National
Network
Security
Framework

N2SF

국가 망 보안체계 실증 사례집

KISA 한국인터넷진흥원

본 사례집은 국가 망 보안체계(N2SF) 보안 가이드라인에 따라 국가·공공기관 업무환경을 대상으로 실증한 사례를 바탕으로 제작되었다. 사례집에서 제시하는 정보서비스 모델의 실증 결과는 기관이 보유한 네트워크 구성, 연동 시스템, 보안 정책 등 인프라 환경의 특성을 고려하여 N2SF 도입 시 참고 자료로 활용할 수 있다. N2SF 를 도입 희망하는 기관은 국가정보원의 N2SF 보안 가이드라인 및 본 사례집을 참고하여 기관에 최적화된 형태로 재설계하여 적용할 것을 권고한다.

발행 이력

순번	제·개정일	이력	담당
1	2026.4.13.	국가 망 보안체계(N2SF) 실증 사례집 발행	AI정부보호팀

목차

I. 국가 망 보안체계(N2SF) 실증 사업 개요 ····· 4

1. 추진 배경 ····· 5

2. 실증 모델 구성 ····· 7

II. 국가 망 보안체계(N2SF) 실증 수행 방법론 ····· 8

1. 실증 수행 절차 종합 ····· 9

2. 단계별 수행 절차 및 작성 방안 ····· 10

III. N2SF 정보서비스 모델별 실증 결과 ····· 22

1. [모델 1] 인터넷 단말의 업무 활용성 제고 ····· 23

2. [모델 2] 업무환경에서 생성형 AI 활용 ····· 41

3. [모델 3] 업무환경에서 외부 클라우드 활용 업무협업 체계 ····· 63

4. [모델 4] 업무 단말의 인터넷 이용 ····· 82

5. [모델 5] 공공데이터의 외부 AI 융합 ····· 108

6. [모델 8] 클라우드 기반 통합 문서체계 ····· 138

IV. 참고자료 ····· 165

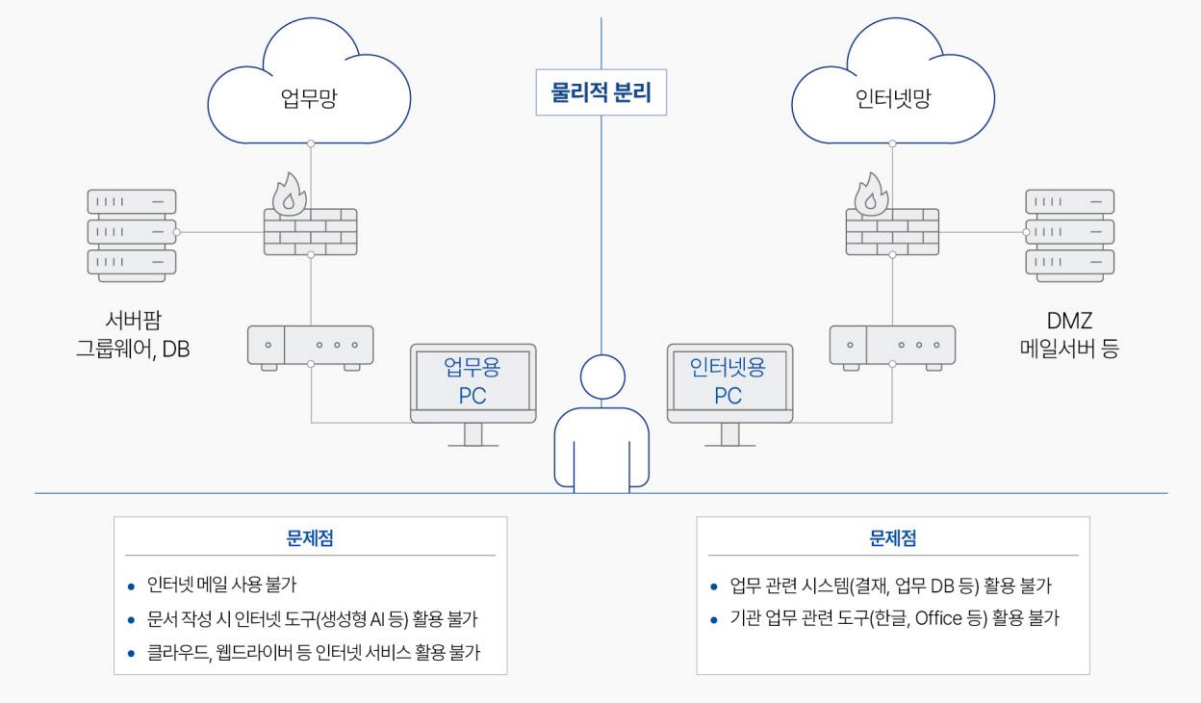
01

국가 망 보안체계(N2SF) 실증 사업 개요

KISA 한국인터넷진흥원

1. 추진 배경

최근 공공 정보화 환경에서는 생성형 AI, 클라우드, 외부 민간 서비스 연계, 데이터 기반 행정이 빠르게 확산되고 있는 반면, 기존의 국가 망 보안정책은 물리적 망분리를 전제로 한 일률적 통제 방식에 기반하고 있어, 변화된 업무환경을 유연하게 수용하는 관점에서 구조적인 한계를 드러내고 있다. 이에 따라 기존의 물리적 망 분리 정책을 개선하여 업무 효율성을 높이고자 하는 수요가 있으나, 외부 접점이 확대되면서 새로운 보안 위협에 노출될 가능성 또한 커지고 있다. 특히 정상 계정 탈취를 통한 내부망 침투나 지능화된 비인가 접근에 의한 정보 유출 위험은 경계 중심의 방어 체계만으로는 대응하기 어려운 현실이다. 따라서 모든 접근에 대해 지속적인 인증과 검증을 수행하고 데이터의 중요도에 따라 보안 통제를 차등 적용하는 체계 도입이 필요해졌다.



이에 국가정보원은 보안성을 확보하면서 공공데이터 활용 활성화와 업무 효율성 제고를 동시에 달성할 수 있는 '국가 망 보안체계(이하 N2SF)'를 수립하였다. N2SF는 정보서비스의 성격과 취급하는 업무정보의 중요도에 따라 보안 모델을 구분하고, 각 모델별로 최적화된 통제 항목을 설정하는 것을 핵심으로 한다. 이는 모든 시스템에 일률적인 보안정책을 적용하던 과거 방식에서 벗어나, 서비스별 위험도를 평가하여 차등적인 보안 가중치를 부여하고자 한다. 본 실증은 이러한 N2SF의 모델별 보안 통제 항목들이 실제 정부 기관의 정보서비스 운영 환경에서 원활히 작동하는지 확인하고, 도입을 검토 중인 기관에 구체적인 실무 데이터를 제공하고자 수행하였다.

실증 단계별로 도출된 산출물은 N2SF를 처음 접하는 기관들이 개별 정보서비스의 특성에 맞춰 보안 모델을 설계하고 구축하는 단계에서 활용하는 것을 목표로 한다. N2SF가 제시하는 모델별 보안 통제 항목이 실제 행정 현장의 복잡한 인프라 내에서 안정적으로 구동되는지 검증하고, 보안 강화와 업무 효율성 사이의 최적점을 도출하는 데 중점을 두었다.

실무 과정에서는 정보서비스 별 특성에 따른 네트워크 구성안, 보안 설정값, 다중 인증 체계 연동 등 현장에서 활용할 수 있는 결과물을 도출하였다. 본 사례집은 이러한 실증 과정의 산출물들을 체계적으로 정리하여 제공함으로써, 각 기관이 N2SF 기반의 보안 환경을 구성할 때 시행착오를 최소화하고 안정적인 체계 전환을 추진할 수 있도록 지원하고자 발간하였다.

국가 망 보안체계 보안 가이드라인 1.0 부록 2 – 정보서비스 모델

1	망 분리 인터넷 단말의 업무 효율성 제고	현행 망 분리된 인터넷 단말 기준, 인터넷 단말에서의 문서 편집기·협업 SW·클라우드 및 기관이 필요한 다양한 SW 를 자유롭게 활용
2	업무환경에서 생성형 AI 활용	업무 단말에서 ChatGPT 등 생성형 AI 서비스에 접속, 업무에 활용
3	업무환경에서 외부 클라우드 활용 업무협업 체계	업무 단말에서 업무 생산성·효율성 제고 목적 외부 협업도구(업무용 SaaS) 활용
4	업무 단말의 인터넷 이용	업무 단말 OS 의 악성코드 감염 차단 등 보안대책을 적용한 환경에서 인터넷 접속
5	공공데이터의 외부 AI 융합	국가·공공 클라우드(행정망)를 기반으로 업무정보의 AI 서비스 연계
6	연구 목적 단말의 신기술 활용	기관에서 지급한 연구 목적·업무환경에서 인터넷의 다양한 신기술 활용
7	개발 환경 편의성 향상 및 원격 개발	개발 환경에서 오픈소스 등 활용이 용이하도록 인터넷을 활용하고, 필요시 원격 개발 가능
8	클라우드 기반 통합 문서체계	기관 내·외부에서 통합 문서체계를 활용하여 업무자료 생산·공유·협업
9	모바일 업무환경 정보 연계	스마트폰, 태블릿 등 모바일 단말을 이용해 국가·공공기관 행정업무 서비스 활용
10	무선 업무환경 운용 체계	기관 청사 내에서 Wi-Fi 등 무선 업무환경 운용
11	정보 연계를 위한 CDS 구성	기관 내 보안영역 연계 지점에서, 도메인간 안전한 정보 전달 환경을 구성

본 사례집을 활용하는 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 본 실증 사례를 유연하게 참고해야 한다. 기관마다 보유한 정보 인프라의 형태와 취급하는 데이터의 성격이 상이하므로, 사례집에 수록된 시나리오별 실증 결과와 구성도를 자사의 운영 환경에 맞추어 검토하고 벤치마킹하는 과정이 필요하다. 이번 실증을 통해 확보된 결과물들이 각급 기관 보안 담당자들에게 실질적인 참고서 역할을 수행하기를 바라며, 이를 통해 향후 인공지능, 클라우드 등 보안 기술의 발전과 국가 망 보안 경쟁력 강화에 기여하고자 한다.

2. 실증 모델 구성

본 사례집은 국가 망 보안체계 적용을 위한 준비, 운용, 점검 등 전 과정에서 고려해야 하는 주요 절차와 기술적 사항을 체계적으로 정리하여 수록한다. 특히 기존 시스템과 신규 시스템의 특성을 반영하여 정보서비스 모델을 구분하고, 각 환경에 최적화된 보안통제 항목 설정 사례를 상세히 설명한다. 정부기관 업무망의 안정적 운영과 망간 보안 연계체계 강화에 중점을 두고 시스템에 필요한 보안 통제를 실증하였다. 이러한 구체적인 실증 결과물이 각 기관 담당자들에게 실질적인 가이드가 되어 국가 망 보안체계를 현장에서 안정적으로 도입하는 데 도움이 되도록 한다.

N2SF 정보서비스 모델 사례 구성

모델 1	인터넷 단말의 업무 효율성 제고
모델 2	업무환경에서 생성형 AI 활용
모델 3	외부 클라우드 활용 업무협업 체계
모델 4	업무 단말의 인터넷 이용
모델 5	공공데이터의 외부 AI 융합
모델 8	클라우드 기반 통합 문서체계

02

국가 망 보안체계(N2SF) 실증 수행 방법론

KISA 한국인터넷진흥원

1. 실증 수행 절차 종합

본 장에서는 『국가 망 보안체계 보안 가이드라인 1.0(이하 가이드라인)』에 명시된 N2SF 정보 서비스 도입을 위한 실증 수행 방법론을 제시한다.

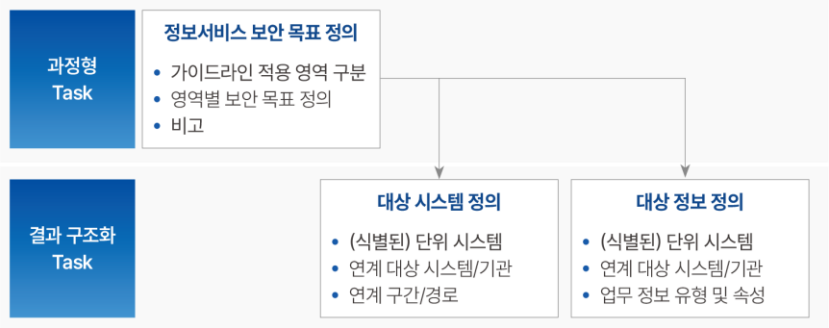
실증은 국가정보원 가이드라인에서 제시하는 절차대로 수행하였으며, 이외에 보안통제의 정합성 및 보안 안정성을 검증하기 위한 실증 및 점검을 추가 수행하였다. 추가 수행절차는 안전한 체계 도입을 위해 기관 환경에 따라 필요시 적용하면 된다.

