부록 2-9

1.0

국가 망 보안체계 보안 가이드라인

정보서비스 모델 해설서

모델 9. 모바일 업무환경 정보 연계

2025. 9

국가정보원

NSR 국가보안기술연구소

부록 2-9

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서

모델 9. **모바일 업무환경 정보 연계**

2025. 9

국가정보원

NSR 국가보안기술연구소

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 - 모델 9. 모바일 업무환경 정보 연계

부록 2-9

문서이력

개정일	버전	내역	비고
2025.1.	Draft	「국가 망 보안체계 보안 가이드라인 – 정보서비스 모델 해설서」 발간	
2025.9.	1.0	「국가 망 보안체계 보안 가이드라인 – 정보서비스 모델 해설서 – 모델 9. 모바일 업무환경 정보 연계」 발간	모델별 분리

CONTENTS

CONTENTS

Table List

Figure List

제1장

정보서비스 모델 해설서 개요

제1절

정보서비스 모델 해설서 개요

1. 개요

본 해설서는 국가·공공기관에서 정보서비스[1] 구축·운영시 국가 망 보안체계(N2SF) 적용을 위한 보안 가이드라인 부록으로, 정보서비스 모델의 보안대책 수립을 위한 위협식별, 보안 요구사항 도출 및 보안통제 항목 선정 방법 제시를 목적으로 한다.

각급기관에서 구축·운영하고자 하는 정보서비스는 업무 환경 및 기관 특성에 따라 다른 형태로 구현되는 것이 일반적이지만, 다수 기관에서 생성형 AI, 외부 클라우드 서비스의 업무 활용 등 유사한 목적과 기능을 갖는 정보서비스의 구축이 이루어질 것으로 예상된다.

본 문서에서는 유사한 목적의 공통 정보서비스 모델을 도출하여 상위 수준에서 서비스 구조 및 구현 방법 등을 구체화하는데 참고할 수 있는 참조 모델을 제시한다. 각급기관에서 요구되는 정보서비스 모델을 정의하고 해당 모델에 적합한 보안대책 제시를 통해, 정보서비스 모델 구축·운용 시 필요한 보안대책 수립을 지원하고자 한다.

정보서비스 모델 해설서에서는 국가 망 보안체계 적용을 통해 변화하는 공공부문 주요 정보서비스 모델을 선정하여 보안 위협식별 및 그에 따르는 보안 요구사항 도출을 통한 보안 대책 수립에 초점을 맞추었으며, 각급기관이 해설서를 참조하여 보안대책을 적용 가능하도록 구성하였다.

1) 정보서비스는 업무정보를 이용해 특정 서비스를 제공하기 위해 하나 이상의 정보시스템으로 구성된 체계를 의미한다. 정보화 사업에서 정보시스템은 구축 및 운영의 대상이며, 정보시스템을 통해서 정보서비스를 제공하게 된다.

2. 문서 구조

본 문서는「모바일 업무환경 정보 연계」정보서비스 모델에 대해 설명하고 있으며, 3장은 정보서비스 개요, 위협식별, 보안대책 수립 등 총 3개의 절을 포함하고 있다. 3장에 대응하는 N2SF 단계/활동은 다음과 같다.

표 1-1 3장과 N2SF 단계/활동의 대응 관계

절	항	N2SF 단계	N2SF 활동명	세부 내용
제1절 정보서비스 개요	-	-	-	N2SF 정보서비스 개요 설명
제2절 정보서비스 보안위협 식별	1. 정보서비스 구성요소 분석	준비 (Prepare)	「활동-1-5」 정보서비스 식별	정보서비스를 구성하는 네트워크, 정보시스템, 업무정보 등 세부구성 분석, 사용 시나리오 정의 등
	2. 모델링 및 C/S/O 평가	위협식별 (Identify)	「활동-3-1」 모델링 및 C/S/O 평가	정보서비스의 각 구성요소(네트워크, 정보시스템 등)에 대한「위치-주체-객체」모델링 및 C/S/O 평가
	3. 보안원칙 적용		「활동-3-2」 보안원칙 적용	「정보 생산·저장」보안원칙 및「정보 이동」보안원칙 적용을 통하여 보안통제가 필요한 영역 확인
	4. 보안위협 식별		「활동-3-3」 보안위협 식별	정보서비스 구성에 기반하여 보안 위협 대상이 되는 정보시스템 및 네트워크 연계 지점, 서비스 위치를 파악하고 보안위협 요소 도출
제3절 보안 요구사항 및 보안대책	1. 이용자 단말	보안대책 수립 (Select)	「활동-4-1」 보안 요구사항 도출	정보서비스 구축·운영 과정에서 필요한 이용자 단말 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			「활동-4-2」 보안통제 선택	
	2. 모바일 업무환경 연계체계		「활동-4-1」 보안 요구사항 도출	기관 전산망과 네트워크 연계가 이루어지는 지점에 필요한 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			「활동-4-2」 보안통제 선택	
	3. 모바일 업무 시스템		「활동-4-1」 보안 요구사항 도출	모바일 업무용 시스템 운용 시 필요한 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			「활동-4-2」 보안통제 선택	

제2절

정보서비스 모델 해설서 활용 방안

본 해설서는 각급기관이 국가 망 보안체계에 따라 획일적인 망 분리 정책에서 탈피하여 새로운 보안체계 하에서 AI·클라우드 등 신기술을 적용한 정보서비스를 도입하는 과정에서 도움이 될 수 있다. 2장에서 정보서비스에서 발생할 수 있는 보안 위협을 고려하여 보안통제 항목을 조정·반영한 결과의 예시를 제안하고 있다.

본 문서에서 제안하는 보안통제 항목은 절대적인 기준이 아닌 검토 사항으로 기관의 특성에 맞게 유연하게 적용할 필요가 있다. 즉, 본 문서에서 제시하는 보안통제 항목을 모두 구현해야 한다거나 제시되지 않은 보안통제 항목은 구현하지 않아도 된다는 것을 의미하는 것은 아니다. 담당자는 보안통제 항목의 선택 및 구현 방안에 대해 신중히 결정하여야 하며, 특히 새로운 정보서비스 모델을 구축하거나 여러 정보서비스 모델을 동시에 구축하고자 할 경우, 제안된 보안위협 외에 다양한 보안위협을 추가로 고려하여 보안통제 항목을 폭넓게 검토하고 보안대책을 수립하는 것이 필요하다.

담당자는 3장 1절에서와 같이 각급기관이 운영하고자 하는 정보서비스를 간단히 정의한 후, 3절 1항에서와 같이 준비 단계의 일환으로 정보서비스 구성요소 등을 분석(「활동-1-5」)할 수 있다.

또한, 2절의 위협 식별 단계 중 모델링 및 C/S/O 평가(「활동-3-1」), 보안원칙 적용(「활동-3-2」) 활동에서 어떤 원칙에 위배될 수 있는지를 파악하고 보안위협 식별(「활동-3-3」) 활동에서 기관 네트워크 환경구성 및 보안통제 적용 구조 등을 고려하여 제시되어 있는 보안 위협 외에 추가 보안위협에 대해 분석하여야 한다.

3절에서 제시된 보안대책 수립 단계에서는 상기 위협을 바탕으로 보안 요구사항 도출(「활동-4-1」) 활동을 진행하게 되는데 앞서 추가로 제시된 위협 및 기관 네트워크 환경구성, 관련 규정 등을 고려하여 보안 요구사항을 최종적으로 도출한다. 보안통제 선택(「활동-4-2」) 활동에서는 필요시 기존에 제시된 보안통제 항목 외에 추가로 보안통제 항목을 선택하거나 제시된 보안통제 항목을 수정·삭제하는 등 세부사항을 조정하는 것이 가능하다.

제2장

모바일 업무환경 원칙 및 유형

제1절

모바일 업무환경 개요

모바일 업무환경은 스마트폰, 태블릿 등 모바일 단말을 이용해 국가·공공기관 행정업무 서비스를 활용하는 것을 말한다. 모바일 행정업무는 국가·공공기관 업무시스템의 메일·전자결재·회계처리 등을 전자적 업무방식으로 수행하는 「내부행정 업무」 및 현장에서 민원인 또는 사물 등을 대상으로 현장 확인·사후관리·생활민원 등을 전자적 업무방식으로 수행하는 「현장행정 업무」로 구분한다.

표 2-1 모바일 업무환경 구분

구분	정의
모바일 내부행정 업무	국가·공공기관 공무원 및 종사자 간에 행해지는 전자적 업무방식으로 모바일을 활용한 내부메일·전자결재·회계처리 등 그룹웨어 서비스 형태의 행정업무
모바일 현장행정 업무	국가·공공기관 공무원 및 종사자가 현장에서 민원인 또는 사물 등을 대상으로 수행하는 전자적 업무방식으로 현장확인·사후관리·생활민원 등에 대한 모바일을 활용한 현장업무

행정업무를 위한 모바일 단말은 노트북 등 이동 가능한 PC류를 제외한 모바일 전용의 범용 OS를 사용하는 스마트폰과 태블릿으로 한정한다. 모바일 단말은 이동통신망을 통한 데이터 통신이 가능한 단말로, 행정업무 앱 사용시 보안통제로 인해 WiFi 사용이 불가하므로 WiFi 전용 단말은 활용할 수 없다.

모바일 행정업무는 기관 외부의 모바일 단말이 접속하는 모바일 연계체계와 기관 내 정보시스템과의 정보 연계가 필요한 경우가 있다. 또한, 모바일 행정업무는 개인용 모바일 기기를 활용하여 기관 내·외부에서 모두 활용이 가능하다. 따라서, 모바일 행정업무의 보안성 및 기밀성을 유지하면서 개인용 모바일 기기를 활용하기 위해서는 모바일 업무 유형에 따른 보안통제를 적용해야 한다.

제2절

모바일 업무환경 원칙 및 유형

1. 모바일 업무환경 기본 원칙

모바일 업무환경을 위한 정보서비스 구축·운영 시에는 다음과 같은 기본 원칙을 준수해야 한다.

표 2-2 모바일 업무환경 기본 원칙

원칙	내용
모바일 시스템 분리	• 내부행정을 위한 모바일 업무시스템과 현장행정을 위한 모바일 업무시스템은 보안통제가 상이하므로 별도 분리하여 구축·운영하는 것을 권고한다. • 내부행정·현장행정 앱은 별도로 분리하여 설치·사용해야 한다.
모바일 연계체계 차등화	• 내부행정·현장행정 S등급 이상 업무 수행을 위한 모바일 단말은 모바일 연계체계(중계시스템)를 통해서만 통신을 수행하며, 모바일 업무시스템 및 기관 내부 업무시스템 등과의 직접적인 접속은 금지한다. • S등급 이상을 처리하는 업무는 모바일 가상화 플랫폼 등 보안통제가 적용된 모바일 업무시스템을 활용한다.(이하 모바일 업무시스템) • 재난·안전 현장 등 O등급을 처리하는 업무는 일반적인 모바일용 웹 서비스로 구성된 모바일 공개시스템을 활용할 수 있다.(이하 모바일 공개시스템)
접근 통제 강화	• 모바일 업무환경 정보서비스에 인증체계를 구축하여, 인가된 이용자·단말만 서비스를 이용할 수 있도록 접근을 통제해야 한다. • 관리자 기능에 대한 접근 통제를 강화해야 한다.
통신구간 암호화	• 모바일 서비스 통신구간은 End-to-End 암호화를 구현하여야 한다.
허가된 앱 배포·사용	• 모바일 업무 앱 배포시 배포앱에 대한 사전 안전성을 검증하여 검증된 앱만 공식 앱관리 프로그램을 통해 배포해야 한다.
업무자료 보안	• S등급 이상의 업무정보는 중요도에 따라 정보 열람만이 가능하도록 스트리밍 방식으로 전송한다.
중요 장비 이중화 및 백업	• 모바일 업무환경 시스템은 장애 발생시 대응을 위해 네트워크 스위치, 스토리지 등 중요 장비를 이중화하고 서비스 가용성 보장을 위한 백업체계를 구축해야 한다. • 백업·비상복구·변경관리·침해사고대응 등 모바일 업무환경 운영 절차를 수립해야 한다.

