-302
서비스 거부 (DoS/DDoS)	- 지속적인 통화연결 및 데이터 전송요청 등을 통한 배터리 소진 등 단말기 서비스 거부 공격	MTE-401
	- 좀비 PC, 좀비 모바일 단말기 등을 이용한 내부 서버 대상의 서비스 거부 공격	MTE-402
권한탈취	- 단말기-내부시스템 간 중간자(Man-in-the-Middle) 공격을 통한 사용자 권한 획득	MTE-501
	- SQL 인젝션(Injection) 공격을 통한 인증 우회	MTE-502
	- 단말기 루팅, 탈옥을 통해 관리자(Root) 권한 탈취	MTE-503
	- 버퍼 오버플로우 공격을 통한 관리자 권한 탈취	MTE-504
	- 단말기와 내부 시스템 간에 맺어진 세션 탈취	MTE-505

위협	내 용	위협코드(MTE)
악성코드 · 해킹	- 악의적인 스크립트 실행으로 공격자가 악성코드를 삽입한 웹사이트 접속	MTE-601
	- 불필요한 서비스(포트) 사용 취약점	MTE-602
	- 모바일 애플리케이션 소스코드 분석(리버스 엔지니어링)을 통한 취약점 분석	MTE-603
	- 단말기에서 제공하는 테더링 기능을 사용하여 서버 보안 정책 우회 및 공격 경로로 활용	MTE-604
	- 단말기를 USB 이동저장매체로 사용하여 악성코드 전파	MTE-605
정보유출	- 내부자에 의한 기업 내부 정보자산 유출	MTE-701
	- 단말기 분실, 도난, 양도, 공공장소 사용에 따른 내부정보 유출	MTE-702
	- 단말기 녹음, 녹화, 화면캡처, 메모 기능을 통해 생성·저장된 정보 유출	MTE-703
	- 비인가 AP를 통한 정보유출	MTE-704
	- 키로거(Key Logger) 감염에 의한 사용자 입력정보 탈취	MTE-705
	- 블루투스 및 Wi-Fi Direct 취약점을 이용한 정보유출	MTE-706
	- 비인가 애플리케이션 설치에 따른 정보유출	MTE-707
	- 비인가자의 정보 획득 및 업무처리 기능 접근	MTE-708

※ MTE : Mobile office security Threats Enumeration

1. 개인정보 침해

개인정보 침해 위협은 모바일 오피스 단말기를 통해 특정 개인을 식별할 수 있거나 프라이버시를 침해할 수 있는 정보가 유출되는 위협이다.

MTE-101 위치정보 탈취를 통한 개인정보 침해

- 공격자는 모바일 단말기에 악성 프로그램을 설치하여, 단말기에 내장된 위치기반서비스(LBS, Location Based Service) 기능을 이용해 사용자의 위치정보를 수집하고, 이를 통해 사용자의 이동경로, 생활 패턴 등을 파악할 수 있다.

MTE-102 카메라, 마이크 등 단말기의 하드웨어 자원을 이용한 개인정보 침해

- 공격자는 악성 프로그램을 이용해 단말기 하드웨어 사용 권한을 획득한 후, 카메라, 마이크 등을 원격 제어하여 사용자의 사생활 침해 또는 업무 활동 등을 감시할 수 있다.

2. 도청

도청 공격은 모바일 오피스 애플리케이션을 통해 전송되는 업무정보(문서, 음성·영상정보 등)를 탈취하는 공격이다.

MTE-201 네트워크로 전송되는 데이터 패킷 도청

- 무선 네트워크를 통해 사용자 단말기에서 회사 내부시스템으로 데이터 패킷전송 시 이를 중간에서 탈취하는 도청(스니핑:Sniffing)이 가능하다.

MTE-202 mVoIP 사용 시 음성 및 영상 통화 도청

- 사용자 단말기에 악성 프로그램을 설치하여, 모바일 인터넷전화(mVoIP) 사용 시 음성/영상 통화내용을 도청하는 공격이다.
- 애플리케이션 계층에서 동작하는 mVoIP 프로그램의 음성/영상 패킷이 암호화되지 않은 경우 또는 가짜 AP를 통한 중간자 공격을 통해 도청이 이루어질 수 있다.

3. 피싱(Phishing) 및 파밍(Pharming)

모바일 오피스 이용자의 부주의를 악용한 공격으로, 주로 사회공학적 기법을 활용한 개인정보 및 업무정보 유출, 또는 후속 공격을 위한 악성코드 삽입 등의 공격으로 분류될 수 있다.

MTE-301 악의적인 사이트를 이용한 사용자 정보 입력 유도

- 사용자 개인정보 및 업무정보를 취득하기 위해 공격자가 악성코드를 삽입한 악의적인 웹페이지를 정상적인 것처럼 위장하여 사용자가 정보를 입력하도록 유도하는 공격이다.

MTE-302 문자 메시지, 이메일 등을 이용하여 악의적인 애플리케이션 설치 유도

- 공격자는 근무하는 회사 또는 관련 업체인 것처럼 가장하여 문자 메시지, 이메일 등에 악의적인 웹사이트 주소(URL)를 삽입하여 전송한다.
- 사용자가 웹사이트에 접속하면, 악의적인 애플리케이션 설치, 악성코드 감염, 모바일 결제 등이 실행된다.

4. 서비스 거부(DoS/DDoS)

모바일 오피스를 이용하는 단말기나 내부시스템의 서비스 가용 자원을 소모시켜 정상적인 동작이 불가능하도록 만드는 공격이다.

MTE-401 지속적인 통화연결 및 데이터 전송요청 등을 통한 배터리 소진 등 단말기 서비스 거부 공격

- 사용자의 단말기에 악성 프로그램을 설치하여 배터리 소모, 지속적인 통화 요청, 네트워크 사용 금지 등 업무처리가 불가능하도록 단말기를 마비시키는 공격이다.

MTE-402 좀비 PC, 좀비 모바일 단말기 등을 이용한 내부 서버 대상의 서비스 거부 공격

- 악성코드에 감염된 단말기를 통해 내부시스템이 처리할 수 없을 정도로 큰 용량의 쿼리(Query), 정보 요청 등을 지속적으로 전송함으로써 시스템을 마비시키는 공격이다.

5. 권한탈취

공격자가 단말기, 애플리케이션, 네트워크 영역에서 모바일 오피스 사용자 계정(ID/PW), 쿠키, 세션 등 인증 및 권한 정보를 탈취하여 정상적인 사용자로 위장하는 공격이다.

MTE-501 단말기-내부시스템 간 중간자(Man-In-The-Middle) 공격을 통한 사용자 권한 획득

- 권한탈취 공격은 일반적으로 단말기와 내부 시스템 사이에서 정보를 탈취하는 중간자(Man-In-The-Middle, MITM) 공격을 통해 이루어진다.
- 단말기와 내부 시스템이 통신을 시작할 때, 공격자는 단말기에게 자신이 내부 시스템, 또는 내부 시스템에게 자신이 단말기인 척 하여 중간에서 전송되는 모든 정보를 수집·열람할 수 있는 권한을 획득할 수 있다.

MTE-502 SQL 인젝션(Injection) 공격을 통한 인증 우회

- 웹 애플리케이션의 입력값 검증 취약점을 이용하는 공격 중 하나이다.
- 웹 애플리케이션의 사용자 입력값(계정정보 등)으로 데이터베이스 조회 언어인 SQL 구문을 프로그램에 강제로 삽입할 경우 사용자 인증 우회를 통한 권한 획득 및 데이터 유출이 가능하다.

MTE-503 단말기 루팅, 탈옥을 통해 관리자(Root) 권한 탈취

- 루팅 또는 탈옥을 수행한 단말기의 경우, 공격자가 해당 단말기의 관리자 권한을 쉽게 획득할 수 있으며, 이를 통해 모바일 오피스를 이용하면서 전송·저장되는 업무정보를 탈취할 수 있다.
- ※ 루팅, 탈옥 : 안드로이드 또는 iOS 기반 단말기에서 관리자(Root) 권한을 획득하는 해킹 기술

MTE-504 버퍼 오버플로우(Buffer Overflow) 공격을 통한 관리자 권한 탈취

- 프로그램의 메모리 스택 또는 힙 영역에 예상치 못한 값을 보내어 오버플로우를 일으킴으로서 에러를 유발시키는 공격이다.
- 프로그램에 에러를 유발시킬 때 특정 코드 또는 특수한 실행 프로그램을 넣어두면, 에러가 발생한 프로그램이 관리자 권한으로 동작하게 됨으로써, 관리자 인증을 우회하여 서비스를 이용할 수 있다.

MTE-505 단말기와 내부 시스템 간에 맺어진 세션 탈취

- 단말기와 내부 시스템 간에 유지하고 있는 세션(Session)을 공격자가 가로채는 공격으로 세션 하이재킹(Session Hijacking)이라 불린다.

6. 악성코드 · 해킹

모바일 오피스 단말기의 물리적 · 관리적 운영 소홀로 인한 악성코드 감염 및 내부시스템으로의 전파, 해킹을 통한 내부시스템 불법 접근 등의 공격이 이루어질 수 있다.

MTE-601 악의적인 스크립트 실행으로 공격자가 악성코드를 삽입한 웹사이트 접속

- 대표적인 스크립트 삽입 공격으로 XSS(Cross Site Scripting)가 존재한다.
- 공격자는 모바일 웹 또는 하이브리드 기반의 모바일 오피스 애플리케이션에 탑재된 게시판, 이메일 등에 악성 스크립트를 삽입한 후, 사용자가 해당 게시물이거나 메일 등을 클릭했을 때 스크립트가 동작하도록 유도한다.

MTE-602 불필요한 서비스(포트) 사용 취약점

- 모바일 서비스 제공자가 운영하는 서버 운영 플랫폼의 미사용 서비스 포트를 통해 내부 시스템에 대한 정보수집(스캐닝)이 가능하다.
- 공격자는 스캐닝으로 수집한 내부시스템 정보(운영체제, 네트워크 상태 등)를 통해 취약점 분석 및 2차 공격을 수행할 수 있다.

MTE-603 모바일 애플리케이션 소스코드 분석(리버스 엔지니어링)을 통한 취약점 분석

- 공격자는 앱스토어, 마켓을 통해 공개된 모바일 오피스 애플리케이션을 다운로드 후, 소스코드 분석(리버스 엔지니어링)을 수행할 수 있다.
 - ※ 리버스 엔지니어링 : 애플리케이션을 소스코드 및 기계어 수준으로 역 분석함으로써, 애플리케이션의 내부 동작과 설계를 추적하는 방법
- 이 과정에서 공격자는 해당 애플리케이션에 내재된 취약점을 발견하여 애플리케이션의 내부 프로세스의 임의변조 및 악성코드 삽입이 가능하다.

MTE-604 단말기에서 제공하는 테더링 기능을 사용하여 서버 보안정책 우회 및 공격 경로로 활용

- 단말기의 테더링 기능을 사용하여 네트워크에 접속할 경우, 내부시스템에 정의된 보안정책을 우회하여 외부 서버로의 접근이 가능하다.
- 테더링을 통한 보안정책 우회 및 악의적인 사이트 등에 접속하게 될 경우 업무용 PC에 악성코드 감염 등이 이루어질 수 있다.

MTE-605 단말기를 USB 이동저장매체로 사용하여 악성코드 전파

- 모바일 단말기는 USB 이동저장매체로 활용될 수 있으며, 이로 인해 PC에 존재하는 악성코드가 단말기로 감염될 수 있다. 악성코드 감염 단말을 업무용 PC에 연결할 경우 내부시스템으로의 추가 감염·전파가 이루어질 수 있다.

7. 정보유출

모바일 오피스 단말기와 내부시스템에 저장된 정보가 기술적·관리적 부주의로 인해 비인가된 제 3자에게 유출되는 보안위협이다.

MTE-701 내부자에 의한 기업 내부 정보자산 유출

- 내부 직원이 모바일 오피스용 단말기 또는 내부시스템의 정보자산을 악의적인 목적으로 유출할 수 있다.

MTE-702 단말기 분실, 도난, 양도, 공공장소 사용에 따른 내부정보 유출

- 공공장소에서 모바일 오피스를 이용해 업무를 처리할 때 타인이 그 과정을 지켜보거나, 단말기를 분실 및 도난, 또는 타인에게 대여 및 양도할 때 사용자 부주의로 인한 정보유출이 발생할 수 있다.

MTE-703 단말기 녹음, 녹화, 화면캡처, 메모 기능을 통해 생성·저장된 정보 유출

- 업무의 신속성 및 편의를 위해 업무정보를 녹음, 녹화, 화면캡처 등의 기능을 사용하여 단말기에 저장한 경우, 이는 단말에 설치된 악성코드, 악성 애플리케이션 등을 통해 유출될 수 있다.

MTE-704 비인가 AP를 통한 정보유출

- 비인가 AP를 이용할 경우, 모든 업무정보가 공격자의 AP를 경유하여 전송되기 때문에 공격자가 이를 도청하거나 외부로 유출할 수 있다.
- ※ 비인가 AP : 기업에서 정상적인 목적으로 허가하여 설치 및 운영하지 않는, 보안이 적용되지 않은 AP를 지칭하며, 주로 공격자가 악의적인 목적으로 설치하여 운영

MTE-705 키로거(Key Logger)²⁾ 감염에 의한 사용자 입력정보 탈취

- 키로거에 감염될 경우, 모바일 단말기 사용자가 입력하는 키패드 정보(인증정보, 패스워드, 모바일 뱅킹 정보 등)값이 유출될 수 있다.

