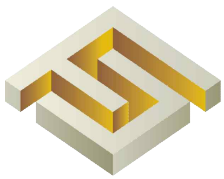
AGR-VII-2016-②-40

금융권 모바일 오피스 보안 가이드

2016. 12.

금융미래를 열어가는 금융보안파트너



금융보안원
FINANCIAL SECURITY INSTITUTE

목 차

제1장 개요

1. 목적

본 가이드는 금융회사 및 전자금융업자(이하 '금융회사')가 모바일 오피스를 구축·운영 시 안전한 업무 이용환경을 조성하기 위한 보호기능을 제시함을 목적으로 한다.

2. 구성

본 가이드는 총 4장으로 구성된다.

가. 제1장에서는 가이드의 목적, 구성, 활용, 용어 정의, 관련 법규에 대해 서술한다.

나. 제2장에서는 모바일 오피스의 구성과 보안 위협에 대해 서술한다.

다. 제3장에서는 모바일 오피스의 구성 요소별 보안 요구사항을 서술한다.

라. 제4장에서는 모바일 오피스의 구성 요소별 보안기능을 서술한다.

3. 활용

가. 금융회사는 모바일 오피스 활용 시 도입·운영 단계에서 보안대책 마련을 위한 참고자료로 활용한다.

나. 금융회사는 내부 방침에 따라 본 가이드에서 제시하는 보안기능뿐만 아니라 보안 수준에 문제가 없다고 판단되는 대책을 적용할 수 있다.

4. 용어 정의

본 가이드에서 사용하는 용어의 정의는 다음과 같다.

가. “모바일 단말기(이하 ‘단말기’)”라 함은 이동성을 제공하는 스마트 단말기(스마트폰, 스마트패드 등)를 말하며 PC(노트북 포함)는 제외한다.

나. “무선통신망”이라 함은 무선랜(Wi-Fi), 이동통신망 등 무선 설비·전파를 이용하는 통신망을 말한다.

다. “모바일 오피스”라 함은 단말기와 무선통신망을 활용하여 시간적, 공간적 제약 없이 업무를 수행할 수 있는 근무 형태를 말한다.

라. “이용자”라 함은 모바일 오피스를 이용하는 금융회사의 임직원을 말한다.

마. “중요정보”라 함은 고객정보, 금융거래정보 및 금융회사의 기밀정보 등을 말한다.

바. “서비스”라 함은 금융회사가 단말기를 통해 이용자에게 제공하는 모바일 오피스 업무를 말한다.

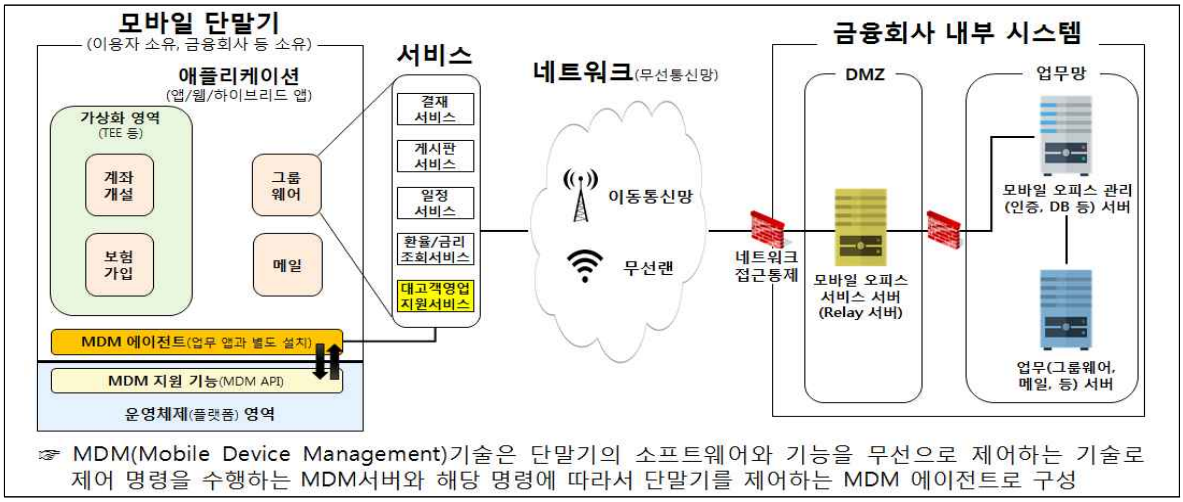
5. 관련 법규

본 가이드는「전자금융거래법」,「개인정보 보호법」,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 ‘정보통신망법’) 등 관련 법규를 참조한다.

제2장 모바일 오피스 구성과 보안 위협

1. 모바일 오피스 구성

가. 모바일 오피스 구성도



<그림 2> 모바일 오피스 구성도(예시)

나. 구성요소

① 단말기

- 모바일 오피스 서비스를 이용하는 이용자 단말로서 이용자 소유의 단말기와 금융회사가 소유한 단말기로 구분된다.
- 일부 단말기는 가상화 기술*을 통해 모바일 오피스 애플리케이션(이하 '애플리케이션')과 연동이 가능하다.