원칙	내용
도입 전산장비 안전성 확인	• 모바일 보안 및 정보보호 제품은 보안인증제도에 따라 안전성을 검증받은 제품으로 도입한다.
모바일 가상화 플랫폼 활용	• 모바일 단말 내 다른 앱 및 기능을 통한 내부행정·현장행정 업무 무단 접근을 방지하기 위해 모바일 가상화 플랫폼을 활용하여 업무환경을 구축·운용할 수 있다. • 모바일 가상화 플랫폼은 모바일 공통기반 플랫폼(행정안전부) 활용 또는 기관이 별도 구축할 수 있다.
공개·공유 데이터 관리	• 모바일 업무 수행 중 재난 상황 전파, 현장 대응 매뉴얼 열람, 비상 상황 공유 등을 위한 공개·공유 데이터 활용·관리 절차를 수립해야 한다.

기관은 모바일 업무환경 구축·운용 시 제시된 모바일 업무환경 기본 원칙을 준수해야 하며, 관리적 운영 원칙을 수립해야 한다.

기관은 모바일 업무 범위를 정의해야 한다. 모바일 업무환경은 기관 외부에서 모바일 단말을 이용하여 업무에 활용하므로, 분실, 악성코드 감염 등 보안위협에 대비하기 위해 행정업무의 허용범위를 제한해야 한다. 허용하는 모바일 업무의 정의는 각 기관의 업무 특성과 보안사항에 의거하여 명확히 정의해야 하며, 국가·공공기관 문서 분류 기준, 개인정보보호법, 공공기록물 관리에 관한 법률 시행규칙 등 법률 기준을 고려해야 한다.

또한, 개인 모바일 단말을 이용하여 모바일 업무를 수행하는 경우, 개인 모바일 단말의 다른 앱으로부터의 모바일 업무 정보보호, 개인 데이터 혼용 방지, 분실 및 기기 교체에 따른 보안대책 등 BYOD(Bring Your Own Device) 정책을 수립해야 한다.

그 외 기관이 필요하다고 판단하는 보안 인프라, 단말 관리 등 정책을 수립해야 한다.

2. 모바일 업무 유형 분류

가. 내부행정 업무 유형 분류

이용자가 모바일 단말을 통해 내부행정 업무를 수행하는 경우 활용하는 업무정보의 중요도 및 업무 유형에 따라 다음과 같이 분류할 수 있다.

표 2-3 내부행정 업무 유형 분류(예)

유형		내부행정 서비스	보안등급
행정 업무	공식문서	• 공문·보고서 원문 등 공식문서 관련 서비스	S
	내부메일	• 기관 내부 이용자 간 전자메일 서비스	S
	전자결재	• 내부 전자결재 서비스	S
	행정관리	• 인사·급여·자산·회계·평가·사업 등 행정 특화 서비스	S
	근태관리	• 출장·휴가·초과 근무 관리 서비스	S
	문서관리	• 증명서 신청·발급 관리 서비스	S
	메모보고	• 메모 보고 작성·열람 서비스	S
공유 업무	게시판	• 경조사, 인사발령, 교육·세미나 안내, 공지사항 등 알림 게시판	O
		• 동호회 등 커뮤니티 게시판	O
		• 언론보도 자료 및 언론 스크랩 게시판	O
		• 직원 조회 게시판	O
	자원관리	• 주차, 회의실, 공용차량 예약·조회 서비스	O
	출입관리	• 청사 방문객 예약 관리	O
	일정관리	• 일정 작성·조회, 개인 업무	O
	협업·소통	• 화상통화, 영상회의, 메신저 등 서비스	O
대외 업무	외부메일	• 인터넷 메일 서비스	O
	외부교육	• 인터넷 교육, 스마트 러닝 등 서비스	O
	외부연계	• 정부지식행정시스템 등 기존 외부 제공 서비스	O

해당 모바일 내부행정 업무의 보안등급 분류(C/S/O)는 예시이며, 기관은 모바일 업무환경 구축·운영 시 기관의 업무와 특성을 고려하여 보안등급을 분류하고, 모바일 업무·공개 시스템을 통해 모바일 내부행정 서비스를 제공해야 한다. 공유업무 및 대외업무 등 O등급 정보 업무는 모바일 공개시스템으로 구성할 수 있으며, 공공 클라우드 보안정책에 따른 외부 협업용 클라우드 서비스를 활용할 수 있다.

내부 행정업무는 개인용 모바일 단말을 이용하여 업무에 활용하므로 해킹 가능성 및 중요 자료의 유출 가능성에 대비하기 위해 내부행정 업무의 허용범위를 제한해야 하며, 허용하는 업무범위는 각 기관의 업무 특성과 보안상에 의거하여 명확하게 정의하여야 한다. 모바일 내부행정 업무 중 다음과 같은 기준에 해당하는 업무는 모바일 서비스에서 제외하여야 한다.

- (문서분류기준) 국가·공공기관 문서 분류 기준에 따라 대외비 이상의 비밀문서와 대외주의, 배포제한, 비공개 등 보안을 요구하거나 민감한 정보를 포함하는 문서 열람이 가능한 모바일 서비스
- (법률기준) '개인정보보호법', '공공기록물 관리에 관한 법률 시행규칙' 등 관련 법령이나 규정 등에 따라 보안관리 정책에 위배되는 행정업무의 모바일 서비스
- (업무기준) 정보공개법 등에 따라 대외 비공개 정보에 해당하는 모바일 전자결재 서비스

※ 전자결재 정책·방식 등 이외 세부 보안 요구사항은 국가정보원과 협의·시행

나. 현장행정 업무 유형 분류

이용자가 모바일 단말을 통해 현장행정 업무를 수행하는 경우 활용하는 업무정보의 중요도 및 업무 유형에 따라 다음과 같이 분류할 수 있다.

표 2-4 현장행정 업무 유형 분류(예)

유형		현장행정 서비스	보안등급
관리 업무	정보 관리	• 시설물, 측정기, 장비 현황, 사업장 현황 등 정보 관리 서비스	S
	재료 관리	• 자재, 폐기물, 시료 등 재료 물품 정보 관리 서비스	S
	대상자 관리	• 보호관찰자, 수강명령 대상자, 환자 등 대상자 관리 서비스	S
	시스템 관리	• 현장업무 관련 시스템 운영·관리 서비스	S
조회 업무	현장상황 조회	• 민원 결과, 토지 정보, 분쟁 등 조회 서비스	S
	개인정보 조회	• 출입국 정보, 혈액 정보, 휴대전화 번호 등 조회 서비스	S

유형		현장행정 서비스	보안등급
단속 업무	현장 단속	• 불법체류, 폐기물투기, 금연구역, 불법주정차 등 단속 서비스	S
	현장 처분	• 체납통합영치, 세외수입, 범죄수사 등 처분 서비스	S
지원 업무	위치 지원	• 국가지점번호, 현장 시설물 등 조회 지원	O
	출동 지원	• 출동지원, 차량동태확인, 차량관제, 차량예약 관리 등 지원	O
	구조 지원	• 인명구조 위치, 구조 설비시설 위치 등 정보 조회 지원	O
	활동 지원	• 현장자료 변환·공유·출력, 대응 매뉴얼 열람 등 지원	O
	협업 지원	• 영상전송, 화상회의, 무전, 알림 메시지 등 협업 지원	O
	전자기록 지원	• 전자동의, 의무기록 등 전자기록 지원	O
	재난·안전 지원	• 태풍·홍수·산불·화재 등 재난 및 안전 현장 지원	sO

해당 모바일 현장행정 업무의 보안등급 분류(C/S/O)는 예시이며, 기관은 모바일 업무환경 구축·운영 시 기관의 업무와 특성을 고려하여 보안등급을 분류하고, 모바일 업무·공개 시스템을 통해 모바일 현장행정 서비스를 제공해야 한다.

또한, 재난 현장 대응 및 응급 상황 처리 등 O등급의 현장 지원업무 수행시 모바일 단말에서 생성된 사진, 동영상, 음성, 보고자료 등을 모바일 공개시스템을 통해 처리할 수 있다.

제3장

모바일 업무환경 정보 연계

제1절

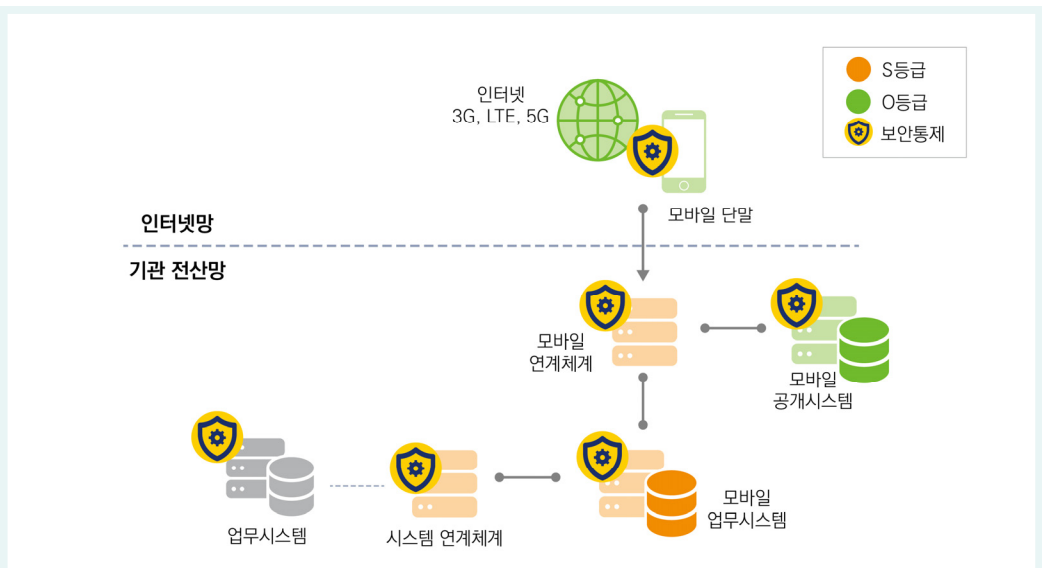
정보서비스 개요

본 정보서비스 모델에서는 모바일(스마트폰, 태블릿 등) 단말을 이용해 내부행정, 현장행정 업무 수행을 위한 보안 요구사항 및 대책을 제시한다.

