부록 2-10

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서

모델 10. 무선 업무환경 운용 체계

2025. 9

국가정보원

NSR 국가보안기술연구소

부록 2-10

1.0

국가 망 보안체계 보안 가이드라인

정보서비스 모델 해설서

모델 10. 무선 업무환경 운용 체계

2025. 9

국가정보원

NSR 국가보안기술연구소

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 - 모델 10. 무선 업무환경 운용 체계

부록 2-10

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 10. 무선 업무환경 운용 체계」 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.

이에 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.

본 문서에서는 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「무선 업무환경 운용 체계」정보서비스 모델에 대해 설명하고 있으며, 2장은 정보서비스 개요, 위협식별, 보안대책 수립 등 총 3개의 절을 포함하고 있다. 2장에 대응하는 N2SF 단계/활동은 다음과 같다.

표 1-1 2장과 N2SF 단계/활동의 대응 관계

절	항	N2SF 단계	N2SF 활동명	세부 내용
제1절 정보서비스 개요	-	-	-	N2SF 정보서비스 개념 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. 무선 AP		[활동-4-1] 보안 요구사항 도출	정보서비스 구축·운영 과정에서 필요한무선 AP 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			[활동-4-2] 보안통제 선택	
	3. 연계체계		[활동-4-1] 보안 요구사항 도출	기관 무선망과 네트워크 연계가 이루어지는 지점에 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 2장 1절에서와 같이 각급기관이 운영하고자 하는 정보서비스를 간단히 정의한 후, 2절 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

무선 업무환경 운용 체계

제1절

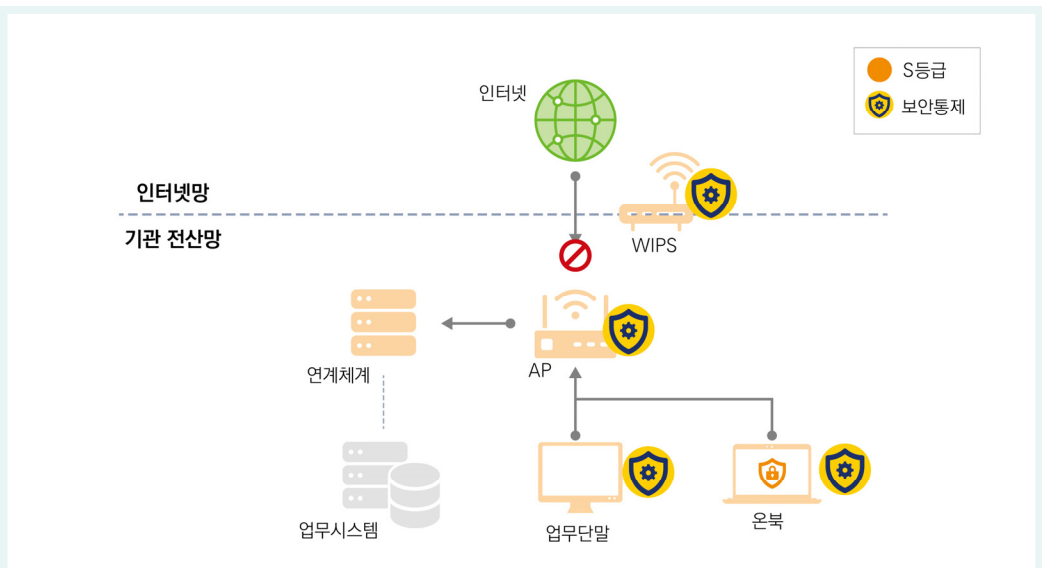
정보서비스 개요

본 정보서비스 모델은 기관 청사 내에서 Wi-Fi 등 무선 업무환경을 운용하기 위한 보안 요구사항 및 대책을 제시한다.

1절은 이용자 단말(업무 단말, 온북 등)이 Wi-Fi 등 무선 통신을 통한 업무 수행을 위해 무선 업무환경을 운용하는 정보서비스 구성을 보여주고, 2절은 구성요소 분석, 모델링 및 보안등급 평가, 보안원칙 적용을 통한 보안위협 식별 절차를 수행한다. 3절은 보안위협에 대응하기 위한 필수 보안 요구사항과 보안통제 항목을 적용한 보안대책을 기술한다.

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

그림 2-1 무선 업무환경 운용 체계 정보서비스 개요



제2절

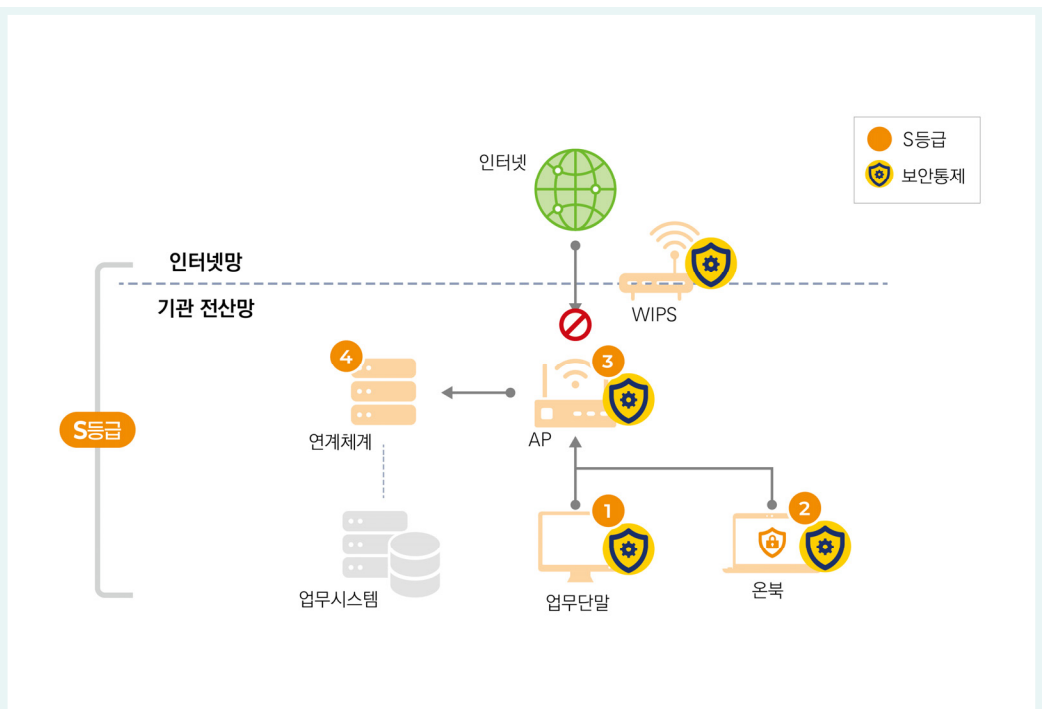
정보서비스 보안위협 식별

1. 정보서비스 구성요소 분석

본 정보서비스 모델은 이용자 단말이 기관 전산망 업무시스템에 접속하는 환경에서, 업무 이동성 확보 및 효율성 향상을 위해 Wi-Fi 등을 활용하는 무선 업무환경 구축·운용 모델이다.

본 정보서비스는 무선 통신이 가능한 이용자 단말(업무 단말, 온북)과 기관 전산망 내에서 운용하는 무선 AP(Access Point), WIPS(Wireless Intrusion Prevention System) 및 연계체계로 구성되며, 모든 구성 시스템은 S등급이다.