* 애플리케이션 가상화, H/W지원 가상화(Trusted Execution Environment: TEE) 등의 형태로 운영체제와 애플리케이션의 무결성을 강화하는 플랫폼보안 기술

② 애플리케이션

- 애플리케이션은 구현 방식에 따라 '앱*(Application software)', '웹**(Web application)', '하이브리드 앱***(Hybrid application)'으로 분류된다.

* 앱은 스마트폰 등에 다운받아 사용할 수 있는 응용프로그램, ** 웹은 웹 애플리케이션 또는 웹 앱이라 말하며 웹 브라우저 기능이 포함된 앱, *** 하이브리드 앱은 앱과 웹의 장점이 결합한 앱을 의미

- 애플리케이션은 단말기 기능에 따라 처리정보의 민감도 등을 고려하여 가상화 영역에서 실행될 수 있다.

③ 네트워크

- 단말기와 내부시스템 간 네트워크, 내부시스템의 내부 네트워크로 구성되며, 무선통신망과 유선통신망 구간으로 분류된다.

④ 내부시스템

- 금융회사의 내부시스템 영역으로 모바일 오피스 서비스를 위한 인증 서버, 관리 서버, 데이터베이스, 그룹웨어 등으로 구성된다.

⑤ 서비스

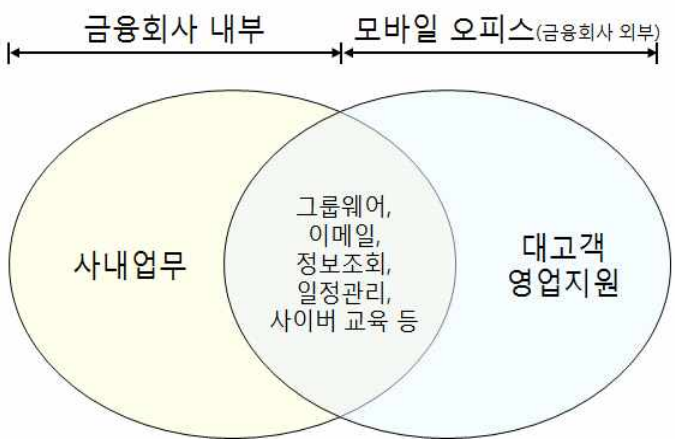
- 금융회사의 외부에서 업무처리가 가능하도록 그룹웨어, 결재, 이메일 등의 업무가 포함된다.
- 각 서비스는 인증·조회·입력 및 편집·파일 저장 및 업로드 등의 기능으로 구성된다.

다. 서비스 범위

모바일 오피스 서비스는 사내 업무 이외에 금융회사의 외부에서 이용자가 업무를 수행하는 것을 포함한다.

☞ 모바일 오피스가 제공하는 서비스는 '중요정보'의 포함여부와 이용자 혹은 고객인 '서비스 대상'에 따라 서비스 민감도가 차등*될 수 있다.

* (낮은 민감도) 중요 정보를 포함하지 않는 일반 업무, (높은 민감도) 중요정보를 포함하는 대고객 영업지원 업무 등



<그림 2> 모바일 오피스 서비스 범위

☞「모바일오피스 이용현황 조사 결과(2016, 금융보안원)」에서는 모바일 오피스 서비스를 결재, 메일 등 그룹웨어 사용과 보험가입, 사고현장 조사 등 대고객 영업지원 서비스 목적으로 사용하는 것으로 나타남

※ 조사기간: 2016.7.20.~8.22., 조사 대상 : 137개 금융회사(전 권역)

2. 모바일 오피스 보안 위협

모바일 오피스는 이동성을 제공하는 단말기에서 인터넷을 통해 금융회사의 내부시스템에 접속하여 업무를 수행하므로 이에 따른 보안 위협은 다음의 5가지 형태로 제시될 수 있다.

가. **(분실·도난)** 단말기 분실 및 도난 시 정당한 이용자 이외 제3자가 해당 단말기에 저장된 민감한 정보에 접근하거나 이를 이용해 금융회사의 내부시스템에 접속을 시도할 가능성이 존재한다.