1절은 국가 망 보안체계(N2SF) 도입에 따른 모바일 업무환경 정보서비스 구성을 보여주고, 2절은 정보서비스 환경에 맞춰 구성요소 분석, 모델링 및 보안등급 평가, 보안원칙 적용을 통한 보안 위협식별 절차를 수행한다. 3절은 보안 위협에 대응하기 위한 필수 보안 요구사항 및 보안통제 항목을 적용한 보안대책을 기술한다.

본 장에서는 국가 망 보안체계(N2SF)「모바일 업무환경 정보 연계」모델에 범용적으로 적용할 수 있는 정보서비스 위협식별 및 보안대책을 제시하고 있으며, 기관 환경 및 특성에 따라 추가적인 방안을 적용할 수 있다.

그림 3-1 모바일 업무환경 정보 연계 정보서비스 개요



제2절

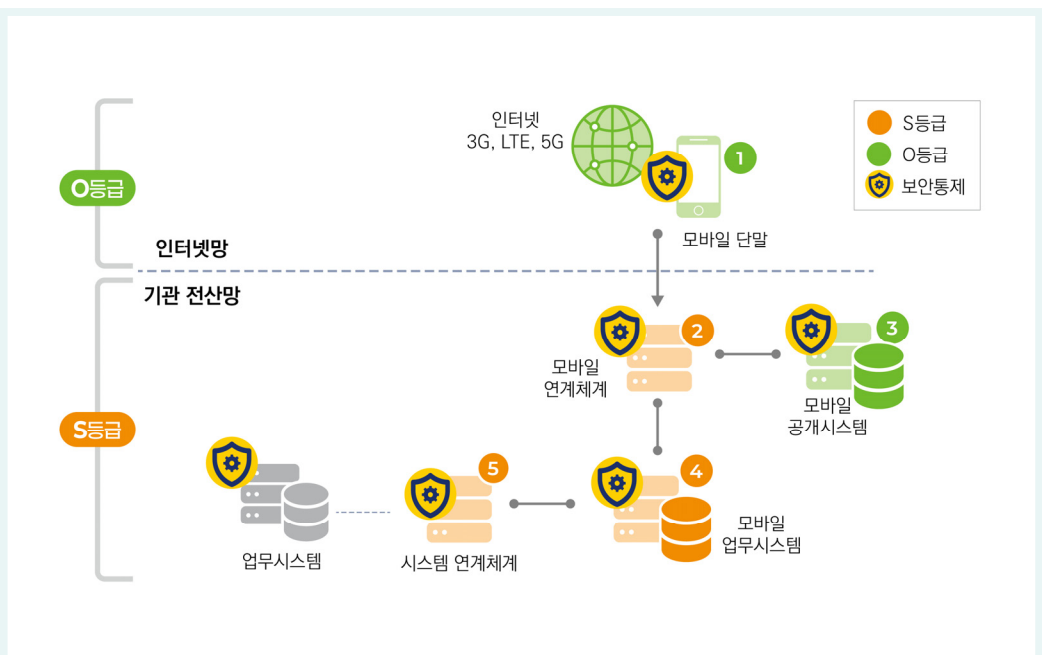
정보서비스 보안위협 식별

1. 정보서비스 구성요소 분석

본 정보서비스 모델은 이동통신망(인터넷망)에 접속한 모바일 단말을 통해 행정업무를 수행하는 환경으로 모바일 연계체계를 통해 내부행정 및 현장행정 업무정보 연계, 공유, 활용 등을 지원한다.

본 정보서비스는 이동통신망(O등급)에 위치한 모바일 단말(O등급)이 기관 전산망에 위치하는 모바일 연계체계(S등급)를 통하여 접근하는 모바일 공개시스템(O등급), 모바일 업무시스템(S등급), 시스템 연계체계(S등급) 및 업무시스템(S등급)으로 구성되며, S·O등급 업무정보를 취급하는 업무수행이 가능하다.

그림 3-2 모바일 업무환경 정보 연계 정보서비스 구성요소 분석



2. 모델링 및 C/S/O 평가

본 정보서비스는 모바일 업무수행 목적 및 단계에 따라 사용 시나리오가 구분되며, 이들에 대해 각각 모델링 및 C/S/O 보안등급을 나눠서 평가할 수 있다.

첫째, 이동통신망 내 이용자 모바일 단말에서 업무수행을 위해 모바일 연계체계에 접속하는 경우는 「위치(이동통신망)-주체(이용자 모바일 단말)-객체(모바일 연계체계)」로 모델링 할 수 있고, 이때 보안등급은 위치 O등급, 주체 O등급 및 객체 S등급으로 평가한다.

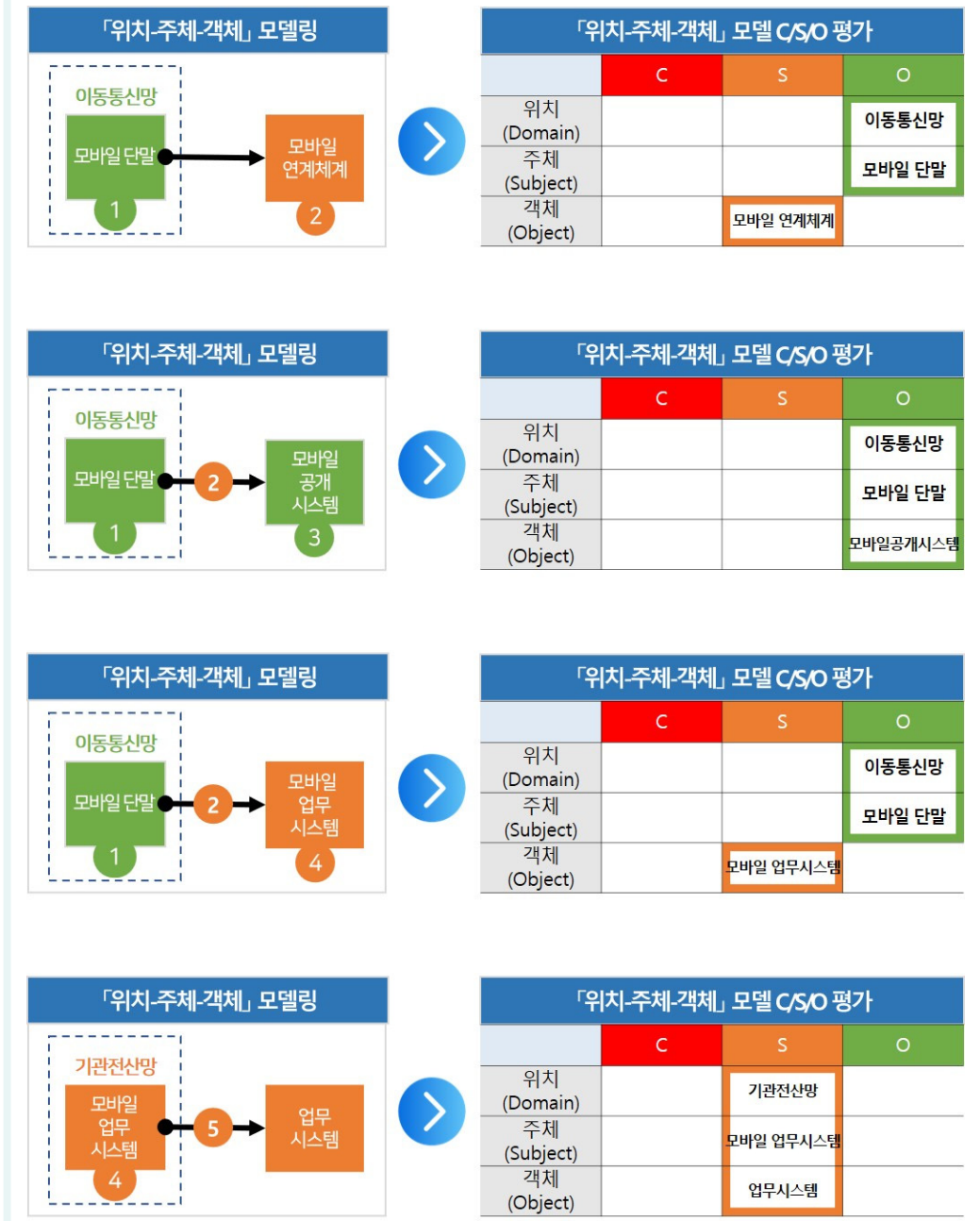
둘째, 모바일 연계체계에 접속한 이용자 모바일 단말에서 공개 정보(O등급) 작성·열람·공유 등을 목적으로 모바일 공개시스템을 활용하는 경우는 「위치(이동통신망)-주체(이용자 모바일 단말)-객체(모바일 공개시스템)」으로 모델링 할 수 있고, 이때 보안등급은 위치 O등급, 주체 O등급 및 객체 O등급으로 평가한다.

셋째, 모바일 연계체계에 접속한 이용자 모바일 단말에서 내부행정 및 현장행정 업무수행 등을 목적으로 모바일 업무시스템을 활용하는 경우는 「위치(이동통신망)-주체(이용자 모바일 단말)-객체(모바일 업무시스템)」으로 모델링 할 수 있고, 이때 보안등급은 위치 O등급, 주체 O등급 및 객체 S등급으로 평가한다.

넷째, 모바일 내부행정 및 현장행정 업무 수행 등을 위해 모바일 업무시스템이 기관 전산망 내 업무시스템과의 정보 연계가 필요한 경우는 「위치(기관전산망)-주체(모바일 업무시스템)-객체(업무시스템)」으로 모델링 할 수 있고, 이때 보안등급은 위치 S등급, 주체 S등급 및 객체 S등급으로 평가한다.

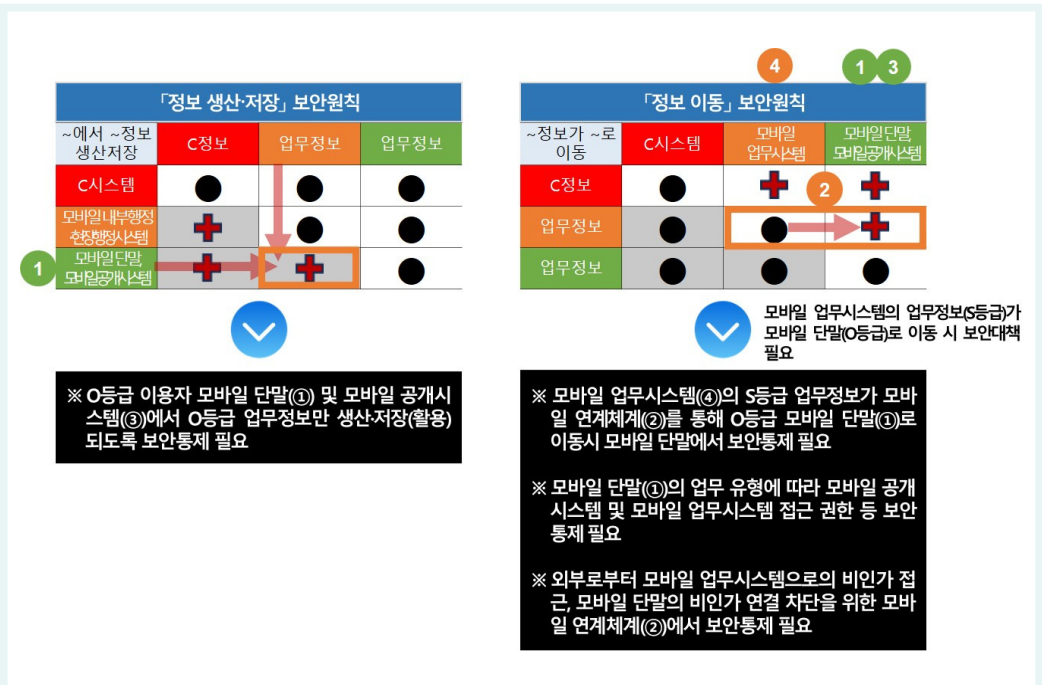
본 해설서는 모바일 업무수행 시 개인 모바일 단말을 활용하는 정보서비스를 대상으로 모델링하여 이용자 모바일 단말을 O등급으로 평가하였으며, 기관에서 지급·관리하는 모바일 업무 전용 단말의 경우 S등급으로 모델링 및 보안등급을 평가할 수 있다.