그림 2-2 정보서비스 구성요소 분석



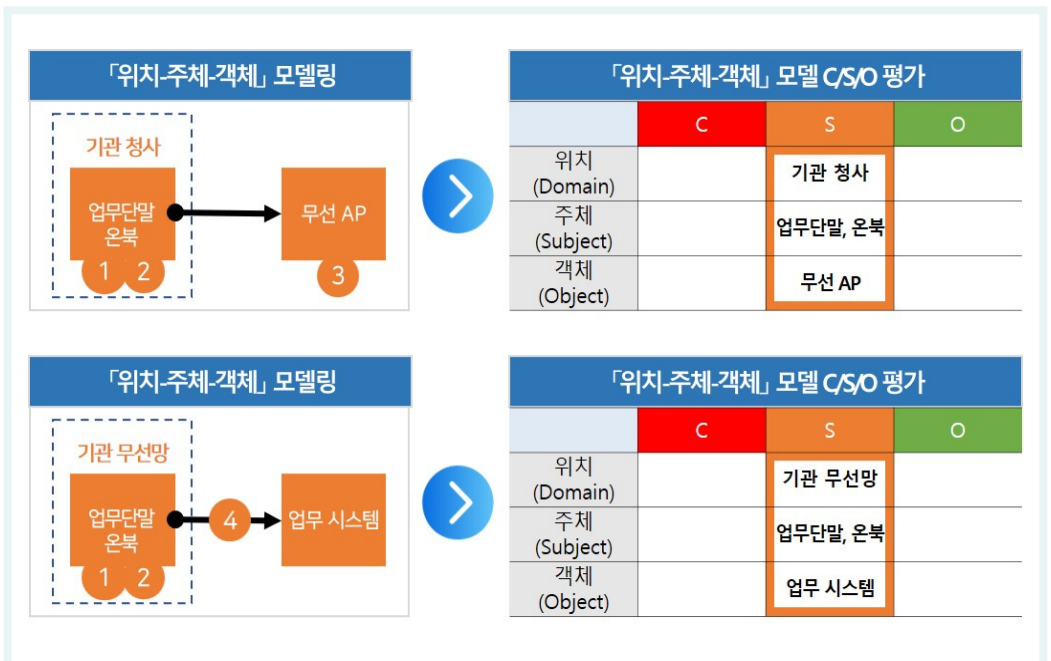
2. 모델링 및 C/S/O 평가

본 정보서비스는 무선 업무환경 구축·운용을 위한 구성요소를 이용자 단말(업무 단말, 온북 등)이 무선 AP에 접속하는 단계와, 무선망에 접속한 이용자 단말이 연계체계를 통해 기관 업무시스템에 접속하는 단계로 구분할 수 있다. 따라서 모델링 및 C/S/O 평가를 각 단계별로 구분하여 평가한다.

첫째, 기관 청사 내 이용자 단말이 무선 AP에 접속하는 단계에서는 「위치(기관 청사)-주체(이용자 단말)-객체(무선 AP)」로 모델링 할 수 있고, 이때 보안등급은 위치 S등급, 주체 S등급 및 객체 S등급으로 평가한다.

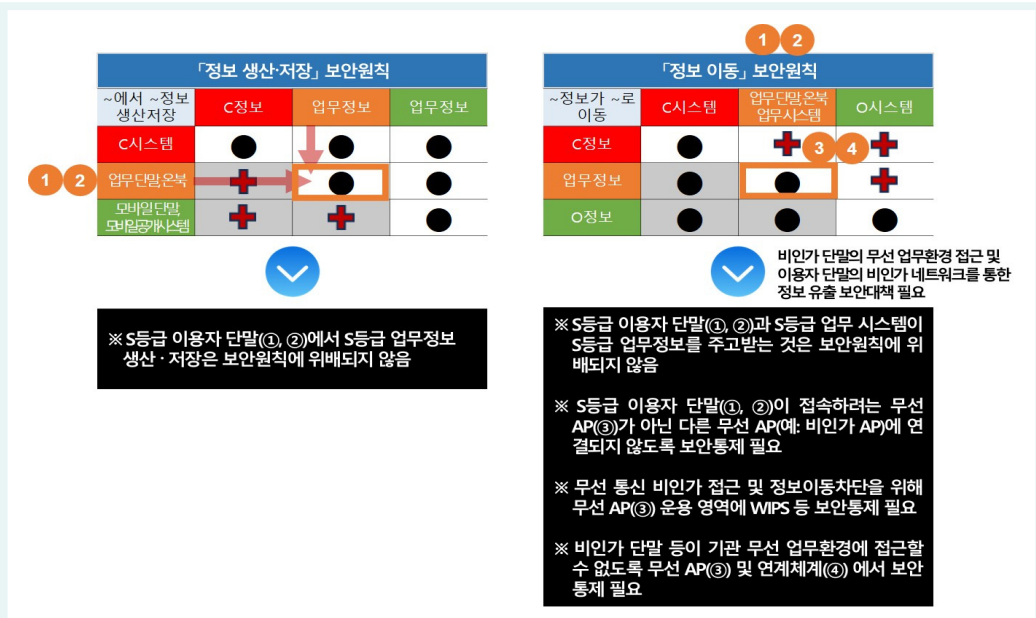
둘째, 기관 무선망에 접속한 이용자 단말이 연계체계를 경유하여 기관 전산망 내 업무시스템에 접속하는 단계에서는 「위치(기관 무선망)-주체(이용자 단말)-객체(업무시스템)」로 모델링 할 수 있고, 이때 보안등급 또한 위치 S등급, 주체 S등급 및 객체 S등급으로 평가한다.

그림 2-3 「위치-주체-객체」 모델링 및 C/S/O 평가



3. 보안원칙 적용

그림 2-4 보안원칙 적용



가. 「정보 생산·저장」 보안원칙 적용

기관 전산망에 위치한 이용자 단말(업무 단말, 온북)은 S등급이며, S등급 및 O등급 업무정보 취급은 「정보 생산·저장」 보안원칙에 위배되지 않는다.

나. 「정보 이동」 보안원칙 적용

기관 전산망에 위치한 이용자 단말(업무 단말, 온북)과 무선 AP는 모두 S등급이며, 무선망에 접속한 이용자 단말이 연계체계를 통해 접속하는 업무시스템 역시 S등급이다.

따라서 이용자 단말(업무 단말, 온북)에서 생성한 S등급 정보를 무선 AP 및 연계체계를 경유해 업무시스템으로 전송하는 것은 「정보 이동」 보안원칙에 위배되지 않는다.

다만, 무선 업무환경 특성상 이용자 단말이 비인가 무선 AP에 접속하거나 이동이 가능한 단말(노트북 등)을 통해 업무 영역 외에서의 업무정보 노출 등 보안위협이 발생할 수 있다. 그러므로 무선 업무환경 운용 시 이용자 단말에 대한 보안통제 적용이 필요하다.

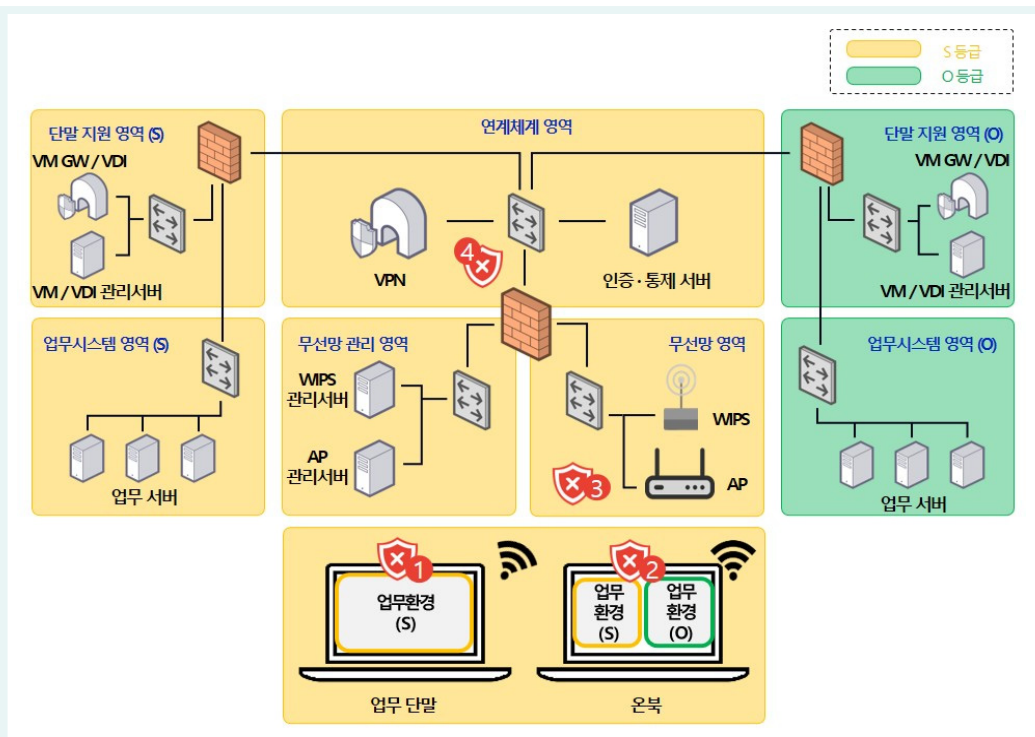
또한, 무선 업무환경 AP를 대상으로 비인가 접근 및 인증 우회 등을 통해 통신 정보 유출, 업무 시스템에 대한 무단 접근 등 보안위협이 발생할 수 있다. 그러므로 무선 AP에 대한 보안통제 적용과 무선 통신 영역 및 업무시스템 영역 간 인증·통제 과정이 필요하다.