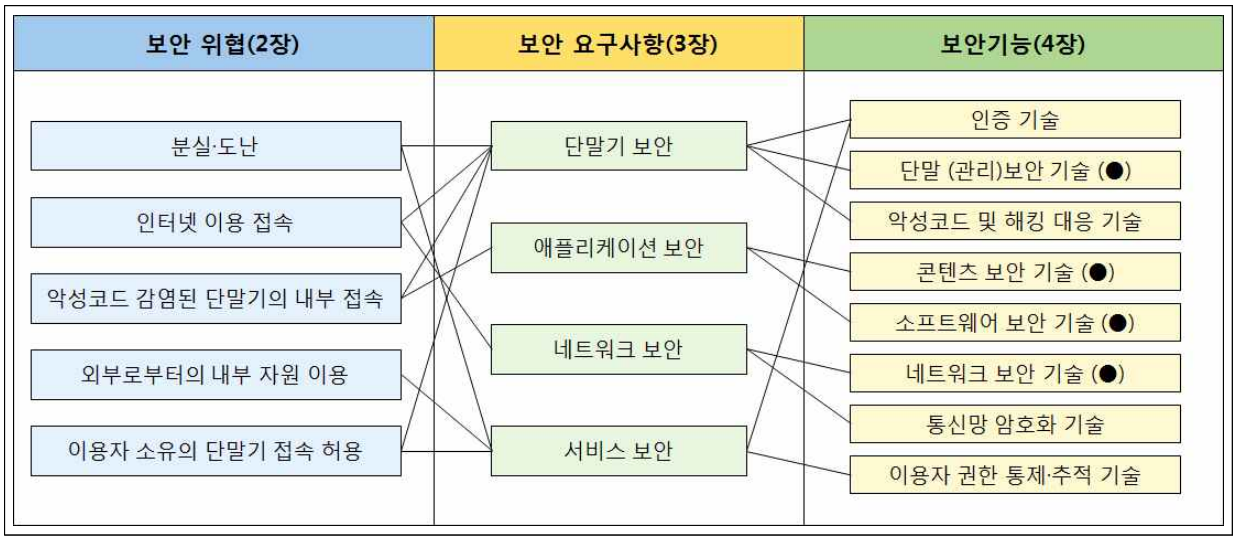
나. **(인터넷 이용 접속)** 금융회사의 외부로부터의 접속은 대부분 유·무선인터넷을 이용하므로 사설망에 비해 상대적으로 안전성이 낮다.

다. **(악성코드 감염된 단말기의 내부 접속)** 인터넷을 접속하여 사용되던 단말기는 악성코드 감염 가능성이 높으며, 이러한

단말기로 금융회사의 내부시스템 접속 시 악성코드를 전파할 가능성이 존재한다.

라. **(금융회사의 외부에서 내부 자원 이용)** 금융회사의 외부에서 내부시스템에 대한 접속 및 자원 이용을 허용하므로 업무정보에 대한 비인가자의 접근 가능성이 존재한다.

마. **(이용자 소유의 단말기 접속 허용)** 보안 통제가 어려운 이용자 소유의 단말기 접속을 허용하는 경우 업무정보의 유출 위험이 존재한다.



<그림 3> 모바일 오피스 보안 위협, 보안 요구사항 및 보안기능의 상관관계

☞ <그림 3>의 '(●)' 표시가 되어있는 보안기능은 MDM 지원 기능(MDM API 등)을 활용하여 구현 가능한 기능을 의미

제3장 모바일 오피스 보안 요구사항

1. 단말기 보안

가. 단말기 접근통제

단말기의 정당한 이용자 사용을 위해 **단말기 접근제어, 자동 잠금, 인증실패 조치**를 위한 대응 방안이 요구된다.

<참고 규정>
☞ **「전자금융감독규정」 제12조제1호** - 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것
☞ **「전자금융감독규정」 제13조제1항제13호** - 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)

나. 단말기 관리 대책

단말기의 **분실·도난, 비인가 타 장치와의 연결, 단말기 자원**(카메라, 마이크 등)**을 통한 정보 유출**을 통제하기 위한 기능이 요구된다.

<참고 규정>
☞ 「**전자금융감독규정」 제12조제1호** - 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것
☞ 「**전자금융감독규정」 제12조제4호** - 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것

다. 플랫폼 보안

단말기의 플랫폼 보안을 위해 **운영체제 임의변조, 단말기 상태 변경에 대한 탐지** 기능을 제공하고, 이 경우 정보 수집 시 수집·이용 대상 및 목적에 따라 **이용자 동의 절차**가 요구된다.

<참고 규정>
☞ 「**전자금융감독규정」 제12조제2호** - 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것
☞ 「**개인정보 보호법」 제15조(개인정보의 수집·이용)제1,2항**
① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할

수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
※ 각 항의 세부 각 호는 동 법 참고

☞「**정보통신망법」 제22조의2(접근권한에 대한 동의) ※ '17년3월 시행예정**

① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신 단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 "접근권한"이라 한다)이 필요한 경우 다음 각 호의 사항을 이용자가 명확하게 인지할 수 있도록 알리고 이용자의 동의를 받아야 한다.
② 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 반드시 필요하지 아니한 접근권한을 설정하는데 이용자가 동의하지 아니한다는 이유로 이용자에게 해당 서비스의 제공을 거부하여서는 아니된다.

라. 악성코드 및 해킹

단말기는 악성코드 및 해킹 대응을 위한 보안기능을 제공하고 해당 기능(예: 프로그램)의 **위·변조를 방지**하여 정상 실행을 점검하는 절차가 요구된다.

2. 애플리케이션 보안

가. 콘텐츠 보안

애플리케이션은 **업무 정보의 안전한 관리, 유출 통제, 중요정보 통제 기능**이 요구된다.

<참고 규정>
☞「**전자금융감독규정」 제13조제1항제13호** - 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)

나. 소프트웨어 보안

모바일 오피스를 위한 **안전한 S/W* 개발**이 요구되며, 모바일 오피스 이용 시 **S/W의 유출 및 위·변조 방지, 비인가 S/W 설치 통제, S/W 상태관리 기능**이 요구된다.