실증 사례는 클라우드, SaaS, 외부 협업 서비스, 생성형AI 등 다양한 정보서비스가 활용되는 환경을 고려하여 N2SF 보안 가이드라인을 실증 환경에 맞게 적용하고 위협 식별 결과 기반으로 보안통제 항목을 선정하고, 통제 적용 지점(단말-연계체계-서비스)별 실증을 통해 향후 공공기관 확산을 위한 기술적·관리적 시사점을 도출하는 과정을 아래와 같은 수행 절차에 의거하여 추진하였다.

2. 단계별 수행 절차 및 작성방안

1) 준비

본 단계에서는 N2SF 가이드라인을 적용하는 시스템과 정보(또는 데이터) 범위를 정의하고 다음 단계인 보안등급 분류가 대상 범위의 누락 없이 시스템과 정보간 연결성을 확보하면서 수행될 수 있도록 대상 시스템 정의와 대상 정보 정의를 수행한다.

수행 목적	● 적용 범위 명확화: 가이드라인 적용 대상 시스템/정보 자산 범위 정의 ● 자산 목록화 기반 확보: 등급 분류를 위한 기초 자산 리스트 작성 ● 수행 결과 정합성 확보: 등급 분류 및 이후 절차와의 연계성 확보
고려 사항	● 범위 누락 방지: 내부망, 외부 연계 등 모든 연결 구간의 자산 포함 여부 확인 ● 정보와 시스템간 연결성 확보: 정보 정의 수준과 시스템 관계 확인 ● 문서 신뢰성 검증: 자료 제공 문서의 최신성/정확도 확인
Input	● 시스템 구성도 (응용, 인프라, 연계) ● 데이터 현황 자료 (상황에 따라 제공 가능한 개념적 데이터 목록 또는 데이터 테이블 정의서)
수행 절차	
Output	● 정보서비스 보안 목표 정의서 ● 대상 시스템 목록 ● 대상 정보 목록

제1단계에서 작성되는 Table에 대한 명칭, 작성 목적과 활용도는 아래와 같이 정의한다.

Table id	Table 명	특성	작성 목적/활용도
1-1	정보서비스 보안 목표 정의서	과정형	보안등급 분류 대상 범위를 분류하고 영역별 보안 목표를 정의함. 대상 시스템 및 정보 목록 정의를 위한 기본 자료 제공
1-2	대상 시스템 목록	결과 구조화	보안등급 분류 대상 시스템별 등급 분류 시 판단 근거가 될 기초 자료 정의
1-3	대상 정보 목록	결과 구조화	보안등급 분류 대상 정보 유형별 등급 분류 시 판단 그거가 될 기초 자료 정의

또한 각 Table을 구성하는 컬럼에 대한 작성 가이드는 아래와 같다.

Table id	Table 명	컬럼명	작성 가이드
1-1	정보서비스 보안 목표 정의서	영역	데이터가 저장/연계되는 시스템 영역, 연계 채널 및 네트워크 영역을 구분
		보안 목표	각 영역별 보안 확보를 위한 기본 방향 제시
		비고	보안등급 분류를 위한 추가 정보. (예: 시스템의 위치)
1-2	대상 시스템 목록	단위 시스템	정보서비스 보안 목표 정의서에서 도출된 시스템 나열
		연계 시스템	단위 시스템과 연계되는 내/외부 시스템 명시
		연계 기관	내/외부 연계 시스템을 운영하는 기관 명시
		연계 구간	외부 연계 시스템과 연계되는 인프라 명칭 표기 (예: 외부망 연계 구간)
		연계 경로	내외부 연계 구간의 망 표기 (예: 내부 업무망 ↔ 외부 서비스)
1-3	대상 정보 목록	단위 시스템	정보서비스 보안 목표 정의서에서 도출된 시스템 나열
		연계 시스템	단위 시스템과 연계되는 내/외부 시스템 명시
		연계 기관	내/외부 연계 시스템을 운영하는 기관 명시
		정보 유형	연계되는 정보를 누락되지 않게 분류하여 명시
		정보 속성	정보의 생성, 저장, 처리, 이동 목적 중심으로 기술
		정형/비정형	정형/비정형 정보 분류

아울러 제1단계 산출물 작성 시 근거가 되는 자료(목표 아키텍처 구성도 등)는 시스템 운영 기관에서 제공하는 자료와 담당자 인터뷰를 통해 확보한다.

2) C/S/O 등급 분류

본 단계에서는 N2SF 가이드라인에 따라 시스템과 업무정보(또는 데이터)에 대한 적정 보호 수준을 정의하고 실효성 있는 보안 등급(C/S/O)을 분류하여, 다음 단계인 보안 시나리오에 대한 보안 위협 요소 및 근거가 누락 없이 식별될 수 있도록 시스템과 업무정보의 보안 등급 분류를 수행한다.

기밀정보 **C 등급, Classified**	비밀, 안보·국방·국방·외교·수사등 기밀정보 및 국민 생활·생명·안전과 직결된 비공개 정보로, 정보공개법 제 9 조제 1 항제 1-4 호가 이에 해당한다.
민감정보 **S 등급, Sensitive**	개인·국가 이익 침해가 가능한 비공개 정보로, 감사·감독·시험·입찰계약·인사관리 ·개인정보 등 정보공개법 제 9 조제 1 항제 5-8 호가 이에 해당한다.
공개정보 **O 등급, Open**	공개 가능한 일반정보로, 기밀·민감정보 이외의 모든 정보, 별도 조치(비식별 등)한 행정·민감정보 및 비공개 필요성 소멸 정보 등이 이에 해당한다.

수행 목적	● 업무정보와 시스템에 대한 적정 보호 수준 정의 ● 업무정보와 시스템간 등급 불일치로 인한 보안 취약 요인 근거 확보 ● 업무 특성을 고려하여 실효성 있는 보안등급 적용
고려 사항	● 보안 등급 분류 목적성과 거리가 있는 BRM 분류체계의 특성을 고려하여 시스템 운영의 목적과 관련 법규 등의 유관 자료 추가 분석 ● 다수의 시스템과 연계되는 정보에 대한 등급 분류 오류 여부 검증 (해당 사례 발생 시 식별된 등급 중 가장 높은 등급 부여)
Input	● 대상 시스템 목록 ● 대상 정보 목록 ● BRM 정의서 (범정부 정보자원관리시스템(IRM) 자료)
수행 절차	
Output	● 정보별 보안등급 분류 결과서 ● 시스템별 보안등급 분류 결과서

제2단계에서 작성되는 Table에 대한 명칭, 작성 목적과 활용도는 아래와 같이 정의한다.

Table id	Table 명	특성	작성 목적/활용도
2-1	BRM 기반 업무정보 특성 분석표	과정형	BRM 기반의 업무적 특성을 반영한 정보 보안등급 초도 분류. '정보별 등급 분류 결과표'와 대조되는 자료로 활용
2-2	업무정보 vs 시스템 매핑표	과정형	정보 연계 구조를 정확히 파악하기 위한 기본 작업으로 '시스템간 연계 구조 분석표'의 근거 자료 제공
2-3	정보별 시스템간 연계 구조 분석표	과정형	시스템 내외부의 정보 흐름 파악. 정보별 등급 분류 결과표와 시스템별 등급 분류 결과표의 근거 자료 제공
2-4	정보별 등급 분류 결과표	결과 구조화	제 3 단계 위험 시나리오 분석의 근거가 되는 보안 등급 분류 결과 제공
2-5	시스템별 등급 분류 결과표	결과 구조화	제 3 단계 위험 시나리오 분석의 근거가 되는 보안 등급 분류 결과 제공

또한 각 Table을 구성하는 컬럼에 대한 작성 가이드는 아래와 같다.

Table id	Table 명	컬럼명	작성 가이드
2-1	BRM 기반 업무정보 특성 분석표	정보 유형	1 단계에서 작성된 대상 정보 목록 내용 기입
		정보 속성	
		연계시스템	
		연계 기관	
		연계 경로	
		정형/비정형	
		정보 처리 목적	정보 공개 민감도를 파악할 수 있는 내용 중심으로 정보의 활용 용도 기입
		BRM 분류체계	BRM 의 대분류, 중분류, 세부 업무, 기능 도메인 내역 반영
		관련 법규	연계 시스템 운영 근거 법령 정보 조사. 정보 공개 관련 조문 확인
		등급 후보값	Table 내 컬럼내에 기술된 등급 연관 키워드를 분석하여 C/S/O 등급 기입
		판정 근거	정보공개법 제 9 조 요건, 관련 법규, 컬럼에서 발견된 키워드 등을 기입
2-2	업무정보 vs 시스템 매핑표	[시스템 명#1]	특정 유형의 정보가 생성, 저장, 처리, 이동되는 경우 체크 표시
		[시스템 명#2]	
		[시스템 명#3]	
2-3	정보별 시스템간 연계 구조 분석표	정보 유형	BRM 기반 업무정보 특성 분석표 내용 기입
		정보 속성	
		Source 시스템	시스템간 연계 케이스별 송신 시스템 기입
		Target 시스템	시스템간 연계 케이스별 수신 시스템 기입
		망 연계 경로	시스템간 연계 케이스의 망 경로 기입 (예: 업무망 내, 업무망 ↔ 인터넷망 등)
2-4	정보별 등급 분류 결과표	정보 유형	정보별 시스템간 연계 구조 분석표 내용 기입
		정보 속성	
		정보 비공개 관련 속성 키워드	BRM 기반 업무정보 특성 분석표 내용 및 추가 식별된 비공개 관련 속성 기입

Table id	Table 명	컬럼명	작성 가이드
		판정 근거	정보공개법 제 9 조 등 참조한 C/S/O 분류 판단 기준 기입
		C/S/O 분류 결과	등급 연관 키워드 및 관련 근거를 기반으로 C/S/O 등급 기입
2-5	시스템별 등급 분류 결과표	시스템명	대상 시스템 목록의 시스템 명 기입
		주요 기능	시스템의 정보보안 중요도/민감도를 판단하기 위한 기능 내역 기입
		데이터 특성	시스템 내 생성, 처리되는 정보의 보안 민감도를 판단하기 위한 특성 정보 기입
		망 환경	정보별 시스템간 연계 구조 분석표의 망 연계 경로 내역을 참고하여 기입
		현행 보안 통제 기술	시스템별 적용되는 보안통제 기술을 조사하여 기입
		C/S/O 분류 결과	Table 내 기술된 등급 연관 키워드를 기반으로 C/S/O 등급 기입

아울러 제2단계 산출물 작성 시 근거가 되는 자료(실데이터/업무기능 등)는 시스템 운영 기관에서 제공하는 자료와 담당자 인터뷰를 통해 확보한다.

3) 위험식별

본 단계에서는 N2SF 가이드라인에 따라 분류한 정보시스템 및 업무정보 보안 등급을 기반으로 정보 이동·저장 구조를 분석하여 정보 서비스 모델 유형(모델1~모델11)을 식별하고, 위치, 주체, 객체 조합별 보안 위협 시나리오 정의를 수행한다.

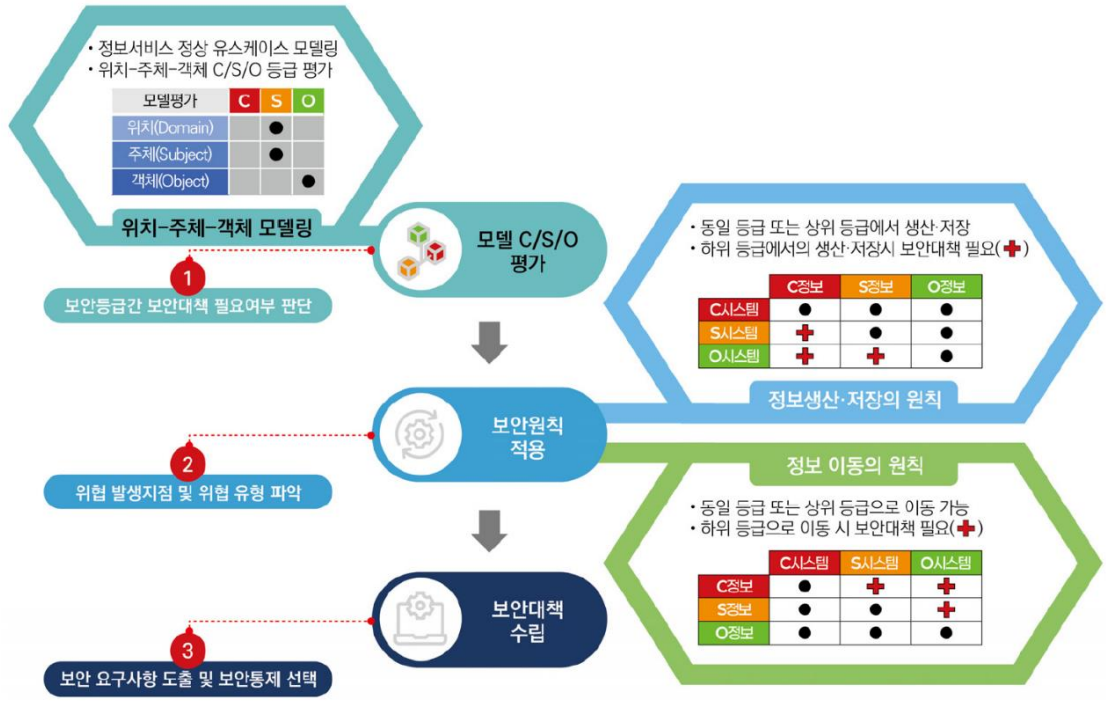
위치-주체-객체 구분

위치	**어디서 접속하는가?**	정보가 보관된 장소 또는 사용자가 접속하는 물리적/논리적 공간을 뜻하며, 업무망, 인터넷망 등이 이에 해당한다.
주체	**누가 접속하는가?**	정보에 접근하여 행위 하려는 대상을 뜻하며, 업무 단말, 기관 시스템 등이 이에 해당한다.
객체	**무엇을 이용하는가?**	주체가 접근하여 읽거나 쓰거나 수정, 활용하려는 대상을 뜻하며, 업무정보, 생성형 AI 서비스, 인터넷 서비스, 문서 편집 SW 등이 이에 해당한다.