만약, 하나의 이용자 단말(온북 등)을 통해 S등급 업무와 O등급 업무를 모두 수행하는 무선 업무환경을 구축하고자 하는 경우, 이용자 단말에서 각 등급 업무 수행을 위한 추가적인 보안통제 적용이 필요하다. 국가 망 보안체계 보안 가이드라인 부록2 모델4에 해당하는 「업무 단말의 인터넷 이용」 보안 요구사항을 참고하여, 기관 업무환경 및 특성을 고려한 보안대책을 수립해야 한다.

4. 보안위협 식별

본 정보서비스 모델은 이용자 단말(①업무 단말, ②온북), 무선 업무환경 운용을 위한 ③무선 AP 및 WIPS, ④연계체계로 구성되며, 〈표 2-1〉과 같이 정보서비스 모델 구성 대상별 보안 위협을 식별한다.

그림 2-5 보안위협 대상 식별



본 정보서비스 모델 보안위협 대상은 내부 업무수행 전용 단말을 운용하는 업무환경과 하나의 이용자 단말에서 S등급(내부 업무)·O등급(인터넷 업무) 업무시스템에 접속하는 업무환경에서 식별하였으며, 기관 업무환경 구성 및 특성을 고려하여 보안위협 대상을 식별해야 한다.

표 2-1 정보서비스 보안 위협

대상	구분	보안위협 번호	보안위협 요소
이용자 단말	① 업무 단말, ② 온북	TH-M10-1	단말 OS 및 SW 취약점 노출
		TH-M10-2	비인가 SW 설치 및 실행
		TH-M10-3	단말 비인가 사용
		TH-M10-4	단말 분실
		TH-M10-5	비인가 네트워크(비인가 무선 AP 등) 연결
		TH-M10-6	업무 수행 중 네트워크 임의 변경
		TH-M10-7	업무정보 비인가 유출
		TH-M10-8	이용자 단말과 무선 AP 간 송수신 데이터 유출
		TH-M10-9	기관 외 영역에서 단말 내 업무정보 화면 노출
		TH-M10-10	기관 무선 AP 인증정보 노출
		TH-M10-11	인가된 영역 외 무단 접근 및 자료 이동
		TH-M10-12	악성코드 유입 및 실행으로 인한 악성코드 감염
무선랜	③ 무선 AP	TH-M10-13	SSID 노출 또는 유추로 인한 비인가 접근
		TH-M10-14	비인가 무선 AP 운용·접속
		TH-M10-15	이전 사용자 접근
		TH-M10-16	비인가 단말의 연결
		TH-M10-17	불필요한 세션 유지
		TH-M10-18	송수신 데이터 유출
		TH-M10-19	인증 플러딩, 재밍 등 무선 AP 서비스 거부 공격
		TH-M10-20	무선 AP 관리자 기능 비인가 접근
연계	④ 연계 체계	TH-M10-21	비인가 단말 인증
		TH-M10-22	이용자 인증 우회
		TH-M10-23	비인가 업무 영역 접근
		TH-M10-24	계정 정보 비인가 접근 및 변경
		TH-M10-25	계정 인증 정보 유출
		TH-M10-26	관리자 기능 비인가 접근
		TH-M10-27	비인가 매체 연결 및 기능 실행

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 식별 과정을 통해 위협을 파악하고, 정보서비스 모델 보안대책 수립 방향성과 국가·공공기관의 정책적 요구사항을 반영하여 보안 요구사항 및 N2SF 보안통제 항목을 선정하였다.

표 2-2 보안 요구사항 및 보안통제 항목

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
이용자 단말	① 업무 단말 ② 온북	(TH-M10-1) 단말 OS 및 SW 취약점 노출 (TH-M10-2) 비인가 SW 설치 및 실행 (TH-M10-12) 악성코드 유입 및 실행으로 인한 악성코드 감염	이용자 단말 보안성 유지	N2SF-LP-1 N2SF-LP-5 N2SF-DA-1 N2SF-DV-12 N2SF-IN-1 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-8 N2SF-IN-16
		(TH-M10-3) 단말 비인가 사용	이용자 단말 사용 보안	N2SF-AM-2 N2SF-AM-9 N2SF-DV-6 N2SF-DV-8
		(TH-M10-4) 단말 분실	이용자 단말 분실 대책	N2SF-MA-5 N2SF-MD-M2 N2SF-AC-3 N2SF-AC-3(1)

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M10-5) 비인가 네트워크(비인가 무선 AP 등) 연결 (TH-M10-6) 업무 수행 중 네트워크 임의 변경	이용자 단말 네트워크 보안	N2SF-SG-4 N2SF-SG-5 N2SF-SG-6 N2SF-EB-6 N2SF-SN-1 N2SF-SN-4 N2SF-SN-6 N2SF-WA-7 N2SF-BC-1 N2SF-DT-1
		(TH-M10-7) 업무정보 비인가 유출 (TH-M10-8) 이용자 단말과 무선 AP 간 송수신 데이터 유출 (TH-M10-9) 기관 외 영역에서 단말 내 업무정보 화면 노출	이용자 단말 데이터 보호	N2SF-DU-2 N2SF-DV-4 N2SF-DV-10
		(TH-M10-10) 기관 무선 AP 인증정보 노출	무선 AP 인증 정보 보호	N2SF-IM-1 N2SF-MD-M2
		(TH-M10-11) 인가된 영역 외 무단 접근 및 자료 이동	무선 업무환경 이용자 단말 관리	N2SF-SG-2 N2SF-SG-5 N2SF-SG-6 N2SF-SG-M1 N2SF-SG-M2 N2SF-SG-M3 N2SF-SG-M4 N2SF-SG-M5 N2SF-LP-M1 N2SF-LP-M3 N2SF-EB-M1 N2SF-AM-5
무선 AP	③ 무선 AP	(TH-M10-13) SSID 노출 또는 유추로 인한 비인가 접근	무선 AP SSID 관리	N2SF-WA-2
		(TH-M10-14) 비인가 무선 AP 운용·접속	비인가 무선 AP 탐지 및 차단	N2SF-WA-4 N2SF-WA-7

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M10-15) 이전 사용자 접근 (TH-M10-16) 비인가 단말의 연결 (TH-M10-17) 불필요한 세션 유지	무선 AP 인증체계 관리	N2SF-WA-1 N2SF-IV-1 N2SF-AC-1(1) N2SF-AC-1(5) N2SF-DA-3 N2SF-LI-2
		(TH-M10-18) 송수신 데이터 유출	무선 AP 송수신 데이터 보호	N2SF-WA-3 N2SF-WA-5
		(TH-M10-19) 인증 플러딩, 재밍 등 무선 AP 서비스 거부 공격 (TH-M10-20) 무선 AP 관리자 기능 비인가 접근	무선 AP 운용 관리	N2SF-WA-6 N2SF-WA-M1 N2SF-LI-M1 N2SF-AC-3 N2SF-AC-M1 N2SF-AC-M2 N2SF-AC-M3 N2SF-SN-M1 N2SF-SN-M2
연계 체계	④ 연계 체계	(TH-M10-21) 비인가 단말 인증	연계체계 이용자 및 단말 인증	N2SF-AC-1(1) N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-1(4) N2SF-AC-3 N2SF-AC-3(2) N2SF-DA-3 N2SF-DA-4 N2SF-LI-1 N2SF-LI-2 N2SF-LI-4
		(TH-M10-22) 이용자 인증 우회	비인가 네트워크 연결 차단	N2SF-IS-4 N2SF-IF-1 N2SF-IF-9 N2SF-EB-1 N2SF-EB-2 N2SF-EB-3 N2SF-EB-5 N2SF-EB-6
		(TH-M10-23) 비인가 업무 영역 접근	이용자 단말과 전용 네트워크 연결	N2SF-IF-6 N2SF-RA-2 N2SF-RA-5 N2SF-RA-6