MTE-706 블루투스 및 Wi-Fi Direct 취약점을 이용한 정보유출

- 보안이 적용되지 않은 블루투스, Wi-Fi Direct 등의 무선 통신기술을 사용하여 정보를 공유 및 전송시킬 경우 정보가 외부로 유출될 수 있다.

MTE-707 비인가 애플리케이션 설치에 따른 정보유출

- 비인가 애플리케이션 내에는 공격자가 심어놓은 악성코드가 포함되어 있을 수 있으며, 이를 통해 업무정보가 유출될 수 있다.
- ※ 비인가 애플리케이션 : 공식 앱 마켓, 앱스토어가 아닌 블랙마켓을 통해 배포되는 서명 인증이 이루어지지 않은 애플리케이션

MTE-708 비인가자의 정보 획득 및 업무처리 기능 접근

- 모바일 오피스 기능에 따라 사용 권한을 설정하지 않거나, 업무정보에 대한 접근 권한이 설정되지 않은 경우, 비인가자에 의한 정보열람 및 외부유출이 이루어질 수 있다.

2) 키로거(Key Logger) : 사용자의 키보드 입력값을 탈취하는 프로그램

모바일 오피스 구성요소(단말기, 애플리케이션, 네트워크, 내부시스템)에 따라 보안위협을 분류하면 다음과 같다.

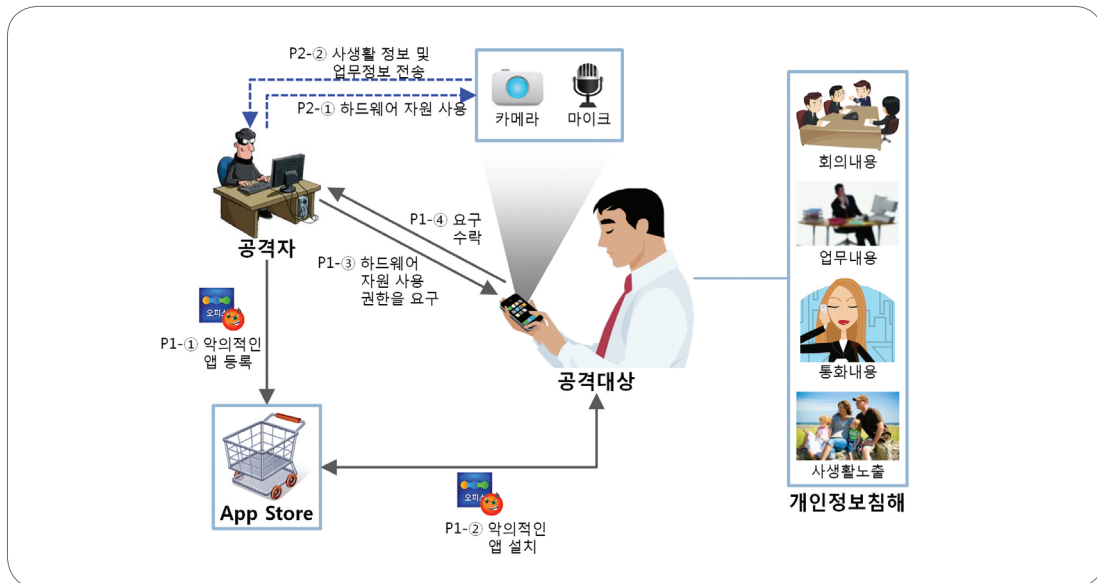
구성 요소	보안위협		
	대분류	소분류	MTE
단 말 기	개인정보 침해	- 위치정보 탈취를 통한 개인정보침해	MTE-101
		- 카메라, 마이크 등 단말기의 하드웨어 자원을 이용한 개인정보 침해	MTE-102
	도청	- mVoIP 사용 시 음성 및 영상 통화 도청	MTE-202
	피싱 및 파밍	- 악의적인 사이트를 이용한 사용자 정보 입력 유도	MTE-301
		- 문자 메시지, 이메일 등을 이용하여 악성 애플리케이션 설치 유도	MTE-302
	서비스 거부 (DoS/DDoS)	- 지속적인 통화연결 및 데이터 전송요청 등을 통한 배터리 소진 등 단말기 서비스 거부 공격	MTE-401
	권한탈취	- 단말기 루팅, 탈옥을 통해 관리자(Root)권한 탈취	MTE-503
	악성코드 · 해킹	- 단말기에서 제공하는 테더링 기능을 사용하여 서버 보안정책 우회 및 공격 경로로 활용	MTE-604
		- 단말기를 USB 이동저장매체로 사용하여 악성코드 전파	MTE-605
	정보유출	- 내부자에 의한 기업 내부 정보자산 유출	MTE-701
		- 단말기 분실, 도난, 양도, 공공장소 사용에 따른 내부정보 유출	MTE-702
		- 단말기 녹음, 녹화, 화면캡처, 메모 기능을 통해 생성·저장된 정보 유출	MTE-703
		- 키로거(Key Logger) 감염에 의한 사용자 입력정보 탈취	MTE-705

구성 요소	보안위협		
	대분류	소분류	MTE
애플리케이션	권한탈취	- SQL 인젝션(Injection) 공격을 통한 인증 우회	MTE-502
		- 버퍼 오버플로우 공격을 통한 관리자 권한 탈취	MTE-504
	악성코드 · 해킹	- 악의적인 스크립트 실행으로 공격자가 악성코드를 삽입한 웹사이트 접속	MTE-601
		- 모바일 애플리케이션 소스코드 분석(리버스 엔지니어링)을 통한 취약점 분석	MTE-603
	정보유출	- 비인가 애플리케이션 설치에 따른 정보유출	MTE-707
		- 비인가자의 정보 획득 및 업무처리 기능 접근	MTE-708
네트워크	도청	- 네트워크로 전송되는 데이터 패킷 도청	MTE-201
		- mVoIP 사용 시 음성 및 영상 통화 도청	MTE-202
	권한탈취	- 단말기-내부시스템에 대한 중간자(Man-in-the-Middle) 공격을 통한 사용자 권한 획득	MTE-501
		- 단말기와 내부 시스템 간에 맺어진 세션 탈취	MTE-505
	악성코드 · 해킹	- 불필요한 서비스(포트) 사용 취약점	MTE-602
	정보유출	- 비인가 AP를 통한 정보유출	MTE-704
		- 블루투스 및 Wi-Fi Direct 취약점을 이용한 정보유출	MTE-706
내부시스템	서비스 거부 (DoS/DDoS)	- 좀비 PC와 좀비 모바일 단말기 등을 이용한 내부 서버 대상의 서비스 거부 공격	MTE-402
	정보유출	- 내부자에 의한 기업 내부 정보자산 유출	MTE-701

제 3 절 보안위협 시나리오

1. 단말기 주요기능 조작을 통한 개인정보 및 업무정보 침해

공격자는 단말기의 카메라, 마이크 등의 하드웨어 자원 제어 권한을 획득하여 사용자의 사생활 침해 및 업무 활동을 감시할 수 있다. 공격자는 카메라를 이용해 사진 또는 영상을 촬영·전송하거나, 마이크를 이용해 사용자 뿐 아니라 주변의 대화도 엿들을 수 있다.



【그림 2-1】 단말기 주요기능 조작을 통한 개인정보 및 업무정보 침해

Phase 1

하드웨어 자원 제어 권한 획득

- ① 공격자는 모바일 오피스 서비스를 위한 단말기 원격 관리 애플리케이션에 하드웨어 제어 및 정보 전송을 수행하는 악성코드를 숨겨 넣어 앱 마켓(App Store)에 등록한다.
- ② 사용자는 공격자가 앱 마켓에 등록한 단말기 원격 관리 애플리케이션을 구매하여 자신의 업무용 단말기에 설치한다.
- ③ 단말기 원격 관리 애플리케이션은 사용자 단말에 설치되는 과정에서 단말기 하드웨어 자원 사용 권한의 확인 및 승인을 요구한다.

※ 단말기 원격 관리 애플리케이션의 하드웨어 자원 사용권한

－ 단말기 도난 및 분실 시 위치추적을 위한 위치정보 수집·활용 권한

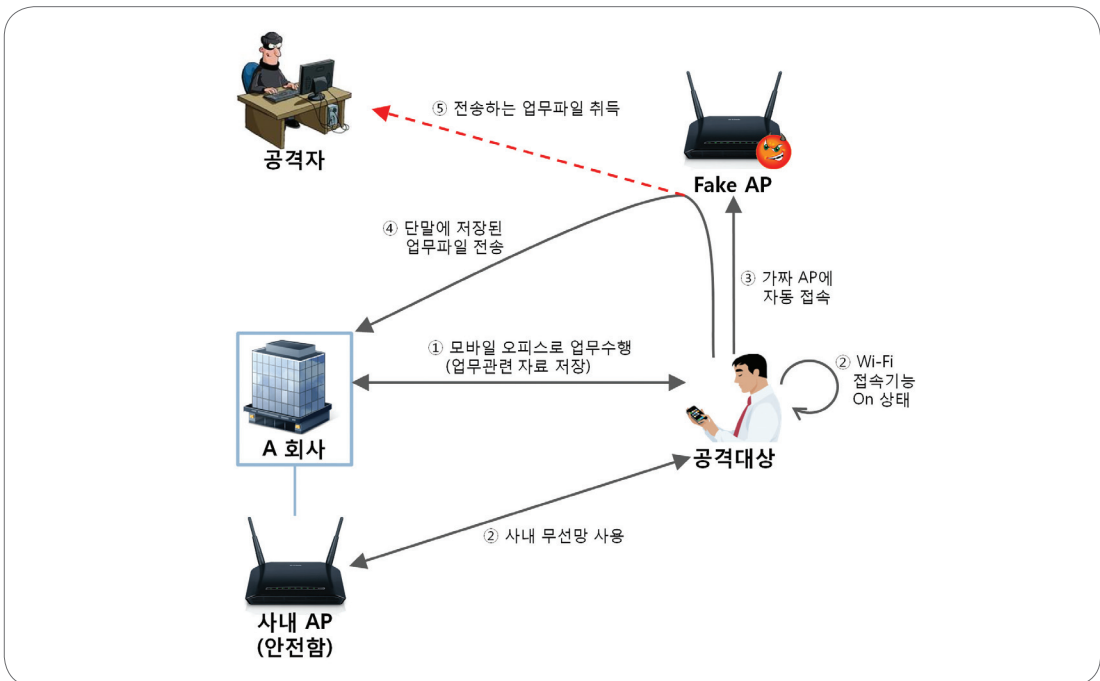
- 단말기 도난 및 분실 시 통화차단을 위한 음성 및 영상 통화 제어 권한
 - 단말기 도난 및 분실 시 SMS 알람을 위한 SMS 제어 권한
- ④ 사용자는 애플리케이션의 자원 사용권한 요청을 수락하며, 해당 애플리케이션은 단말기에 성공적으로 설치된다.

Phase 2

단말기 하드웨어 자원 무단 사용에 따른 개인정보 및 업무정보 침해

- ① 공격자는 하드웨어 제어 악성코드를 이용하여 사용자가 인지할 수 없도록 마이크, 카메라 등의 기능을 동작시킨 후, 사용자의 주변 대화, 통화, 회의내용, SMS 등의 정보를 전송받는다.
- ※ 공격자가 하드웨어 자원을 지속적으로 이용할 경우 단말기의 배터리가 급격하게 소모되어 사용자가 공격을 인지할 수 있기 때문에, 특정시간에 맞춰 공격을 수행할 수 있다.
- ② 공격자는 지속적인 공격을 통해 사용자의 생활 및 업무 패턴, 회의 내용, 업무 관련 통화내용 등을 수집한다.

2. 취약한 무선 네트워크 사용에 따른 정보유출



【그림 2-2】가짜(Fake) AP를 이용한 도청

① A씨는 외부에서 모바일 오피스로 회사업무를 수행할 때, 업무 관련정보를 단말기에 저장한다.

※ 단말기에 업무 관련정보를 저장하는 방법은 다음과 같다.

- 파일 다운로드
- 처리 화면을 캡처
- 통화 내용 또는 회의 내용을 녹음
- 메모 등의 기능을 사용

※ 단말기에 저장되는 정보는 모바일 오피스 애플리케이션을 통해 저장될 경우 암호화가 되어 저장될 수 있으나, 일반적인 단말기의 메모 기능, 음성 녹음 기능, 화면 캡처 기능을 통해 저장된 정보나, 이메일로 다운받은 파일의 경우 암호화가 적용되지 않는다.

②, ③ A씨는 단말기의 무선랜(Wi-Fi) 기능을 활성화하여 사내에서 제공하는 무선 AP에 접속 및 데이터 통신을 시도한다.

※ A씨는 평소에 단말기의 Wi-Fi 기능을 끄지 않으며, 외부에 있을 때 Wi-Fi의 자동 접속 기능을 통해 과거 접속한 이력이 있는 이름의 무선 AP에 자동적으로 접속을 실행하게 된다.