"C/S/O 보안등급"과 "위치-주체-객체 구분"의 관계

위치-주체-객체 구성요소의 보안등급이 같을 경우	보안 원칙에 위배되지는 않는다.
위치-주체-객체 구성요소의 보안등급이 다를 경우	보안 원칙에 위배되어 보안대책을 마련하여야 한다. 높은 등급의 업무정보가 낮은 등급의 위치-주체-객체에서 다뤄질 경우, 업무정보 생산·저장·이동에 대한 보안대책이 필요하다. 반면에 낮은 등급의 업무정보가 높은 등급의 위치-주체-객체에서 다뤄질 경우, 보안 원칙에 위배되지는 않는다.

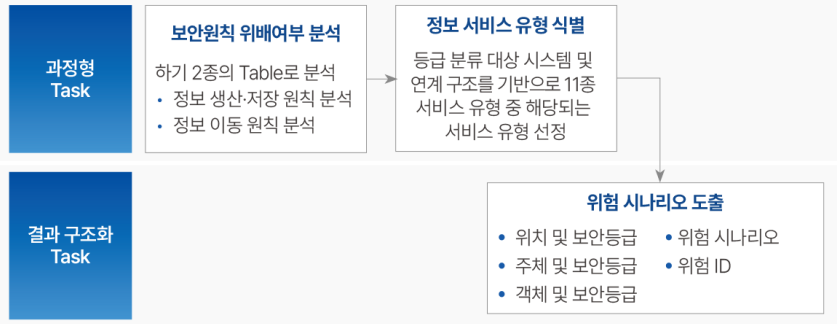
정보서비스에 대한 모델 C/S/O 평가 및 보안원칙 적용



※ (출처) N2SF 보안 가이드라인 1.0

수행 목적	• C/S/O 등급 기준에 맞지 않는 정보 이동·저장 구조를 발견하여 보안정책 미준수 영역 발견 • 서비스 유형별 보안 위험 요소 체계화 • 위치, 주체, 객체 조합별 보안 취약 상황을 시나리오 형태로 표현
고려 사항	• 위험 시나리오 정의 시, 제 4 단계의 통제 항목 선정까지 고려하여 가이드라인 부록 2 에 제시된 '정보서비스 보안위협'과 부합하는 단문 중심으로 표현되어야 함
Input	• 정보 보안 등급 분류 결과 • 시스템 보안 등급 분류 결과

수행 절차



Output	● 위험 시나리오 목록

제3단계에서 작성되는 Table에 대한 명칭, 작성 목적과 활용도는 아래와 같이 정의한다.

Table id	Table 명	특성	작성 목적/활용도
3-1	정보 생산, 저장 원칙 분석표	과정형	정보와 시스템의 보안 등급 분류 결과에 따른 보안 원칙 위배 케이스 발생 여부 식별. 보안 원칙 위배 사례 유형화를 통해 차후 위험 시나리오 및 대응방안 수립을 위한 근거 자료 제공
3-2	정보 이동 원칙 분석표	과정형	
3-3	정보서비스 유형 식별표	과정형	위험 시나리오 수립 대상 정보 서비스 범위 확인
3-4	위험 시나리오 목록	결과 구조화	정보 및 시스템 보안 관점에 부합하는 최적의 보안통제 방안 수립을 위한 위험 시나리오 정의

또한 각 Table을 구성하는 컬럼에 대한 작성 가이드는 아래와 같다.

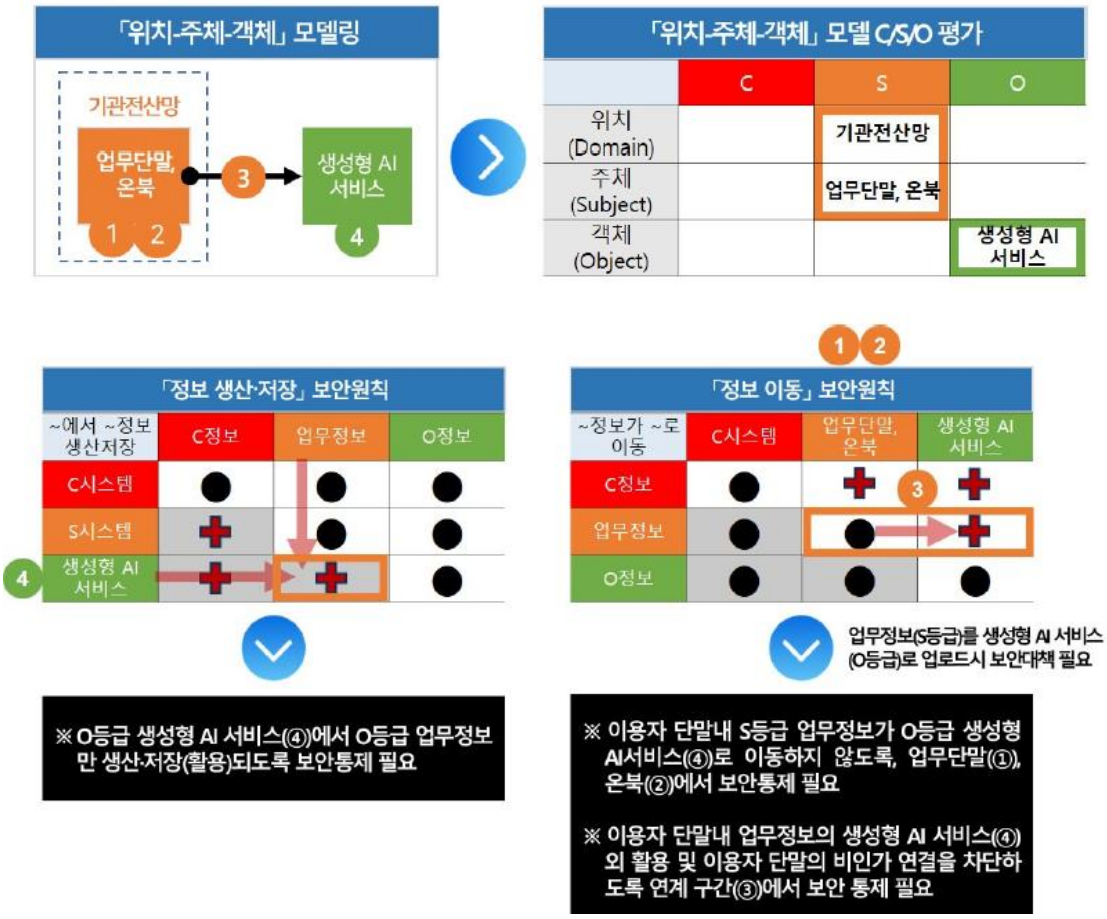
Table id	Table 명	컬럼명	작성 가이드
3-1	정보 생산, 저장 원칙 분석표	정보 유형	정보별 등급 분류 결과표 내용 기입
		정보 등급	
		시스템 명	시스템별 등급 분류 결과표 내용 기입
		시스템 등급	
		정보 생산, 저장 원칙 판정	정보 등급과 시스템 등급간 비교를 통해 적합 또는 위반 기입
		대응 조치/비고	보안 원칙 위반 사례에 대한 적정 대응방안 조사 및 내용 기입

Table id	Table 명	컬럼명	작성 가이드
3-2	업무정보 vs 시스템 매핑표	정보 유형	정보별 등급 분류 결과표 내용 기입
		정보 등급	
		Source 시스템/등급	시스템별 등급 분류 결과표 내용 기입
		Target 시스템/등급	
		정보 이동 원칙 판정	정보 등급과 시스템 등급간 비교를 통해 적합 또는 위반 기입
		대응 조치/비고	보안 원칙 위반 사례에 대한 적정 대응방안 조사 및 내용 기입
3-3	정보서비스 유형 식별표	정보서비스 유형명	가이드라인에 명시된 11 개 서비스 유형명
		부합 여부 분석 결과	서비스 유형을 판정할 수 있는 분석 대상 시스템/망 구조 특징 기술
3-4	위험 시나리오 목록	위치 및 보안등급	망 경계 관점의 망 위치 및 해당 위치의 보안 등급
		주체 및 보안등급	접속 단말 명시 및 해당 단말의 보안 등급
		객체 및 보안등급	접속 시스템 명시 및 해당 시스템의 보안 등급
		위험 시나리오	위치/주체/객체를 종합 고려하여 발생 가능한 보안 위험 케이스를 N2SF 가이드라인에서 정의한 보안위협 항목과 동일하게 (불가피한 경우 유사하게) 위협 요인을 간단/명료하게 기입
		위험 ID	도출된 위험 시나리오에 대해 위치/주체/객체와 관계없이 동일 보안위협 항목에 동일 ID 를 부여 (중복성 회피)

정보서비스 위치-주체-객체 구성요소의 C/S/O 보안등급을 고려하여 위험식별 및 보안대책 필요성에 대하여 판단할 수 있다.

아울러 제3단계 산출물 작성 시 'N2SF 보안 가이드라인 1.0 (부록2) 정보서비스 모델 해설서'를 참고하고, 근거가 되는 자료는 시스템 운영 기관에서 제공하는 자료와 담당자 인터뷰를 통해 확보한다.

위치-주체-객체 모델링 및 C/S/O 평가, 보안원칙 적용 예시

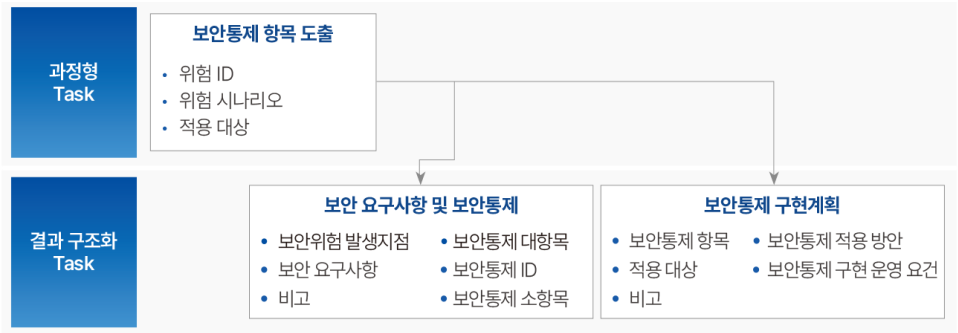


※ (출처) N2SF 보안 가이드라인 1.0 - (부록2) 모델2 업무환경에서 생성형 AI 활용

4) 보안대책 수립

본 단계에서는 N2SF 가이드라인에 따라 식별된 위험 시나리오를 기반으로 보안 적용 대상 별 보안통제 항목을 정의하고, 보안통제 적용 방안(시스템 개발, 솔루션 구현 등)을 도출하여 보안통제 구현 및 운영 요건을 보안 위협으로부터 시스템의 안정성을 확보할 수 있도록 수립한다.

수행 목적	● 위험 시나리오에 대응하는 통제항목을 합당한 근거를 통해 도출 ● 통제 항목의 발생지점, 운영방안간 일관성을 확보하여 실행 가능성 강화
고려 사항	● 보안통제 항목 선정 시 보안등급을 참조하되, 보안요건 키워드는 위험 시나리오와 발생지점으로부터 도출 ● 보안통제 항목이 지나치게 포괄적으로 선정되지 않도록 유의 ● 보안통제 구현 및 운영 측면의 요건을 동시 고려
Input	● 위험 시나리오 목록

수행 절차	
Output	• 보안 요구사항 및 보안통제 목록 • 보안통제 구현계획

제3단계에서 작성되는 Table에 대한 명칭, 작성 목적과 활용도는 아래와 같이 정의한다.