* S/W는 모바일 오피스 업무를 제공하기 위한 애플리케이션을 의미

3. 네트워크 보안

가. 네트워크 보안 대책

모바일 오피스 이용 시 업무정보 유출을 방지하기 위해 안전한 **무선 네트워크를 이용**하는 방안이 요구된다.

<참고 규정>
☞「**전자금융감독규정**」**제15조제6항** - 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다.

1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의 2에 따른 정보보호최고책임자의 승인을 받아 사전에 지정할 것
2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안대책을 수립할 것
3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것
4. 비인가 무선접속장비(Access Point : AP) 설치접속여부, 주요 정보 노출여부를 주기적으로 점검할 것

나. 통신망 암호화 대책

모바일 오피스 이용 시 업무정보 유출을 방지하기 위해 **암호화 통신 기능**이 요구된다.

<참고 규정>
☞「**전자금융감독규정**」**제34조제2항제1호** - 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)

4. 서비스 보안

가. 이용자 인증

정당한 이용자의 접근제어를 위한 **이용자 인증, 접속 관리, 인증 실패 조치, 복합인증, 안전한 비밀번호 생성, 세션 관리, 인증 정보 재사용 방지**를 위한 기능이 요구된다.

<참고 규정>
☞「**전자금융감독규정**」**제32조제3호** - 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

☞「**전자금융감독규정**」**제32조제2호가목** - 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정

나. 서비스 권한통제 및 이용내역 점검

모바일 오피스 이용 시 **이용자별 권한에 따른 서비스 접근 통제**와 **이용자의 이용내역을 관리**하는 기능이 요구된다.

<참고 규정>
☞「**전자금융감독규정**」**제13조제1항제4호** - 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것

☞「**전자금융감독규정**」**제13조제1항제14호** - 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것

☞「**전자금융감독규정**」**제12조제2호** - 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것

☞「**전자금융감독규정**」**제13조제4항** - 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다.

1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록
2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록
3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록

다. 정보유출 보호대책

모바일 오피스 이용 시 업무 정보유출을 방지하기 위한 **조회·파일 저장·업로드 기능 보호**와 **서비스 실행 환경 보호**를 위한 기능이 요구된다.

제4장 모바일 오피스 보안기능

본 장은 '제3장 모바일 오피스 보안 요구사항'에 대응하는 보안 기능을 서술한다.

금융회사는 모바일 오피스 도입 시 단말기의 하드웨어 및 운영체제의 특성, 이용자의 편의성, 개인정보 수집 범위, 단말기의 소유권, 중요정보 포함 여부 등을 고려하여 보안기능을 적용할 수 있다.

1. 단말기 보안

정당한 이용자 이외 제3자에 의한 모바일 오피스 접근 및 정보 유출을 차단하기 위해 단말기 접근통제 및 플랫폼 보호기능을 제시한다.

가. 단말기 접근통제

① **단말기 접근제어**

- 단말기 구동 시 단말기 이용자 인증을 수행해야 한다.

② **자동잠금**

- 이용자가 일정 시간 동안 단말기 미사용 시 단말기 화면이 자동으로 잠기도록 해야 한다.

③ **인증실패 조치**

- 일정 횟수 이상 단말기 이용자 인증 오류 시 단말기 사용을 차단해야 한다.
- 단말기 이용자 인증 오류로 단말기 사용 차단 후 이를 해제할 경우에는 보안 담당자를 통하거나 추가적인 인증 절차를 거치도록 해야 한다.

④ **안전한 비밀번호 관리**

- 유추하기 어려운 비밀번호 생성, 주기적 비밀번호 변경 등 안전한 비밀번호 관리를 수행해야 한다.

나. 단말기 관리 대책

① **단말기 분실·도난 대책**

- 단말기에 대한 원격 잠금 기능(패스워드 강제변경 포함)을 제공해야 한다.
- 단말기 내 애플리케이션 및 데이터에 대해 원격 삭제 기능을 제공해야 한다.
- 분실·도난 단말기에 대한 위치확인 기능을 제공해야 한다.

② **타 장치 연결통제**

- USB, 무선랜, 블루투스, 적외선통신(IR) 등 비인가 장치와의 연결을 제한해야 한다.

③ **단말기 자원 통제**

- GPS, 카메라, 마이크 등 단말기 하드웨어 자원의 기능을 통제해야 한다.

다. 플랫폼 보안

① **운영체제 변조 탐지**

- 플랫폼 위·변조(루팅, 탈옥 등) 방지를 위해 주기적 또는 애플리케이션 구동 시 플랫폼에 대한 무결성 검증을 수행해야 한다.

② **단말기 상태 점검**

- 단말기의 상태정보(USIM 정보, 전화번호, OS 버전, 펌웨어 버전, 보안정책, 기타 식별 정보 등)를 주기적으로 확인해야 한다.