④ A씨는 사내에서 제공하는 무선랜에 정상적으로 접속하였다고 인지한 후, 단말기에 저장된 업무 파일 등의 정보를 타사, 타 부서 또는 팀원 등에게 전송 한다.

※ 사용자는 단말기의 Wi-Fi 자동접속 기능 때문에 사내에서 제공하는 Wi-Fi에 정상적으로 접속하였는지 인지하지 못한다.

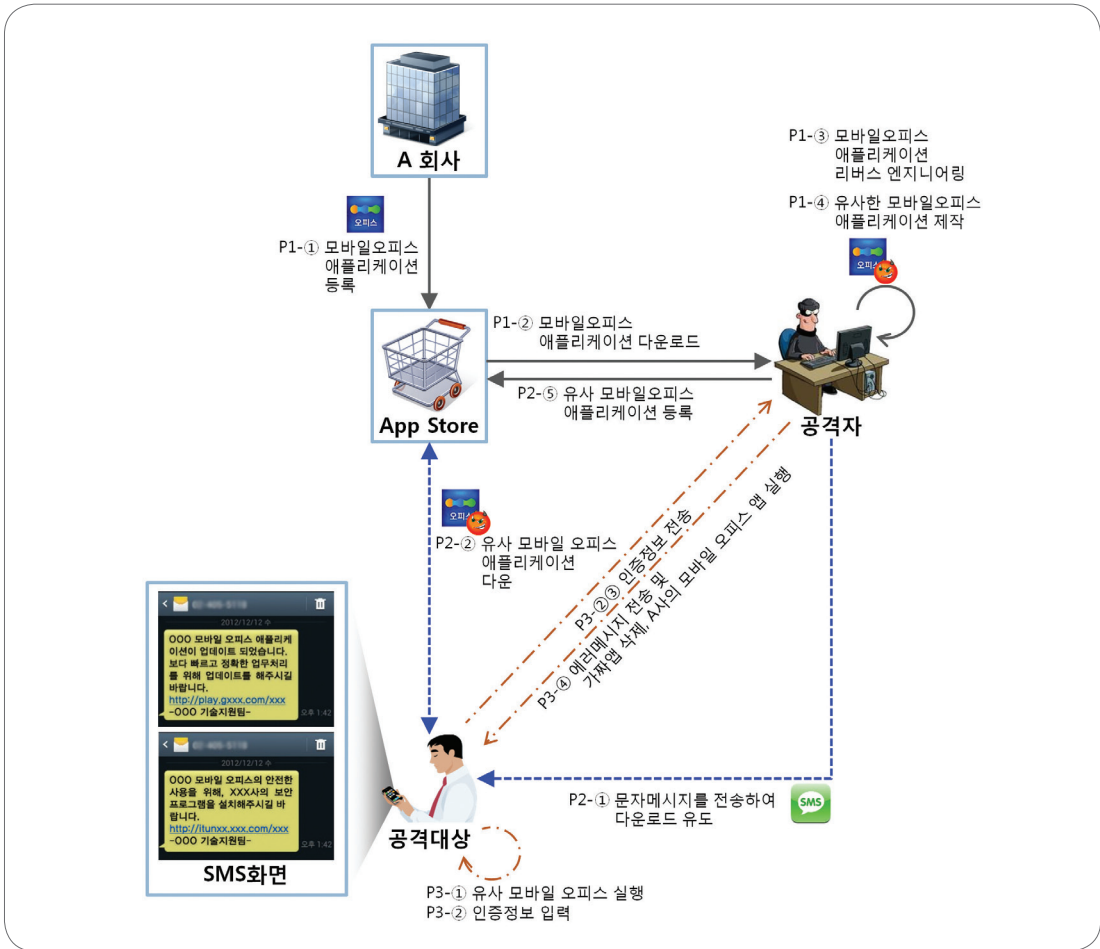
⑤ A씨가 접속한 무선 AP는 사내에서 설치한 무선랜과 동일한 네트워크 이름(SSID)을 가지고 있는 공격자의 가짜(Fake) AP로, A씨가 무선랜을 통해 전송하는 모든 업무정보를 도청 및 탈취한다.

※ 단말기에 저장되어 있던 정보 중 일부 업무정보는 애플리케이션을 통해 저장되지 않아 암호화가 되지 않은 상태이기 때문에, 공격자는 암호를 해독할 필요 없이 업무정보를 손쉽게 수집할 수 있다.

3. 스미싱을 통한 인증정보 탈취

피싱·파밍의 대표적인 공격으로 스미싱(Smishing)³⁾을 통한 악의적인 애플리케이션 설치 유도 및 정보 유출이 이루어질 수 있다.

3) 스미싱(Smishing) : 문자메시지(SMS)와 피싱(Phishing)의 합성어로, 문자메시지 내 인터넷주소를 클릭하면 악성코드가 설치되어 피해자가 모르는 사이에 소액결제 또는 개인·금융정보를 탈취하는 수법



【그림 2-3】 스미싱을 이용한 악의적인 애플리케이션 설치 유도

Phase 1

소스코드 분석(리버스 엔지니어링)을 통한 모바일 애플리케이션 취약점 도출

- ① A사는 자사의 모바일 오피스 애플리케이션을 공개된 앱 마켓에 등록하여 직원들이 다운받아 사용할 수 있도록 한다.
- ② 공격자는 앱 마켓에서 A사가 등록한 모바일 오피스 애플리케이션을 다운로드 받아 리버스 엔지니어링을 통해 애플리케이션의 API, 함수 등 동작원리, 인증방식 등 주요 기능을 분석한다.
- ③ 공격자는 리버스 엔지니어링을 통해 얻은 자료들을 기반으로 A사의 모바일 오피스 애플리케이션과 동일한 인터페이스를 가진 악의적인 가짜 애플리케이션을 제작한다.
- ④ 공격자는 자신이 제작한 A사의 가짜 모바일 오피스 애플리케이션을 앱 마켓에 등록한다.

Phase 2

스미싱을 통해 가짜 애플리케이션 설치 유도

- ① 공격자는 자신이 제작한 가짜 모바일 오피스 애플리케이션을 A사의 직원들이 다운받을 수 있도록 문자메시지를 전송한다.

※ 공격자는 사용자가 이미 모바일 오피스 애플리케이션을 설치하였을 경우를 고려하여, 애플리케이션 업데이트를 가장한 문자를 보낸다.

“OOO 모바일 오피스 애플리케이션이 업데이트 되었습니다. 보다 빠르고 정확한 업무처리를 위해 업데이트를 해주시길 바랍니다. <http://play.gxxx.com/xxx> – OOO 기술지원팀 –”

“OOO 모바일 오피스의 안전한 사용을 위해, XXX사의 보안 프로그램을 설치해주시길 바랍니다. <http://itunxx.xxx.com/xxx> – OOO 기술지원팀 –”

- ② 직원 B씨는 공격자가 보낸 문자의 URL을 통해 공격자가 제작한 가짜 모바일 오피스 애플리케이션을 다운로드하여 설치한다.

Phase 3

악성코드가 삽입된 애플리케이션을 통한 인증정보 탈취

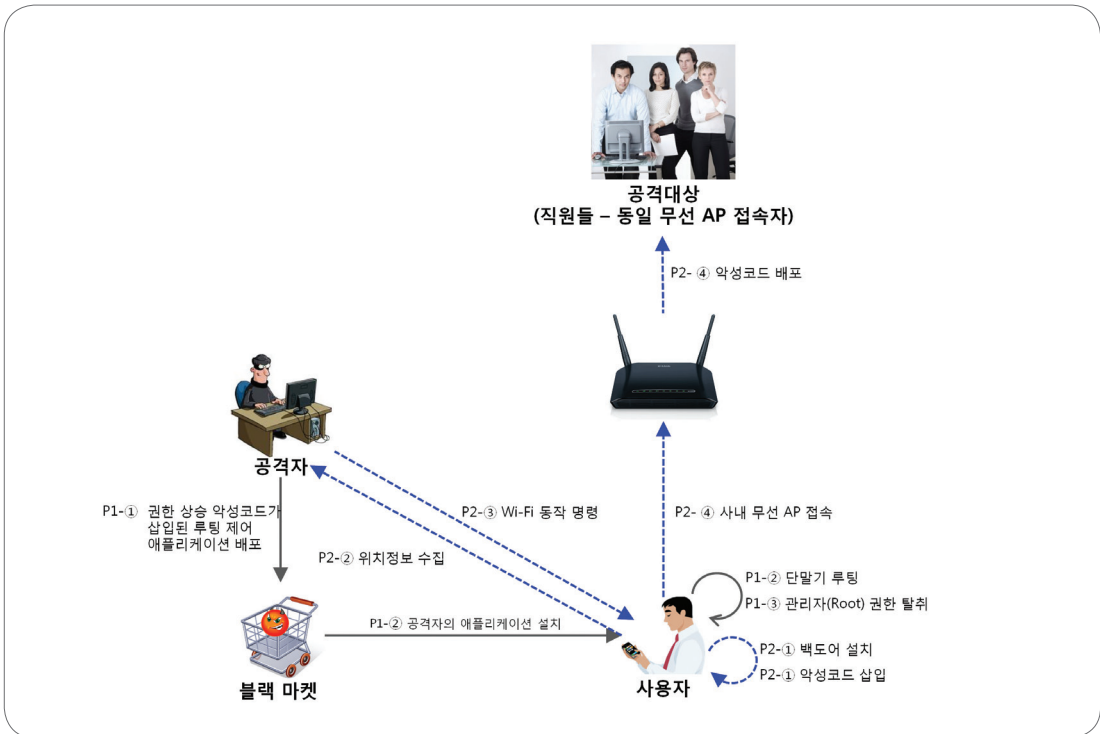
- ① 직원 B씨는 모바일 오피스로 업무를 수행하기 위해 설치한 가짜 모바일 오피스 애플리케이션을 실행한다.
- ② 직원 B씨는 모바일 오피스 사용자 인증을 위해 자신의 계정정보(ID/PW 등)를 입력한다.
- ③ 직원 B씨가 입력한 계정정보는 가짜 모바일 오피스 애플리케이션을 통해 공격자에게 전송된다.
 - ※ 가짜 안티바이러스 프로그램의 경우 백그라운드에서 동작하며, 사용자가 이를 인지할 수 없는 스파이웨어 형태로 제작된다. 직원 B가 실제 모바일 오피스 프로그램을 사용하면서 수행한 모든 업무정보는 백그라운드에서 동작하는 애플리케이션을 통해 공격자로 전송될 수 있다.
- ④ 공격자는 직원 B씨의 인증정보를 취득하고, 직원 B씨의 단말기 화면에 에러 메시지를 보여준 뒤, 정상적인 애플리케이션을 실행시켜 인증정보 취득 사실을 인지하지 못하게 한다.

※ 공격자는 사용자가 공격여부를 알지 못하도록 다음과 같이 할 수 있다.

- 에러 메시지 출력
- “설치가 잘못되었습니다. 재설치 해주세요.”라는 메시지를 출력하고, A사의 정상적인 모바일 오피스 애플리케이션을 설치할 수 있는 페이지로 이동
- 가짜 모바일 오피스 애플리케이션 삭제
- 가짜 모바일 오피스 애플리케이션 강제 종료 후, 실제 모바일 오피스 애플리케이션 실행

4. 권한 상승을 통한 악성코드 배포

공격자는 악성코드를 이용해 단말기의 관리자(Root) 권한을 획득할 수 있으며, 이를 통해 공격자는 단말기 내 모든 기능을 제어할 수 있다.



【그림 2-4】 권한 상승을 이용한 악성코드 배포

Phase 1

단말기 관리자(Root) 권한 탈취

① 공격자는 단말기 권한 상승 악성코드가 삽입된 루팅⁴⁾ 제어 애플리케이션을 배포한다.

※ 루팅 제어 애플리케이션(“테그라크 커널”, “SuperSu” 등)은 루팅된 단말기에서 루팅의 활성화와 비활성화를 제어할 수 있다.

② 사용자는 단말기를 루팅한 후, 공격자가 배포한 루팅 제어 애플리케이션을 다운받아 설치한다.

③ 루팅 제어 애플리케이션에 삽입된 권한 상승 악성코드가 실행되어, 사용자 단말기의 관리자(Root) 권한을 탈취한다.

4) 루팅(Rooting) : 안드로이드 운영체제를 탑재한 모바일기기에서 관리자 권한을 획득하는 것을 말한다(아이폰에서는 ‘탈옥’이라고 함).