그림 3-3 「위치-주체-객체」 모델링 및 C/S/O 평가



3. 보안원칙 적용

그림 3-4 보안원칙 적용



가. 「정보 생산·저장」 보안원칙 적용

이동통신망 O등급 영역에 위치한 이용자 단말(모바일 단말)은 O등급이며, 이용자 단말에서 O등급 업무정보의 작성 및 보관은 「정보 생산·저장」 보안원칙에 위배되지 않는다.

그러나, O등급 이용자 단말에서 O등급보다 상위의 업무정보를 생산·저장하는 것은 「정보 생산·저장」 보안원칙에 위배된다. 따라서, O등급 이용자 단말에서는 O등급 보다 상위 업무정보 취급을 위해서는 보안통제를 적용해야 한다.

나. 「정보 이동」 보안원칙 적용

기관 전산망에 위치한 모바일 업무시스템은 S등급이며, 모바일 공개시스템은 O등급이다. 또한, 인터넷 Wi-Fi 또는 이동통신망과 연결된 이용자 단말(모바일 단말)은 O등급이다.

모바일 업무시스템의 S등급 업무정보와 모바일 공개시스템의 O등급 업무정보는 이용자 단말로 전송될 수 있다. 이때, 내부행정 및 현장행정 업무 수행을 위해 S등급 업무정보를 이용자 모바일 단말로 전송하는 것은「정보 이동」보안원칙에 위배된다. 따라서, 이용자 모바일 단말에서 S등급 업무정보를 활용한 내부행정 및 현장행정 업무 수행을 위해서는 보안통제를 적용해야 한다.

이용자 모바일 단말에서 생성한 O등급 정보를 모바일 업무시스템에 전송하는 것과, 모바일 공개시스템의 O등급 정보를 이용자 모바일 단말로 전송하는 것은「정보 이동」보안원칙에 위배되지 않는다. 단, 기관 환경 및 특성에 따라 내부행정·현장행정 업무 수행 시 O등급 정보의 전송·활용에 대한 추가적인 보안통제를 적용할 수 있으며, 이용자 단말의 업무 유형에 따라 모바일 공개시스템 및 모바일 업무시스템에 접근할 때 인증, 접근 권한 확인 등을 위한 보안 통제가 필요하다.

인터넷 Wi-Fi 또는 이동통신망에 위치한 비인가 모바일 단말이 모바일 연계체계를 통해 기관 전산망으로 접근하거나, 권한 외 모바일 업무정보 접근·취급 등을 방지하기 위해 모바일 연계체계에서 보안통제를 적용해야 한다.

4. 보안 위협식별

본 정보서비스 모델은 이용자 단말(①모바일 단말), 모바일 내부행정·현장행정 등 업무 수행 시 정보 중계를 위한 ②모바일 연계체계, 기관 전산망에 위치한 업무 관련 시스템(③모바일 공개시스템, ④모바일 업무시스템, ⑤시스템 연계체계 및 업무시스템)으로 구성되며, 〈표 2-1〉과 같이 정보서비스 모델 구성 대상별 보안 위협을 식별한다.

그림 3-5 **보안위협 대상 식별**

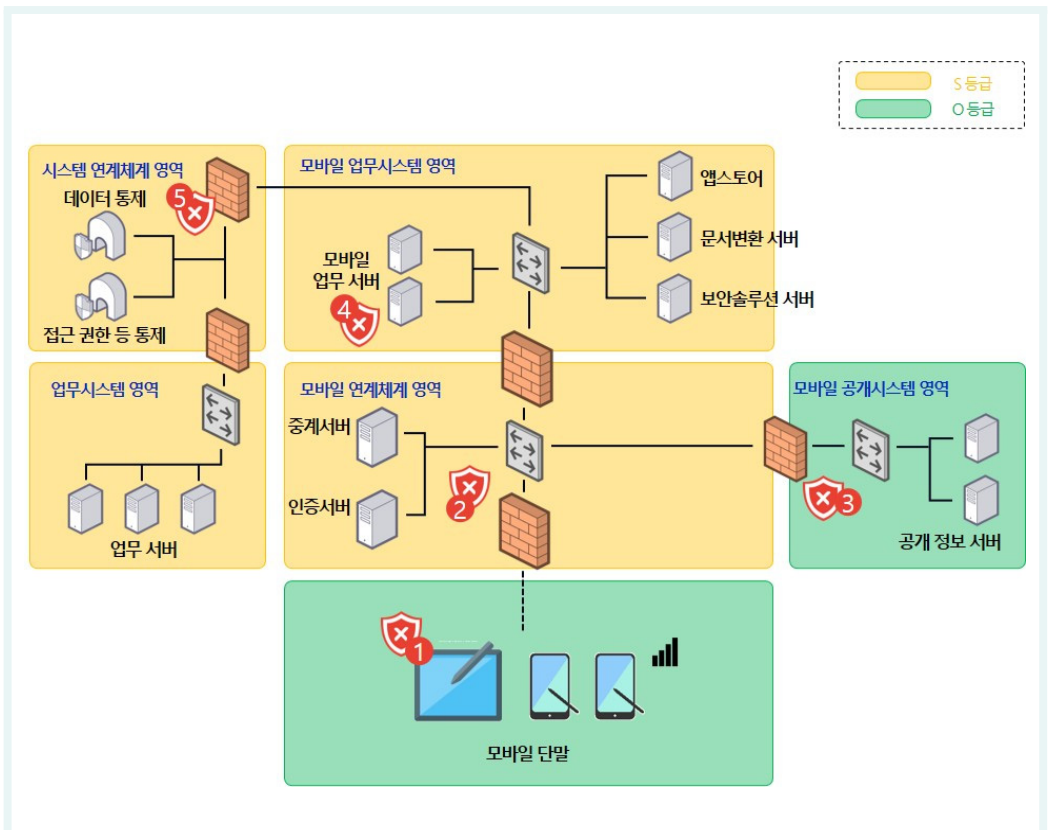


표 3-1 정보서비스 보안위협

대상	구분	보안위협 번호	보안위협 요소
이용자 단말	① 모바일 단말 (스마트폰, 태블릿)	TH-M9-1	안전성이 확인되지 않은 모바일 업무 앱 설치
		TH-M9-2	모바일 단말 악성코드 감염
		TH-M9-3	모바일 OS 변조 및 모바일 업무 앱 위변조
		TH-M9-4	모바일 업무정보 위변조
		TH-M9-5	비인가자의 모바일 업무 단말 사용
		TH-M9-6	모바일 업무정보(첨부파일 포함) 비인가 저장 및 이동·복사
		TH-M9-7	모바일 업무정보 화면캡처 및 출력
		TH-M9-8	모바일 업무 수행 중 비인가 매체 연결
		TH-M9-9	비인가 앱 및 모바일 기능을 통한 모바일 업무정보 접근
		TH-M9-10	모바일 업무 수행 중 업무정보 화면 노출
		TH-M9-11	내부행정·현장행정 업무를 위한 인증 정보 유출
		TH-M9-12	모바일 단말 분실로 인한 모바일 공개·내부행정·현장행정 시스템 비인가 접근
연계 체계	② 모바일 연계체계 ⑤ 시스템 연계체계	TH-M9-13	비인가 단말 접근 및 인증
		TH-M9-14	비인가 및 변조 모바일 업무 앱 접근 및 인증
		TH-M9-15	송수신 데이터 유출
		TH-M9-16	불필요한 세션 유지
		TH-M9-17	단말에 저장할 수 있는 유형의 업무정보 전달
		TH-M9-18	연계체계 우회 등 업무시스템 비인가 접근
		TH-M9-19	관리자 기능 비인가 접근
		TH-M9-20	비인가 매체 연결 및 기능 실행
		TH-M9-21	모바일 연계체계 접근 계정 정보 비인가 접근 및 변경, 정보 유출
모바일 업무용 시스템	③ 모바일 공개시스템 ④ 모바일 업무시스템	TH-M9-22	모바일 업무용 시스템 비인가 접근
		TH-M9-23	모바일 업무용 시스템 비인가 업무정보 접근
		TH-M9-24	모바일 업무용 시스템 비인가 기능 접근
		TH-M9-25	모바일 업무용 시스템 내 업무정보 유출

제3절

보안 요구사항 및 보안대책

기관은 국가 망 보안체계(N2SF) 정보서비스 모델의 안전한 활용을 위해「정보 생산·저장」및「정보 이동」보안원칙을 준수해야 하며, 정보서비스 모델 구성요소 및 연계 지점에서 보안위협을 식별하고 이에 대한 보안대책을 적용해야 한다.

정보서비스 구성요소 분석, 모델링 및 C/S/O 평가, 보안원칙 적용, 보안위협 식별의 과정을 거쳐 식별한 위협에 대한 보안대책 수립 방향성 및 국가·공공기관의 정책적 요구사항을 반영하여 보안 요구사항을 도출하고, 보안 요구사항을 만족하는 N2SF 보안통제 항목을 선정하였다. 각 기관은 모바일 업무환경 구성 및 업무 특성을 고려하여 추가적인 보안 요구사항 및 보안통제 항목을 적용하여 운용할 수 있다.