- 단말기 상태정보를 일정기간 동안 수신하지 못하거나, 상태정보가 임의 변경된 경우 잠재적 분실·도난 상황으로 간주하고 관리자 및 이용자에게 해당 사실을 통지하는 등 조치해야 한다.

③ 이용자 동의 처리

- 단말기 상태정보 등을 수집·이용 시 동의절차*에 따라 이용자 동의**를 얻어야 한다.

* 동의절차 예시) 1. 금융회사는 법규 검토 후 개인정보 취급동의 약관 마련 ⇒ 2. 단말기에 모바일 오피스 앱 설치 시 혹은 최초 접속 시 해당 약관에 대한 이용자 동의 ⇒ 3. 미동의 시 사내 정책에 따라 처리 (예: 관련 앱 설치 불가 등)

** 개인정보 수집 동의(수집·이용 목적 및 항목, 보유·이용 기간, 동의·거부 권리 등 명시) 및 이용 동의(기능 제어 항목, 요금부과 체계, 기타 기능 명시)

<정보 수집 범위 예시>

구 분	예 시
단말기 식별자	단말기를 식별하기 위한 기초 필수 정보로 하나 이상의 정보를 결합하여 단말기를 식별한다. (예) Wi-Fi MAC Address, IMEI, UDID(iOS만 가능), Android ID 등
이용자 식별자	이용자를 구별하기 위한 정보로서 개인 식별자를 말한다. (예) ID, 전화번호, 이름, 이메일 주소, 사원번호(FC 코드 등) 등
단말기 상태정보	단말기를 통제하기 위한 정보로 단말기의 루팅, 탈옥, 정상동작 여부 확인 등을 위해 필요한 정보를 말한다. (예) OS명, OS버전, 단말기모델, 루팅·탈옥 상태 등
앱 정보	모바일 오피스 관련 업무 앱이 정상적으로 설치되었는지 확인하고 해당 앱의 위변조 확인하기 위한 정보를 말한다. (예) 모바일오피스 관련 앱 설치 여부 및 버전, 설치 목록 등
보조 식별자	모바일 보안시스템을 운영 관리하기 위한 추가정보로서 단말기 정보, 개인특징, 업무 관련 정보 등을 말한다. (예) 제조사, 통신사, 부서코드, 직급코드 등

라. 악성코드 및 해킹

① **보안프로그램 설치**

- 백신 프로그램을 설치하고, 최신 엔진상태를 유지해야 하며, 단말기에 대한 주기적 검사 및 실시간 감시를 해야 한다.
- 개인방화벽을 설치하고, 최신 방화벽 정책을 유지해야 한다.
- 보안 프로그램 업데이트 미수행 시 서비스 접속을 제한해야 한다.

② **위·변조 방지**

- 보안 프로그램의 무결성 검증을 주기적 또는 애플리케이션 구동 시 수행해야 한다.
- 보안 프로그램의 정상 실행 여부 점검을 수행해야 한다.

2. 애플리케이션 보안

애플리케이션에서의 업무정보(콘텐츠) 관리와 악성 애플리케이션으로부터 정보유출을 통제하기 위해 보안기능을 제시한다.

가. 콘텐츠 보안

① **안전한 정보 관리**

- 임시파일 생성을 제한하며, 불가피한 경우 휘발성 메모리에 암호화하여 임시 저장하고 서비스 종료 시 즉시 삭제해야 한다.

② **정보유출 통제**

- 업무자료 및 화면은 프린터 등을 통한 외부 출력을 통제해야 한다.
- 서비스 접속 시 화면캡처를 통제해야 한다.

③ **중요정보 통제**

- 중요정보가 저장되지 않도록 하고, 암호화하여 전송한 후 삭제해야 한다.
- 중요정보의 입력·수정·삭제를 통제해야 한다.
- 서버와 단말기 간 보안 통제정책 및 데이터 전송 시 종단간 암호화를 적용해야 한다.

나. 소프트웨어 보안

① **S/W 설치 통제**

- 신뢰할 수 있는 기관의 서명이 존재하지 않거나, 비인가된 모바일 오피스 S/W와 비인가된 범용 S/W의 설치를 제한해야 한다.
- S/W설치 및 업데이트 시 S/W에 대한 무결성을 검증해야 한다.
- S/W설치를 블랙리스트(Black List) 또는 화이트리스트(White List) 기반으로 통제해야 한다.
- 애플리케이션 구동 시 악성코드 및 바이러스 탐지를 수행해야 한다.

② **S/W 유출 및 위·변조 방지**

- 공개 앱 스토어를 통한 S/W의 배포를 금지해야 한다.
- S/W의 위·변조 방지를 위해 주기적 또는 애플리케이션 구동 시 무결성을 검증해야 한다.

③ **안전한 S/W 개발**

- 개발 시 시큐어코딩을 적용해야 한다.
- S/W도입 전, 취약점 분석 및 보안조치를 수행해야 한다.