Table id	Table 명	특성	작성 목적/활용도
4-1	보안통제 항목 표	과정형	위험 시나리오에 명시된 보안 위험 요인을 방지 및 저감하기 위한 적정 보안통제 항목 도출 보안위험 발생지점별 보안 요구사항에 부합하는 보안통제 항목 식별
4-2	보안 요구사항 및 보안통제 표	결과 구조화	
4-3	보안통제 구현계획 표	결과 구조화	도출된 보안통제 항목에 대한 구현 및 운영을 위한 방안 정의

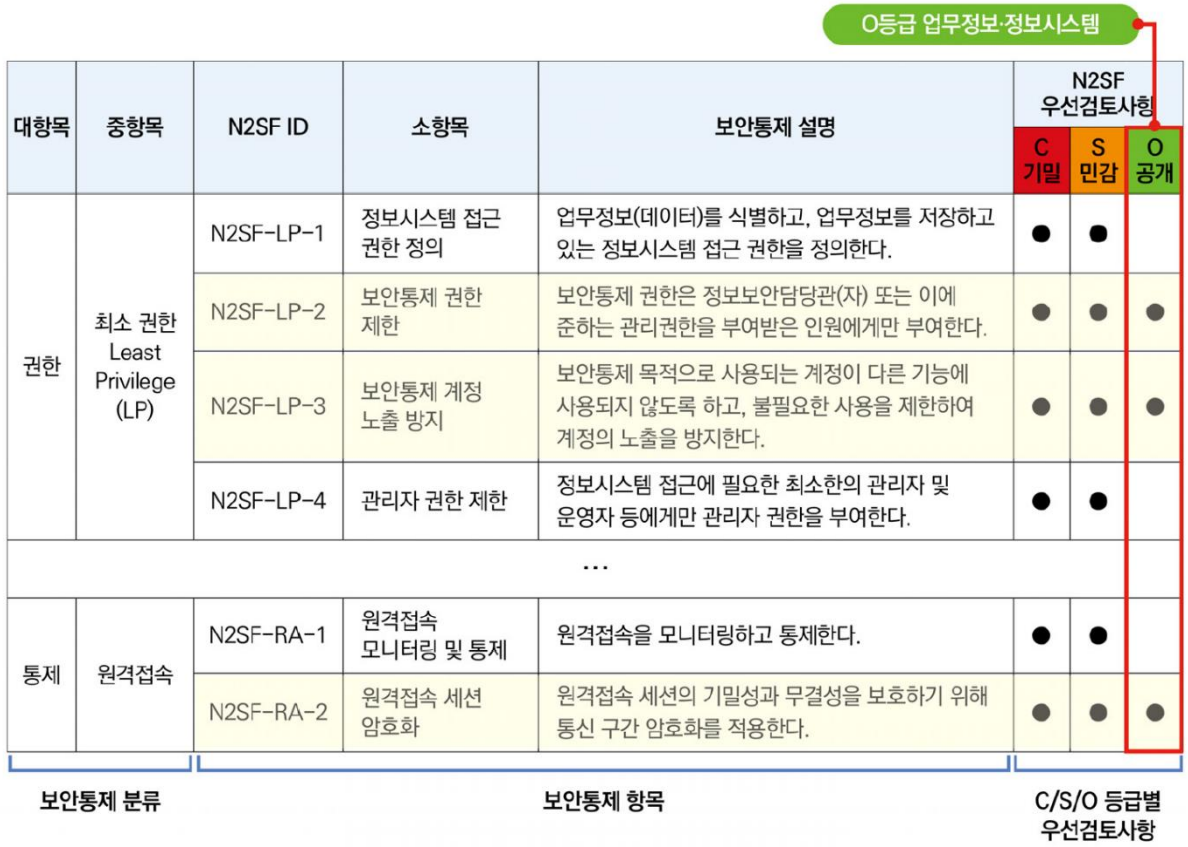
또한 각 Table을 구성하는 컬럼에 대한 작성 가이드는 아래와 같다.

Table id	Table 명	컬럼명	작성 가이드
4-1	보안통제 항목 표	위험 ID	위험 시나리오 목록의 내용 기입
		위험 시나리오	위험 시나리오 목록의 내용 기입
		적용 대상	위치/주체/객체 내용중 주체와 객체에 있는 단말, 시스템, 연계시스템 내용 기입
4-2	보안 요구사항 및 보안통제 표	보안위험 발생지점	보안통제 항목표의 적용 대상 내용 기입

Table id	Table 명	컬럼명	작성 가이드
		보안 요구사항	보안통제 항목표의 위험시나리오 내용과 매칭되는 보안 요구사항을 가이드라인을 참조하여 동일하게 (부득이한 경우 유사하게) 기입
		보안통제 대항목	보안통제 소항목 ID와 매칭되는 소항목을 가이드라인을 참조하여 기입
		보안통제 소항목 ID	보안통제 대항목 내에 있는 소항목 ID를 가이드라인을 참조하여 기입
		보안통제 소항목	보안통제 소항목 ID와 매칭되는 소항목을 가이드라인을 참조하여 기입
		비고	보안통제 항목이 가이드라인에 없는 자체 도출 항목인 경우 내용 표기
4-3	보안통제 구현계획 표	보안통제 항목	보안통제 항목표의 내용 기입 (복수개의 보안통제 항목 나열 가능)
		적용 대상	보안통제 항목표의 내용 기입
		보안통제 적용 방안	솔루션 구현, 시스템 개발 등의 보안통제 적용 수단 기술
		보안통제 구현 운영 요건	보안통제 구현 및 운영 관점의 주요 요건 기술
		비고	보안통제 구현 관련 추가적인 참고사항 기술

아울러 제4단계 산출물 작성 시에는 시스템 운영 기관과의 협의를 통해 설계된 보안체계가 실제 운영 환경에서 문제없이 작동할 수 있도록 보안 솔루션 간의 최적화 및 시스템 구현·운영 가능성 등을 검토한다. 이후 네트워크 구성, 데이터 처리경로 등 다방면으로 검토하여 보안통제 요소가 구체적으로 명시된 시스템 구성도를 작성한다.

국가 망 보안체계 보안통제 항목 선택 방법 예시



※ (출처) N2SF 보안 가이드라인 1.0

5) 적절성 평가·조정

본 단계에서는 N2SF의 전체 단계에서 필수 요구 활동이 올바르게 이행되었는지 평가하고, 도출된 미흡 사항에 대해서는 보안대책 조정, 보완 조치 등을 수행한다. 이러한 일련의 체계적인 검증 과정을 거쳐 확보된 산출물을 종합적으로 정리하여, 이를 기반으로 국가정보원의 보안성 검토를 신청할 수 있다.

03

N2SF 정보서비스 모델별 실증 결과

KISA 한국인터넷진흥원

1. [모델 1] 인터넷 단말의 업무 활용성 제고

본 정보서비스 모델은 기관 전산망 내 망분리된 O등급 영역의 이용자 단말(인터넷 단말 등)에서 문서편집기 및 기타 SW를 설치·이용하며, 협업 SW·클라우드 서비스 등의 인터넷 서비스를 접속하여 업무 활용성을 제고하는 모델이다.

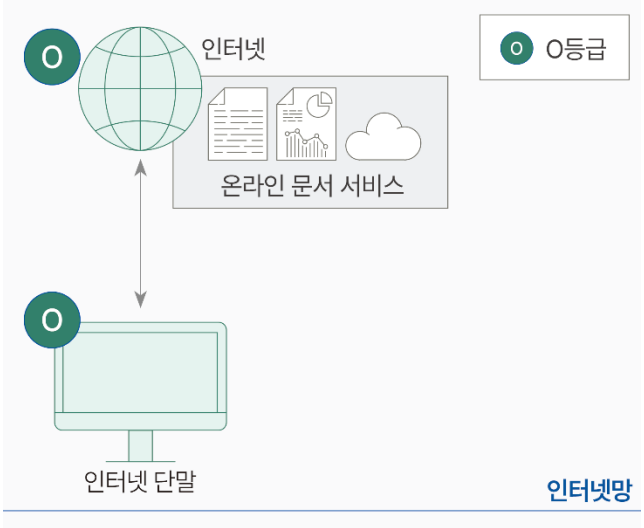
※ (참고자료) N2SF 보안 가이드라인 1.0 - (부록2) 모델1 인터넷 단말의 업무 활용성 제고

본 실증 사례는 망 분리 환경의 인터넷 단말에서 문서 작성 및 생성형 AI를 안전하게 사용하기 위해 2개의 정보서비스 모델을 활용한다. 업무망에서만 문서 생성이 가능한 환경에서, 외부 연결된 인터넷망에서도 공개 가능한 문서를 생성하고 외부 공유가 가능하도록 구현하는 데 중점을 둔다. 이는 기존 망 분리 환경의 인터넷 단말에서 사용이 제한되었던 문서 편집기, 협업 SW, 생성형 AI를 설치·활용함으로써, 업무 활용성을 제고하고자 한다.

각 기관에서는 망 분리가 적용된 환경에서 인터넷 단말의 문서 편집 및 생성형 AI 사용 환경을 구현하여 물리적 제약을 해소하고자 할 때 참고할 수 있다.

1.1 정보서비스 유형 요약

정보서비스 유형 / 모델 No. (N2SF 가이드라인 기준)		모델 1 / 인터넷 단말의 업무 활용성 제고 모델 2 / 업무환경에서 생성형 AI 활용
정보서비스 개요	업무정보	① 기밀 기관 고유업무정보 ② 민감 기관 고유업무정보 ③ 기관 고유업무 자료 ④ 인터넷 수집 정보 ⑤ 인터넷 수집 기반 내부 가공 정보
	정보시스템	① 인터넷 단말 ② 인터넷 서비스
	정보서비스 사용 시나리오	① 인터넷 수집 정보 반입
위치/주체/객체 관점의 정보서비스 구조		



- 인터넷망(O 등급)에서
  인터넷 단말(O 등급)로
  생성형 AI 등 인터넷 서비스(O 등급) 사용

- 위치: 인터넷망(O 등급)
  주체: 인터넷 단말(O 등급)
  객체: 생성형 AI 등 인터넷 서비스(O 등급)

보안통제 대상	① 인터넷 단말 ② 인터넷 연계체계 ③ 생성형 AI 연계체계 ④ 생성형 AI

1.2 최종산출물 서식

[1] 정보서비스 사용 시나리오별 정보시스템 식별

정보서비스 사용 시나리오별 정보시스템 식별

번호	사용 시나리오	관련 정보시스템
1	인터넷 정보 수집	
1-1	인터넷 단말에서 인터넷 서비스를 통해 논문, 보안 기준문서, 취약점 정보, 생성형 AI 결과물 등을 검색·열람	㉠ 인터넷 단말 ㉡ 인터넷 서비스

[2] 정보서비스 보안목표

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 1번 「정보서비스 보안목표」는 아래와 같이 정리됨

No.	영역	보안 목표	비고
1	공통	정보서비스 모델 1. 인터넷 단말의 업무 활용성 제고 구현	N2SF 가이드라인 1.0
2		정보서비스 모델 2. 업무환경에서 생성형 AI 활용 구현	N2SF 가이드라인 1.0
3	네트워크	업무망과 인터넷망은 분리하여 상호 간 직접 통신을 차단하고, 망 간 자료 이동은 허가된 절차를 통해서만 수행되도록 관리	자체
4		인가된 사용자·단말만 업무망 및 인터넷망에 접근할 수 있도록 통제하고, 비인가 단말은 격리·차단 조치 수행	N2SF 가이드라인 1.0
5	업무 단말	비인가 소프트웨어 설치·실행 차단	N2SF 가이드라인 1.0
6		악성코드가 유입·실행되지 않도록 지속적 검사 수행	N2SF 가이드라인 1.0
7		업무 단말에서 생성·저장되는 기밀·민감 기관 고유업무정보는 인터넷 서비스으로의 직접 전송·업로드가 불가능하도록 기술적 차단 조치 적용	N2SF 가이드라인 1.0

No.	영역	보안 목표	비고
8	인터넷 단말	기밀·민감정보 취급 업무정보에 대해 접근권한 통제, DRM 및 로그감사를 적용하여 내부 사용자 오남용 및 비인가 유출 방지	N2SF 가이드라인 1.0
9		생성형 AI 활용 등 인터넷 서비스 사용을 위한 기관 고유업무 자료 반출 시 결재 기반의 통제체계 확립	자체
10		악성코드가 유입·실행되지 않도록 지속적 검사 수행	N2SF 가이드라인 1.0
11		반출이 승인된 기관고유 업무 자료라도 기밀·민감정보가 포함될 가능성이 있으므로, 키워드·패턴·문맥 기반의 필터링을 적용하여 중요정보 유출을 방지	N2SF 가이드라인 1.0

[3] C/S/O 등급분류

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 2번 「C/S/O 등급분류표」는 아래와 같이 정리됨

No.	정보시스템		업무정보		비고
	명칭	C/S/O 등급	명칭	C/S/O 등급	
1	인터넷 단말	O	기관 고유업무 자료	S	반출 승인 허가 확인 필요
			인터넷 수집 정보	O	
2	인터넷 서비스	O	기관 고유업무 자료	S	반출 승인 허가 확인 필요
			인터넷 수집 정보	O	

[4] 위협 식별 - 모델링 및 C/S/O 평가

기관의 정보서비스 구성요소에 따라 유스케이스별로 모델링 및 C/S/O 보안등급을 나누어 평가하며, 「정보 생산·저장」 보안원칙과 「정보 이동」 보안원칙을 적용하여 보안대책의 필요성을 평가한다.

N2SF 보안 가이드라인*에서 본 정보서비스는 기관 전산망 내 **망분리된 영역(위치, O등급)**에 위치하는 **인터넷 단말(주체, O등급) 및 인터넷 영역에 위치하는 서비스(객체, O등급)**로 구성되며, O등급 인터넷 단말, 인터넷 서비스에서 O등급 업무정보만 생산·저장(활용), 이동하도록 보안원칙을 제시하고 있다. 아래 제시하는 실증 사례 및 N2SF 보안 가이드라인에 대하여 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 유연하게 참고하여 보안 원칙을 수립하여야 한다.