Phase 2

탈취한 권한을 이용한 악성코드 배포

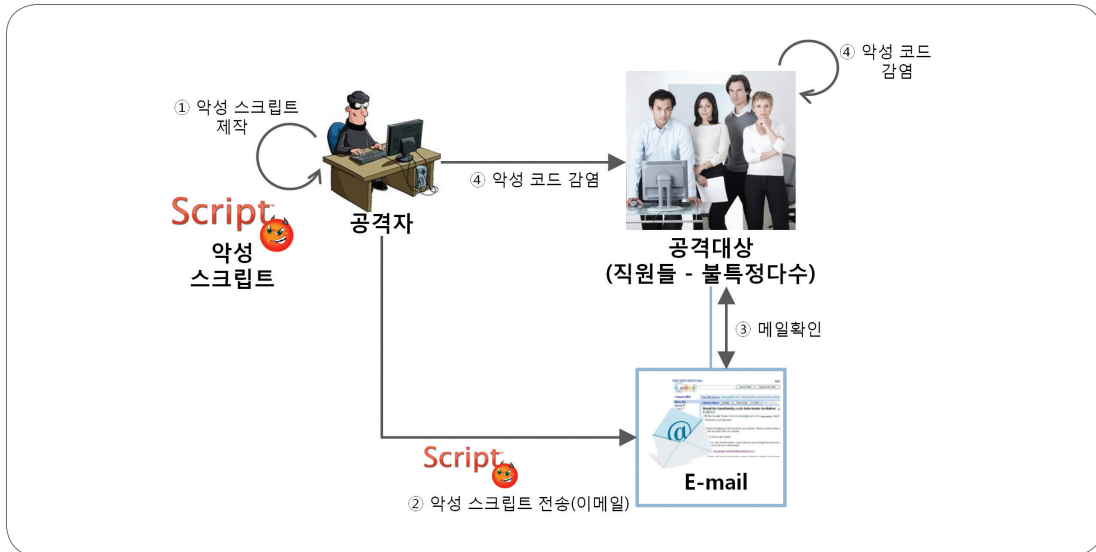
- ① 공격자가 관리자 권한으로 단말 내에 설치된 안티바이러스 소프트웨어를 무력화 시킨 후, 공격자의 명령제어 서버에 연결한다.
- ② 공격자는 사용자 단말에 악성코드를 삽입하며, 단말기의 위치정보를 지속적으로 수집한다.
- ③ 공격자는 수집한 위치정보를 통해 직원이 사내에 위치하였음을 인지한 후, 단말기의 무선랜 기능을 활성화 시켜 사내 무선 AP에 접속시킨다.
- ④ 공격자는 단말기 내에 저장된 악성코드를 사내 무선 AP에 접속한 모든 직원의 단말기로 전파시킨다.

※ 공격자는 SMS, 메신저, 이메일 등을 사용해 악성코드를 배포할 수도 있으며, 모든 송·수신 과정은 사용자가 인지할 수 없도록 제어 가능하다.

5. 사용자 부주의로 인한 악성코드 감염·해킹

모바일 오피스 애플리케이션의 약 75% 이상은 웹 애플리케이션 형태로 구현되어 있기 때문에⁵⁾ 스크립트 변조가 이루어질 수 있으며, 이를 통한 단말기 악성코드 감염 및 전파가 이루어질 수 있다.

가. 웹 애플리케이션 기반 악성코드 감염 공격



【그림 2-5】 웹 애플리케이션 기반에서 XSS 공격을 이용한 악성코드 감염

5) KISA, "모바일 오피스 보안 운영 현황 조사", 2013

① 공격자는 A사의 업무 관련 이슈를 소재로 한 게시물을 스크립트(Script)로 작성한 후, 이를 실행 시 악성코드가 단말기에 심어질 수 있도록 하였다.

※ 웹 또는 하이브리드 기반으로 제작된 모바일 오피스 애플리케이션은 게시판, 이메일, 전자결재 기능 등에서 스크립트를 작성하거나 실행할 수 있다.

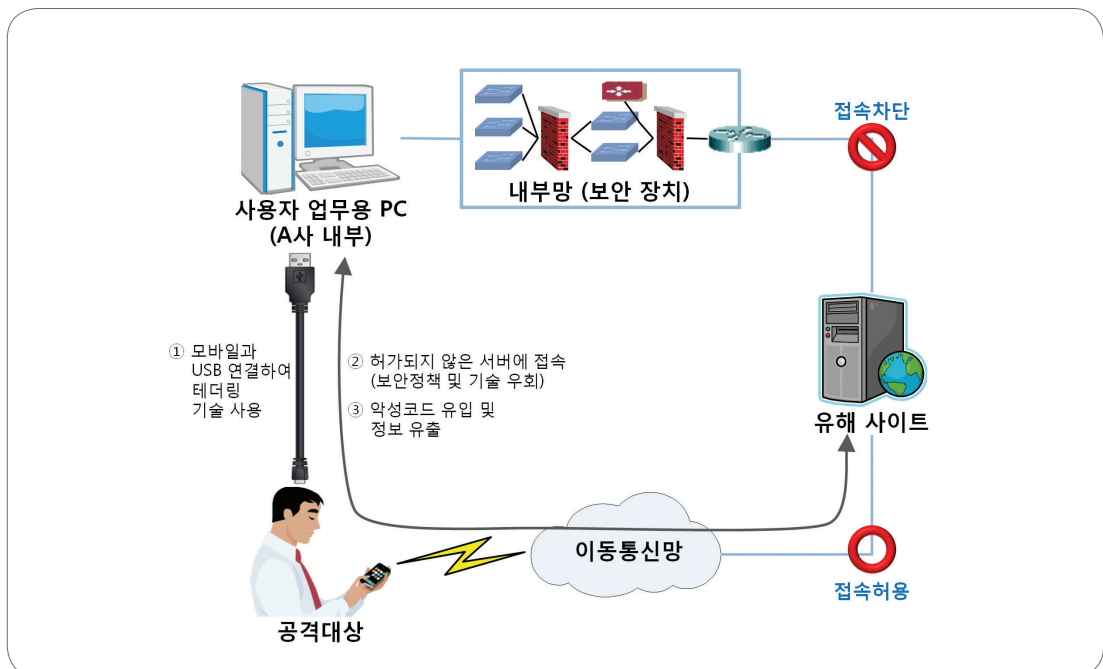
② 공격자는 A사 홈페이지에서 직원 이메일을 검색한 후, 이들에게 악의적인 스크립트가 포함된 메일을 전송한다.

※ 공격자는 내부직원 불특정 다수에게 이메일을 보내거나, 여러 명이 열람할 수 있는 게시판을 이용할 수도 있다.

③, ④ 이메일을 수신한 직원이 이를 확인하면 스크립트가 실행되며, 모바일 단말기는 악성코드에 감염된다.

나. 테더링 사용에 의한 업무용 PC 공격

A사의 내부 시스템은 방화벽, IPS 등의 물리적 보안 장치를 통해 외부로부터의 침입을 차단하고, 보안 정책을 통해 내부직원의 업무용 PC에서 허가받지 않은 서버(웹 하드, 유머 사이트, 상용 이메일 서버 등)로 접속하는 것을 차단한다.



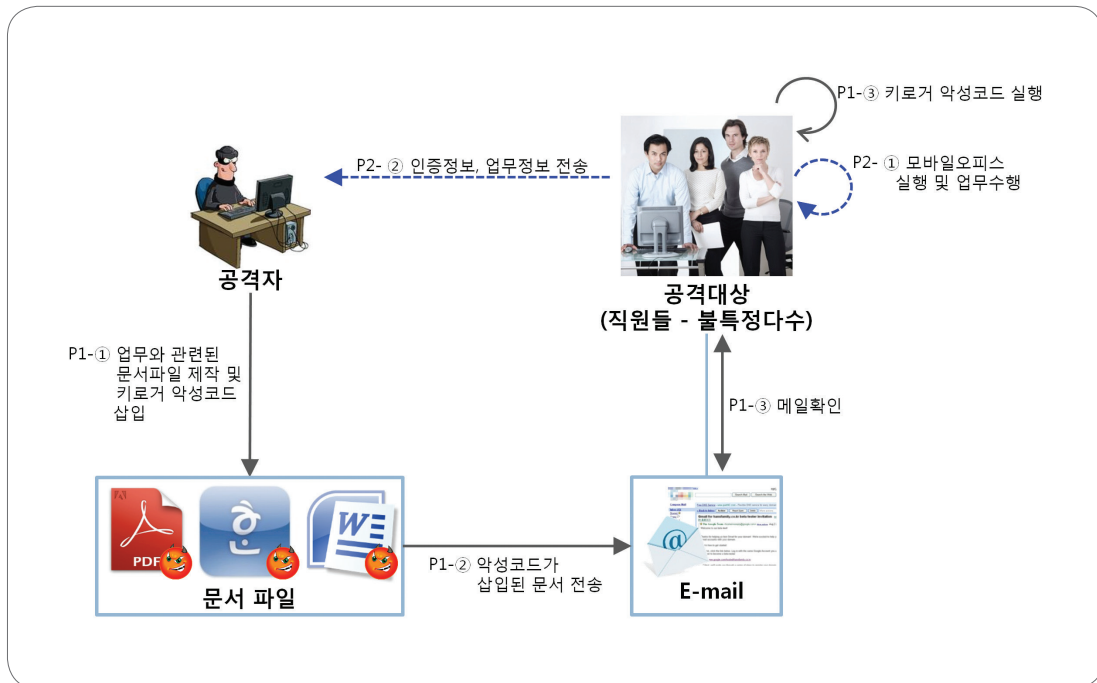
【그림 2-6】 테더링 사용에 의한 업무용 PC 공격

- ① A사의 내부직원 B씨는 업무용 PC를 통해 허가되지 않은 웹하드 사이트에 접속하기 위해, 단말기의 테더링 기능을 이용하여 무선 네트워크에 접속한다.
- ② 테더링으로 연결된 PC는 A사의 물리적 보안 장치나 보안 정책으로 통제되지 않은 네트워크 채널을 생성하게 되고 허가받지 않은 웹하드 사이트에 접속할 수 있게 된다.
- ③ B씨는 웹하드를 통해 악성코드가 삽입된 콘텐츠를 다운받아 업무용 PC에서 이를 설치 및 열람하여 사내망으로 악성코드가 유입된다.

6. 단말기 키로거 감염 또는 관리소홀로 인한 정보 유출

모바일 오피스 정보 유출 공격으로는 키로거(key logger)를 통한 입력정보 유출 또는 단말기 관리소홀로 인한 업무정보 유출이 이루어질 수 있다.

가. 키로거를 통한 업무정보 유출



【그림 2-7】 키로거를 통한 업무정보 유출

Phase 1

키로거 악성코드 삽입

- ① 공격자는 A사의 업무와 관련된 각종 문서 파일을 제작한 후 해당 파일에 키로거 악성코드를 삽입한다.
- ② 공격자는 A사에 근무하는 모든 직원에게 이메일에 악성코드가 삽입된 문서를 첨부하여 전송한다.
 - ※ 공격자는 사용자가 메일을 확인하도록 업무와 관련 있는 청구서, 결재문서, 참고자료 등으로 위장한 이메일을 전송한다.
- ③ 직원이 이메일을 확인하고, 첨부된 문서 파일을 실행하면 문서에 숨겨져 있던 키로거 악성코드가 실행된다.

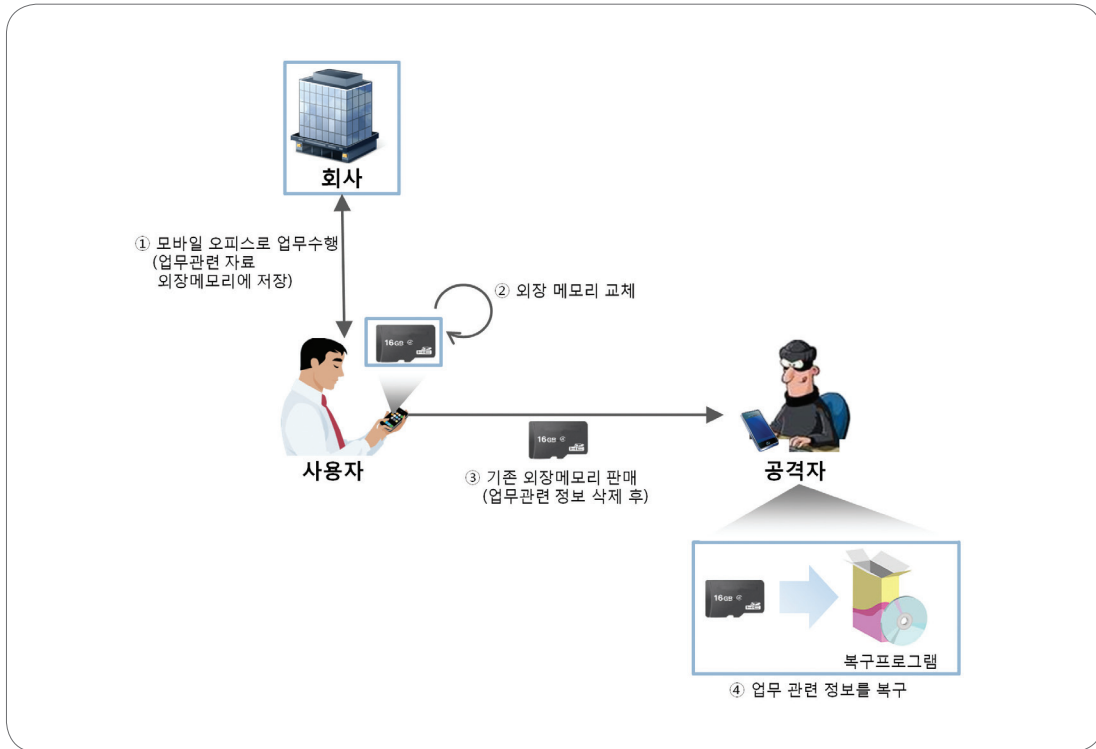
Phase 2

키로거를 통한 입력정보 탈취

- ① 직원은 단말기에 키로거 악성코드가 설치된 사실을 인지하지 못한 채, 모바일 오피스 애플리케이션을 통해 업무를 수행한다.
- ② 직원이 업무를 수행하면서 입력하는 모든 정보는 키로거를 통해서 공격자에게 전송된다.
 - ※ 직원이 모바일 오피스 애플리케이션에 접속하기 위해 입력하는 ID와 Password 등의 인증정보 뿐 아니라, 업무를 위한 금융거래정보, 기업의 회계정보, 고객정보 등 모바일 오피스를 이용하면서 사용자가 입력하는 모든 정보들이 유출될 수 있다.
 - ※ 가상키보드를 지원하는 경우에는 가상키보드 자판을 캡처한 이미지와 직원이 누른 위치(화면의 좌표값)를 전송받아, 두 개의 정보를 대조하여 직원이 입력한 정보를 획득할 수 있다.