<서비스 주요 취약점 예시>

구 분	예 시
인증, 접근통제	취약・디폴트 계정 사용, 이용자 정보변경 후 재 인증절차 미흡, 관리자・이용자정보 변경 페이지 등 접근통제 미흡 등
쿠키 및 세션	쿠키에 중요정보포함, 취약한 세션관리 등
입력・출력・전송값 검증	악의적인 명령어 주입(SQL, Command Injection), 악의적인 명령어 실행(XSS, CSRF 등), 파일업로드·다운로드 취약점, 소스 코드 노출, 매개변수 부정조작 등
부적절한 환경설정	디렉터리 인덱싱, 부적절한 에러 처리, 불필요한 Method지원 등
불필요한 파일 존재	백업·임시파일 존재, 샘플 및 디폴트 페이지·테이블 존재 등
기타	버퍼오버플로, 개인정보노출, 암호화통신 미흡, 인증서 검증 미흡(유효기간, 유효성, 인증내용) 등

④ S/W 상태관리

- 주기적 또는 애플리케이션 구동 시 보안패치 및 업데이트를 수행해야 한다.
- 보안프로그램 및 애플리케이션 업데이트의 미수행 시 서비스 접속을 제한해야 한다.

3. 네트워크 보안

전송 구간에서 업무정보 유출을 방지하기 위한 네트워크 보호 기능을 제시한다.

가. 네트워크 보안 대책

① 안전한 무선랜 접속

- 무선랜을 통한 서비스 이용 시 안전한 보호대책이 적용된 AP(Access Point)를 이용해야 한다.

< 안전한 무선랜 접속 예시 >

- (현장·이동근무 시) 악의적인 목적으로 설치된 무선 AP접속 금지 등 보호조치가 적용된 단말기에서 암호통신, 이용자·단말기 인증 등이 적용된 무선 AP에 접속하는 경우
- (금융회사의 내부 근무 시) 금융회사의 무선랜 사용 통제 및 보호 대책이 적용된 무선랜을 접속하는 경우

나. 통신망 암호화 대책

① **암호 통신 제공**

- 안전한 통신채널 암호화 방식(SSL/TLS, WPA2-PSK(AES) 등) 또는 가상사설망(VPN)을 사용해야 한다.
- VPN 클라이언트는 보안담당자의 통제를 받아 인가된 이용자에게 배포해야 한다.
- VPN 이용 시 동작하는 타 프로세스들의 통신은 모두 차단해야 한다.

4. 서비스 보안

모바일 오피스 서비스 이용 시 이용자 인증 및 권한통제, 정보유출 통제에 대한 보안기능을 제시한다.

가. 이용자 인증

① **애플리케이션 접근제어**

- 애플리케이션 구동 시 애플리케이션 이용자 인증을 수행해야 한다.

② **자동 접속종료**

- 일정 시간 동안 미사용 시 자동으로 접속이 해제되도록 해야 하며, 재접속 시 다시 인증을 수행해야 한다.

③ **인증실패 조치**

- 일정횟수 이상 애플리케이션 이용자 인증 오류 시 애플리케이션 사용을 차단해야 한다.
- 애플리케이션 이용자 인증 오류로 애플리케이션 사용 차단 후 이를 해제할 경우에는 보안 담당자를 통하거나 추가적인 인증 절차를 거치도록 해야 한다.

④ **복합인증 수행**

- 계정(ID)·비밀번호 이외에도 단말기 고유 정보(Wi-Fi MAC 등), 생체인증, OTP 등을 이용한 복합인증을 수행해야 한다.

⑤ **안전한 비밀번호 생성**

- 추측하기 어려운 비밀번호를 사용해야 하며, 주기적으로 비밀번호를 변경해야 한다.
- 계정(ID)·비밀번호 등 인증정보는 단말기 내 저장을 금지해야 한다.
- 초기 할당된 비밀번호는 이용자 로그인 후 변경하도록 해야 한다.

⑥ **세션관리 방안**

- 다중로그인을 통제해야 한다.
- 이용자 인증값이 재사용될 수 없도록 해야 한다.

⑦ **인증정보 유출방지**

- 인증정보의 입력 및 전송 시 노출 및 위·변조를 방지해야 한다.

나. 서비스 권한통제 및 이용내역 점검

① **서비스 이용자 권한 관리**

- 담당업무, 직급 등에 따라 접근권한을 차등 부여해야 한다.
- 휴직, 교육, 퇴직 등 인사변경사항에 따른 접근통제를 수행해야 한다.

② **서비스 이용내역 관리**

- 이용자가 서비스에 접속하여 수행한 작업내역을 기록·보관해야 한다.
- 이용내역의 유출, 위·변조를 방지하고, 작업내역의 정당성 등을 주기적으로 확인·점검해야 한다.

다. 정보유출 보호대책

① **조회 기능**

- 단말기 내 파일저장 없이 문서뷰어를 통해 조회하도록 해야 한다.

② **파일 저장·업로드**

- 중요정보를 서버에 저장 시 안전성이 검증된 암호알고리즘을 기반으로 암호화하여 저장해야 한다.
- 파일 업로드 시 화이트리스트 기반으로 특정 파일 타입 및 확장자만 업로드 되도록 해야 한다.
- 이용자 입력에 의한 파일 업로드 시 허용된 크기, 특수문자 변환 등 필터링을 수행해야 한다.