* N2SF 보안 가이드라인 1.0 - (부록2) 모델1 인터넷 단말의 업무 활용성 제고

사례: 인터넷 정보 수집

(1) 인터넷 단말에서 인터넷 서비스를 통해 논문, 보안 기준문서, 취약점 정보, 생성형 AI 결과물 등을 검색·열람

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C 등급 / S 등급 / O 등급 위치 Domain / 인터넷망 주체 Subject / 인터넷 단말 객체 Object / 인터넷 서비스 인터넷망(O 등급)에서 인터넷 단말(O 등급)을 이용해 인터넷 서비스(O 등급)를 이용하는 경우, 위치, 주체, 객체 모두 O 등급으로 같아 보안 대책 불요.	아니오
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C 정보 / S 정보 / 인터넷 수집 정보 C 시스템 / ● / ● / ● S 시스템 / + / ● / ● 인터넷 단말 / + / + / ● 인터넷 단말(O 등급)에서 인터넷 서비스(O 등급)를 사용하여 생산·저장된 인터넷 수집 정보은 인터넷 서비스을 통해 생성된 데이터이므로 O 등급에 해당됨. 따라서, 인터넷 단말과 이에 생성·저장되는 인터넷 수집 정보 모두 O 등급이므로 보안 대책 불요.	아니오
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / S 시스템 / 인터넷 단말 C 정보 / ● / + / + S 정보 / ● / ● / + 인터넷 수집자료 / ● / ● / ● 인터넷 서비스(O 등급)로부터 생성된 인터넷 수집 자료(O 등급)는 인터넷 단말(O 등급)에 이동됨. 인터넷 수집 자료와 인터넷 단말 모두 O 등급이므로 보안 대책 불요.	아니오

[5] 보안요구사항 및 보안통제

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 3번 「보안 요구사항 및 보안통제」는 아래와 같이 작성할 수 있다.

※ 보안 가이드라인에 없는 신규 자체정의 보안통제 항목: N2SF-ORG3

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
1	인터넷 단말	이용자 단말 보안성 유지	N2SF-LP-1 N2SF-DA-1 N2SF-DA-2 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-8 N2SF-IN-10 N2SF-IN-16	N2SF 모델 1번 N2SF 모델 2번
		이용자 단말 사용 보안	N2SF-AM-2 N2SF-AM-9 N2SF-DV-6 N2SF-DV-8	N2SF 모델 1번 N2SF 모델 2번
		이용자 단말 네트워크 보안	N2SF-SG-4 N2SF-SG-5 N2SF-SG-6 N2SF-IF-9 N2SF-EB-6 N2SF-SN-1 N2SF-WA-7 N2SF-BC-1 N2SF-DT-1	N2SF 모델 1번 N2SF 모델 2번
		이용자 단말 데이터 보호	N2SF-DU-2	N2SF 모델 2번
		이용자 계정 정보 보호	N2SF-IM-1	N2SF 모델 2번
		생성형 AI 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1 N2SF-EB-M1 N2SF-DU-M3	N2SF 모델 2번

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
		인터넷 수집 정보와 반출 정보 분리 저장·관리	N2SF-ORG3-1	자체정의 통제항목
2	인터넷 연계체계	업무 무관 유해사이트(게임, 도박 등) 및 비인가 사이트 접속 통제	N2SF-EB-1 N2SF-EB-2 N2SF-EB-14 N2SF-EB-15 N2SF-EB-M2	N2SF 모델 1번
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3 N2SF-IF-5	N2SF 모델 1번
		연계체계 보안성 유지	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-13 N2SF-DV-4 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-11	N2SF 모델 1번
		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-IF-M1 N2SF-IF-M2 N2SF-IF-M3 N2SF-IF-M4	N2SF 모델 1번

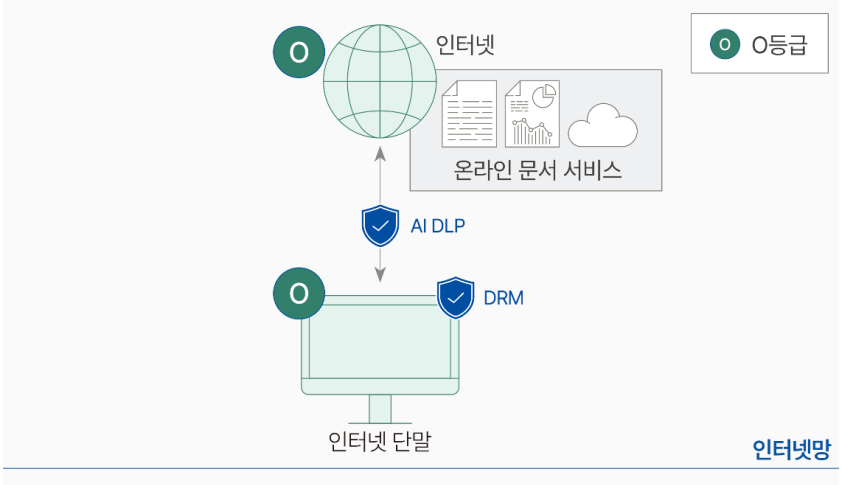
No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
			N2SF-IF-M5 N2SF-EB-M3 N2SF-EB-M4 N2SF-EB-M5	
3	AI 연계체계	생성형 AI 서비스 이용자 및 단말 인증	N2SF-AC-1 N2SF-AC-1(1) N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-1(4) N2SF-AC-3 N2SF-AC-3(2) N2SF-DA-3 N2SF-DA-4 N2SF-LI-1 N2SF-LI-2 N2SF-LI-4	N2SF 모델 2번
		비인가 네트워크 연결 차단	N2SF-IS-4 N2SF-IF-1 N2SF-IF-9 N2SF-EB-1 N2SF-EB-2 N2SF-EB-3 N2SF-EB-5 N2SF-EB-6 N2SF-EB-14 N2SF-EB-15	N2SF 모델 2번
		생성형 AI 서비스 활용 시 데이터 보호	N2SF-IF-2 N2SF-IF-6 N2SF-IF-7 N2SF-IF-8 N2SF-IF-10 N2SF-IF-14	N2SF 모델 2번
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3 N2SF-IF-5	N2SF 모델 2번
		연계체계 보안성 유지	N2SF-LP-4 N2SF-LP-4(1) N2SF-LP-4(4)	N2SF 모델 2번

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
			N2SF-AC-1(5) N2SF-AC-3(1) N2SF-EB-8 N2SF-EB-10 N2SF-EB-11 N2SF-EB-13 N2SF-DV-4 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-11	
		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-IF-M1 N2SF-IF-M2 N2SF-IF-M3 N2SF-IF-M4 N2SF-IF-M5 N2SF-EB-M3 N2SF-EB-M4 N2SF-EB-M5	N2SF 모델 2 번
4	생성형 AI	생성형 AI 서비스 계정 관리	N2SF-EI-M1	N2SF 모델 2 번
		생성형 AI 서비스 활용 데이터 관리	N2SF-DU-M3	N2SF 모델 2 번

[6] 보안통제 구현계획

국가정보원 보안성 검토 시 제출하는 문서 중, 자국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 4번 「보안통제 구현계획표」는 아래와 같이 작성할 수 있다.

보안통제적용 정보서비스 구성도



(가) 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
1	N2SF-LP-1	인터넷 단말	계정·접근제어 시스템을 통해 권한 승인/변경을 중앙 관리	권한 변경 이력 로깅·보관 및 정기 점검	PDP (ICAM)
2	N2SF-DA-1	인터넷 단말	부팅 구성정보·펌웨어 무결성 점검을 자산관리/EDR로 수행	무결성 실패 단말은 NAC로 인가망 접근 제한	PDP (ICAM), UEM
3	N2SF-DV-12	인터넷 단말	자산관리 기반 미검증 펌웨어 사용 여부 탐지	탐지 시 업데이트 중지/격리 및 조치 이력 관리	내PC 지키미, PMS, VDI
4	N2SF-IN-1(1)	인터넷 단말	자산/패치관리 도구로 SW 최신 상태 유지 및 자동 배포	배포 정책(테스트→승인→배포) 운영 및 실패 시 롤백/재시도	ITAM, 내PC 지키미, VDI, PMS
5	N2SF-IN-5	인터넷 단말	보안 설정 점검 및 무결성 점검으로 비인가 변경 탐지	기준선(Baseline) 관리, 변경 발생 시 알림·복구 절차 적용	내PC 지키미, PDP (ICAM), VDI
6	N2SF-IN-6	인터넷 단말	자산관리 기반 미사용 서비스/포트 비활성화	정기 스캔 및 예외 등록·만료 관리	UEM, 내PC 지키미, PMS, VDI
7	N2SF-IN-8	인터넷 단말	DLP/앱 제어로 비인가 SW 실행 차단	차단 이벤트 로깅 및 반복 위반 사용자 조치 기준 운영	내PC 지키미

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
8	N2SF-IN-10	인터넷 단말	관리자 권한관리로 SW 설치 권한 분리	승인된 설치 경로/권한 부여 프로세스 운영	내PC 지키미
9	N2SF-IN-16	인터넷 단말	백신·EDR 기반 실시간 탐지 및 행위 기반 차단	탐지 시 격리/치료/조사 절차 및 대응 기록 보관	백신, EDR
10	N2SF-AM-2	인터넷 단말	비밀번호 보안수준 점검 및 주기적 변경 정책 적용	최소 길이/복잡도/재사용 금지·만료 정책 강제	PDP (ICAM)
11	N2SF-AM-9	인터넷 단말	OTP/모바일 인증 기반 MFA 적용	MFA 예외(분실/교체) 처리 및 재등록 절차 운영	2 Factor 인증 (생체인증, 모바일 인증, OTP 등)
12	N2SF-DV-6	인터넷 단말	매체제어로 통신기능 탑재 저장장치 사용 통제	장치 연결 시 자동 차단, 승인 기반 허용 및 로그 관리	매체제어 솔루션
13	N2SF-DV-8	인터넷 단말	단말 정책으로 일정 시간 미사용 시 자동 잠금	화면 잠금 시간/해제 인증 기준 설정 및 준수 점검	내PC 지키미, 매체제어 솔루션
14	N2SF-SG-4	인터넷 단말	VLAN/NAC 로 단말 구역 분리	구역별 접근정책 정의 및 단말 분류/이동 관리	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
15	N2SF-SG-5	인터넷 단말	운영관리용 네트워크를 별도 구성	관리망 접근 주체·경로 제한 및 접속 이력 점검	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
16	N2SF-SG-6	인터넷 단말	보안 에이전트 구성요소 접근권한 최소화	보안 설정/정책 변경은 관리자 승인 체계로만 수행	PDP (ICAM)
17	N2SF-EB-6	인터넷 단말	웹필터링·방화벽(FW)으로 악성 통신 차단	EDR 기반 C2 추적 및 발신 제어 운영	방화벽(FW), Web Filtering, EDR, SWG (유해사이트 차단)
18	N2SF-SN-1	인터넷 단말	SSO 세션 종료 시 토큰 무효화 처리	토큰 만료/폐기 정책 및 세션 재사용 방지 점검	PDP (ICAM), UEM, DLP, RBI, DRM 등
19	N2SF-WA-7	인터넷 단말	비인가 무선어댑터 채널 차단 정책 적용	예외 허용 시 범위/기간 제한 및 사용 이력 관리	매체제어 솔루션
20	N2SF-BC-1	인터넷 단말	블루투스 데이터 채널 차단 정책 적용	예외 허용 시 범위/기간 제한 및 사용 이력 관리	매체제어 솔루션