나. 관리 소홀로 인한 업무정보 유출

- ① A씨는 모바일 오피스 애플리케이션을 이용해 업무를 수행할 때, 업무의 신속성과 편의를 위해 업무 관련정보를 단말기 내 외장 메모리에 저장한다.
 - ※ 단말기에 업무 관련정보를 저장하는 방법은 다음과 같다.
 - 파일 다운로드
 - 처리 화면을 캡처
 - 통화 내용 또는 회의 내용을 녹음
 - 메모 등의 기능을 사용
 - ※ 단말기에 저장되는 정보는 모바일 오피스 애플리케이션을 통해 저장될 경우 암호화가 되어 저장될 수 있으나, 일반적인 단말기의 메모 기능, 음성 녹음 기능, 화면 캡처 기능을 통해 저장된 정보나, 이메일로 다운로드 받은 파일의 경우 암호화가 이루어지지 않는다.



【그림 2-8】 관리 소홀로 인한 업무정보 유출

- ② A씨는 단말기의 메모리 공간 부족을 해결하기 위해, 기존 외장 메모리보다 저장 공간이 큰 신규 외장 메모리로 교체 한다.
 - ③ A씨는 기존 외장 메모리 내 저장된 업무 관련 정보를 삭제한 후, 타인에게 양도 및 판매한다.
 - ④ 외장 메모리를 양도 및 구입한 제 3자는 시중에 유통되는 메모리 복구 프로그램을 사용해, 외장 메모리에서 삭제된 업무 관련 정보를 복구할 수 있다.
- ※ 일반적인 외장 메모리 내 데이터 삭제 및 초기화 시 실제 데이터가 삭제되는 것이 아니라, 데이터가 저장된 주소값을 삭제하는 효과밖에 없기 때문에 이를 복구할 수 있다.

제 2 장 모바일 오피스 보호대책

제 1 절 보안 유형별 모바일 오피스 보호대책

본 장에서는 지금까지 살펴본 모바일 오피스 보안위협에 대한 대책들을 살펴본다. 모바일 오피스 보안대책은 크게 사용자 인증, 단말기 관리, 플랫폼 및 소프트웨어 보안, 콘텐츠 및 정보 자산 보안, 악성코드 및 해킹 대응, 통신망 보안, 보안 정책으로 분류할 수 있다.

● 사용자 인증

비인가 사용자의 모바일 오피스 서비스 이용 또는 비인가 단말기에서 서비스가 이용되는 보안위협을 막기 위한 대책이다.

● 단말기 관리

사용자가 단말기의 기능을 잘못 이용하거나, 관리 부주의로 인해 내부 자산이 유출 및 탈취될 수 있는 위협을 막기 위한 대책이다.

● 플랫폼 및 소프트웨어 보안

모바일 오피스 단말기의 플랫폼 및 소프트웨어에서 발생할 수 있는 보안위협에 대응하기 위한 대책이다.

● 콘텐츠 및 정보자산 보안

모바일 오피스 서비스에서 이용되는 내부 정보자산 및 콘텐츠의 기술적 · 관리적 문제로 인한 유출을 방지하기 위한 대책으로, 단말기 영역 및 내부시스템 영역에서의 보안대책으로 분류된다.

● 악성코드 및 해킹 대응

모바일 오피스 단말기에 악성코드가 설치되거나, 외부 공격자의 시스템 침입 및 유해 행위에 대응하기 위한 보안대책이다.

● 통신망 보안

모바일 오피스 데이터 전송 채널로 사용되는 무선랜, 이동통신망 등 통신망에서 발생할 수 있는 비인가자의 정보탈취 및 외부 유출 등의 보안위협으로부터 대응하기 위한 대책이다.

● 보안 정책

모바일 오피스 관리 부주의로 인한 보안위협이 발생하지 않도록 운영자가 수행해야 할 보안대책이다.

1. 기술적 보호대책

대분류	소분류	세부 내용	MME
단 말 기 보 안	사용자 인증 대책	- 단말기 구동 시 사용자 인증 수행	MME-101
		- 일정 시간 단말기 미사용 시 자동 잠금	MME-102
		- 일정횟수 이상 사용자 인증 오류 시 사용 차단	MME-103
		- 기기인증서 또는 단말기 고유정보를 이용한 단말기 인증	MME-104
	단말기 관리 대책	- 분실, 도난 단말기에 대한 원격 잠금 및 삭제 기능 제공	MME-201
		- 이동저장매체 사용 제한	MME-202
		- 테더링 사용 제한	MME-203
		- GPS, 카메라, 마이크 등 하드웨어 자원 접근통제	MME-204
	플랫폼 보안 대책	- 플랫폼 위·변조 방지를 위한 무결성 검증	MME-301
	콘텐츠 보안 대책	- 업무관련 파일에 DRM 등 저작권 보호 기술 적용	MME-401
		- 단말기 내 시스템 메모리 및 내장 메모리 데이터 암호화 저장	MME-402
		- 화면캡처 제한	MME-403
	악성코드 · 해킹 대응	- 안티바이러스 설치 및 백그라운드 동작	MME-501
		- 가상 키패드 보안 프로그램 사용	MME-502
		- 허가되지 않은 외부 서버 접속 차단	MME-503

대분류	소분류	세부 내용	MME
애플리케이션 보안	사용자 인증 대책	- 애플리케이션 구동 시 사용자 인증 수행	MME-601
		- 일정 시간 미사용 시 자동 접속 종료	MME-602
		- 일정횟수 이상 사용자 인증 오류 시 사용 차단	MME-603
		- ID/PW외 인증서, OTP 등을 이용한 복합인증	MME-604
	소프트웨어 보안	- 신뢰된 기관으로부터의 서명이 존재하지 않거나, 비인가된 S/W 설치 제한	MME-701
		- 소프트웨어 위 · 변조 방지를 위한 무결성 검증	MME-702
		- 비인가 네트워크를 통한 S/W 설치 및 업데이트 금지	MME-703
	악성코드 · 해킹 대응	- 시큐어코딩 적용	MME-801
네트워크 보안	통신망 보안 대책	- 불법 AP, 애드혹 연결차단 및 탐지	MME-901
		- 비인가 AP 접속 차단 및 탐지	MME-902
		- 블루투스 연결 시 사용자 인증 수행	MME-903
		- 비인가 장치와의 통신 제한	MME-904
	통신망 암호화 대책	- 안전한 암호화 통신채널(SSL/TLS, WPA2-PSK(AES) 등) 사용	MME-1001
		- mVPN을 이용한 인증 및 보안채널 사용	MME-1002
내부 시스템 보안	악성코드 · 해킹 대응	- 불필요한 서비스(포트) 차단	MME-1101
		- 허가되지 않은 스크립트 사용 제한	MME-1102
		- 방화벽, IPS 등 보안장비 구축 및 운영	MME-1103
		- 내부 시스템 및 애플리케이션에서의 로그 및 보안 이벤트 기록	MME-1104

대분류	소분류	세부 내용	MME
내부 시스템 보안	사용자 인증 대책	- 내부 시스템 접근 시 사용자 인증 수행	MME-1201
		- 일정 시간 미사용 시 자동 접속 해제	MME-1202
		- ID/PW외 인증서, OTP 등을 이용한 복합인증	MME-1203
	정보 자산 보안대책	- 내부시스템 저장 정보 암호화	MME-1301
		- 내부시스템 정보의 위·변조 방지를 위한 무결성 검증	MME-1302

※ MME : Mobile office Measures Enumeration

2. 관리적 보호대책

대분류	소분류	세부 내용	MME
단말기 보안	사용자 인증 대책	- 추측하기 어려운 패스워드 사용	MME-105
		- 주기적인 패스워드 변경	MME-106
	단말기 관리 대책	- 보안 담당자의 통제 하에 단말기 수리 및 교체	MME-205
	플랫폼·S/W 보안대책	- 업무용 소프트웨어 도입 전, 취약점 분석 및 보안조치 적용	MME-302
		- 주기적인 무결성 검증, 보안패치 및 업데이트 수행	MME-303
		- 업데이트 미수행 시 서비스 접속 제한	MME-304
	콘텐츠 보안	- 보안 필름 사용	MME-404
	악성코드 해킹 대응	- 주기적인 보안패치 및 업데이트 수행	MME-504
		- 주기적인 취약점 점검, 안티바이러스 점검 등 보안성 검증/보안 조치	MME-505
		- 업데이트 미수행 시 서비스 접속 제한	MME-506

대분류	소분류	세부 내용	MME
애플리케이션 보안	사용자 인증 대책	- 추측하기 어려운 패스워드 사용	MME-605
		- 주기적인 패스워드 변경	MME-606
	S/W 관리	- 공개 앱스토어를 통한 모바일 오피스 관련 S/W 배포금지	MME-704
		- 업무용 소프트웨어 도입 전, 취약점 분석 및 보안조치 수행	MME-705
		- 주기적인 무결성 검증, 보안패치 및 업데이트 수행	MME-706
		- 업데이트 미수행 시 서비스 접속 제한	MME-707
내부 시스템 보안	악성코드 · 해킹 대응	- 주기적인 보안패치 및 업데이트 수행	MME-1105
		- 주기적인 모의해킹, 취약점 점검 등 보안 검증/보안 조치 적용	MME-1106
		- 내부 시스템 및 애플리케이션 로그 및 보안 이벤트 분석	MME-1107
		- 24시간 보안관제	MME-1108
	사용자 인증 대책	- 추측하기 어려운 패스워드 사용	MME-1204
		- 주기적인 패스워드 변경	MME-1205
보안 정책	정책 수립 및 조직, 권한 정의	- 모바일 오피스 보안정책 수립 및 주기적 검토	MME-1401
		- 모바일 오피스 보안 담당자 지정 및 수행역할 정의	MME-1402
		- 모바일 오피스의 주요기능과 정보자산 접근 권한체계 정의 및 적용	MME-1403
	감사 및 모니터링	- 보안정책의 실효성에 대한 주기적 검토 및 모니터링 수행	MME-1404
		- 보안정책 및 체계에 대한 주기적인 내부감사를 수행하고 결과를 반영	MME-1405
	사고 대응	- 모바일 오피스 침해사고 대응 매뉴얼 개발	MME-1406
	보안 교육	- 모바일 오피스 이용자 대상의 정기교육, 훈련계획 수립 및 이행	MME-1407

제 2 절 정보 유형별 모바일 오피스 보호대책

정보 유형에 따른 모바일 오피스 보호대책은 구축, 개발 단계에서 고려되어야 하며, 이는 모바일 오피스에 이용되는 중요정보(사용자 인증, 개인정보, 업무정보, 금융정보 등)를 보호하기 위함이다.

1. 인증정보 보호대책

인증정보는 모바일 오피스 이용 시 적합한 사용자 또는 단말기인지 여부를 식별 및 인증하기 위해 사용되는 정보로 각 유형별 세부 보호대책은 다음과 같다.

가. 접근 통제 및 서비스 제한

- 단말/사용자에 대한 식별 · 인증정보를 이용해 모바일 오피스 기능별 사용 권한, 정보 열람 권한 부여 등 접근 통제를 적용해야 한다.
- 단말/사용자에 대한 식별 · 인증정보의 등록은 오프라인에서 이루어져야하며, 모바일 오피스 애플리케이션 상에서 변경이 불가능해야 한다.

나. 인증정보 구성

- 아이디는 영문 대 · 소문자, 숫자 등의 문자열을 조합하여 만들어야 하며, 이름, 직원번호, 이메일 주소 등 공격자가 유추하기 쉬운 단어를 사용하지 않아야 한다.
- 패스워드는 영문 대 · 소문자, 숫자, 특수문자 등의 문자열을 조합하여 사용해야 하며, 주민등록 번호 뒷자리, 직원번호 등 공격자가 쉽게 유추할 수 있는 단어는 사용하지 않아야 한다.

다. 인증정보 입력 및 관리

- 키로거, 입력 상태창 훑쳐보기, 단말기 자판 훑쳐보기 등을 통해 인증정보가 유출되지 않도록 가상키보드, 화면캡처 제한, 단말기 자판 임의(random)배열 등과 같은 입력방식 보호기술을 적용하는 것이 안전하다.
- 인증정보는 단말기에 저장하지 않아야 하며, 평문으로 전송하지 않아야 한다.
- 쿠키(cookie)정보로 인증정보를 대체하여 사용할 경우 평문으로 저장하지 않아야 하며, 모바일 애플리케이션 종료 또는 일정시간이 지난 후 삭제되어야 한다.
- 인증정보 분실로 인한 임시 아이디 또는 패스워드를 제공하는 경우, 이메일 또는 SMS 등을 이용하여 제공하는 것이 안전하다.