표 3-2 보안 요구사항 및 보안통제 항목

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
이용자 단말	① 모바일 단말	(TH-M9-1) 안전성이 확인되지 않은 모바일 업무 앱 설치 (TH-M9-2) 모바일 단말 악성코드 감염 (TH-M9-3) 모바일 OS 변조 및 모바일 업무 앱 위변조 (TH-M9-4) 모바일 업무정보 위변조 (TH-M9-5) 비인가자의 모바일 업무 단말 사용 (TH-M9-15) 송수신 데이터 유출	모바일 업무 단말 관리	N2SF-DA-2 N2SF-DA-4 N2SF-DA-5 N2SF-AM-5 N2SF-AM-7 N2SF-IM-5 N2SF-MD-M1

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M9-2) 모바일 단말 악성코드 감염 (TH-M9-3) 모바일 OS 변조 및 모바일 업무 앱 위변조 (TH-M9-14) 비인가 및 변조 모바일 업무 앱 접근 및 인증	모바일 단말 보안성 유지	N2SF-MD-1 N2SF-MD-2 N2SF-MD-3 N2SF-MD-7 N2SF-MD-8 N2SF-MD-9 N2SF-DA-1 N2SF-IN-8 N2SF-IN-16
		(TH-M9-5) 비인가자의 모바일 업무 단말 사용 (TH-M9-15) 송수신 데이터 유출	모바일 단말을 이용한 업무 수행 시 인증	N2SF-DA-3 N2SF-DA-3(1) N2SF-DA-3(2) N2SF-AM-1 N2SF-AM-2 N2SF-AM-3 N2SF-AM-6 N2SF-AM-7 N2SF-AP-1 N2SF-AP-2 N2SF-AU-M1 N2SF-AU-M2 N2SF-MA-2
		(TH-M9-6) 모바일 업무정보(첨부파일 포함) 비인가 저장 및 이동·복사 (TH-M9-7) 모바일 업무정보 화면캡처 및 출력 (TH-M9-8) 모바일 업무 수행 중 비인가 매체 연결 (TH-M9-15) 송수신 데이터 유출	모바일 단말 내 업무정보 유출·저장 방지	N2SF-MD-5 N2SF-MD-6 N2SF-IN-6 N2SF-DV-3 N2SF-DV-4
		(TH-M9-5) 비인가자의 모바일 업무 단말 사용 (TH-M9-9) 비인가 앱 및 모바일 기능을 통한 모바일 업무정보 접근 (TH-M9-10) 모바일 업무 수행 중 업무정보 화면 노출	모바일 업무정보 비인가 접근 및 노출 차단	N2SF-AC-1(4) N2SF-MD-M2 N2SF-DV-8

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M9-11) 내부행정·현장행정 업무를 위한 인증 정보 유출 (TH-M9-21) 모바일 연계체계 접근 계정 정보 비인가 접근 및 변경, 정보 유출	모바일 업무 계정 정보 관리	N2SF-AC-1 N2SF-AC-1(1) N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-2 N2SF-AC-M2 N2SF-IM-1
		(TH-M9-12) 모바일 단말 분실로 인한 모바일 공개·내부행정·현장행정 시스템 비인가 접근	모바일 단말 분실 대책 수립	N2SF-MA-5 N2SF-MD-7 N2SF-MD-M2 N2SF-AC-3(1)
연계 체계	② 모바일 연계 체계 ⑤ 시스템 연계 체계	(TH-M9-1) 안전성이 확인되지 않은 모바일 업무 앱 설치 (TH-M9-3) 모바일 OS 변조 및 모바일 업무 앱 위변조 (TH-M9-13) 비인가 단말 접근 및 인증 (TH-M9-14) 비인가 및 변조 모바일 업무 앱 접근 및 인증	모바일 업무환경 단말 및 앱 인증	N2SF-DA-3 N2SF-DA-3(1) N2SF-DA-3(2) N2SF-MD-9 N2SF-MD-M1
		(TH-M9-5) 비인가자의 모바일 업무 단말 사용	모바일 업무환경 이용자 인증	N2SF-LI-2 N2SF-LI-3 N2SF-LI-4 N2SF-LI-M1 N2SF-MA-2 N2SF-MA-5
		(TH-M9-16) 불필요한 세션 유지 (TH-M9-18) 연계체계 우회 등 업무시스템 비인가 접근 (TH-M9-19) 관리자 기능 비인가 접근 (TH-M9-20) 비인가 매체 연결 및 기능 실행	모바일 연계체계 비인가 접근 차단	N2SF-LP-5 N2SF-LP-M3 N2SF-LP-M4 N2SF-AM-5

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M9-15) 송수신 데이터 유출	모바일 연계체계 업무정보 유출 차단	N2SF-EB-6 N2SF-SN-6 N2SF-SN-M1
		(TH-M9-15) 송수신 데이터 유출 (TH-M9-25) 모바일 업무용 시스템 내 업무정보 유출	시스템 연계체계 데이터 통제	N2SF-IF-1 N2SF-IF-6 N2SF-DU-M3
		(TH-M9-17) 단말에 저장할 수 있는 유형의 업무정보 전달 (TH-M9-23) 모바일 업무용 시스템 비인가 업무정보 접근 (TH-M9-24) 모바일 업무용 시스템 비인가 기능 접근	업무 유형 및 권한에 따른 업무정보 전송	N2SF-DT-1 N2SF-DT-2 N2SF-DT-3 N2SF-IF-8 N2SF-IF-M1 N2SF-IF-M2 N2SF-AC-2
		(TH-M9-18) 연계체계 우회 등 업무시스템 비인가 접근	모바일 단말과 기관 업무시스템의 직접 연결 방지	N2SF-EB-1 N2SF-EB-2 N2SF-EB-3 N2SF-EB-5 N2SF-IF-1 N2SF-IF-9 N2SF-IF-10
		(TH-M9-21) 모바일 연계체계 접근 계정 정보 비인가 접근 및 변경, 정보 유출	모바일 업무환경 계정 정보 관리	N2SF-LI-9 N2SF-IM-2 N2SF-AC-1 N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-3 N2SF-AC-3(1)
		(TH-M9-19) 관리자 기능 비인가 접근	모바일 업무환경 연계체계 시스템 관리자 기능 관리	N2SF-RA-4 N2SF-LP-4
		(TH-M9-15) 송수신 데이터 유출	모바일 업무환경 연계체계 시스템 로그 관리	N2SF-RA-M2 N2SF-EB-M2 N2SF-EB-M3 N2SF-SN-M2

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
모바일 업무용 시스템	③ 모바일 공개 시스템 ④ 모바일 업무 시스템	(TH-M9-15) 송수신 데이터 유출 (TH-M9-25) 모바일 업무용 시스템 내 업무정보 유출	전송 업무정보 저장 방지	N2SF-DU-4 N2SF-DU-M3 N2SF-IN-13
		(TH-M9-23) 모바일 업무용 시스템 비인가 업무정보 접근	모바일 업무 권한 통제	N2SF-LP-1 N2SF-LP-M1 N2SF-LP-M2 N2SF-LP-M3 N2SF-DA-4 N2SF-AU-M1
		(TH-M9-3) 모바일 OS 변조 및 모바일 업무 앱 위변조 (TH-M9-9) 비인가 앱 및 모바일 기능을 통한 모바일 업무정보 접근	모바일 단말 보안기능 제공	N2SF-MD-3 N2SF-MD-7 N2SF-MD-10 N2SF-MD-M2
		(TH-M9-22) 모바일 업무용 시스템 비인가 접근 (TH-M9-23) 모바일 업무용 시스템 비인가 업무정보 접근 (TH-M9-24) 모바일 업무용 시스템 비인가 기능 접근 (TH-M9-25) 모바일 업무용 시스템 내 업무정보 유출	모바일 업무용 시스템 관리자 기능 관리	N2SF-RA-4 N2SF-LP-4
		(TH-M9-22) 모바일 업무용 시스템 비인가 접근 (TH-M9-23) 모바일 업무용 시스템 비인가 업무정보 접근 (TH-M9-24) 모바일 업무용 시스템 비인가 기능 접근 (TH-M9-25) 모바일 업무용 시스템 내 업무정보 유출	모바일 업무용 시스템 로그 관리	N2SF-RA-M2 N2SF-EB-M2 N2SF-EB-M3 N2SF-SN-M2

1. 이용자 단말

O등급 이용자 단말(모바일 단말)로 내부행정·현장행정 업무 수행을 위해서는 모바일 연계체계 접속 시부터 업무 수행 종료 시까지 보안통제가 적용되어야 한다. 다음은 이용자 단말에 적용해야 할 보안 요구사항 및 보안대책이다.

그림 3-6 이용자 및 모바일 단말 인증 체계

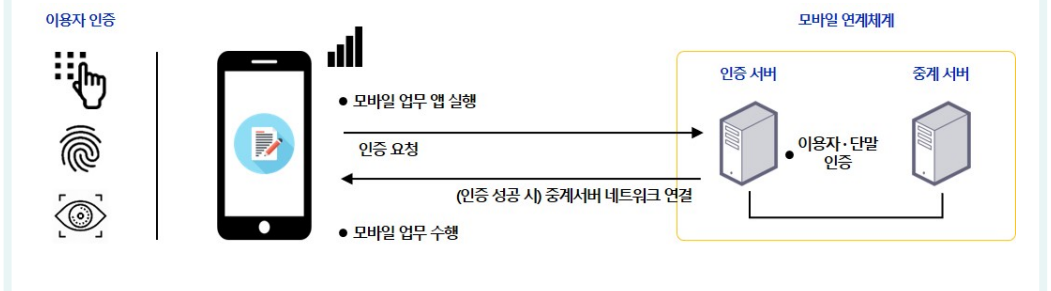
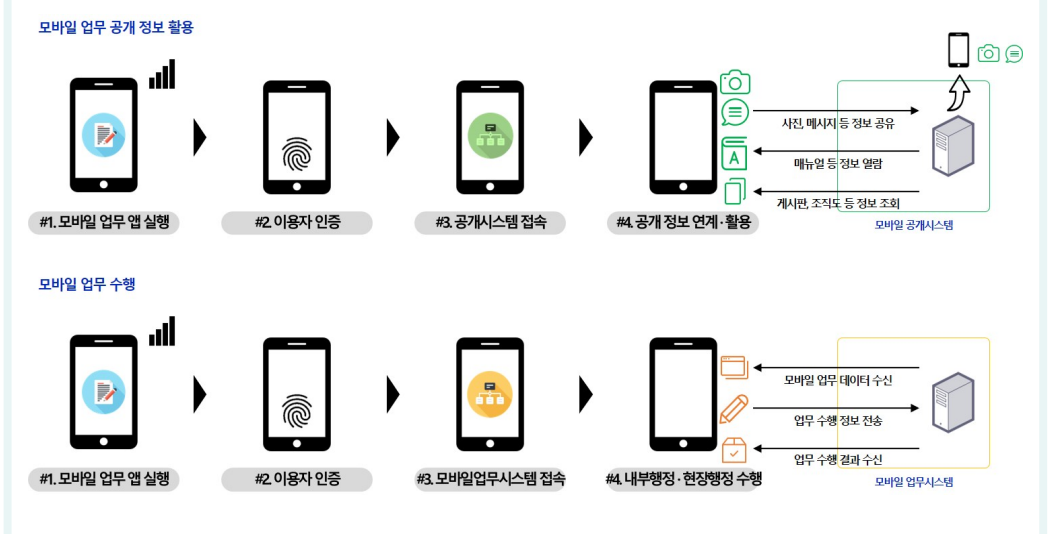


그림 3-7 모바일 업무 수행 시나리오(예) – 모바일 공개시스템(O등급) 및 모바일 업무시스템(S등급 이상)



이용자 모바일 단말은 모바일 업무환경 운영 절차를 통해 사용자·단말 인증 및 보안 조치가 완료된 모바일 단말로 S등급 이상의 내부·현장행정 업무는 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

① 모바일 업무 단말 관리

이용자 모바일 단말은 기관 전산망 내에 존재하는 인증·통제시스템을 통해 모바일 내부행정 및 현장행정 업무 수행을 사전에 승인·등록 후, 업무 유형별 모바일 업무 앱 및 보안기능 설치 등의 보안조치가 완료되어야 한다.

이용자 모바일 단말은 행정안전부가 제공하는 모바일 공통기반 또는 자체 구축한 모바일 플랫폼에서 운용·관리해야 한다.