③ **서비스 실행 환경 보호**

- 애플리케이션을 통한 허가되지 않은 외부 서버와의 접속을 차단해야 한다.
- 애플리케이션 구동 시 업무정보 유출 경로로 활용 가능한 타 장치 연결 사용(1-나-②), 단말기 자원 사용(1-나-③), 무선랜 사용(3-가-①)을 통제해야 한다.

[첨부]

모바일 오피스 도입 시 보안 점검항목

☞ 금융회사는 모바일 오피스 도입 시 단말기의 하드웨어 및 운영체제의 특성, 이용자의 편의성, 개인정보 수집 범위, 단말기의 소유권, 중요정보 포함 여부 등을 고려하여 보안기능을 적용할 수 있다.

1. 단말기 보안

대분류	소분류	보안기능	비고
단말기 접근통제	단말기 접근제어	• 단말기 구동 시 단말기 이용자 인증을 수행해야 한다.	
	자동 잠금	• 이용자가 일정 시간 동안 단말기 미사용 시 단말기 화면이 자동으로 잠기도록 해야 한다.	
	인증실패 조치	• 일정 횟수 이상 단말기 이용자 인증 오류 시 단말기 사용을 차단해야 한다.	
		• 단말기 이용자 인증 오류로 단말기 사용 차단 후 이를 해제할 경우에는 보안 담당자를 통하거나 추가적인 인증 절차를 거치도록 해야 한다.	
	안전한 비밀번호 관리	• 유추하기 어려운 비밀번호 생성, 주기적 비밀번호 변경 등 안전한 비밀번호 관리를 수행해야 한다.	
단말기 관리 대책	단말기 분실·도난 대책	• 단말기에 대한 원격 잠금 기능을 제공해야 한다.	
		• 단말기 내 애플리케이션 및 데이터에 대해 원격 삭제 기능을 제공해야 한다.	
		• 분실·도난 단말기에 대한 위치확인 기능을 제공해야 한다.	
	타 장치 연결통제	• USB, 무선랜, 블루투스, 적외선통신(IR) 등 비인가 장치와의 연결을 제한해야 한다.	
	단말기 자원 통제	• GPS, 카메라, 마이크 등 단말기 하드웨어 자원의 기능을 통제해야 한다.	
플랫폼 보안	운영체제 변조 탐지	• 플랫폼 위·변조(루팅, 탈옥 등) 방지를 위해 주기적 또는 애플리케이션 구동 시 플랫폼에 대한 무결성 검증을 수행해야 한다.	

대분류	소분류	보안기능	비고
	단말기 상태 점검	• 단말기의 상태정보를 주기적으로 확인해야 한다.	
		• 단말기 상태정보를 일정기간 동안 수신하지 못하거나, 상태정보가 임의 변경된 경우 잠재적 분실·도난 상황으로 간주하고 관리자 및 이용자에게 해당 사실을 통지하는 등 조치해야 한다.	
	이용자 동의 처리	• 단말기 상태정보 등을 수집·이용 시 동의절차에 따라 이용자 동의를 얻어야 한다.	
악성코드 및 해킹	보안 프로그램 설치	• 백신 프로그램을 설치하고, 최신 엔진상태를 유지해야 하며, 단말기에 대한 주기적 검사 및 실시간 감시를 해야 한다.	
		• 개인방화벽을 설치하고, 최신 방화벽 정책을 유지해야 한다.	
		• 보안 프로그램 업데이트 미수행 시 서비스 접속을 제한해야 한다.	
	위·변조 방지	• 보안 프로그램의 무결성 검증을 주기적 또는 애플리케이션 구동 시 수행해야 한다.	
		• 보안 프로그램의 정상 실행 여부 점검을 수행해야 한다.	

2. 애플리케이션 보안

대분류	소분류	보안기능	비고
콘텐츠 보안	안전한 정보 관리	• 임시파일 생성을 제한하며, 불가피한 경우 휘발성 메모리에 암호화하여 임시 저장하고 서비스 종료 시 즉시 삭제해야 한다.	
	정보유출 통제	• 업무자료 및 화면은 프린터 등을 통한 외부 출력을 통제해야 한다.	
		• 서비스 접속 시 화면캡처를 통제해야 한다.	
	중요정보 통제	• 중요정보가 저장되지 않도록 하고, 암호화하여 전송한 후 삭제해야 한다.	
		• 중요정보의 입력·수정·삭제를 통제해야 한다.	