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M10-24) 계정 정보 비인가 접근 및 변경 (TH-M10-25) 계정 인증 정보 유출	연계체계 인증 정보 보호	N2SF-AU-5 N2SF-AU-5(1) N2SF-AU-5(2) N2SF-AU-M1
		(TH-M10-26) 관리자 기능 비인가 접근	연계체계 보안성 유지	N2SF-LP-1 N2SF-LP-4 N2SF-LP-4(1) N2SF-LP-4(4) N2SF-AC-1(5) N2SF-AC-3(1) N2SF-EB-8 N2SF-EB-10 N2SF-EB-11 N2SF-EB-12 N2SF-EB-13 N2SF-DV-4 N2SF-DV-10 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-10 N2SF-IN-11
		(TH-M10-27) 비인가 매체 연결 및 기능 실행	연계체계 운용 관리	N2SF-LP-M1 N2SF-LP-M2 N2SF-AC-1(2) N2SF-AC-M1 N2SF-AC-M2 N2SF-AC-M3 N2SF-LI-M1 N2SF-LI-M2 N2SF-IS-2 N2SF-IF-M1 N2SF-IF-M2 N2SF-IF-M3 N2SF-IF-M4 N2SF-IF-M5 N2SF-EB-M3 N2SF-EB-M4 N2SF-EB-M5

1. 이용자 단말

무선 업무환경 운용 체계 정보서비스 모델에서는 이용자 단말이 무선 AP 접속 시부터 업무 수행 종료 시까지 보안통제가 적용되어야 한다. 본 해설서에서는 하나의 이용자 단말을 통해 S등급 기관 전산망(내부 업무 수행) 및 O등급 기관 전산망(인터넷 업무 수행)에 접속하는 환경 구성으로 기술하며, 이용자 단말 업무환경은 기관 환경 및 특성을 고려하여 구성 가능하다.

그림 2-6 이용자 단말 업무환경 구성(예) – 노트북 기반 다양한 OS 운영환경 구성

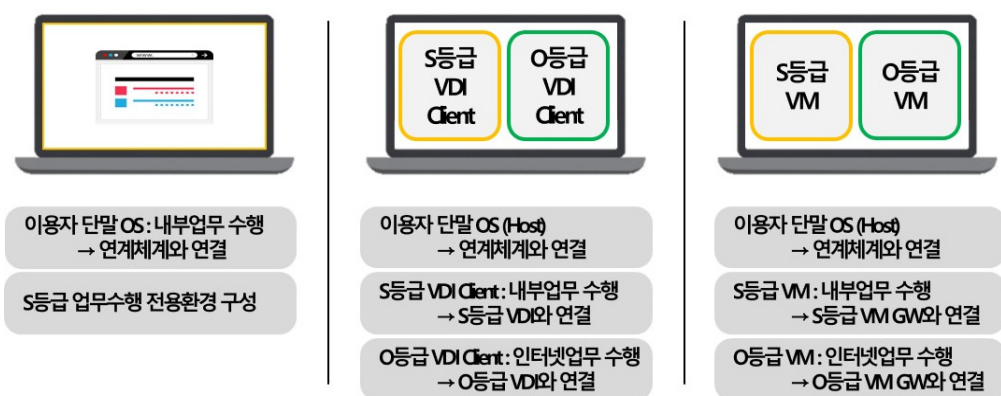
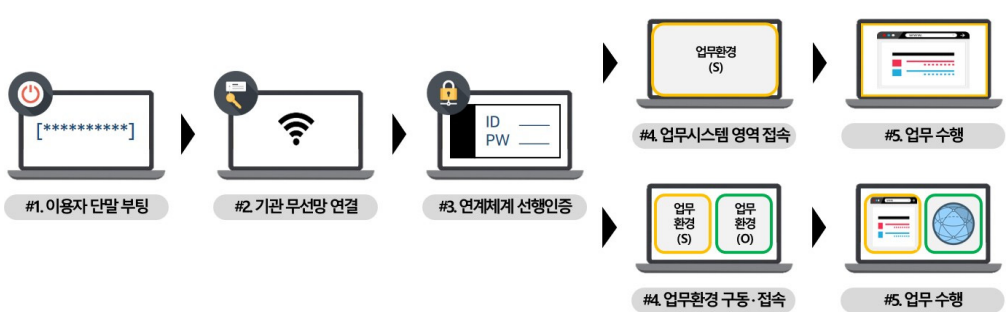


그림 2-7 이용자 단말 사용 시나리오(예)



무선망 기반의 업무용 노트북은 기관 무선망 연결(#2) 또는 외부의 무선망 연결시 연계체계 선행인증(#3)이 완료된 이후에만 이용자가 노트북에 설치된 OS 사용이 가능하도록 상호 인증체계를 연동하여 구성하여야 한다.

만약 사용자가 기관 무선망 또는 외부의 무선망 인증만을 완료하고 연계체계 선행인증이 완료되지 않은 상태에서는 노트북에 설치된 OS의 활용은 불가능한(또는 불능) 상태로 유지되어야 하며, 사용자가 임의의 조치를 통해 인증절차가 무력화 또는 우회되지 않도록 기술적 수단을 적용해야 한다.

또한, 업무용 노트북이 업무시스템 영역 접속이 완료되면 이외 인터넷 접속 및 블루투스·USB 테더링 등을 통한 우회 통신망이 구성되지 않도록 차단되어야 한다.

업무용 노트북의 인터넷 이용이 필요한 경우 '업무 단말의 인터넷 이용(정보서비스 모델 4)에 정의한 보안통제를 적용하고 기관 전산망을 경유한 인터넷 이용만이 가능하다.

온북과 같이 노트북 1대로 인터넷·업무 이용이 가능하도록 보안통제가 적용된 경우 별도의 보안조치 없이 활용할 수 있다.

다음은 이용자 단말(업무 단말, 온북)에 적용해야 할 보안 요구사항 및 보안대책이다.

이용자 단말(①업무 단말, ②온북)은 사전에 무선 업무환경 사용을 승인받은 사용자 및 무선 네트워크 연결이 가능한 단말로 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

① 「**이용자 단말**」 **보안성 유지**

무선 업무환경 이용자 단말의 악성코드 감염, OS 변조, 비인가 SW 실행 등 방지를 위해 단말 중앙관리시스템, 보안 업데이트, 백신 운용, 실행파일 검증 등을 통한 이용자 단말 보안성을 유지·관리해야 한다.

이용자 단말은 기관 무선 AP를 통해 업무시스템에 접속 및 업무 수행을 사전에 승인·등록해야 하며, 무선 업무환경 운용을 위한 보안통제 적용 등 보안 조치가 완료되어야 한다.

② 「**이용자 단말**」 **사용 보안**

비인가자의 단말 사용 등을 차단하기 위해 이용자 단말 부팅·사용 및 일정 시간 이상 단말 미사용 시 사용자 인증 등을 통해 단말을 사용할 수 있도록 보안 조치를 수행해야 한다.

③「이용자 단말」분실 대책 수립

이용자 단말이 이동 가능한 노트북 등의 형상으로 변경됨에 따라 단말 분실 시 업무 자료 유출을 방지하기 위한 기관 네트워크 연결 후 인증 절차 진행, 전체 데이터 암호화 등의 보안통제를 적용해야 한다.

또한, 기관 특성을 고려하여 단말 내 데이터 원격 삭제 등의 보안통제를 적용할 수 있다.

④「이용자 단말」네트워크 보안

이용자 단말의 비인가 무선 AP 접속, 사용자 인증 후 단말의 연결된 네트워크 임의 변경 등을 방지하기 위한 보안통제를 적용해야 한다.

또한, 무선 통신 중 정보 유출을 방지하기 위해 송수신 데이터에 대한 보안통제를 적용해야 한다.

⑤「이용자 단말」데이터 보호

이용자 단말 내 업무정보 무단 이동, 복사 등을 방지하기 위한 데이터 보호 조치를 적용하고, 인증 전 단말 내 정보 보호를 위해 연계체계 인증 후 운영체제 로그인을 수행하도록 조치하거나 이에 준하는 보호조치를 적용해야 한다.