② 「모바일 단말」 보안성 유지

내부행정·현장행정 업무 수행을 위한 이용자 모바일 단말에 대해 모바일용 보안제품 등을 활용하여 보안성을 확보하여야 한다.

모바일 단말 내 다른 앱 및 기능 등을 통해 업무정보 무단 접근을 방지하기 위해 모바일 가상화 플랫폼을 이용하여 업무를 수행해야 한다.

구분	단말 유형	주요 보안대책
내부행정	개인단말	• 모바일 OS 보호 • 앱 위변조 방지 • 악성코드 대응 • 감사 및 모니터링 • 단말 잠금 및 사용자 인증 • 매체제어 및 우회통신 연결 차단
현장행정	전용단말	• 모바일 OS 보호 • 앱 위변조 방지 • 악성코드 대응 • 감사 및 모니터링 • 단말 잠금 및 사용자 인증 • 매체제어 및 우회통신 연결 차단 • 비인가 소프트웨어 통제

③ 「모바일 단말」을 이용한 업무 수행 시 인증

비인가자의 모바일 단말 사용 및 모바일 단말 내 내부행정·현장행정 앱 실행을 방지하기 위해, 이용자 모바일 단말 잠금 해제 및 모바일 업무 앱 실행 시 사용자 인증을 수행해야 한다.

모바일 업무 앱 실행 시 사용자 인증은 모바일 연계체계 인증 서버에서 수행할 수 있으며, 자동 로그인은 차단한다.

④ 「모바일 단말」 내 업무정보 유출·저장 방지

내부행정·현장행정 업무 수행 중 모바일 연계체계 중계 서버를 통해 수신한 S등급 업무정보의 이용자 모바일 단말 저장을 방지하기 위해 업무정보 이동·복사, 화면 캡처·출력, 비인가 매체 연결 금지 및 무선랜(WiFi)·블루투스 등 우회통신이 가능한 매체를 차단해야 하며, 모바일 업무 종료 시 임시 저장된 자료를 포함하여 모든 업무정보를 삭제해야 한다.

또한, 이용자 모바일 단말과 중계 서버 간 통신 과정 중 업무정보 유출을 방지하기 위한 보안대책을 적용해야 한다.

⑤ 모바일 업무정보 비인가 접근 및 노출 차단

모바일 업무 수행 중 일정 시간 이상 활동이 없는 경우 모바일 단말 화면을 통한 업무정보 노출을 차단하기 위해 보안대책을 적용해야 한다.

또한, 이용자 모바일 단말을 통한 내부행정·현장행정 업무 수행 중 모바일 단말 내 다른 앱 및 기능을 통한 업무정보 무단 접근을 차단해야 한다.

다만, 기관의 모바일 업무 특성을 고려하여 모바일 공개시스템을 통해 수신한 정보 및 모바일 단말 내 다른 앱·기능 등을 통해 생성한 사진, 영상 등 업무에 필요한 정보는 업무 수행 시 활용할 수 있다.

⑥ 모바일 업무 계정 정보 관리

내부행정·현장행정 업무 수행을 위한 계정 정보는 기관 업무시스템 계정 정보와 분리하여 관리되어야 하며, 모바일 업무 수행을 위한 인증 정보는 유출되지 않도록 관리해야 한다.

⑦ 「모바일 단말」 분실 대책 수립

모바일 단말 분실로 인한 정보 유출을 방지하기 위해 모바일 업무 앱 및 업무정보 원격 삭제 등 분실 대책을 수립·운영해야 한다.

기관은 위와 같은 보안 요구사항 및 〈표 3-3〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 3-3 이용자 모바일 단말 보안통제 항목

코드	보안통제 항목	내용
① 모바일 업무 단말 관리		
N2SF-DA-2	정보서비스 식별 및 제한	• 인증절차를 통해 사전 승인한 정보서비스만을 활용하도록 제한한다.
N2SF-DA-4	인증된 단말의 접속 관리	• 인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근 권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.
N2SF-DA-5	외부 단말 접속 제어	• 외부에서 접근하는 단말은 보안 VPN, MFA, 장치검증 등 추가 보안 절차를 거쳐서만 제한된 자원에 접근하도록 구성한다.
N2SF-AM-5	인증수단 보호	• 정보시스템의 보안수준에 준하여 인증수단을 보호한다.
N2SF-AM-7	캐시된 인증수단 재사용 차단	• 캐시된 인증수단이 세션 유효 시간이 만료된 이후에 재사용되는 것을 차단한다.
N2SF-IM-5	속성 유지관리 및 보호	• 안전하게 보호조치가 된 저장소에서 고유하게 식별된 각 개인, 그룹, 장치 또는 서비스에 대한 속성을 유지하고 보호한다.
N2SF-MD-M1	장비 식별 및 사용자 연동 관리	• 모바일 장치 고유 ID와 사용자 계정을 연동하여 통합 식별 및 통제를 수행한다.
② 모바일 단말 보안성 유지		
N2SF-MD-1	모바일 코드 다운로드 및 실행 금지	• 허용되지 않은 모바일 코드 다운로드 및 실행을 금지한다.
N2SF-MD-2	자동 실행 금지	• 응용프로그램에서 모바일 코드의 자동 실행을 방지한다.
N2SF-MD-3	제한된 환경에서의 실행	• 모바일 코드를 제한된 환경(가상머신 등)에서만 실행하도록 제한한다.
N2SF-MD-7	탈옥·루팅 탐지 및 차단	• 루팅 또는 탈옥된 모바일 기기의 접근을 탐지하고 차단한다.
N2SF-MD-8	블루투스·USB 제어 설정 모바일 장치 암호화 기술	• 블루투스, USB 등 외부 입출력 통신 기능을 제어하고 정책에 따라 허용한다.
N2SF-MD-9	비인가 앱 탐지 및 차단	• 관리자가 승인하지 않은 앱이 설치되거나 실행되면 알림 및 차단한다.
N2SF-DA-1	단말 무결성 검증	• 단말 내 신뢰 가능한 모듈(TPM 등)을 통한 구성정보(BIOS 설정정보, Disk 설치 정보 등) 등을 확인한다.
N2SF-IN-8	비인가 소프트웨어 실행 차단	• 허가되지 않은 소프트웨어(응용프로그램)가 실행되지 않도록 차단한다.
N2SF-IN-16	악성코드 감염 차단	• 악성코드 유입 및 실행 등으로 인한 악성코드 감염을 실시간 탐지하고 차단한다.

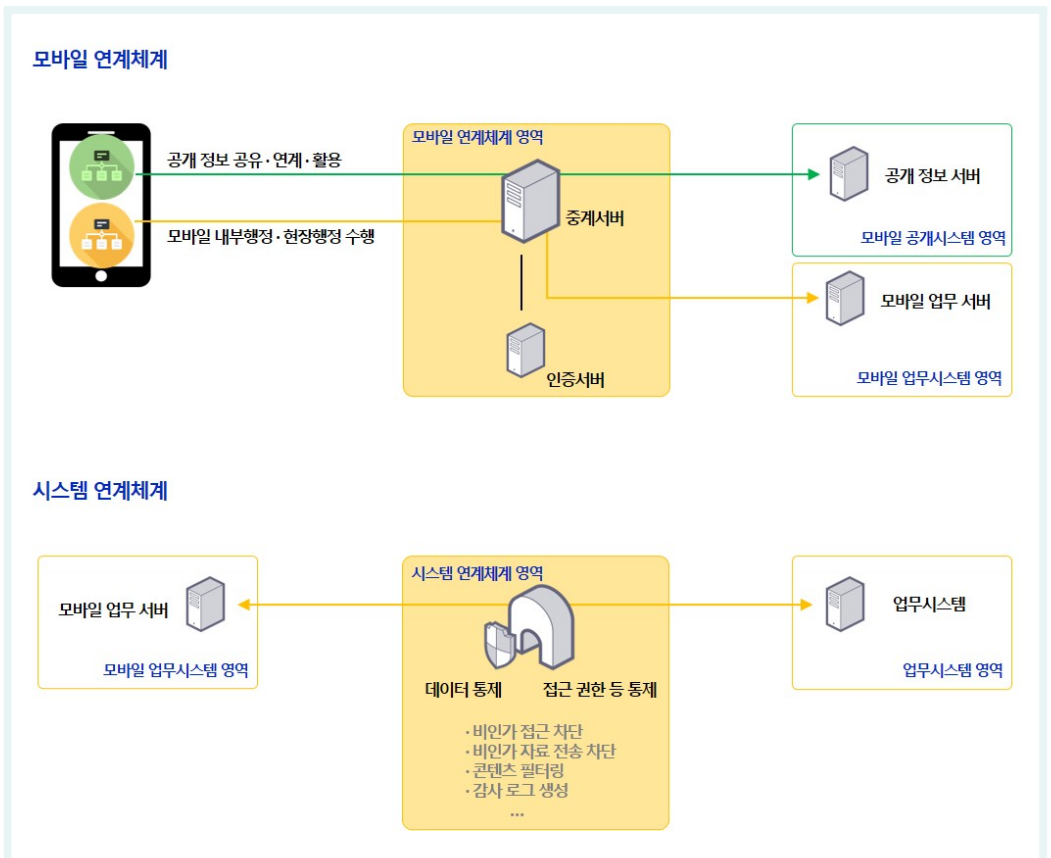
코드	보안통제 항목	내용
③ 모바일 단말을 이용한 업무 수행 시 인증		
N2SF-DA-3	단말 식별 및 인증	• 단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증을 통해 시스템에 접근할 수 있도록 한다.
N2SF-DA-3(1)	인가 단말 인증	• 조직 내 등록되어 인가된 단말에 한해 인증 수단(디지털 인증서, 장치지문 등)을 통해 접근을 허용한다.
N2SF-DA-3(2)	비인가 단말 인증	• 등록되지 않았거나 보안 기준을 충족하지 못한 단말은 인증 요청을 차단하거나 별도 네트워크 구역으로 격리한다.
N2SF-AM-1	암호모듈 기반 인증	• 관련 법규, 정책 및 규정 등을 준수한 암호모듈 인증체계를 적용한다.
N2SF-AM-2	비밀번호 기반 인증	• 숫자·문자·특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.
N2SF-AM-3	공개키 기반 인증	• 신뢰할 수 있는 인증 기관(CA)을 통해 발급된 인증서의 유효성을 검증하고, 인증서의 발급, 갱신, 폐지 등을 관리한다.
N2SF-AM-6	암호화 되지 않은 인증수단 내장 금지	• 암호화되지 않은 인증수단이 응용프로그램 또는 스크립트 등에 내장되거나 기능키 등에 삽입되지 않아야 한다.
N2SF-AM-7	캐시된 인증수단 재사용 차단	• 캐시된 인증수단이 세션 유효 시간이 만료된 이후에 재사용되는 것을 차단한다.
N2SF-AP-1	기관 발급 증명수단 인증 활용	• 기관에서 발급한 자격 증명수단(모바일 공무원증 등)을 활용하여 사용자를 인증한다.
N2SF-AP-2	인증 프로파일 활용	• 사용자의 직무나 역할에 따라 인증 기준을 정하고, 그에 맞게 관리한다.
N2SF-AU-M1	인증 정보 접근 권한 통제 및 관리	• 인증 정보는 최소한의 인원만 접근할 수 있도록 제한하고 기록을 남긴다.
N2SF-AU-M2	인증 위협 및 취약점 관리	• 인증 관련 취약점을 점검하고 위협 대응 방안을 마련해 운영한다.
N2SF-MA-2	사용자 계정 다중요소 인증 (MFA, Multi-factor Authentication)	• 지정되지 않은 접속 경로 또는 사전 승인되지 않은 단말을 통한 사용자 계정에 대해 다중요소 인증을 적용한다.
④ 모바일 단말 내 업무정보 유출·저장 방지		
N2SF-MD-5	모바일 장치 암호화 기술	• 모바일 장비 저장공간 암호화 또는 컨테이너 기반 저장공간 분리 및 암호화를 적용한다.
N2SF-MD-6	데이터 자동삭제 또는 초기화	• 특정 상황 또는 조건에 따라 단말 내부에 저장된 데이터를 자동 삭제하거나 초기화한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.