2. 개인정보 보호대책

개인정보는 성명, 주민등록번호, 전화번호 등 특정 개인을 식별할 수 있는 정보를 의미하며, 모바일 오피스 환경에서 개인정보의 불법 수집·관리가 이루어지지 않도록 다음과 같은 보호조치가 적용되어야 한다.

- 모바일 오피스 애플리케이션 개발 시 단말기에 저장된 연락처, 사진, 위치정보 등의 개인정보를 사용자 동의 없이 변경 또는 삭제되지 않도록 해야 한다.
- 모바일 오피스 애플리케이션을 통한 개인정보 수집 시 사용자의 동의를 얻어야 하며, 수집한 개인정보를 단말기 내에 저장하거나 내부 시스템으로 전송 시 암호화가 이루어져야 한다.
- 모바일 오피스 애플리케이션을 통해 개인정보를 취급 시 사용자가 동의한 목적 내에서만 취급되어야 한다.

3. 업무정보 보호대책

업무정보는 이메일, 결재정보, 메신저 내용, 문서 파일 등의 업무 수행 시 이용되는 모든 정보를 통칭하며, 업무정보가 외부에 유출되지 않도록 다음과 같은 보호대책들이 마련되어야 한다.

- 업무정보는 단말기에 저장되지 않고 뷰(View) 기능을 통해서만 열람되는 것이 안전하다.
- 업무정보를 단말기에 저장해야 할 시 암호화 등의 보호조치가 이루어 져야 하며, 비인가된 기기에서 정보를 열람할 수 없도록 DRM 등과 같은 암호화 및 접근통제 기술이 적용되는 것이 안전하다.
- 업무정보가 모바일 애플리케이션과 내부 시스템 간에 전송될 경우, 암호화하여 전송하는 것이 안전하다.
- 업무정보의 취급은 모바일 애플리케이션을 통해서만 이루어져야 하며, 일반 이메일 애플리케이션, 정보공유 애플리케이션, 업무용 Office 애플리케이션 등을 통해 취급되지 않아야 한다.
- 모바일 애플리케이션에서 업무정보 취급 시 내부시스템과 동일하게 서비스 이용, 정보 접근·처리 등과 관련한 로그를 기록 및 보관하여 업무정보 이력관리를 수행해야 한다.

4. 금융정보 보호대책

금융정보는 모바일 오피스를 활용한 전자상거래 시 취급되는 정보로, 이에 대한 보호대책은 다음과 같다.

- 금융정보는 단말기에 저장되지 않아야 한다.
- 금융정보가 모바일 애플리케이션과 내부 시스템 간 전송될 경우, 암호화하여 전송해야 한다.

제 3 절 모바일 오피스 보안 점검항목

지금까지 살펴본 모바일 오피스 보호대책을 기반으로, 다음과 같은 보안점검 항목들의 검토를 통해 안전한 모바일 오피스 구축 및 운영이 가능할 것이다.

1. 운영자를 위한 보안 점검항목

대분류	소분류	세부 내용	Yes	No
단 말 기 보 안	사용자 인증 대책	- 일정횟수 이상 인증 오류 시 사용 차단을 하고 있습니까?		
		- 사용자의 단말기 인증을 하고 있습니까? ※ 단말기인증 : 기기인증서, 단말기고유정보 등		
		- 사용자가 주기적으로 패스워드를 변경할 수 있도록 하고 있습니까?		
	단말기 관리 대책	- 단말기 분실, 도난에 대처할 수 있는 보안 기술을 제공하고 있습니까? ※ 원격 잠금 및 원격 데이터 삭제 등		
		- 단말기를 이동저장매체로 사용하지 못하도록 하고 있습니까?		
		- 단말기의 테더링 기능을 사용하지 못하도록 하고 있습니까?		
		- 단말기의 하드웨어 자원에 대한 통제를 하고 있습니까? ※ GPS, 카메라, 마이크 등		
		- 사용자의 단말기 수리 및 교체 시 정보유출을 방지 할 수 있도록 관리하고 있습니까?		
	플랫폼 · S/W 보안 대책	- 사용자 단말기의 플랫폼이 위·변조 되었는지 검증하고 있습니까? ※ 루팅, 탈옥 등		
		- 업무용 소프트웨어 도입 전, 취약점 분석 및 보안조치 수행하고 있습니까?		
		- 주기적으로 플랫폼 및 SW의 무결성 검증 및 보안패치, 업데이트를 수행하고 있습니까?		
		- 플랫폼 및 SW가 보안패치 및 업데이트 미수행 시 서비스 접속 제한하고 있습니까?		
	콘텐츠 보안 대책	- 업무 문서를 보호하기 위한 기술을 적용하고 있습니까? ※ DRM, Forensic Marking, Water Marking, Digital Finger Print 등		
		- 단말기 내 데이터를 암호화하여 저장하고 있습니까?		
		- 단말기의 화면캡처 기능을 사용하지 못하도록 하고 있습니까?		

대분류	소분류	세부 내용	Yes	No
단말기 보안	악성코드 · 해킹 대응	- 안티바이러스가 백그라운드에서 동작하도록 제공하고 있습니까?		
		- 가상 키패드 보안 프로그램 사용하고 있습니까?		
		- 허가되지 않은 외부 서버 접속을 차단하고 있습니까?		
		- 바이러스 검사 후 서비스를 이용할 수 있도록 하고 있습니까?		
		- 안티바이러스 프로그램이 최신 버전이 아닐 경우 서비스 접속을 제한하고 있습니까?		
애플리케이션 보안	사용자 인증 대책	- 애플리케이션 구동 시 사용자 인증을 수행하고 있습니까? ※ ID/Password, OTP, 보안카드, 인증서 등		
		- 애플리케이션을 일정 시간 미사용 시 접속이 종료되도록 하고 있습니까?		
		- 일정횟수 이상 인증 오류 시 사용 차단하고 있습니까?		
		- 사용자 인증을 ID/Password 이외에 다른 인증서, OTP 등을 이용한 복합인증이 이루어지고 있습니까?		
		- 사용자의 Password를 영문, 숫자, 특수문자를 조합하여 사용하도록 하고 있습니까?		
		- 사용자의 Password를 주기적으로 변경하도록 하고 있습니까? ※ 사용자 교육, 강제 변경 기술		
	S/W 관리	- 신뢰할 수 없는 S/W의 설치를 제한하고 있습니까? ※ 신뢰된 기관으로부터의 서명이 존재하지 않은 SW, 허가받지 않은 S/W, 블랙마켓의 SW 등		
		- 주기적으로 S/W의 위·변조 여부를 검사하고 있습니까? ※ S/W 무결성 검증		
		- 신뢰되지 않은 네트워크를 통한 S/W 설치 및 업데이트를 금지하고 있습니까?		
		- 모바일 오피스 서비스 관련 S/W를 기업용 앱 스토어를 통하여 배포하고 있습니까?(공개용 앱 스토어를 통한 배포 금지)		
		- S/W 및 패치파일을 도입 전 취약점 분석 및 보안 조치를 수행하고 있습니까? ※ 시큐어코딩, 취약점 점검 등		
		- S/W가 최신 버전이 아닐 경우 서비스 접속을 제한하고 있습니까?		
	악성코드 해킹 대응	- 시큐어코딩을 적용하고 있습니까?		

대분류	소분류	세부 내용	Yes	No
네트워크 보안	통신망 연결 대책	- 신뢰되지 않은 네트워크의 접속을 차단하고 있습니까? ※ 불법 AP, 애드혹 연결차단 및 탐지		
		- 블루투스 연결 시 사용자 인증을 수행하고 있습니까?		
		- 비인가 장치와의 통신을 제한하고 있습니까?		
	통신망 암호화 대책	- 안전한 암호화 통신채널을 사용하고 있습니까? ※ SSL/TLS, WPA2-PSK(AES) 등		
		- mVPN을 이용한 인증 및 보안채널 사용하고 있습니까?		
내부 시스템 보안	악성 코드 · 해킹 대응	- 불필요한 서비스(포트) 차단하고 있습니까?		
		- 허가되지 않은 스크립트 사용을 제한하고 있습니까?		
		- 보안장비 구축 및 운영하고 있습니까? ※ 방화벽, IPS 등		
		- 내부 시스템 및 애플리케이션을 이용한 작업내역 로그 및 보안이벤트 기록 및 분석하고 있습니까?		
		- 서버 시스템 및 서버 보안프로그램들의 주기적인 보안패치 및 업데이트를 수행하고 있습니까?		
		- 주기적인 모의해킹, 취약점 점검 등 보안 검증/보안 조치 후 서비스 실시하고 있습니까?		
		- 24시간 보안관제를 수행하고 있습니까?		
	사용자 인증 대책	- 내부 시스템 접근 시 인증을 수행하고 있습니까?		
		- 일정 시간 미사용 시 내부 시스템 접속을 종료하고 있습니까?		
		- ID/Password 이 외 인증서, OTP 등을 이용한 복합 인증을 사용하고 있습니까?		
		- 사용자의 Password를 영문, 숫자, 특수문자를 조합하여 사용하도록 하고 있습니까?		
		- 주기적으로 패스워드를 변경하고 있습니까?		
	정보 자산 보안대책	- 정보 자산에 암호화 적용하고 있습니까?		
		- 정보 자산 무결성 검증을 통한 위 · 변조 방지기술을 적용하고 있습니까?		

대분류	소분류	세부 내용	Yes	No
보안 정책	정책 수립 및 조직, 권한 정의	- 모바일 애플리케이션 서비스 이용에 따른 정보보안 정책 수립하고, 주기적으로 검토하고 있습니까?		
		- 모바일 애플리케이션 서비스 정보보안 담당자를 지정하고, 임무 및 역할을 정의하고 있습니까?		
		- 모바일 애플리케이션 서비스 기능과 정보자산에 대한 접근 권한체계를 정의하고 적용하고 있습니까?		
	감사 및 모니터링	- 주기적인 보안 정책의 효율성 검토 및 모니터링을 수행하고 있습니까?		
		- 보안정책 및 체계에 대한 주기적인 내부감사를 수행하고 결과를 반영하고 있습니까?		
	사고 대응	- 모바일 애플리케이션 침해위협에 대한 대응 매뉴얼 개발하여 수행하고 있습니까?		
	보안 교육	- 모바일 애플리케이션 사용자를 대상으로 정기적인 교육과 훈련계획 수립하고, 이행하고 있습니까?		

2. 사용자를 위한 보안 점검항목

대분류	세부 내용	Yes	No
단말기 사용	- 단말기 구동 시 사용자 인증을 수행하고 있습니까? ※ Password, 패턴 잠금 등		
	- 단말기를 일정 시간 미사용 시 자동 잠금 또는 재인증을 하고 있습니까?		
	- 단말기에서 일정횟수 이상 인증 오류 시 단말기 사용을 차단하고 있습니까?		
	- 신뢰되지 않은 S/W를 다운로드 하지 않았습니까?		
	- 신뢰하지 않은 사이트나, URL에 접속하지 않았습니까?		
	- 플랫폼을 위·변조 하지 않았습니까?		
	- 단말기를 이동저장매체로 사용하지 않았습니까?		
	- 주기적으로 안티 바이러스 프로그램을 사용하여 검사하고 있습니까?		
	- 보안 필름을 사용하고 있습니까?		
	- 주기적으로 플랫폼과, 안티바이러스, 모바일 오피스 관련 S/W를 업데이트 하고 있습니까?		
애플리 케이션 사용	- 안전한 경로를 통해 모바일 오피스와 관련된 S/W를 다운로드 받았습니까?		
	- 모바일 오피스의 인증 Password를 영문, 숫자, 특수문자를 혼합하여 사용하고 있습니까?		
	- 모바일 오피스의 인증 Password를 주기적으로 변경하고 있습니까?		
	- 업무 내용에 관련된 파일을 단말기에 저장해 두고 있지 않습니까? ※ 문서, 녹음, 화면캡처 이미지 등		
네트워크 사용	- 신뢰되지 않은 네트워크를 이용하지 않습니까?		
	- Wi-Fi, 블루투스를 사용할 때에만 기능을 켜놓고 있습니까? (항상 On 상태를 유지하지 않음)		
	- 단말기의 테더링 기능을 사용하지 않습니까?		



결론

모바일 오피스 정보보호 안내서

모바일 오피스는 단말기, 애플리케이션, 네트워크, 내부 시스템으로 분류할 수 있으며, 각 구성요소의 취약점으로 인해 개인정보침해, 정보유출, 악성코드 등의 보안위협이 나타날 수 있다.

본 안내서에서는 모바일 오피스 환경에서 발생할 수 있는 보안위협들을 도출하여 이를 이해하기 쉽도록 시나리오 형태로 구성하고, 이에 대한 보안대책을 제시하고 있다.

모바일 오피스 보안대책은 기술적·관리적 측면에서 각 구성요소 뿐 아니라 모바일 오피스가 취급하는 정보 유형별로 설명하고 있으며, 이에 대한 보안 점검항목을 마련하여 모바일 오피스 정보보호 수준을 손쉽게 점검하고 보안대책을 마련할 수 있도록 하였다.