또한, 이동 가능한 노트북 등의 단말 사용 시 기관 사무실 외 영역에서 화면을 통한 업무정보 노출을 차단하기 위해 일정 시간 이상 활동이 없는 경우 단말 잠금을 수행하는 등 보안대책을 적용해야 한다.

⑥ 무선 AP 인증 정보 보호

무선 업무환경 접속을 위한 인증 정보는 유출되지 않도록 관리해야 한다.

또한, 인사이동 등으로 인한 무선 업무환경 접속 인가자 변동 시 해당 내용을 무선 AP 인증체계에 즉각 반영하거나, 이용자 개별 인증 체계를 구축해야 한다.

⑦ 무선 업무환경「이용자 단말」관리

무선 업무환경 이용자 단말 사전 승인, 보안통제 적용 및 인증 등 관리 절차를 수립해야 한다.

하나의 이용자 단말을 통해 업무 수행을 위해 S/O 등 보안등급이 다른 기관 전산망에 접속이 필요한 경우, 이용자 단말 내 업무환경 분리, 별도 구성 등을 통해 무선 업무환경을 운영·관리해야 한다.

기관은 위와 같은 보안 요구사항 및 〈표 2-3〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 2-3 이용자 단말(업무 단말, 온북) 보안통제 항목

코드	보안통제 항목	내용
① 이용자 단말 보안성 관리		
N2SF-LP-1	정보시스템 접근 권한 정의	• 업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.
N2SF-LP-5	코드 실행권한 제한	• 코드는 필요한 권한으로만 실행되도록 제한하고, 사용자 권한으로 실행되는 코드가 관리자 영역으로 접근되지 않도록 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-DV-12	장치 펌웨어 업데이트 검증	• 펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.
N2SF-IN-1	구성요소 목록 중앙관리	• 정보시스템 구성요소 목록을 통합관리하기 위한 중앙화된 저장소를 운용한다.
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	• 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
N2SF-IN-5	비인가 변경 방지	• 인가되지 않은 정보시스템 구성요소 변경을 방지한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.
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.
② 이용자 단말 사용 보안		
N2SF-AM-2	비밀번호 기반 인증	• 숫자·문자·특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.
N2SF-AM-9	소유기반 인증	• 생체인증, 모바일 인증 및 하드웨어 토큰 등을 활용한 인증체계를 적용한다.
N2SF-DV-6	통신 기능이 포함된 저장장치 제한	• 통신기능이 포함된 저장장치를 사용을 제한한다.
N2SF-DV-8	장치 자동 잠금	• 사용자가 일정시간 이상 정보시스템을 사용하지 않거나 방치할 경우 잠금 기능을 활성화하고, 화면에 표시되는 정보는 표출되지 않아야 한다.
③ 이용자 단말 분실 대책 수립		
N2SF-MA-5	특정상황에서의 다중요소 인증	• 특정 상황 또는 조건에서는 다중요소 인증을 적용하여 사용자를 인증한다.
N2SF-MD-M2	정책 위반 자동 조치	• 정책 위반 시 자동으로 앱 차단, 로그아웃, 초기화 등 사전 정의된 조치를 수행한다.

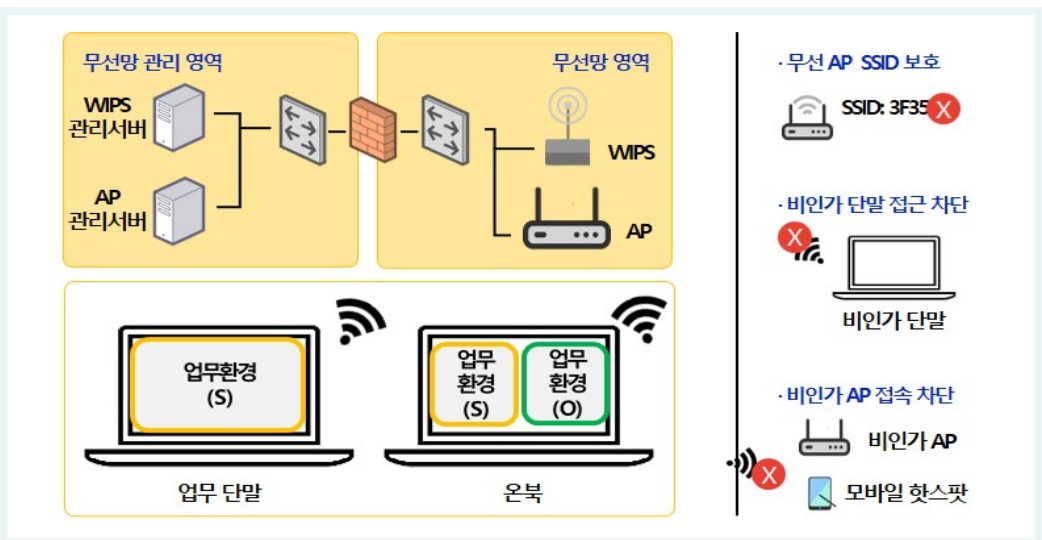
코드	보안통제 항목	내용
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.
④ 이용자 단말 네트워크 보안		
N2SF-SG-4	IP체계	• 서로 다른 영역 또는 정보자산(기능 등)별IP체계를 분리하고, 보안통제를 적용한다.
N2SF-SG-5	보안·운영관리 인프라 분리	• 보안·운영관리 인프라를 물리적으로 분리된 네트워크로 구성하여 이외 정보시스템과 분리한다.
N2SF-SG-6	보안 기능과 사용자 기능 분리	• 인증, 감사 및 데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 애플리케이션 실행 등 사용자 기능을 분리한다.
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-1	로그아웃 세션 처리	• 로그아웃 또는 비정상 세션 종료 시 연결되었던 모든 세션의 식별자를 즉시 무효화하며, 더 이상 세션이 유효하지 않도록 한다.
N2SF-SN-4	세션 종료	• 세션 종료 요청이 있거나 세션 종료 조건 발생 시 자동으로 세션을 종료한다.
N2SF-SN-6	네트워크 연결 해제	• 정상 세션 종료 또는 일정 시간 비활성 상태가 유지될 경우 네트워크 연결을 자동 해제한다.
N2SF-WA-7	비인가 무선망 접속 차단	• 인가되지 않은 무선망 접속을 차단한다.
N2SF-BC-1	블루투스 데이터 통신 제한	• 블루투스 장치 연결 시 키보드, 마우스, 오디오 등을 위한 입출력 기능 외 데이터 통신은 차단한다.
N2SF-DT-1	전송 권한 확인	• 데이터가 전송되기 전에 이를 처리하는 개인이나 정보시스템이 적절한 권한을 보유하고 있는지 확인한다.
⑤ 이용자 단말 데이터 보호		
N2SF-DU-2	데이터 암호화 저장	• 데이터 대상 암호기술을 적용하여 기밀성을 보장한다.
N2SF-DV-4	포트 및 입출력 장치 제어	• 정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.
N2SF-DV-10	저장장치 연결 금지	• 정보시스템 기동 및 종료 또는 재시작하는 동안 쓰기 가능한 저장장치 연결을 금지한다.
⑥ 무선 AP 인증 정보 보호		
N2SF-IM-1	공개된 식별자의 계정 사용 금지	• 정보시스템 계정 식별자로 개인의 공개된 식별자 사용을 금지한다.
N2SF-MD-M2	정책 위반 자동 조치	• 정책 위반 시 자동으로 앱 차단, 로그아웃, 초기화 등 사전 정의된 조치를 수행한다.