대분류	소분류	보안기능	비고
		• 서버와 단말기 간 보안 통제정책 및 데이터 전송 시 종단간 암호화를 적용해야 한다.	
소프트웨어 보안	S/W 설치 통제	• 신뢰할 수 있는 기관의 서명이 존재하지 않거나, 비인가된 모바일 오피스 S/W와 비인가된 범용 S/W의 설치를 제한해야 한다.	
		• S/W설치 및 업데이트 시 S/W에 대한 무결성을 검증해야 한다.	
		• S/W설치를 블랙리스트(Black List) 또는 화이트리스트(White List) 기반으로 통제해야 한다.	
		• 애플리케이션 구동 시 악성코드 및 바이러스 탐지를 수행해야 한다.	
	S/W 유출 및 위・변조 방지	• 공개 앱 스토어를 통한 S/W의 배포를 금지해야 한다.	
		• S/W의 위・변조 방지를 위해 주기적 또는 애플리케이션 구동 시 무결성을 검증해야 한다.	
	안전한 S/W 개발	• 개발 시 시큐어코딩을 적용해야 한다.	
		• S/W도입 전, 취약점 분석 및 보안조치를 수행해야 한다.	
	S/W 상태관리	• 주기적 또는 애플리케이션 구동 시 보안패치 및 업데이트를 수행해야 한다.	
		• 보안프로그램 및 애플리케이션 업데이트의 미수행 시 서비스 접속을 제한해야 한다.	

3. 네트워크 보안

대분류	소분류	보안기능	비고
네트워크 보안 대책	안전한 무선랜 접속	• 무선랜을 통한 서비스 이용 시 안전한 보호대책이 적용된 AP(Access Point)를 이용해야 한다.	
통신망 암호화 대책	암호 통신 제공	• 안전한 통신채널 암호화 방식(SSL/TLS, WPA2-PSK(AES) 등) 또는 가상사설망(VPN)을 사용해야 한다.	

대분류	소분류	보안기능	비고
		• VPN 클라이언트는 보안담당자의 통제를 받아 인가된 이용자에게 배포해야 한다.	
		• VPN 이용 시 동작하는 타 프로세스들의 통신은 모두 차단해야 한다.	

4. 서비스 보안

대분류	소분류	보안기능	비고
이용자 인증	애플리케이션 접근제어	• 애플리케이션 구동 시 애플리케이션 이용자 인증을 수행해야 한다.	
	자동 접속종료	• 일정 시간 동안 미사용 시 자동으로 접속이 해제되도록 해야 하며, 재접속 시 다시 인증을 수행해야 한다.	
	인증실패 조치	• 일정횟수 이상 애플리케이션 이용자 인증 오류 시 애플리케이션 사용을 차단해야 한다.	
		• 애플리케이션 이용자 인증 오류로 애플리케이션 사용 차단 후 이를 해제할 경우에는 보안 담당자를 통하거나 추가적인 인증 절차를 거치도록 해야 한다.	
	복합인증 수행	• 계정(ID)·비밀번호 이외에도 단말기 고유 정보(Wi-Fi MAC 등), 생체인증, OTP 등을 이용한 복합인증을 수행해야 한다.	
	안전한 비밀번호 생성	• 추측하기 어려운 비밀번호를 사용해야 하며, 주기적으로 비밀번호를 변경해야 한다.	
		• 계정(ID)·비밀번호 등 인증정보는 단말기 내 저장을 금지해야 한다.	
		• 초기 할당된 비밀번호는 이용자 로그인 후 변경하도록 해야 한다.	
	세션관리 방안	• 다중로그인을 통제해야 한다.	
		• 이용자 인증값이 재사용될 수 없도록 해야 한다.	
	인증정보 유출방지	• 인증정보의 입력 및 전송 시 노출 및 위·변조를 방지해야 한다.	

대분류	소분류	보안기능	비고
서비스 권한통제 및 이용내역 점검	서비스 이용자 권한 관리	• 담당업무, 직급 등에 따라 접근권한을 차등 부여해야 한다.	
		• 휴직, 교육, 퇴직 등 인사변경사항에 따른 접근통제를 수행해야 한다.	
	서비스 이용내역 관리	• 이용자가 서비스에 접속하여 수행한 작업내역을 기록·보관해야 한다.	
		• 이용내역의 유출, 위·변조를 방지하고, 작업내역의 정당성 등을 주기적으로 확인·점검해야 한다.	
정보유출 보호대책	조회 기능	• 단말기 내 파일저장 없이 문서뷰어를 통해 조회하도록 해야 한다.	
	파일 저장·업로드	• 중요정보를 서버에 저장 시 안전성이 검증된 암호알고리즘을 기반으로 암호화하여 저장해야 한다.	
		• 파일 업로드 시 화이트리스트 기반으로 특정 파일 타입 및 확장자만 업로드 되도록 해야 한다.	
		• 이용자 입력에 의한 파일 업로드 시 허용된 크기, 특수문자 변환 등 필터링을 수행해야 한다.	
	서비스 실행 환경 보호	• 애플리케이션을 통한 허가되지 않은 외부 서버와의 접속을 차단해야 한다.	
		• 애플리케이션 구동 시 업무정보 유출 경로로 활용 가능한 타 장치 연결 사용(1-나-②), 단말기 자원 사용(1-나-③), 무선랜 사용(3-가-①)을 통제해야 한다.	

금융권 모바일 오피스 보안 가이드

2016년 12월 발행

발행인 : 허 창 언

발행처 : 금융보안원

경기도 용인시 수지구 대지로 132

전 화 : (02) 3495-9000

<비 매 품>