코드	보안통제 항목	내용
N2SF-DV-3	하드웨어 장치(device) 사용 제한	• 정보자산 배포 또는 설치 전 특정 하드웨어 장치(USB포트, 무선통신 모듈 등)를 비활성화 또는 제거 등으로 사용을 제한한다.
N2SF-DV-4	포트 및 입출력 장치 제어	• 정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.
⑤ 모바일 업무정보 비인가 접근 및 노출 차단		
N2SF-AC-1(4)	계정 자동 로그아웃	• 비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.
N2SF-MD-M2	정책 위반 자동 조치	• 정책 위반 시 자동으로 앱 차단, 로그아웃, 초기화 등 사전 정의된 조치를 수행한다.
N2SF-DV-8	장치 자동 잠금	• 사용자가 일정시간 이상 정보시스템을 사용하지 않거나 방치할 경우 잠금 기능을 활성화하고, 화면에 표시되는 정보는 표출되지 않아야 한다.
⑥ 모바일 업무 계정 정보 관리		
N2SF-AC-1	계정 관리 자동화	• 정보시스템 계정 관리를 효율화하고, 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정 관리를 수행한다.
N2SF-AC-1(1)	동적 계정 관리	• 사용자 상태(입사, 퇴사, 부서 이동 등)에 따라 계정 정보를 실시간으로 반영하고, 시스템 간 계정 동기화를 통해 계정 수명주기 관리를 자동화한다.
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-1(3)	계정 자동 비활성화	• 계정 사용 기간이 종료되거나 일정 기간 미사용된 계정은 자동으로 비활성화한다.
N2SF-AC-2	공유 및 그룹 계정 사용 제한	• 공유 및 그룹 계정 사용은 필요한 경우로 제한하며, 가능하면 개인별 계정 사용을 권장한다.
N2SF-AC-M2	감사기록 생성	• 계정 활동에 대한 감사 기록을 생성하여 보관하고 분석할 수 있도록 한다.
N2SF-IM-1	공개된 식별자의 계정 사용 금지	• 정보시스템 계정 식별자로 개인의 공개된 식별자 사용을 금지한다.
⑦ 모바일 단말 분실 대책 수립		
N2SF-MA-5	특정상황에서의 다중요소 인증	• 특정 상황 또는 조건에서는 다중요소 인증을 적용하여 사용자를 인증한다.
N2SF-MD-6	데이터 자동삭제 또는 초기화	• 특정 상황 또는 조건에 따라 단말 내부에 저장된 데이터를 자동 삭제하거나 초기화한다.
N2SF-MD-M2	정책 위반 자동 조치	• 정책 위반 시 자동으로 앱 차단, 로그아웃, 초기화 등 사전 정의된 조치를 수행한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.

2. 모바일 업무환경 연계체계

이용자 모바일 단말은 모바일 연계체계 중계서버를 통해 모바일 업무시스템(내부행정·현장행정 등) 및 모바일 공개시스템에서 제공하는 정보를 기반으로 모바일 업무를 수행할 수 있다. 또한, 시스템 연계체계를 통해 기관 업무시스템에 존재하는 업무정보를 모바일 업무시스템에 연계하여 모바일 업무를 수행할 수 있다.

그림 3-8 모바일 업무환경 연계체계



사전 승인받은 이용자 모바일 단말은 인증 절차 후 모바일 연계체계 중계서버를 통해 내부행정·현장행정 업무 수행 및 공개 정보 활용을 할 수 있으며, 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

① 모바일 업무환경 단말 및 앱 인증

내부행정·현장행정 등 모바일 업무 수행을 위해 사전 승인받은 모바일 단말 및 모바일 업무 앱에 대한 인증을 수행한다.

비인가 단말 및 비인가·변조 모바일 앱의 인증 요청은 차단하고, 해당 요청은 중계시스템에서도 차단하도록 통제한다.

② 모바일 업무환경 이용자 인증

모바일 업무 수행을 위한 이용자 인증을 수행한다. 이용자 인증은 모바일 업무 수행을 위한 사전 승인 시 등록한 정보를 통해 수행한다.

반복적인 이용자 인증 요청, 일정 횟수 이상 인증 실패, 다중 사용자 인증 등의 경우 해당 이용자 계정은 잠금상태로 전환하여, 관리자를 통한 계정 잠금 해제 절차를 수행한다.

또한, 이용자 모바일 단말 위치를 확인하여, 필요시 추가적인 사용자 인증 절차를 수행할 수 있다.

③「모바일 연계체계」 비인가 접근 차단

내부행정·현장행정 및 공개 정보 활용 등 모바일 업무 수행을 위해 사전 승인받은 모바일 단말 및 모바일 업무 앱이 아닌 비인가 단말 및 비인가·변조 모바일 앱의 모바일 업무환경 연계체계 접근을 차단해야 한다.

또한, 인증·통제시스템을 통해 인증을 수행하지 않은 모바일 단말 및 앱의 접속을 차단해야 한다.

④「모바일 연계체계」 업무정보 유출 차단

내부행정·현장행정 업무 수행을 위해 이용자 모바일 단말에 전송하는 업무정보의 통신 과정 유출 방지를 위한 보안대책을 적용하고, 일정 시간 이상 업무 수행을 하지 않는 모바일 단말과의 세션은 차단해야 한다.

⑤「시스템 연계체계」 데이터 통제

모바일 업무시스템을 통해 내부행정·현장행정 등 업무 수행 시 데이터 및 접근 권한 등에 대한 통제를 수행해야 한다.

⑥ 업무 유형 및 권한에 따른 업무정보 전송

모바일 업무환경 연계체계는 인증·통제시스템을 통해 설정된 업무 유형 및 접근 권한에 따라 모바일 내부행정·현장행정 시스템의 업무정보를 중계해야 한다.

⑦「모바일 단말」과 기관「업무시스템」의 직접 연결 방지

이용자 모바일 단말과 기관 내 내부행정·현장행정·공개 정보 활용을 위한 모바일 업무용 시스템의

직접 연결이 아닌, 연계체계를 통한 간접 연결을 통해 업무 수행을 위한 각종 정보 요청 및 응답에 대한 흐름을 통제해야 한다.

⑧ 모바일 업무환경 계정 정보 관리

인증·통제시스템 내 모바일 업무환경 이용자 계정 정보의 비인가 접근, 비인가 정보 변경 등을 통제해야 한다.

⑨ 모바일 업무환경「연계체계」시스템 관리자 기능 관리

모바일 업무환경 연계체계 시스템에 대한 관리자 접속 기록(관리자 ID, 접속 시간, 접속 단말 정보 등), 작업 이력 등을 로그로 저장·관리해야 한다. 로그에 대한 접근 권한은 정보보안담당자(관)으로 최소화하며, 임의로 변경, 삭제되지 않도록 해야 한다.

또한, 중계시스템에 대한 매체 연결, 기능 실행·중지에 대한 로그도 저장·관리해야 한다.

⑩ 모바일 업무환경「연계체계」시스템 로그 관리

모바일 업무환경 연계체계 시스템에 대한 이용자 모바일 단말 접속 기록(이용자 ID, 접속 시간, 업무 유형, 요청 경로 등), 데이터 처리 내역, 요청 및 응답 내역 등을 로그로 저장·관리해야 한다. 로그에 대한 접근 권한은 정보보안담당자(관)으로 최소화하며, 임의로 변경, 삭제되지 않도록 해야 한다.

기관은 위와 같은 보안 요구사항 및 〈표 3-4〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 3-4 모바일 업무환경 연계체계 보안통제 항목

코드	보안통제 항목	내용
① 모바일 업무환경 단말 및 앱 인증		
N2SF-DA-3	단말 식별 및 인증	• 단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증을 통해 시스템에 접근할 수 있도록 한다.
N2SF-DA-3(1)	인가 단말 인증	• 조직 내 등록되어 인가된 단말에 한해 인증 수단(디지털 인증서, 장치지문 등)을 통해 접근을 허용한다.
N2SF-DA-3(2)	비인가 단말 인증	• 등록되지 않았거나 보안 기준을 충족하지 못한 단말은 인증 요청을 차단하거나 별도 네트워크 구역으로 격리한다.
N2SF-MD-9	비인가 앱 탐지 및 차단	• 관리자가 승인하지 않은 앱이 설치되거나 실행되면 알림 및 차단한다.
N2SF-MD-M1	장비 식별 및 사용자 연동 관리	• 모바일 장치 고유 ID와 사용자 계정을 연동하여 통합 식별 및 통제를 수행한다.

코드	보안통제 항목	내용
② 모바일 업무환경 이용자 인증		
N2SF-LI-2	로그인 실패에 따른 접속 제한	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.
N2SF-LI-3	로그인 실패에 따른 인증요소 추가	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 추가 인증수단(생체인증, OTP, ARS 등)을 적용한다.
N2SF-LI-4	계정 잠금 해제 인증요소 추가	• 계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.
N2SF-LI-M1	로그인 실패 모니터링 및 보고	• 반복 실패, 의심 로그인 시도 등의 실패 패턴을 실시간 감지하고 관리자에게 보고한다.
N2SF-MA-2	사용자 계정 다중요소 인증 (MFA, Multi-factor Authentication)	• 지정되지 않은 접속 경로 또는 사전 승인되지 않은 단말을 통한 사용자 계정에 대해 다중요소 인증을 적용한다.
N2SF-MA-5	특정상황에서의 다중요소 인증	• 특정 상황 또는 조건에서는 다중요소 인증을 적용하여 사용자를 인증한다.
③ 모바일 연계체계 비인가 접근 차단		
N2SF-LP-5	코드 실행권한 제한	• 코드는 필요한 권한으로만 실행되도록 제한하고, 사용자 권한으로 실행되는 코드가 관리자 영역으로 접근되지 않도록 차단한다.
N2SF-LP-M3	접근권한 사전 설정	• 기본적으로 필요 최소한의 권한만을 부여하는 사전 권한 설정 기준을 마련하고 운영한다.
N2SF-LP-M4	접근권한과 정보 연계	• 접근권한 부여 시 정보 접근 범위를 명확히 연계하여 통제하며, 불필요한 정보 접근을 차단한다.
N2SF-AM-5	인증수단 보호	• 정보시스템의 보안수준에 준하여 인증수단을 보호한다.
④ 모바일 연계체계 업무정보 유출 차단		
N2SF-EB-6	외부로의 사이버위협 통신 발신 제한	• 내부에서 외부 네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단하고, 발신자(사용자 및 정보자산 등)를 식별한다.
N2SF-SN-6	네트워크 연결 해제	• 정상 세션 종료 또는 일정 시간 비활성 상태가 유지될 경우 네트워크 연결을 자동 해제한다.
N2SF-SN-M1	세션 관리 정책 수립	• 세션 유지 시간, 비활성화 조건, 동시 접속 허용 수 등 세션 운용 정책을 수립하고 문서화한다.
⑤ 시스템 연계체계 데이터 통제		
N2SF-IF-1	정보흐름의 동적 통제	• 정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.
N2SF-IF-6	필터링 규칙 정보흐름 통제	• 보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.
N2SF-DU-M3	데이터 사용 정책 수립	• 데이터의 사용 목적, 접근 권한, 보존 기간, 폐기 절차 등을 포함하는 데이터 사용 정책을 문서화하고 전사적으로 적용 및 관리한다.