코드	보안통제 항목	내용
⑦ 무선 업무환경 이용자 단말 관리		
N2SF-SG-2	운영체제(OS) 기반 분리	• 하나의 시스템에 다수 OS가 존재하더라도, 각 운영체제는 서로 독립된 환경으로 분리되도록 구성한다.
N2SF-SG-5	보안·운영관리 인프라 분리	• 보안·운영관리 인프라를 물리적으로 분리된 네트워크로 구성하여 이외 정보시스템과 분리한다.
N2SF-SG-6	보안 기능과 사용자 기능 분리	• 인증, 감사 및 데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 애플리케이션 실행 등 사용자 기능을 분리한다.
N2SF-SG-M1	분리 정책 및 절차 수립	• 자산 간 분리 기준, 설정 방식, 승인 절차 등을 포함한 정책과 문서화된 절차를 수립한다.
N2SF-SG-M2	보안·운영 인프라 접근 책임 및 역할 관리	• 분리된 인프라에 접근 가능한 대상 및 책임자를 지정하고 권한 기반 접근 통제를 적용한다.
N2SF-SG-M3	분리된 시스템 정기적 평가 및 감사	• 분리된 영역의 적절성, 위협, 취약점 등을 정기적으로 점검하고, 감사 결과에 따라 개선 조치를 수행한다.
N2SF-SG-M4	분리환경 접근권한 관리 및 모니터링	• 분리된 환경에 대한 접근권한을 사용자, 장비, 서비스 단위로 설정하고 이를 모니터링한다.
N2SF-SG-M5	분리 위반사항 대응체계 운영	• 분리 정책 위반 발생 시 자동 경고, 세션 차단, 감사 로그 저장 등 즉시 대응이 가능하도록 대응 체계를 운영한다.
N2SF-LP-M1	특별권한 사용자 지정	• 일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.
N2SF-LP-M3	접근권한 사전 설정	• 기본적으로 필요 최소한의 권한만을 부여하는 사전 권한 설정 기준을 마련하고 운영한다.
N2SF-IM-2	사용자 상태 식별	• 개인과 조직의 구별, 사용자 상태(활성, 비활성, 임시계정 등)를 식별하고 관리한다.
N2SF-EB-M1	개인 식별정보 보호	• 외부와 통신 시 개인을 식별하거나 특정 개인과 관련된 정보를 포함하는 경우 노출되지 않도록 조치한다.
N2SF-AM-5	인증수단 보호	• 정보시스템의 보안수준에 준하여 인증수단을 보호한다.

2. 무선 AP

무선 업무환경에서의 업무 수행을 위해 이용자 단말은 무선 AP에 접속하여야 한다. 이때, 무선 AP의 안전한 운용을 위해 사전 승인받은 이용자 단말만 접속을 허용하는 등 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

그림 2-8 무선망 구성요소 및 보안 요구사항



① 「무선 AP」 SSID 관리

무선 업무환경 운용 시 비인가 단말의 무단 접근 방지를 위해 무선 AP의 기본 SSID를 쉽게 예측할 수 없도록 변경하고, 숨김 모드로 운용해야 한다.

② 비인가 「무선 AP」 탐지 및 차단

무선 AP에 대한 비인가 접속을 탐지하고, WIPS 등을 이용하여 차단해야 한다.

③ 「무선 AP」 인증 체계 관리

무선 AP 인증 정보 주기적 변경, WPA2, WPA-EAP 등 보안성이 강화된 인증 프로토콜 체계를 적용해야 한다.

무선 AP에 접근하는 단말 인증을 위해 인증·통제 시스템과 연계하여 사전 승인받은 단말만 접속할 수 있도록 보안통제를 적용하고, 단말 인증정보는 VPN 인증체계와도 상호 연동하여 단말을 지속 검증하도록 구성한다.

단말 인증에 사용되는 식별자는 쉽게 위조가 가능한 MAC 등을 활용할 수 없으며, 하드웨어 속성에 기반한 고유한 식별자를 생성·사용하고, MFA(다중요소 인증)를 필수 적용해야 한다.

또한, 인사이동 등으로 인해 권한이 없는 사용자의 접근을 방지하기 위한 보안통제를 적용해야 한다.

④「무선 AP」 송수신 데이터 보호

무선 AP의 전파 출력을 조절하거나 무선 AP의 전파 범위를 고려하여 설치 위치를 조절해야 하며, 무선 AP를 통한 업무정보 유출 방지를 위해 송수신 데이터를 보호해야 한다.

⑤「무선 AP」 운용 관리

무선 AP의 고장, 서비스 거부 공격 등 장애 시 업무 연속성을 보장하기 위해 이중화 구축 또는 이용자 단말 영역 예비 업무 회선 구축 등 장애 대책을 수립·운용해야 한다.

무선 AP에 대한 관리자 접속 기록(관리자 ID, 접속 시간, 접속 단말 정보 등), 작업 이력 등과 무선 AP에 대한 이용자 단말 접속 기록(단말 정보, 접속 시간 등) 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 2-4〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 2-4 무선 AP 보안통제 항목

코드	보안통제 항목	내용
① 무선 AP SSID 관리		
N2SF-WA-2	업무용 무선망 인증정보 보호	• 업무용 무선 통신망 서비스 식별 정보(SSID 등)를 경계지역 외부에서 확인할 수 없도록 적용하고, 무선 통신망 인증정보의 무단 사용 및 외부 유출을 방지한다.
② 무선 AP 비인가 접속 탐지 및 차단		
N2SF-WA-4	비인가 무선장비 설치 차단	• 업무용 무선망 서비스에 비인가 무선장비가 설치되거나 가동되는 것을 탐지하고 운용되지 않도록 한다.
N2SF-WA-7	비인가 무선망 접속 차단	• 인가되지 않은 무선망 접속을 차단한다.
③ 무선 AP 인증체계 관리		
N2SF-WA-1	업무용 무선망 인증 및 암호화	• 사용자 인증, 기기(단말 등) 인증 및 무선통신 구간 암호화를 적용한다.
N2SF-IV-1	관리자 승인	• 정보시스템 사용자 계정(대민서비스 등 서비스 이용자 계정 제외) 부여를 위한 계정 등록 절차에 정보시스템 관리자(정보화담당관 또는 이에 준하는 관리자)의 승인을 포함한다.

코드	보안통제 항목	내용
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(5)	불필요한 관리자 권한 계정 제거	• 관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.
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-LI-2	로그인 실패에 따른 접속 제한	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.
④ 무선 AP 송수신 데이터 보호		
N2SF-WA-3	업무용 무선망 신호 보호	• 무선 통신환경에 적합한 안테나를 선택하고 송수신 출력을 교신에 필요한 최저 출력으로 유지하여 경계지역 외부로 전파 되는 것을 방지한다.
N2SF-WA-5	외부인 전용 무선망 구성	• 업무용 네트워크 또는 무선망과 분리하여 외부인 전용망을 구성한다.
⑤ 무선 AP 운용 관리		
N2SF-WA-6	무선망 관리기능 보호	• 무선망 관리기능은 무선망에 노출되지 않아야 하며, 지정된 관리자만 접속되도록 통제한다.
N2SF-WA-M1	무선망 세션/로그 분석	• 무선 접속 로그와 세션 데이터를 통해 이상행위를 분석한다.
N2SF-LI-M1	로그인 실패 모니터링 및 보고	• 반복 실패, 의심 로그인 시도 등의 실패 패턴을 실시간 감지하고 관리자에게 보고한다.
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-AC-M1	감사 활동 자동화	• 계정 사용 및 관련된 감사 활동을 자동화하여 관리한다.
N2SF-AC-M2	감사기록 생성	• 계정 활동에 대한 감사 기록을 생성하여 보관하고 분석할 수 있도록 한다.
N2SF-AC-M3	세션 감사	• 세션 활동을 기록하고 주기적으로 감사하여 비정상적 행위를 탐지한다.
N2SF-SN-M1	세션 관리 정책 수립	• 세션 유지 시간, 비활성화 조건, 동시 접속 허용 수 등 세션 운용 정책을 수립하고 문서화한다.
N2SF-SN-M2	세션 감사 및 로그 기록	• 세션 생성, 종료, 중복, 충돌 등 관련 활동을 로깅하고 보안 감사가 가능하도록 구성한다.

3. 연계체계

연계체계는 기관 무선망에 접속한 이용자 단말이 업무 수행을 위해 기관 전산망 접속을 위한 인증을 수행하며, 기관 전산망 보안등급에 따른 단말 업무환경 및 업무정보 연계에 대한 통제를 수행한다.

업무 단말은 무선망 인증이 완료되었더라도 업무시스템 영역 접속을 위한 VPN 인증절차 및 보안 정책 업데이트가 완료되지 않을 경우 운영체제의 로그인 승인 절차가 진행되지 않도록 구현한다.