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
21	N2SF-DT-1	인터넷 단말	전송 전 사용자/단말 식별 및 권한 검증	NAC 인증 기반 단말 권한 확인 및 차단 로그 보관	PDP (ICAM), UEM, NAC
22	N2SF-DA-2	업무단말, 온북	PDP(ICAM)에 기관 단말 및 BYOD 등록 후 접근 정책 설정	허가된 단말만 기관 자원 접근 가능하도록 접근 시점마다 통제	PDP (ICAM), RBI, DLP, MDM
23	N2SF-DU-2	업무단말, 온북	전송 구간 암호화(TLS, 안전한 암호 알고리즘) 적용	개인정보 및 인증정보 전송 시 암호화 강제	VPN (IPsec), TLS, HTTPS
24	N2SF-IM-1	업무단말, 온북	개인정보 포함 문자열을 계정 식별자로 사용하지 않도록 기준 수립	계정 생성·운영 시 식별자 기준 준수 여부 점검	PDP (ICAM)
25	N2SF-EB-M1	업무단말, 온북	DLP를 사용해 개인정보 전송 통제	개인정보 전송 탐지 시 차단 및 로그 관리	DLP
26	N2SF-IF-9	업무단말, 온북	NAC 기반 네트워크 인증 적용	단말 인증 및 문서 접근 권한 검증	SWG (유해사이트 차단), NAC
27	N2SF-DU-M3	업무단말, 온북	데이터 관리 정책 수립	정책 문서화 및 전사 적용	보안정책 및 관리적 보안
28	N2SF-AC-1	AI 연계체계	ICAM 기반 계정 생성·변경·삭제 자동화	계정 상태를 지속적으로 모니터링	PDP (ICAM)
29	N2SF-AC-1(1)	AI 연계체계	ICAM을 통한 계정 생명주기 및 권한 변경 관리	권한 변경 이력 기록 및 점검	PDP (ICAM)
30	N2SF-AC-1(3)	AI 연계체계	ICAM을 통한 계정 상태 관리	비활성·임시 계정 정기 점검	PDP (ICAM)
31	N2SF-AC-1(4)	AI 연계체계	PDP(ICAM) 정책을 통한 세션 관리	세션 타임아웃 정책 적용 및 자동 로그아웃	PDP (ICAM), 내PC 지키미
32	N2SF-EB-1	인터넷 연계체계	웹 필터링 및 방화벽(FW)을 통해 최소 통신 정책 적용	허용/차단 정책을 문서화하고 정기적으로 점검	Web Filtering, RBI, DLP, 방화벽(FW), SWG
33	N2SF-AC-3	AI 연계체계	PDP(ICAM) 및 보안솔루션 기반 계정 이상행위 탐지	의심 계정에 대한 조사 및 조치 수행	PDP (ICAM), UEBA, EDR SIEM
34	N2SF-AC-3(2)	AI 연계체계	AI 유료계정 관리 기능 및 ICAM 연계 모니터링	비정상 계정 활동 차단	PDP (ICAM), UEM, DLP
35	N2SF-DA-3	AI 연계체계	UEM으로 단말 고유정보를 PDP(ICAM)에 사전 등록	등록 단말만 접근 허용 및 인증 절차 적용	PDP (ICAM), UEM, NAC
36	N2SF-DA-4	AI 연계체계	ICAM 기반 접근권한 관리 및 통제 적용	DLP 연계로 접근 이력 기록·감사	PDP (ICAM), DLP

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
37	N2SF-IF-9	AI 연계체계	방화벽(FW)·NMS 및 PAM G/W–DLP 연동으로 연결 식별	사용자–AI 서비스 연결 시 인증·식별 로그 관리	SWG (유해사이트 차단), NAC
38	N2SF-LI-1	AI 연계체계	인증 채널 암호화 정책 적용	암호화 미적용 채널 접속 차단	PDP (ICAM)
39	N2SF-LI-2	AI 연계체계	로그인 실패 제한 정책 운영	실패 횟수 초과 시 계정 잠금	PDP (ICAM)
40	N2SF-LI-4	AI 연계체계	계정 잠금 해제 시 추가 인증 적용	MFA 인증 완료 후 해제 허용	PDP (ICAM)
41	N2SF-IS-4	AI 연계체계	방화벽(FW), DLP, 유해사이트 차단 및 내부 DNS 정책 적용	인가되지 않은 외부 서비스 접속 차단	VLAN, 방화벽(FW), NAC 기반 업무망·인터넷망 분리
42	N2SF-IF-1	AI 연계체계	Routing, Subnet 기반 네트워크 흐름 통제	외부 공격은 보안장비로 차단, 내부→외부 트래픽은 DLP 로 통제	방화벽(FW), Network IPS, WAF, SWG, DLP, EDR
43	N2SF-EB-2	인터넷 연계체계	승인된 외부 서비스 목록 기반 접근 통제	프록시·게이트웨이를 통해 지정 서비스만 허용	방화벽(FW), Web Filtering, SWG (유해사이트 차단), RBI 솔루션 및 Proxy 서버, Gateway 네트워크 구성
44	N2SF-EB-3	AI 연계체계	웹격리 솔루션 기반 내부 시스템 접근 통제	허용된 시스템만 접속 가능하도록 제한	PDP (ICAM), UEM, Web Filtering, NAC, RBI, SWG (유해사이트 차단)
45	N2SF-EB-5	AI 연계체계	RBI 기반 외부 접근 통제 및 문서중앙화 연계	내부 저장 시 문서중앙화 솔루션 강제	PDP (ICAM), UEM, RBI
46	N2SF-EB-14	인터넷 연계체계	임의 DNS 요청 차단 정책 적용	우회 접속 시도 탐지 및 경보·로그 관리	내 PC 지키미, 방화벽(FW), SWG (유해사이트 차단)

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
47	N2SF-EB-15	인터넷 연계체계	EDR 기반 행위 분석으로 비인가 터널링 탐지	탐지 시 자동 차단 및 사고 대응 절차 연계	EDR, SWG (유해사이트 차단)
48	N2SF-EB-M2	인터넷 연계체계	통신 허용 정책을 문서화하여 관리	정책 정기 재검토 및 변경 이력 관리	보안정책 및 관리적 보안
49	N2SF-IF-2	AI 연계체계	SSL/TLS 프록시 및 복호화 DLP 적용	암호화 채널 내 정보 흐름 검사 수행	SSL/TLS Proxy, SSL 복호화 및 가시성
50	N2SF-IF-6	AI 연계체계	Network DLP 또는 Proxy 기반 트래픽 검사	중요정보 탐지 시 차단	DLP
51	N2SF-IF-7	AI 연계체계	DLP 기반 비인가 전송 차단	정책 위반 트래픽 탐지·차단	CDS, DLP
52	N2SF-IF-8	AI 연계체계	중요 데이터 식별·분류·모니터링 솔루션 적용	민감 데이터 탐지 시 차단 조치	DLP, Web Filtering, DRM, 매체제어 솔루션
53	N2SF-IF-10	AI 연계체계	PAM G/W 및 DLP 기반 허용 통신만 사용하도록 통제	중요정보 유출 시도 차단	방화벽(FW), Metwork IPS, WAF, DLP
54	N2SF-IF-14	AI 연계체계	데이터 등급별 보안 솔루션 및 DLP 필터링 적용	AI 서비스 전송 정보 사전 통제	DRM, CDS
55	N2SF-EI-M1	AI 연계체계	외부 인증수단 ICAM 연계 관리	인증 연동 현황 일괄 관리	PDP (ICAM), UEM, NAC
56	N2SF-DU-M3	AI 연계체계	데이터 관리 정책 수립	정책 문서화 및 전사 적용	보안정책 및 관리적 보안
57	N2SF-IF-3	인터넷 연계체계	DLP 기반 문서 내 비인가 데이터 삽입 점검	위반 시 전송 차단 및 로그 보관	DLP, 문서중앙화 솔루션, EDR
58	N2SF-IF-5	인터넷 연계체계	민감 구간 간 정보 전송 차단	전송 시도 이력 로깅 및 감사 가능 상태 유지	CDS
59	N2SF-LP-4	인터넷 연계체계	관리자 권한 최소 부여 및 역할 기반 권한관리	권한 변경 시 승인 절차 및 이력 기록	PDP (ICAM)
60	N2SF-LP-4(1)	인터넷 연계체계	관리자 원격 접근 제한 정책 적용	VPN+MFA 기반 인증 필수화	보안정책 및 관리적 보안
61	N2SF-LP-4(4)	인터넷 연계체계	관리자 명령 실행 로그 중앙 수집	EDR 기반 실행 행위 추적 및 감사 수행	PDP (ICAM), SIEM
62	N2SF-AC-1(5)	인터넷 연계체계	계정 정기 검토를 통한 관리 강화	미사용 관리자 계정 자동 비활성화	PDP (ICAM)

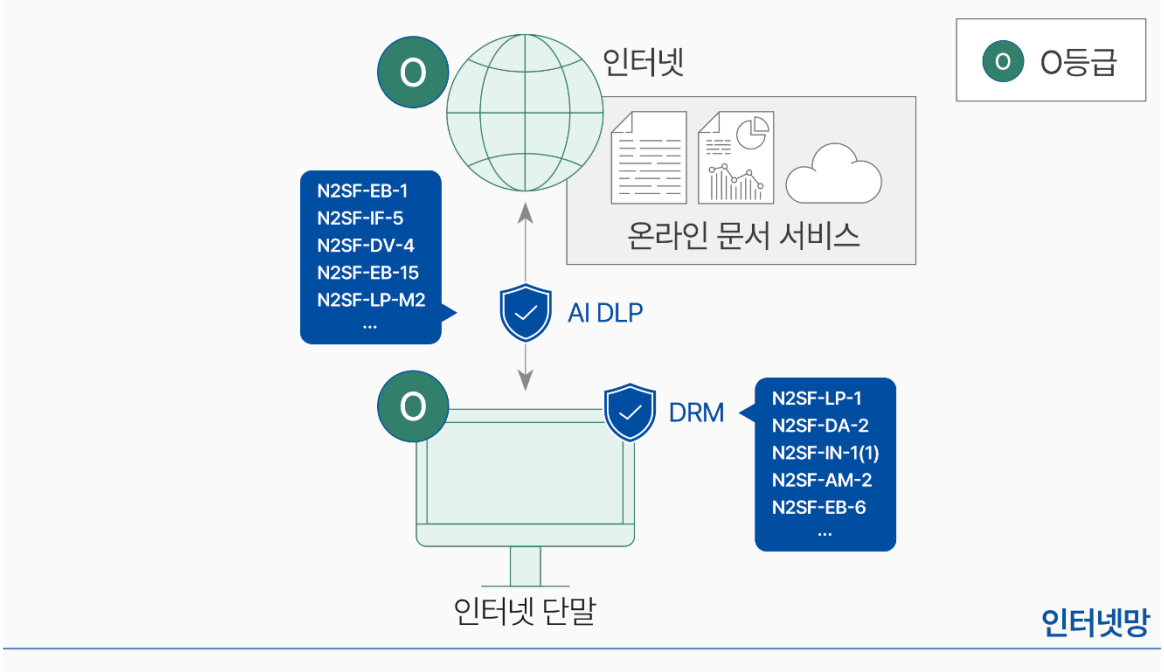
No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
63	N2SF-AC-3(1)	인터넷 연계체계	이상 행위 계정 탐지 시 즉시 통제	계정 비활성화 및 인증 재검증 절차 운영	PDP (ICAM), UEM, NAC
64	N2SF-EB-8	인터넷 연계체계	관리용 포트 외부 접근 차단	인증 기반 사용 제한 및 접근 이력 관리	매체제어 솔루션
65	N2SF-EB-10	인터넷 연계체계	관리 인터페이스 접근 범위 제한	내부망에서만 접근 가능하도록 설정	Routing, Subnet, 방화벽(FW) 정책
66	N2SF-EB-11	인터넷 연계체계	경계 장비 장애 대비 기본 차단 정책 적용	장애 시에도 단말 보안 에이전트 정책 유지	Anti-DDoS, 방화벽(FW), Network IPS, WAF 이중화 구성
67	N2SF-EB-13	인터넷 연계체계	오류 메시지 최소화 정책 적용	내부 구성정보가 외부에 노출되지 않도록 설정	보안정책 및 관리적 보안
68	N2SF-DV-4	인터넷 연계체계	USB·무선 통신 등 장치 사용 통제	승인된 보안 USB장치만 사용 허용	매체제어 솔루션
69	N2SF-DV-12	인터넷 연계체계	비인가 펌웨어 적용 차단 정책 적용	승인·서명된 펌웨어만 설치 허용	내PC 지키미, PMS, VDI
70	N2SF-IN-1(1)	인터넷 연계체계	패치관리 시스템으로 최신 버전 유지	미적용 시 자동 알림 및 강제 적용	ITAM, 내PC 지키미, VDI, PMS
71	N2SF-IN-5	인터넷 연계체계	단말 설정 무결성 감시 적용	변경 탐지 시 관리자 확인 및 복구 절차 수행	내PC 지키미, PDP (ICAM), VDI
72	N2SF-IN-6	인터넷 연계체계	미사용 서비스 자동 식별 정책 적용	식별 결과 기반 자동 비활성화	UEM, 내PC 지키미, PMS, VDI
73	N2SF-IN-11	인터넷 연계체계	부팅 시 구성요소 무결성 검증	검증 실패 시 실행 차단 및 관리자 통보	보안정책 및 관리적 보안
74	N2SF-LP-M1	인터넷 연계체계	고위험 역할 계정 별도 지정	승인 기반 관리 및 사용 이력 점검	보안정책 및 관리적 보안
75	N2SF-LP-M2	인터넷 연계체계	계정 행위 이상 탐지 정책 적용	이상 행위 발생 시 계정 제한 조치	PDP (ICAM), UEBA
76	N2SF-AC-1(2)	인터넷 연계체계	계정 생명주기 상태 모니터링	생성·변경·삭제 이력 상시 점검	PDP (ICAM)
77	N2SF-AC-M1	인터넷 연계체계	계정 사용 감사 로그 자동 생성	감사 로그 장기 보관 및 위변조 방지	PDP (ICAM), UEM