본 안내서는 기업을 위한 첫 번째 모바일 오피스 정보보호 안내서로, 운영자 및 사용자가 본 안내서를 통해 모바일 오피스의 안전한 구축 및 운영에 대한 정보를 습득함으로써, 국내 모바일 오피스 정보보호 수준이 향상될 것으로 기대한다.



용 어 정 리

▶ BYOD (Bring Your Own Device)	- 개인 소유의 노트북이나 스마트폰 같은 정보 단말기를 업무에 활용하는 것을 뜻하는 용어
▶ MME	- Mobile office security Measures Enumeration - 모바일 오피스 보안대책 목록
▶ MTE	- Mobile office security Threats Enumeration - 모바일 오피스 보안 위협 목록
▶ 모바일 인터넷 전화 (mVoIP)	- mobile Voice over Internet Protocol - 이통통신망, Wi-Fi 등 무선망을 통해 음성 및 영상 통화 서비스를 제공하는 것
▶ 가짜(Fake) AP	- 공격자가 설치한 무선 AP로써, 이용자는 공격자가 설치한 AP인지 확인할 수 없음
▶ 리버스 엔지니어링 (Reverse Engineering)	- 이미 만들어진 시스템을 역으로 추적하여 처음의 문서, 파일 구조 등의 자료를 얻어 내는 행위
▶ 보이스 피싱	- 전화를 통하여 신용카드 번호 등의 개인정보를 알아낸 뒤 이를 범죄에 이용하는 전화금융사기 수법
▶ 서비스 거부 (DoS/DDoS)	- "Denial of Service/Distributed Denial of Service"의 약어로, 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격
▶ 세션(Session)	- 두 대의 기기 간 통신을 위한 논리적 연결을 의미

용 어 정 리

▶ 스마트워크 (Smart Work)	<ul style="list-style-type: none"> - 시간과 장소에 얽매이지 않고 언제 어디서나(Anytime, Anywhere) 편리하고 효율적으로 일을 할 수 있는 미래 지향적인 업무 환경 - 재택근무, 모바일 근무, 스마트워크 센터 등
▶ 스택 영역 (Stack Area)	<ul style="list-style-type: none"> - 프로그램의 함수 호출시 생성되는 지역변수와 매개변수가 저장되는 영역
▶ 악성코드 (Malicious Code)	<ul style="list-style-type: none"> - 맬웨어, 악성 프로그램 이라고도 함 - 악의적인 목적을 위해 작성된 실행 가능한 코드의 통칭으로 자기 복제 능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이 목마 등으로 분류
▶ 쿠키(Cookie)	<ul style="list-style-type: none"> - 인터넷 사용자가 어떠한 사이트를 방문할 경우, 그 사이트가 사용하고 있는 서버에서 인터넷 사용자의 컴퓨터에 설치하는 작은 기록 정보 파일
▶ 파밍(Pharming)	<ul style="list-style-type: none"> - 새로운 피싱 기법 - 사용자가 정확한 웹 페이지 주소를 입력해도 가짜 웹 페이지에 접속하게 하여 인증정보, 신용카드 정보, 개인정보 등을 탈취하는 공격
▶ 패킷(packet)	<ul style="list-style-type: none"> - 데이터가 네트워크를 통해 전송하기 쉽도록 분할한 데이터의 전송 단위
▶ 피싱(Phishing)	<ul style="list-style-type: none"> - 이메일, 메신저 등을 사용해서 신뢰 할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 공격 - 인증정보 및 신용카드 정보, 개인정보 등 기밀을 요하는 정보를 탈취하거나, 악성코드를 설치하도록 함
▶ 힙 영역 (Heap Area)	<ul style="list-style-type: none"> - 프로그래머의 필요에 의해서 메모리 공간이 할당 및 소멸되는 메모리영역

참 고 문 헌

- [1] 방송통신위원회, 한국인터넷진흥원, “안전한 모바일 오피스 도입과 운영을 위한 정보보호 수칙”, 2012.
- [2] 방송통신위원회, “스마트워크 활성화 추진계획”, 2011.
- [3] 한국인터넷진흥원, “모바일 오피스 보안이슈”, Internet & Security Focus, 2013.
- [4] 한국인터넷진흥원, “모바일 오피스 보안 운영 현황조사 결과 보고서”, 2013.
- [5] 한국인터넷진흥원, “모바일 클라우드 서비스 보안 침해 대응 방안”, 2010.
- [6] 한국인터넷진흥원, “신규 IT 서비스 보안위협 분석 및 대응방안 연구”, 2012.
- [7] 한국인터넷진흥원, “안전한 스마트 오피스 구축, 운영을 위한 보안대책”, 2010.
- [8] 행정안전부, “모바일 전자정부 서비스 보안 가이드라인”, 2011.

부 록

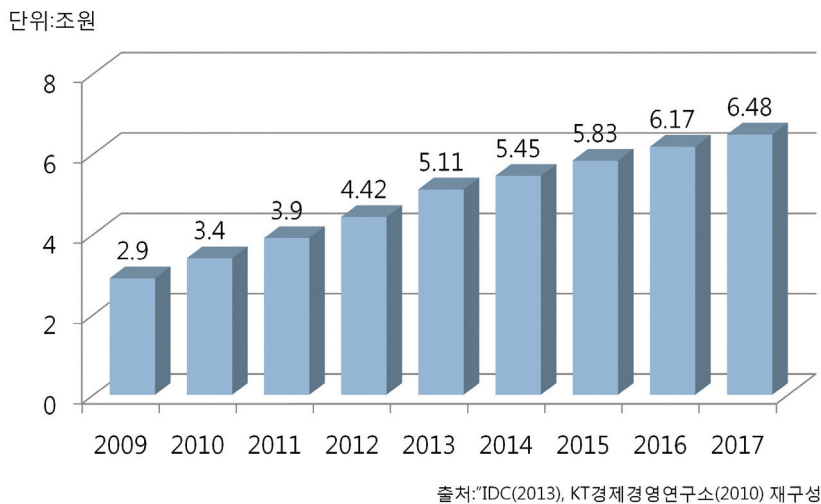
제 1 장 모바일 오피스 현황 및 분류	46
제 1 절 모바일 오피스 시장 및 서비스 현황	46
제 2 절 모바일 오피스 유형 분류	50
제 2 장 보안위협 및 보안대책 매칭표	53

제 1 장 모바일 오피스 현황 및 분류

제 1 절 모바일 오피스 시장 및 서비스 현황

국내 스마트폰 가입자가 약 3,500만명(2012.12 기준)을 넘어가면서, 스마트폰 기반의 모바일 오피스 시장이 본격적으로 활성화되고 있다. 모바일 오피스 시장은 2010년 행정용 모바일 오피스의 도입으로 형성되기 시작하였으며, 미래창조과학부(구 방송통신위원회)는 2015년까지 국내 30% 이상 근로자의 모바일 오피스 사용을 목표로 하는 “스마트워크 활성화 추진계획(2010)”을 세우는 등 모바일 오피스 시장은 지속적으로 성장할 것으로 기대되고 있다.

이러한 기대감에 힘입어 2012년 국내 기업 모바일 시장 약 6조 1천억원 중 모바일 오피스가 차지하는 비중은 70%이상으로 약 4조 4,200억원 규모를 나타냈으며⁶⁾ 2014년 약 5조 4,500억원에서, 2017년까지 약 6조 4,800억원 규모로 성장할 것으로 예상되고 있다.⁷⁾

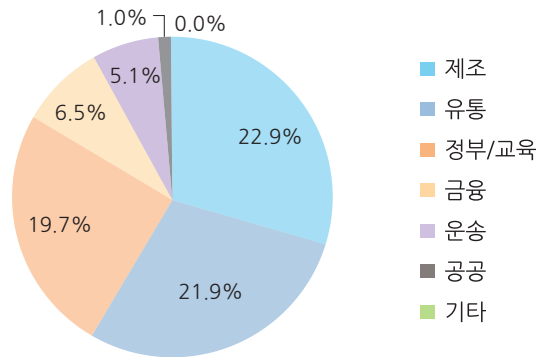


【그림 1-1】 국내 모바일 오피스 시장 전망

6) IDC(International Data Corporation), “국내 엔터프라이즈 모빌리티 시장 전망”, 2013.

7) KT경제경영연구소, “모바일 오피스 시장 동향 및 기업고객 Needs 조사”, 2010.

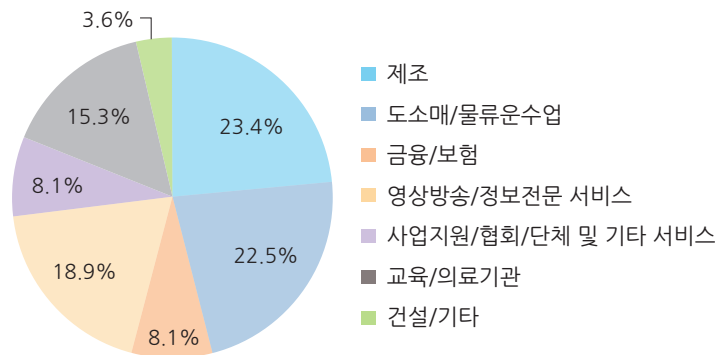
모바일 오피스 서비스는 제조, 금융, 유통, 교육 등 다양한 분야 및 업종에서 도입하여 운영되고 있다. 업종에 따라 전 세계 모바일 오피스 도입·운영 기업들을 분류하면 ‘제조업(22.9%)’이 가장 많았으며, 그 뒤로 ‘유통업(21.9%)’, ‘정부/교육(19.7%)’, ‘금융업(6.5%)’, ‘운송업(5.1%)’ 순으로 나타났다.⁸⁾



출처 : Ovum, 2009.6, IDC, 2010.8

【그림 1-2】 업종별 세계 모바일 오피스 서비스 현황

국내의 경우, 세계시장과 유사하게 ‘제조업(23.4%)’이 가장 큰 비중을 차지하고 있고, 그 뒤로 ‘도소매/물류업(22.5%)’, ‘영상방송/정보전문(18.9%)’, ‘교육/의료(15.3%)’, ‘금융/보험’과 ‘사업지원/협회/단체 및 기타 서비스’가 각각 8.1%를 차지하는 것으로 나타났다.⁹⁾



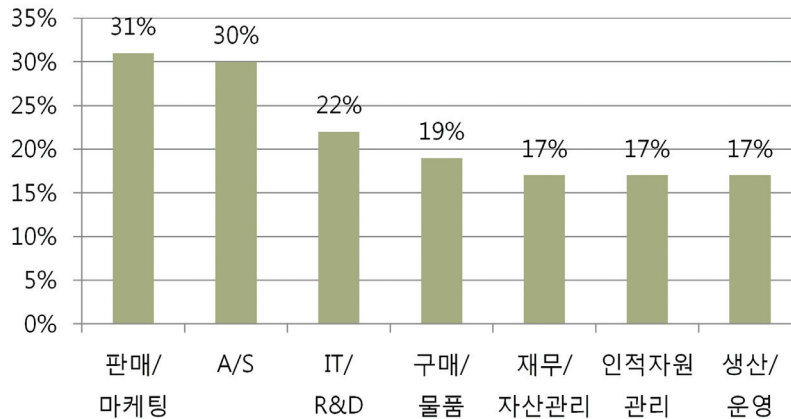
출처 : KISA, “모바일 오피스 보안 운영 현황 조사”, 2013

【그림 1-3】 업종별 국내 모바일 오피스 서비스 현황

8) KT경제경영연구소, “모바일 오피스 시장 동향 및 기업고객 Needs 조사”, 2010.

9) KISA, “모바일 오피스 보안 운영 현황 조사”, 2013.

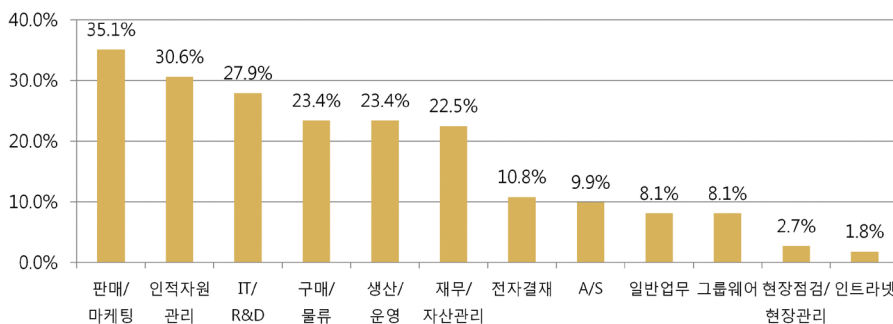
또한, 전세계 기업들의 업무 유형에 따른 모바일 오피스 이용현황을 살펴보면, ‘판매/마케팅(31%)’, ‘A/S(30%)’, ‘IT/R&D(22%)’, ‘구매/물품(19%)’, ‘재무/자산관리(17%)’ 순으로 나타나고 있다.