무선 업무환경 연계체계는 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

그림 2-9 연계체계 구성요소 및 인증 절차

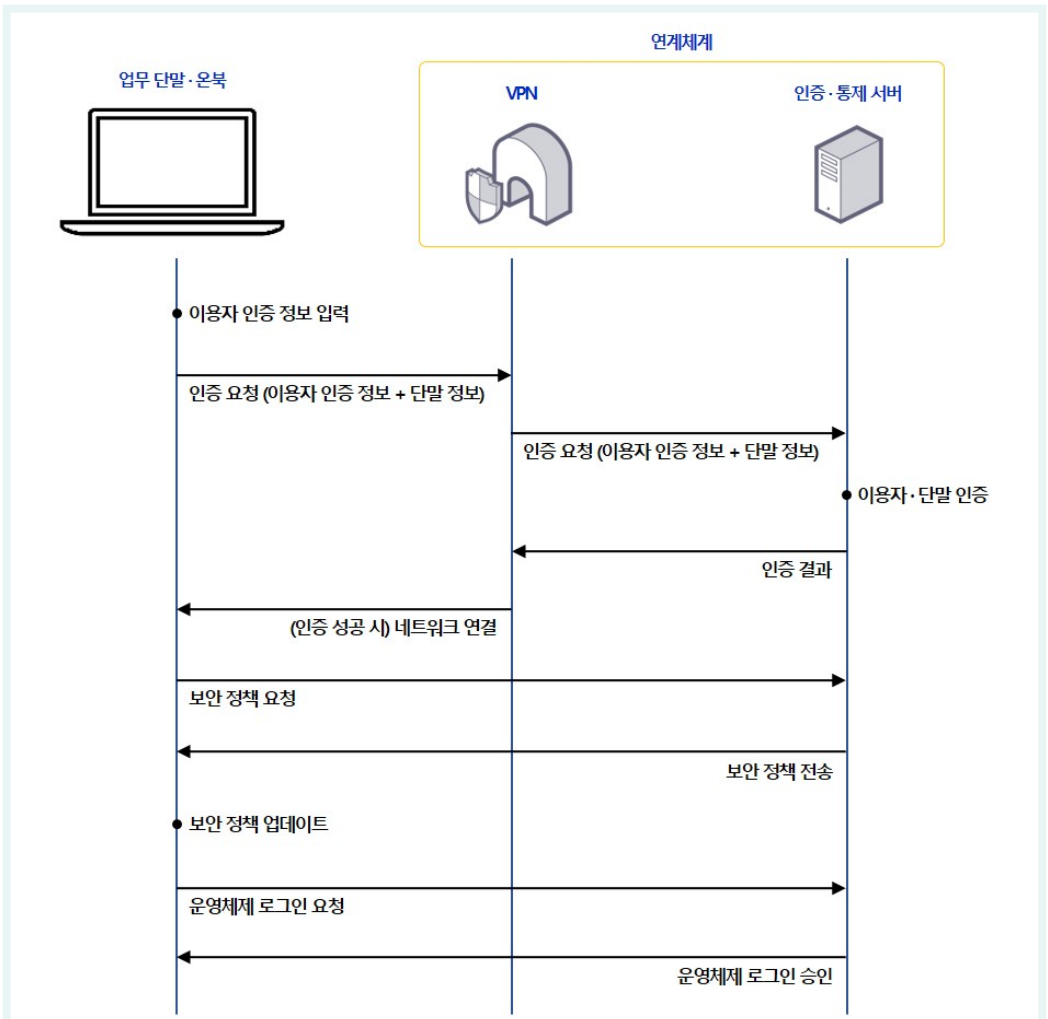
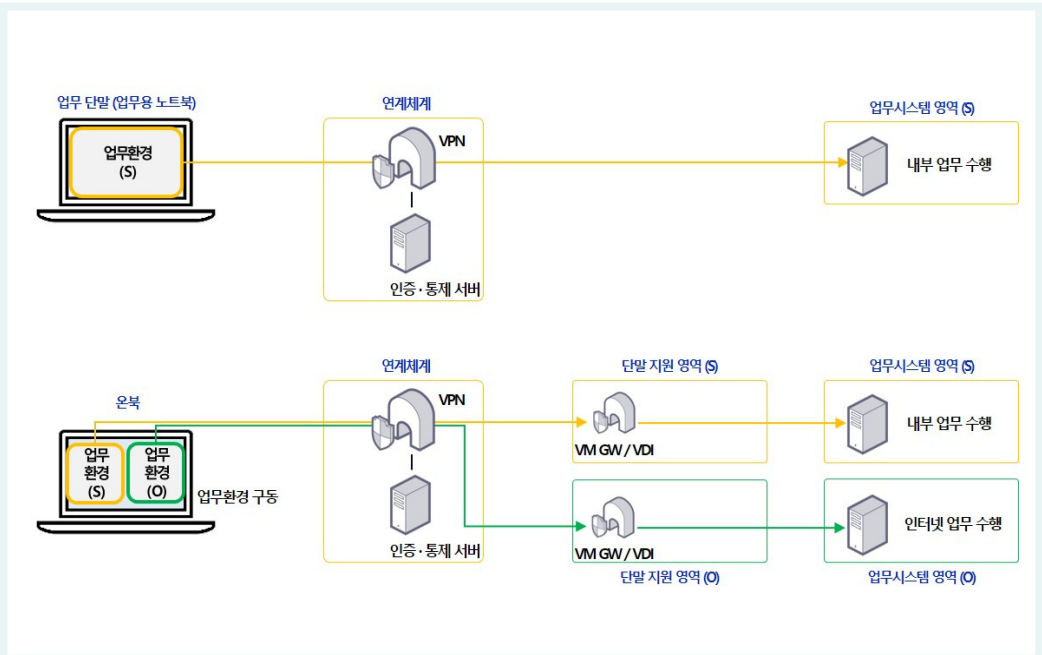


그림 2-10 연계체계 경유 업무시스템 접속



기관 무선망에 접속한 S등급 이용자 단말(업무 단말, 온북)은 연계체계를 통해 기관 전산망에 접속할 수 있으며 다음과 같은 보안 요구사항을 고려해야 한다. 또한, 기관 환경 및 특성을 반영하여 추가적인 보안통제 적용·조정 등을 고려해야 한다.

① 연계체계 이용자 및 단말 인증

이용자 및 단말의 기관 전산망 접속을 위한 인증을 수행해야 하며, 인증 과정에서 사용자 및 단말 정보가 노출되지 않도록 보안통제를 적용해야 한다.

기관 전산망에 접속한 이용자 및 단말의 의심스러운 활동 및 일정 시간 이상 비활동인 계정에 대한 보안조치를 적용해야 한다.

이용자 단말의 휴대성 향상에 따른 단말 내 정보 보호를 위해 연계체계 인증 후 단말 OS 로그인을 수행하도록 하거나 이에 준하는 보호조치를 적용해야 한다.

일정 횟수 이상 인증 실패에 대한 보호조치 및 잠금 해제 대책을 적용해야 한다.

② 비인가 네트워크 연결 차단

이용자 단말의 연계체계 우회 시도 및 사전 승인된 기관 전산망 외 비인가 네트워크로의 접근을 차단해야 한다.

연계체계를 통해 이용자 단말과 기관 전산망 업무시스템의 통신을 연계해야 하며, 서로 다른 보안 등급의 기관 전산망이 이용자 단말을 통해 연결되지 않도록 네트워크 격리 등 보안대책을 적용해야 한다.

비인가 네트워크 프로토콜은 차단해야 한다.

③ 이용자 단말과 전용 네트워크 연결

연계체계와 이용자 단말의 업무환경 연결을 VPN 등 전용 네트워크로 연결하여 송수신 데이터에 대한 보호 및 네트워크 보안위협 노출을 차단해야 한다.

④ 연계체계 인증 정보 보호

연계체계 이용자 및 단말 인증 정보 변경에 대한 관리 정책을 수립하여, 무단 변경 등을 방지해야 한다.

⑤ 연계체계 보안성 유지

연계체계 관리자 권한 계정을 일반 사용자 계정과 분리하여 관리해야 하며, 비인가 장치의 연결 등을 통제해야 한다.