코드	보안통제 항목	내용
⑥ 업무 유형 및 권한에 따른 업무정보 전송		
N2SF-DT-1	전송 권한 확인	• 데이터가 전송되기 전에 이를 처리하는 개인이나 정보시스템이 적절한 권한을 보유하고 있는지 확인한다.
N2SF-DT-2	정보교환 중단	• 정보교환 대상 정보시스템 등에 대한 식별 및 통제가 확인되지 않을 경우 정보교환을 중단한다.
N2SF-DT-3	전송간 암호화 적용	• 물리적 보안수단에 의해 전송 간 보호되지 않는 경우 전송 구간에 대한 암호기술을 적용한다.
N2SF-IF-8	인가되지 않은 정보 전송 통제	• 인가되지 않은 정보가 포함되었는지 검사하고 보안정책에 따라 해당 정보의 전송을 차단한다.
N2SF-IF-M1	정보흐름 통제 정책 수립 및 갱신	• 정보 흐름에 대한 통제 기준 및 예외 절차를 문서화하고 정기적으로 갱신한다.
N2SF-IF-M2	정보흐름 로그 기록 및 보존	• 정보 흐름 통제 활동(허용/차단 등)을 로깅하고, 법적/감사 목적으로 일정 기간 보관한다.
N2SF-AC-2	공유 및 그룹 계정 사용 제한	• 공유 및 그룹 계정 사용은 필요한 경우로 제한하며, 가능하면 개인별 계정 사용을 권장한다.
⑦ 모바일 단말과 기관 업무시스템의 직접 연결 방지		
N2SF-EB-1	연결 접점 제한	• 정보시스템의 외부 네트워크 연결 접점 수를 제한한다.
N2SF-EB-2	서비스별 외부 통신 통제	• 외부와 통신하는 서비스의 경계마다 통신흐름을 통제한다.
N2SF-EB-3	화이트리스트 기반 통신 허용	• 기본적으로 모든 통신을 차단한 상태에서 필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용한다.
N2SF-EB-5	통신 경유(proxy) 강제화	• 인가된 정보시스템을 경유하여 통신하도록 통신경로를 강제화한다.
N2SF-IF-1	정보흐름의 동적 통제	• 정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	• 정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.
N2SF-IF-10	정보 전송 방식 제한	• 정보 전송 시 특정 매체나 방식만 허용하고 나머지는 차단한다.
⑧ 모바일 업무환경 계정 정보 관리		
N2SF-LI-9	계정 정보 변경 알림	• 로그인(사용자 인증 성공) 후 사용자 계정 관련 정보 변경 이력이 존재하는 경우, 일정 기간동안 사용자에게 해당 내용 알림을 표시한다.
N2SF-IM-2	사용자 상태 식별	• 개인과 조직의 구별, 사용자 상태(활성, 비활성, 임시계정 등)를 식별하고 관리한다.
N2SF-AC-1	계정 관리 자동화	• 정보시스템 계정 관리를 효율화하고, 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정 관리를 수행한다.

코드	보안통제 항목	내용
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.
⑨ 모바일 업무환경 연계체계 시스템 관리자 기능 관리		
N2SF-RA-4	관리자 권한 통제	• 원격접속을 통한 관리자 권한은 제한된 조건에서만 허용해야 하며, 관리자 권한으로 실행한 명령어 이력 등은 유지한다.
N2SF-LP-4	관리자 권한 제한	• 정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.
⑩ 모바일 업무환경 연계체계 시스템 로그 관리		
N2SF-RA-M2	원격접속 로그 보존 및 감사	• 원격접속 활동 기록을 수집하여 정기 감사가 가능하도록 보존한다.
N2SF-EB-M2	외부 경계 정책 수립 및 갱신	• 외부 통신 및 경계 보안 정책을 수립하고 주기적으로 갱신한다.
N2SF-EB-M3	외부 통신 로그 기록 및 감사	• 외부 통신 활동과 설정 변경 사항을 기록하고 감사 가능하게 한다.
N2SF-SN-M2	세션 감사 및 로그 기록	• 세션 생성, 종료, 중복, 충돌 등 관련 활동을 로깅하고 보안 감사가 가능하도록 구성한다.

3. 모바일 업무 시스템

이용자 모바일 단말은 내부행정·현장행정 업무 수행 및 공개 정보 활용을 위해 모바일 연계체계를 경유하여 모바일 업무시스템 및 공개시스템에 접근한다. S등급 이상의 업무정보를 처리하는 모바일 업무시스템은 이용자 모바일 단말에 대한 보안성 제공 및 업무정보 유출 방지와 관련한 보안관리를 수행해야 하며, 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

① 전송 업무정보 저장 방지

모바일 연계체계를 통해 전달되는 내부행정·현장행정 업무 자료의 이용자 모바일 단말 저장 및 정보 유출을 방지하기 위해 VMI 환경 제공, 스트리밍 전송 방식 등을 통해 모바일 단말로의 직접적 데이터 송·수신을 통제하거나, 암호화된 파일 전송 후 모바일 업무 앱에서만 열람 및 삭제되도록 통제해야 한다.

단, 모바일 단말을 현장행정 등을 위한 전용 단말로 운용하거나 S등급 업무정보 연계가 없는 현장 생성 정보, 모바일 공개시스템의 업무정보 등의 경우, 필요시 저장 가능한 유형의 정보를 이용자 모바일 단말로 전송할 수 있다.

② 모바일 업무 권한 통제

이용자의 모바일 업무 유형에 따라 내부행정, 현장행정 등 업무정보의 접근을 통제해야 한다.

③ 모바일 단말 보안기능 제공

모바일 업무환경을 위한 모바일 단말 관리 솔루션(MDM), 사용자 입력 정보 키로깅 방지, 모바일 업무 앱 보안 업데이트 등 보안 기능을 제공해야 한다.

④ 모바일 업무용 시스템 관리자 기능 관리

모바일 업무시스템 및 공개시스템에 대한 관리자 접속 기록(관리자 ID, 접속 시간, 접속 단말 정보 등), 작업 이력 등을 로그로 저장·관리해야 한다. 로그에 대한 접근 권한은 정보보안담당자(관)으로 최소화하며, 임의로 변경, 삭제되지 않도록 해야 한다.

또한, 모바일 업무시스템 및 공개시스템에 대한 매체 연결, 기능 실행·중지에 대한 로그도 저장·관리해야 한다.

⑤ 모바일 업무용 시스템 로그 관리

모바일 업무시스템 및 공개시스템에 대한 이용자 접근 기록(이용자 ID, 이용자 단말 및 앱 정보, 인증 요청 시간, 인증 요청 위치 등), 데이터 처리 내역, 요청 및 응답 내역 등을 로그로 저장·관리해야 한다. 로그에 대한 접근 권한은 정보보안담당자(관)으로 최소화하며, 임의로 변경, 삭제되지 않도록 해야 한다.

기관은 위와 같은 보안 요구사항 및 〈표 3-5〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 3-5 모바일 업무용 시스템 보안통제 항목

코드	보안통제 항목	내용
① 전송 업무정보 저장 방지		
N2SF-DU-4	데이터 갱신 및 삭제	• 필요 시 데이터를 갱신하거나 생성하여 사용하고, 필요 목적이 종료되면 데이터는 삭제한다.
N2SF-DU-M3	데이터 사용 정책 수립	• 데이터의 사용 목적, 접근 권한, 보존 기간, 폐기 절차 등을 포함하는 데이터 사용 정책을 문서화하고 전사적으로 적용 및 관리한다.

코드	보안통제 항목	내용
N2SF-IN-13	정보의 비지속성	• 정보시스템이 종료되거나 재부팅될 때 관련 정보(데이터 등)는 자동 삭제하여 유지되지 않도록 한다.
② 모바일 업무 권한 통제		
N2SF-LP-1	정보시스템 접근 권한 정의	• 업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.
N2SF-LP-M1	특별권한 사용자 지정	• 일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.
N2SF-LP-M2	주요 사용자 위험 관리	• 주요 사용자의 권한과 활동을 모니터링하고 이상 징후를 탐지하여 위험을 사전에 관리한다.
N2SF-LP-M3	접근권한 사전 설정	• 기본적으로 필요 최소한의 권한만을 부여하는 사전 권한 설정 기준을 마련하고 운영한다.
N2SF-DA-4	인증된 단말의 접속 관리	• 인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근 권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.
N2SF-AU-M1	인증 정보 접근 권한 통제 및 관리	• 인증 정보는 최소한의 인원만 접근할 수 있도록 제한하고 기록을 남긴다.
③ 모바일 단말 보안기능 제공		
N2SF-MD-3	제한된 환경에서의 실행	• 모바일 코드를 제한된 환경(가상머신 등)에서만 실행하도록 제한한다.
N2SF-MD-7	탈옥·루팅 탐지 및 차단	• 루팅 또는 탈옥된 모바일 기기의 접근을 탐지하고 차단한다.
N2SF-MD-10	위치 기반 보안 정책	• 단말의 물리적 위치(GPS)에 따라 특정 앱 실행 또는 네트워크 접근을 제한한다.
N2SF-MD-M2	정책 위반 자동 조치	• 정책 위반 시 자동으로 앱 차단, 로그아웃, 초기화 등 사전 정의된 조치를 수행한다.
④ 모바일 업무용 시스템 관리자 기능 관리		
N2SF-RA-4	관리자 권한 통제	• 원격접속을 통한 관리자 권한은 제한된 조건에서만 허용해야 하며, 관리자 권한으로 실행한 명령어 이력 등은 유지한다.
N2SF-LP-4	관리자 권한 제한	• 정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.
⑤ 모바일 업무용 시스템 로그 관리		
N2SF-RA-M2	원격접속 로그 보존 및 감사	• 원격접속 활동 기록을 수집하여 정기 감사가 가능하도록 보존한다.
N2SF-EB-M2	외부 경계 정책 수립 및 갱신	• 외부 통신 및 경계 보안 정책을 수립하고 주기적으로 갱신한다.
N2SF-EB-M3	외부 통신 로그 기록 및 감사	• 외부 통신 활동과 설정 변경 사항을 기록하고 감사 가능하게 한다.
N2SF-SN-M2	세션 감사 및 로그 기록	• 세션 생성, 종료, 중복, 충돌 등 관련 활동을 로깅하고 보안 감사가 가능하도록 구성한다.

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 모델 9. **모바일 업무환경 정보 연계**

부록 2-9