출처 : Ovum, 2009.6, IDC, 2010.8

【그림 1-4】 업무별 세계 모바일 오피스 서비스 현황

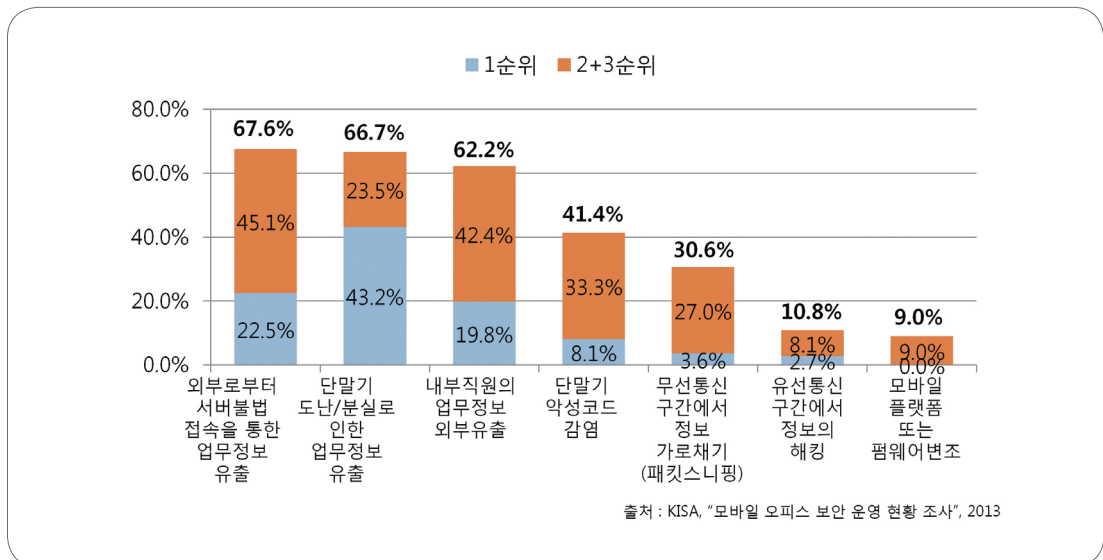
국내의 경우, ‘판매/마케팅(35.1%)’, ‘인적자원 관리(30.6%)’, ‘IT/R&D(27.9%)’, ‘구매/물품(23.4%)’과 ‘생산/운영(23.4%)’, ‘재무/자산(22.5%)’ 순으로 나타나고 있다.



출처 : KISA, “모바일 오피스 보안 운영 현황 조사”, 2013

【그림 1-5】 업무별 국내 모바일 오피스 서비스 현황

이렇듯 모바일 오피스가 널리 사용될 것으로 예상되는 가운데, 최근 스마트폰의 해킹이나 악성코드가 증가하고 분실/도난 등에 대한 문제들이 제기되면서, 모바일 오피스 보안 문제에 대한 우려도 점차 커지고 있다. 국내 모바일 오피스를 도입한 회사를 대상으로 모바일 오피스를 도입 및 운영함에 있어 침해가 예상되는 보안위협에 대해 조사한 결과, 대다수의 기업에서 ‘외부로부터의 서버 불법 접속을 통한 업무 유출(67.6%)’, ‘단말기 도난/분실로 인한 업무정보 유출(66.7%)’, ‘내부직원의 업무정보 외부 유출(62.2%)’을 우려하고 있는 것으로 나타났다. 이외에도 ‘단말기 악성코드 감염(41.4%)’, ‘무선통신 구간에서 정보 가로채기(패킷 스니핑)(30.6%)’ 등 다양한 보안위협들이 발생할 것으로 예상되고 있다.



【그림 1-6】 모바일 오피스 보안위협

제 2 절 모바일 오피스 유형 분류

앞서 살펴본 것처럼 모바일 오피스는 다양한 업종 및 분야에서 활용되고 있다. 모바일 오피스 서비스는 [표 1-1]과 같이 다양한 기준에 따라 유형을 분류할 수 있다.

【표 1-1】 모바일 오피스 유형 분류

유형분류 기준	세부 유형
업종	- 제조업, 운수업, 시설관리, 교육, 의료, 도·소매업 등
업무 형태	- 그룹웨어 서비스, 현장업무 서비스
수행 기능	- 인증, 조회, 입력, 파일 저장, 파일 업로드 등

먼저, 모바일 오피스 서비스는 제조업, 운수업, 교육, 의료, 도·소매업, 영업관리 등과 같이 업종에 따라 분류할 수 있다. 각 업종별로 특화된 서비스에 따라 모바일 오피스 유형을 분류하면 [표 1-2]와 같다.

【표 1-2】 업종별 특화 서비스에 따른 모바일 오피스 분류

제조업	자재관리, 생산스케줄관리, 협업
운수업(택배, 철도 등)	물품관리, 배차관리, 물품배송, 차량위치추적, 금융결제
시설관리	시설물관리, 위치정보 활용
교육	강의시간관리, 학생정보, 강의자료 관리, 출석 및 성적관리
의료	의료진정보관리, 진단, 환자정보, 시설예약
도·소매업(판매)	물품관리, 매출관리, 금융결제
영업관리	고객관리, 녹취/청취, 금융결제

모바일 오피스를 업무형태에 따라 분류하면, [표 1-3]과 같이 크게 그룹웨어 서비스와 현장업무 서비스로 구분할 수 있다. 그룹웨어 서비스는 메일, 전자결재 등의 일반적인 업무를 처리할 수 있는 환경을 제공하며, 대부분의 모바일 오피스에서 기본적으로 제공하고 있다. 현장업무 서비스의 경우, 기업 특성 및 업무형태에 따라 서비스를 다르게 제공한다.

【표 1-3】 업무형태에 따른 분류

그룹웨어 서비스	메일, 전자결재, 회계처리 등의 일반 업무를 모바일 단말기로 제공하는 서비스
현장업무 서비스	현장단속, 시설물관리, 보험 상담 등 기업의 현장업무를 모바일 단말기로 제공하는 서비스

모바일 오피스를 이용한 업무형태를 보다 세분화 하면 [표 1-4]와 같이 분류할 수 있다.

【표 1-4】 세분화된 업무형태에 따른 분류

이메일	업무를 위한 메일 작성 및 확인, 전송 등의 기능을 제공하는 서비스
그룹웨어	메일, 전자결재 등을 제외한 사내공지, 일정관리 등 기업의 일반적인 업무를 제공하는 서비스
전자결재	기업 내부 전자문서 결재 요청, 승인 등 전자결재 서비스
현장업무	시설물관리, 단속 등과 같이 현장에서 수행하는 업무를 위해 제공하는 서비스
고객관리	고객정보 입력/조회, 상담내용 기록 등 고객관리를 위해 제공하는 서비스
주문/배송관리	물품의 주문, 판매, 배송을 확인하기 위해 제공하는 서비스
문서작성/편집	한글(Hwp), 엑셀(Excel) 등 문서파일의 작성, 편집, 열람 등의 기능을 제공하는 서비스
고객/협력사와 커뮤니케이션	고객/협력사와의 원활한 커뮤니케이션 수행을 위한 게시판, 메신저 등의 서비스
매출관리	물품 구매/판매내역 파악 등을 위한 매입/매출 관리 서비스
설비관리	시설물 사용 예약, 수리 등록 등 시설관리 업무처리 서비스

금융결제	기업자금 결제 및 이체 등 업무를 위한 금융 서비스
모바일 영상회의	모바일 단말기의 카메라 기능을 이용한 원격 영상회의 서비스
연구과제 관리	연구내용 및 실적, 결과물 등을 입력/편집/조회 서비스
교육	내부직원을 교육을 위한 영상, 문서파일 제공 서비스
모바일 회의자료 공유	회의내용, 파일 등의 공유 및 확인 서비스
항만물류	선박 운항, 항만시설 관리, 화물 정보 등의 확인 서비스

마지막으로, 모바일 오피스는 제공하는 서비스 기능에 따라 분류할 수 있다. 서비스 기능이란 업무를 처리하기 위해 단말기에서 수행되는 행위를 말하며, [표 1-5]와 같이 인증, 조회, 입력 및 편집, 단말기에 파일 저장, 파일 업로드로 분류할 수 있다.

【표 1-5】 서비스 기능에 따른 분류

인증	모바일 오피스 단말 또는 애플리케이션 사용자가 인가받은 정당한 사용자인지 식별 및 검증하는 기능으로 ID/Password, PIN(Personal Identification Number) 등을 이용 가능
조회	모바일 오피스 애플리케이션을 통한 업무처리 정보를 확인하는 기능으로, 해당 정보를 단말기로 다운로드 받지 않고 뷰(View) 형태로 조회하는 기능도 포함
입력 및 편집	모바일 오피스 애플리케이션을 통해 업무처리를 위한 정보의 입력/편집을 수행하는 기능
단말기 내 파일 저장	모바일 오피스 애플리케이션을 통해 업무용 문서, 이미지, 실행 파일, 음성 파일 등을 단말기에 저장하는 기능
파일업로드	모바일 단말기에 저장되어 있는 업무용 문서, 이미지, 영상, 음성 등의 파일을 내부 업무 서버로 전송하는 기능

제 2 장 보안위협 및 보안대책 매칭표

구성 요소	보안위협	보안대책		
		기술적 보안대책	관리적 보안대책	
			보안 정책 외	보안 정책
단 말 기	MTE-101	MME-204 MME-501 MME-701 MME-801	MME-302, MME-303, MME-304 MME-504, MME-505, MME-506 MME-705, MME-706, MME-707	MME-1401 MME-1402 MME-1403 MME-1404 MME-1405 MME-1406 MME-1407 MME-1408
	MTE-102	MME-204 MME-501 MME-701 MME-801	MME-302, MME-303, MME-304 MME-504, MME-505, MME-506 MME-705, MME-706, MME-707	
	MTE-202	MME-204 MME-501 MME-701 MME-801	MME-302, MME-303, MME-304 MME-504, MME-505, MME-506 MME-705, MME-706, MME-707	
	MTE-301	MME-503		
	MTE-302	MME-503 MME-701	MME-704	
	MTE-401	MME-204 MME-501 MME-701	MME-302, MME-303, MME-304 MME-504, MME-505, MME-506	
	MTE-503	MME-301	MME-303	
	MTE-605	MME-202		
	MTE-701	MME-202 MME-401 MME-403 MME-1104 MME-1301	MME-1107, MME-1108	

구성 요소	보안위협	보안대책		
		기술적 보안대책	관리적 보안대책	
			보안 정책 외	보안 정책
단 말 기	MTE-702	MME-101, MME-102 MME-103, MME-201 MME-202, MME-401 MME-402, MME-403 MME-601, MME-602 MME-603, MME-604 MME-1104	MME-105, MME-106 MME-205, MME-404 MME-605, MME-606 MME-1107, MME-1108	
	MTE-703	MME-202, MME-204 MME-401, MME-402 MME-403, MME-1104	MME-1107, MME-1108	
	MTE-705	MME-501, MME-502	MME-302, MME-303, MME-304 MME-504, MME-505, MME-506	
애플리케이션	MTE-504	MME-301, MME-801	MME-302, MME-303, MME-304 MME-504, MME-505, MME-506 MME-705, MME-706, MME-707	
	MTE-502	MME-301, MME-801	MME-302, MME-303, MME-304, MME-504, MME-505, MME-506 MME-705, MME-706, MME-707	
	MTE-601	MME-501, MME-503 MME-801, MME-1102	MME-302, MME-303, MME-304, MME-504, MME-505, MME-506 MME-705, MME-706, MME-707	
	MTE-603	MME-703, MME-801	MME-704	
	MTE-708	MME-101, MME-102 MME-103, MME-601 MME-602, MME-603 MME-604	MME-105, MME-106 MME-605, MME-606 MME-1107, MME-1108	
	MTE-707	MME-701, MME-703		

구성 요소	보안위협	보안대책		
		기술적 보안대책	관리적 보안대책	
			보안 정책 외	보안 정책
네 트 워 크	MTE-201	MME-1001, MME-1002		MME-1401 MME-1402 MME-1403 MME-1404 MME-1405 MME-1406 MME-1407 MME-1408
	MTE-202	MME-901, MME-902 MME-904, MME-1001 MME-1002		
	MTE-501	MME-1001, MME-1002		
	MTE-505	MME-1001, MME-1002		
	MTE-602	MME-1101, MME-1103	MME-1105, MME-1107 MME-1108	
	MTE-704	MME-901, MME-902 MME-904, MME-1001 MME-1002		
	MTE-706	MME-204, MME-903 MME-904		
내 부 시 스 템	MTE-402	MME-204, MME-301 MME-501, MME-503 MME-701, MME-702 MME-1103, MME-1104	MME-1105, MME-1106 MME-1107, MME-1108	
	MTE-701	MME-1103, MME-1104 MME-1201, MME-1202 MME-1203, MME-1301	MME-1105, MME-1106 MME-1107, MME-1108 MME-1204, MME-1205	

모바일 오피스 정보보호 안내서

발행처 : 미래창조과학부 · 한국인터넷진흥원

경기도 과천시 관문로 정부과천청사
미래창조과학부
TEL : (국번없이) 1335

서울특별시 송파구 중대로 109 대동빌딩
한국인터넷진흥원
TEL : (02) 405-4118

(비매품)

본 안내서 내용의 무단 전재를 금하며, 가공·인용할 때에는 반드시
미래창조과학부 · 한국인터넷진흥원 『모바일 오피스 정보보호 안내서』
라고 출처를 밝혀야 합니다.