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
78	N2SF-AC-M2	인터넷 연계체계	접근·권한 변경 이벤트 수집	중앙 로그 저장 및 감사 대응	PDP (ICAM), UEM
79	N2SF-AC-M3	인터넷 연계체계	사용자 세션 활동 기록	비정상 세션 탐지 시 강제 종료	PDP (ICAM), UEM
80	N2SF-LI-M1	인터넷 연계체계	로그인 실패 패턴 분석 적용	반복 실패 시 경고 및 계정 잠금	PDP (ICAM)
81	N2SF-LI-M2	인터넷 연계체계	세션·토큰 무결성 검증	위변조 탐지 시 세션 폐기	PDP (ICAM)
82	N2SF-IF-M1	인터넷 연계체계	정보 전송 허용 기준 정의	기준 문서화 및 정기 개정	보안정책 및 관리적 보안
83	N2SF-IF-M2	인터넷 연계체계	업·다운로드 이력 중앙 저장	감사·추적 가능하도록 장기 보관	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등
84	N2SF-IF-M3	인터넷 연계체계	전송 우회 및 차단 실패 점검	점검 결과 기반 개선 조치 수행	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등
85	N2SF-IF-M4	인터넷 연계체계	키워드·패턴·문맥 기반 탐지	위반 시 자동 차단 및 관리자 확인	DLP, NAC, SIEM
86	N2SF-IF-M5	인터넷 연계체계	차단 실패 탐지 체계 적용	실패 발생 시 자동 보고 및 대응 추적	보안정책 및 관리적 보안
87	N2SF-EB-M3	인터넷 연계체계	외부 통신 이력 수집	장기 보존 및 정기 분석 수행	PDP (ICAM), UEM, Web Filtering, NAC, RBI, SWG (유해사이트 차단)
88	N2SF-EB-M4	인터넷 연계체계	외부 통신 이상 행위 탐지	위험 통신 실시간 경고 및 차단	DLP, NDR
89	N2SF-EB-M5	인터넷 연계체계	침해 징후 발생 시 외부 통신 차단	사고 대응 절차에 따라 즉시 격리	방화벽(FW)

(나) 자체정의 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건
1	N2SF-ORG3-1	단말	동일 등급(C/S/O) 내 정보에 대해 생성경로, 출처, 활용 목적, 외부 반출 여부 등을 기준으로 차등 통제 정책을 수립	정보 수명주기 중 상태 전이 발생 시 통제 수준이 자동으로 변경되도록 정책을 연동하여 운영

1.3 정보서비스 적용 기관 망 구성도 예시



수립한 보안 요구사항 및 보안통제 항목 구현 사항 등 산출물을 토대로 국가정보원 보안성 검토 신청 시, N2SF를 적용한 기관의 실제 망 구성도를 작성하여 첨부하여야 한다.

2.[모델 2] 업무환경에서 생성형 AI 활용

본 정보서비스 모델은 기관 전산망 내 이용자 단말(업무 단말, 온북 등)을 통해 업무시스템에 접속하여 업무를 수행하는 환경에서, 업무 효율성 향상을 위해 인터넷 영역에 위치하는 생성형 AI 서비스를 활용하는 모델이다.

※ (참고자료) N2SF 보안 가이드라인 1.0 - (부록2) 모델2 업무환경에서 생성형 AI 활용

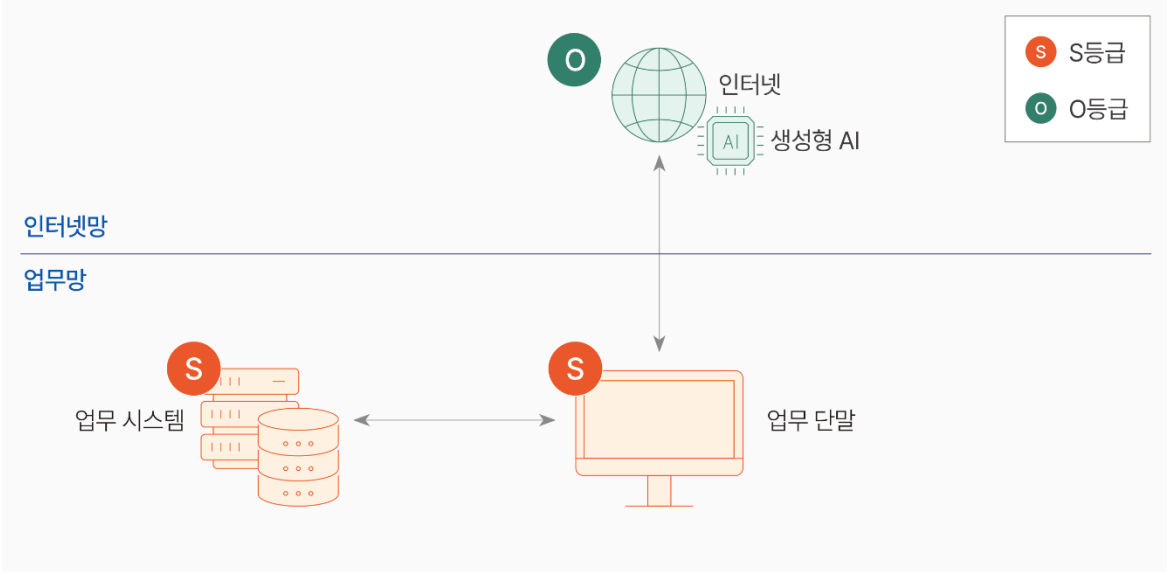
본 실증 사례는 망 분리 환경의 업무 단말에서 외부 생성형 AI를 안전하게 사용하기 위해 1개의 정보서비스 모델을 활용한다. 외부 연결이 불가하여 단순 문서 생산 및 업무 시스템 접속만 가능한 업무망에서 생성형 AI에 즉각적인 접속 및 활용이 가능하도록 구현하는 데 중점을 둔다.

각 기관에서는 망 분리가 적용된 환경에서 생성형 AI를 업무 전반에 도입하여 정보 검색 및 자료 분석 효율을 높이고자 할 때 참고할 수 있다.

2.1 정보서비스 유형 요약

정보서비스 유형 / 모델 No. (N2SF 가이드라인 기준)		모델 2 / 업무환경에서 생성형 AI 활용
정보서비스 개요	업무정보	① 인터넷 수집자료 ② 인터넷 수집자료 취합문서 ③ 일반 업무 자료 ④ 상위 기관 업무 관련 자료 ⑤ 보안 과제 관련 자료 ⑥ 감사 자료
	정보시스템	① 업무 단말 ② 생성형 AI 서비스
	정보서비스 사용 시나리오	① 생성형 AI 서비스 활용

위치/주체/객체 관점의 정보서비스 구조



- 위치: 업무망(S 등급), 주체: 업무 단말(S 등급), 객체: 생성형 AI 서비스 (O 등급)
- 업무망(S 등급)에서, 업무 단말(S 등급)을 이용해 생성형 AI 서비스(O 등급) 이용
- 업무단말(S 등급)은 일차적으로 내부 시스템 – 업무 시스템 (S 등급) - 에 접속하여 식별, 인증 및 권한 확인 과정을 거친 후 생성형 AI 서비스 (O 등급)에 접속

보안통제 대상	① 업무 단말 ② 생성형 AI 연계체계 ③ 생성형 AI

2.2 최종산출물 서식

[1] 정보서비스 사용 시나리오별 정보시스템 식별

정보서비스 사용 시나리오별 정보시스템 식별

번호	사용 시나리오	관련 정보시스템
1	생성형 AI 서비스 활용	
1-1	업무 단말에서 생성형 AI 서비스로 단순 질의	㉠ 업무 단말 ㉡ 생성형 AI 서비스
1-2	업무 단말에서 생성형 AI 서비스로 업무정보를 활용해 질의	㉠ 업무 단말 ㉡ 생성형 AI 서비스
1-3	업무 단말에서 생성형 AI 서비스로 결과물 생성	㉠ 업무 단말 ㉡ 생성형 AI 서비스

[2] 정보서비스 보안목표

국가정보원 보안성 검토 시 제출하는 문서중, 자체 보안대책에 대한 최종 산출물 서식 1번 「정보서비스 보안목표」는 아래와 같이 정리됨

No.	영역	보안 목표	비고
1	공통	정보서비스 모델 2. 업무환경에서 생성형 AI 활용	N2SF 가이드라인 1.0
2		특정 생성형 AI 서비스로 접속 제한	자체
3	네트워크	업무목적에 적합한 인터넷 서비스로 접속 제한	자체
4		유해사이트 접속 차단	자체

[3] C/S/O 등급분류

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 2번 「C/S/O 등급 분류표」는 아래와 같이 정리됨

No.	정보시스템		업무정보	
	명칭	C/S/O 등급	명칭	C/S/O 등급
1	업무 단말	S	인터넷 수집자료	O
			인터넷 수집자료 취합문서	S
			일반 업무 자료	S
			상위 기관 업무 자료	S
			보안 과제 관련 자료	S
			감사 자료	O
2	생성형 AI 서비스	O	인터넷 수집자료	O

[4] 위협 식별 - 모델링 및 C/S/O 평가

기관의 정보서비스 구성요소에 따라 유스케이스별로 모델링 및 C/S/O 보안등급을 나누어 평가하며, 「정보 생산·저장」 보안원칙과 「정보 이동」 보안원칙을 적용하여 보안대책의 필요성을 평가한다.

N2SF 보안 가이드라인*에서 본 정보서비스는 기관 전산망 영역에 위치하는 **업무시스템(위치, S등급), 이용자 단말(주체, S등급)**과 인터넷 영역에 위치하는 **생성형 AI 서비스(객체, O등급)**로 구성되며, O등급의 생성형 AI 서비스에서 S등급 업무정보가 생산·저장(활용), 이동하지 않도록 보안 원칙을 제시하고 있다. 아래 제시하는 실증 사례 및 N2SF 보안 가이드라인에 대하여 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 유연하게 참고하여 보안 원칙을 수립하여야 한다.

* N2SF 보안 가이드라인 1.0 - (부록2) 모델2 업무환경에서 생성형 AI 활용

사례: 생성형 AI 서비스 활용

(1) 업무 단말에서 생성형 AI 서비스로 단순 질의

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C등급 / S등급 / O등급 위치 Domain: 업무망 주체 Subject: 업무 단말 객체 Object: 생성형 AI 서비스 업무망(S 등급)에서 업무 단말(S 등급)을 이용해 생성형 AI 서비스(O 등급)를 이용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안 대책 필요.	예
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C 정보 / S 정보 / 인터넷 수집자료 C 시스템: ● ● ● 업무 단말: + ● ● 생성형 AI 서비스: + + ● 생성형 AI 서비스(O 등급)에 업무 단말의 업무정보를 업로드하지 않고 단순 질의하는 경우, O 등급인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)를 다룰 수 있음. 따라서 보안원칙에 위배되지 않아 보안대책 불요.	아니오
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / 업무 단말 / 생성형 AI 서비스 C 정보: ● + + S 정보: ● ● + 인터넷 수집자료: ● ● ● 업무 단말(S 등급)이 생성형 AI 서비스(O 등급)에 접속하는 경우, 인터넷 수집자료(O 등급)와 같은 O 등급 업무정보만을 주고받을 수 있음. 따라서 업무 단말의 정보를 업로드하지 않고 단순 질의하게 되는 경우 보안원칙에 위배되지 않아 보안대책 불요.	아니오

(2) 업무 단말에서 생성형 AI 서비스로 업무정보를 활용해 질의

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C 등급 / S 등급 / O 등급 위치 Domain: 업무망 주체 Subject: 업무 단말 객체 Object: 생성형 AI 서비스 업무망(S 등급)에서 업무 단말(S 등급)을 이용해 생성형 AI 서비스(O 등급)를 이용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안 대책 필요.	예
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C 정보 / 업무 단말 내 S 정보 / 인터넷 수집자료 C 시스템: ● / ● / ● 업무 단말: + / ● / ● 생성형 AI 서비스: + / ⃠ + / ● 생성형 AI 서비스(O 등급)에 업무 단말의 업무정보를 업로드하여 질의하는 경우, 생성형 AI 서비스(O 등급)는 O 등급인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)를 다룰 수 있음. 그러나 그 외의 업무 단말 내 S 등급 업무정보를 다루는 경우 보안원칙에 위배됨. 따라서 생성형 AI 서비스 내 S 등급 업무정보를 생산 및 저장하지 않도록 연계 구간에 적절한 보안 대책 필요.	예
「정보 이동」 보안원칙	~정보가~로 이동 / C 시스템 / 업무 단말 / 생성형 AI 서비스 C 정보: ● / + / + 업무 단말 내 S 정보: ● / ● / ⃠ + 인터넷 수집자료: ● / ● / ● 업무 단말(S 등급)이 생성형 AI 서비스(O 등급)에 접속하는 경우, 인터넷 수집자료(O 등급)와 같은 O 등급 업무정보만을 주고받을 수 있으며, 그 외 업무 단말 내 존재하는 S 등급 업무정보를 주고받는 경우 보안원칙에 위배됨. 따라서 생성형 AI 서비스로 S 등급 업무정보를 이동하지 않도록 연계 구간에 적절한 보안 대책 필요.	예

(3) 업무 단말에서 생성형 AI 서비스로 결과물 생성

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C 등급 / S 등급 / O 등급 위치 Domain: 업무망 주체 Subject: 업무 단말 객체 Object: 생성형 AI 서비스 업무망(S 등급)에서 업무 단말(S 등급)을 이용해 생성형 AI 서비스(O 등급)를 이용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안 대책 필요.	예
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C 정보 / 업무 단말 내 S 정보 / 인터넷 수집자료 C 시스템: ● / ● / ● 업무 단말: + / ● / ● 생성형 AI 서비스: + / ⃠ + / ● 생성형 AI 서비스(O 등급)를 통해 결과물을 생성해 단말 내 업무정보로 저장할 경우, 생성형 AI 서비스(O 등급)는 O 등급인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)를 다룰 수 있음. 그러나 그 외의 업무 단말 내 S 등급 업무정보를 다루는 경우 보안원칙에 위배됨. 따라서 생성형 AI 서비스 내 S 등급 업무정보를 생산 및 저장하지 않도록 연계 구간에 적절한 보안 대책 필요.	예
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / 업무 단말 / 생성형 AI 서비스 C 정보: ● / + / + 업무 단말 내 S 정보: ● / ● / ⃠ + 인터넷 수집자료: ● / ● / ● 업무 단말(S 등급)이 생성형 AI 서비스(O 등급)에 접속하는 경우, 인터넷 수집자료(O 등급)와 같은 O 등급 업무정보만을 주고받을 수 있으며, 그 외 업무 단말 내 존재하는 S 등급 업무정보를 주고받는 경우 보안원칙에 위배됨. 따라서 생성형 AI 서비스로 S 등급 업무정보를 이동하지 않도록 연계 구간에 적절한 보안 대책 필요.	예

[5] 보안요구사항 및 보안통제

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 3번 「보안 요구사항 및 보안통제」는 아래와 같이 작성할 수 있다.