연계체계의 취약점으로 인해 보안위협이 발생하지 않도록 최신 보안 업데이트 등 보안성을 유지해야 한다.

연계체계에 비인가 소프트웨어 설치·실행 및 단말 형상 비인가 변경으로 인한 보안위협이 발생하지 않도록 형상관리 등을 수행해야 한다.

그 외 기관 업무환경에 필요한 연계체계의 보안 조치가 완료되어야 한다.

⑥ 연계체계 운용 관리

연계체계 관리자 및 관리 단말 지정 등 운용 관련 체계를 수립해야 한다.

연계체계 운용에 대한 감사 로그를 생성·관리하고, 이용자 단말 인증, 세션, 정보흐름 통제 등 관련 정보를 모니터링 해야 한다.

연계체계 침해, 장애 등에 대한 대응체계 절차를 수립해야 한다.

기관은 위와 같은 보안 요구사항을 고려하여 〈표 2-5〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 2-5 연계체계 보안통제 항목

코드	보안통제 항목	내용
① 연계체계 이용자 및 단말 인증		
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-1(4)	계정 자동 로그아웃	• 비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-AC-3(2)	내부 사용자 모니터링	• 내부 사용자의 계정 사용 및 활동을 지속적으로 모니터링한다.
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-4	인증된 단말의 접속 관리	• 인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근 권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.
N2SF-LI-1	유효한 인증정보 노출 방지	• 인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.
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-4	계정 잠금 해제 인증요소 추가	• 계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.
② 비인가 네트워크 연결 차단		
N2SF-IS-4	네트워크 격리	• 내부망, 외부망, 보안망 등 네트워크 간에 방화벽, 라우팅 제어 등으로 트래픽을 분리하여 정보 유출 또는 확산을 방지한다.
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-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.

코드	보안통제 항목	내용
N2SF-EB-5	통신 경유(proxy) 강제화	• 인가된 정보시스템을 경유하여 통신하도록 통신경로를 강제화한다.
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.
③ 이용자 단말과 전용 네트워크 연결		
N2SF-IF-6	필터링 규칙 정보흐름 통제	• 보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.
N2SF-RA-2	원격접속 세션 암호화	• 원격접속 세션의 기밀성과 무결성을 보호하기 위해 통신구간 암호화를 적용한다.
N2SF-RA-5	원격접속 정보 유출 방지	• 원격접속에 관한 정보를 무단으로 사용하거나 외부로 유출되는 것을 방지한다.
N2SF-RA-6	원격접속 자동 종료 및 비활성화	• 일정시간 경과 등 조건에 따라 원격접속을 자동 종료하거나, 원격접속 목적이 달성된 경우 비활성화한다.
④ 연계체계 인증 정보 보호		
N2SF-AU-5	인증 시스템 구성 및 관리	• 인증 시스템의 구성 요소를 안전하게 설정하고 변경 시 보안에 영향이 없도록 관리한다.
N2SF-AU-5(1)	비밀번호 보안수준 점검	• 자동화된 도구를 이용하여 비밀번호 정책에 적합하게 설정·유지되고 있는지 점검한다.
N2SF-AU-5(2)	대체 보안수단 강구	• 보안 기능을 구현 또는 제공하는 주요 수단을 사용할 수 없거나 손상되었을 상황을 대비한 대체 보안수단을 강구한다.
N2SF-AU-M1	인증 정보 접근 권한 통제 및 관리	• 인증 정보는 최소한의 인원만 접근할 수 있도록 제한하고 기록을 남긴다.
⑤ 연계체계 보안성 유지		
N2SF-LP-1	정보시스템 접근 권한 정의	• 업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.
N2SF-LP-4	관리자 권한 제한	• 정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.
N2SF-LP-4(1)	원격접속을 통한 관리자 권한 접속제한	• 기관 네트워크 내부에서 관리자 권한 접속이 제한되는 경우 등 불가피한 상황에서만 한시적으로 기관 네트워크 외부에서의 관리자 권한 접속을 허용하며, 목적이 달성된 경우 외부에서의 관리자 권한 접속을 즉시 차단한다.
N2SF-LP-4(4)	관리자 권한 실행 로깅 및 감사	• 관리자 권한 기능 실행 내역은 로깅하고 주기적인 사용 내역 감사를 실시한다.
N2SF-AC-1(5)	불필요한 관리자 권한 계정 제거	• 관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.

코드	보안통제 항목	내용
N2SF-EB-8	운영관리용 포트의 물리적 연결 차단	• 운영관리용 포트에 인가되지 않은 장치의 포트 연결을 차단한다.
N2SF-EB-10	정보시스템 구성요소 외부 노출 차단	• 정보시스템 운영관리 및 서비스를 제공하는 구성요소가 외부 노출되지 않도록 차단한다.
N2SF-EB-11	외부 경계 보호 기능 유지	• 외부 경계를 보호하는 정보자산(보안시스템 등) 장애 시에도 보호기능은 유지되도록 구성한다.
N2SF-EB-12	외부 통신용 정보자산(장치) 설치 금지	• 외부 네트워크와 통신하는 인가되지 않은 정보자산(장치) 설치를 금지한다.
N2SF-EB-13	오류정보 발신자 전송 제한	• 네트워크 규약에 따른 통신 오류 발생 시 발신자에게 피드백이나 경고를 통해 정보시스템 구성이나 취약점이 전송되지 않도록 한다.
N2SF-DV-4	포트 및 입출력 장치 제어	• 정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.
N2SF-DV-10	저장장치 연결 금지	• 정보시스템 기동 및 종료 또는 재시작하는 동안 쓰기 가능한 저장장치 연결을 금지한다.
N2SF-DV-12	장치 펌웨어 업데이트 검증	• 펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	• 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성 요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
N2SF-IN-5	비인가 변경 방지	• 인가되지 않은 정보시스템 구성요소 변경을 방지한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.
N2SF-IN-11	재기동 서비스 신뢰성 확보	• 정보시스템 구성요소와 서비스가 재기동(재부팅) 할 때 소프트웨어와 데이터는 신뢰된 곳으로부터 획득한다.
⑥ 연계체계 운용 관리		
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-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-M1	감사 활동 자동화	• 계정 사용 및 관련된 감사 활동을 자동화하여 관리
N2SF-AC-M2	감사기록 생성	• 계정 활동에 대한 감사 기록을 생성하여 보관 및 분석할 수 있도록 함

코드	보안통제 항목	내용
N2SF-AC-M3	세션 감사	• 세션 활동을 기록하고 주기적으로 감사하여 비정상적 행위 탐지
N2SF-LI-M1	로그인 실패 모니터링 및 보고	• 반복 실패, 의심 로그인 시도 등의 실패 패턴을 실시간 감지하고 관리자에게 보고
N2SF-LI-M2	주기적 로그인 정보 무결성 점검	• 로그인 관련 데이터(세션, 토큰, 사용자 매핑 정보 등)에 대해 주기적인 무결성 점검 및 이상 여부 확인
N2SF-IS-2	정보시스템 운영·관리 기능 표출 제한	• 일반 사용자에게 정보시스템 관리와 관련된 기능 및 인터페이스 표출을 제한한다.
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-IF-M3	정보흐름 통제 감사 및 이행 점검	• 정보 흐름 통제의 적용 현황을 정기적으로 점검하여 정책 미준수 사항 식별 및 개선
N2SF-IF-M4	비인가 흐름 탐지 자동화	• 정책을 우회하거나 비정상적 흐름을 탐지하기 위한 자동화 도구 또는 시스템 구축
N2SF-IF-M5	통제 실패·예외 보고 체계	• 통제가 실패하거나 예외 발생 시 담당자에게 자동 보고하고 이를 기록하는 체계를 마련한다.
N2SF-EB-M3	외부 통신 로그 기록 및 감사	• 외부 통신 활동과 설정 변경 사항을 기록하고 감사 가능하도록 조치
N2SF-EB-M4	외부 경계 위협 탐지 자동화	• 이상 행위를 자동으로 탐지하는 시스템을 운영한다.
N2SF-EB-M5	비상 시 외부 통신 격리	• 침해 발생 시 외부 통신을 즉시 차단할 수 있는 절차를 마련한다.

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 모델 10. 무선 업무환경 운용 체계

부록 2-10