※ 보안 가이드라인에 없는 신규 자체정의 보안통제 항목: N2SF-ORG1

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
1	업무 단말	이용자 단말 보안성 유지	N2SF-LP-1
			N2SF-DA-1
			N2SF-DA-2
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-8
			N2SF-IN-10
			N2SF-IN-16
		이용자 단말 사용 보안	N2SF-AM-2
			N2SF-AM-9
			N2SF-DV-6
			N2SF-DV-8
		이용자 단말 네트워크 보안	N2SF-SG-4
			N2SF-SG-5
			N2SF-SG-6
			N2SF-IF-9
			N2SF-EB-6
			N2SF-SN-1
			N2SF-WA-7

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-BC-1
			N2SF-DT-1
		이용자 단말 데이터 보호	N2SF-DU-2
		이용자 계정 정보 보호	N2SF-IM-1
		생성형 AI 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1
			N2SF-EB-M1
			N2SF-DU-M3
		정보 등급 변화 정책 수립	N2SF-ORG1-1
		정보 등급 변화 내역 기록 및 관리	N2SF-ORG1-2
2	AI 연계체계	생성형 AI 서비스 이용자 및 단말 인증	N2SF-AC-1
			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
		비인가 네트워크 연결 차단	N2SF-IS-4
			N2SF-IF-1
			N2SF-IF-9

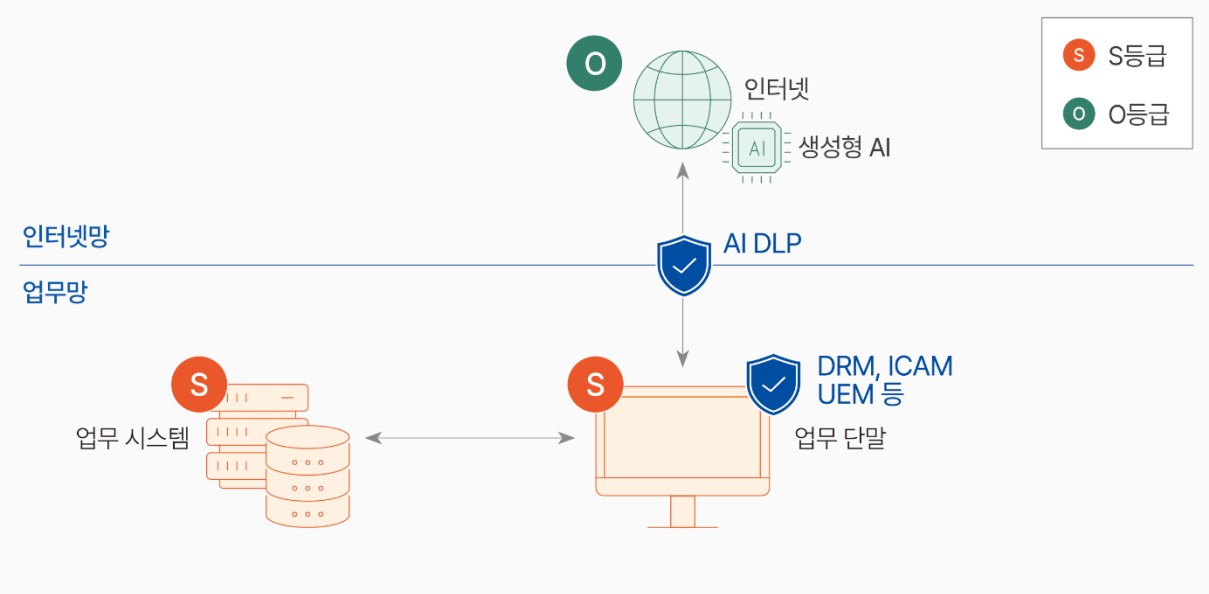
No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-EB-1
			N2SF-EB-2
			N2SF-EB-3
			N2SF-EB-5
			N2SF-EB-6
			N2SF-EB-14
			N2SF-EB-15
		생성형 AI 서비스 활용 시 데이터 보호	N2SF-IF-2
			N2SF-IF-6
			N2SF-IF-7
			N2SF-IF-8
			N2SF-IF-10
			N2SF-IF-14
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3
			N2SF-IF-5
		연계체계 보안성 유지	N2SF-LP-4
			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-13

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-DV-4
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-11
		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-IF-M1
			N2SF-IF-M2
			N2SF-IF-M3
			N2SF-IF-M4
			N2SF-IF-M5
			N2SF-EB-M3
			N2SF-EB-M4
			N2SF-EB-M5
3	생성형 AI	생성형 AI 서비스 계정 관리	N2SF-EI-M1
		생성형 AI 서비스 활용 데이터 관리	N2SF-DU-M3

[6] 보안통제 구현계획

국가정보원 보안성 검토 시 제출하는 문서중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 4번 「보안통제 구현계획표」는 아래와 같이 작성할 수 있다.

보안통제적용 정보서비스 구성도



(가) 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
1	N2SF-DA-1	단말	UEM을 통해 단말 고유정보를 수집하여 PDP(ICAM)에 사전 등록	등록된 단말만 접속 허용하며, 접속 시 단말·사용자 인증을 필수 수행	PDP (ICAM), UEM, NAC, EDR, Endpoint DLP
2	N2SF-DA-2	단말	PDP(ICAM)에 기관 단말 및 BYOD 등록 후 접근 정책 설정	허가된 단말만 기관 자원 접근 가능하도록 접근 시점마다 통제	PDP (ICAM), RBI, DLP, MDM
3	N2SF-DV-12	단말	PC 관리솔루션을 활용한 단말 중앙 관리	관리 정책 적용 상태를 지속적으로 점검	내 PC 지키미, PMS, VDI
4	N2SF-IN-5	단말	UEM 및 내 PC 지키미를 통해 단말 구성 변경 탐지	변경 탐지 시 위험도 평가 후 수준별 대응 적용	내 PC 지키미, PDP (ICAM), VDI

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
5	N2SF-IN-6	단말	UEM 및 PC 관리솔루션으로 불필요 소프트웨어 관리	불필요·미승인 소프트웨어 설치 여부 정기 점검	UEM, 내 PC 지키미, PMS, VDI
6	N2SF-IN-8	단말	PC 관리솔루션을 통한 비인가 소프트웨어 설치·실행 통제	비인가 행위 탐지 시 차단 및 관리자 확인 수행	내 PC 지키미
7	N2SF-IN-10	단말	PC 관리솔루션 기반 소프트웨어 설치 관리	승인되지 않은 소프트웨어 설치 제한	내 PC 지키미
8	N2SF-IN-16	단말	백신 솔루션을 통한 악성코드 탐지 및 차단	백신 최신 상태 유지 및 탐지 로그 점검	백신, EDR
9	N2SF-DV-8	단말	화면 보호기 설정 및 단말 보안 설정 적용	화면 보호기 설정 여부를 주기적으로 점검	윈도우 화면 보호기, 내 PC 지키미
10	N2SF-BC-1	단말	매체제어솔루션을 통한 블루투스 통신 차단	정책 위반 통신 시 자동 차단	매체제어 솔루션
11	N2SF-DA-3	단말	UEM 기반 단말 고유정보 사전 등록	등록 단말만 인증 및 서비스 접근 허용	PDP (ICAM), UEM, NAC
12	N2SF-DA-4	단말	PDP(ICAM)에 단말 등록 및 권한 설정	접근 이력 기록 및 주기적 감사 수행	PDP (ICAM), DLP
13	N2SF-AC-3(1)	단말	UEM 기반 단말 위험 탐지 기능 적용	위험 단말은 AI 서비스 연결 차단 및 조사	PDP (ICAM), UEM, NAC
14	N2SF-DV-4	단말	매체제어 및 PC 보안 솔루션 적용	악성코드 유입 및 정보유출 시도 차단	매체제어 솔루션
15	N2SF-DV-12	단말	안전한 펌웨어 업데이트 절차 수립	코드사이닝 및 무결성 검증 시에만 업데이트 허용	내 PC 지키미, PMS, VDI
16	N2SF-IN-1(1)	단말	PC 관리솔루션을 통한 단말 자산 목록 관리	자산 변경 시 즉시 목록 갱신	ITAM, 내 PC 지키미, VDI, PMS
17	N2SF-IN-5	단말	PDP(ICAM)을 통한 단말 등록 관리	인가된 절차를 거친 단말만 등록 유지	내 PC 지키미, PDP (ICAM), VDI

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
18	N2SF-IN-6	단말	UEM 및 PC 관리솔루션 기반 단말 운영 관리	정책 준수 여부 정기 점검	UEM, 내 PC 지키미, PMS, VDI
19	N2SF-IN-11	단말	안전한 단말 재기동 프로세스 적용	재기동 시 무결성 및 신뢰성 검증 수행	보안정책
20	N2SF-IN-1(1)	연계체계	PDP(ICAM)를 통해 사용자·단말·서버·애플리케이션 통합 등록 관리	미등록 객체의 연계 및 접근 차단	ITAM, 내 PC 지키미, VDI, PMS
21	N2SF-LP-1	연계체계	외부 AI 서비스에 대해 유료 계정 기반 접근 체계 적용	1인 1계정 원칙 및 계정 운영 정책 수립·운영	PDP (ICAM)
22	N2SF-AM-2	연계체계	PDP(ICAM) 기반 사용자 기본 인증 체계 적용	인증 실패 시 접근 차단	PDP (ICAM)
23	N2SF-AM-9	연계체계	PDP(ICAM) 기반 다중요소인증(MFA) 적용	소유 기반 MFA 인증 필수화	2 Factor 인증 (생체인증, 모바일 인증, OTP 등)
24	N2SF-DV-6	연계체계	매체제어 솔루션을 활용하여 외부 저장매체 사용을 통제	비인가 매체 연결 및 사용을 차단하고, 매체 사용 이력을 기록·관리	매체제어 솔루션
25	N2SF-SN-1	연계체계	PDP(ICAM)를 통한 요청 단위 접근 인가	자원 접근 시마다 인가 여부 재확인	DP (ICAM), UEM, DLP, RBI, DRM
26	N2SF-DT-1	연계체계	데이터 전송 전 PDP(ICAM) API로 사용자·단말 권한 확인	미인가 전송 요청 차단	PDP (ICAM), UEM, NAC
27	N2SF-AC-1	연계체계	ICAM 기반 계정 생성·변경·삭제 자동화	계정 상태를 지속적으로 모니터링	PDP (ICAM)
28	N2SF-AC-1(1)	연계체계	ICAM을 통한 계정 생명주기 및 권한 변경 관리	권한 변경 이력 기록 및 점검	PDP (ICAM)
29	N2SF-AC-1(2)	연계체계	ICAM 기반 계정 상태 모니터링	비정상 계정 상태 탐지 시 조치	PDP (ICAM)

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
30	N2SF-AC-1(3)	연계체계	ICAM을 통한 계정 상태 관리	비활성·임시 계정 정기 점검	PDP (ICAM)
31	N2SF-AC-1(4)	연계체계	PDP(ICAM) 정책을 통한 세션 관리	세션 타임아웃 정책 적용 및 자동 로그아웃	PDP (ICAM), 내 PC 지키미
32	N2SF-AC-3	연계체계	PDP(ICAM) 및 보안솔루션 기반 계정 이상행위 탐지	의심 계정에 대한 조사 및 조치 수행	PDP (ICAM), UEBA, EDR SIEM
33	N2SF-AC-3(2)	연계체계	AI 유료계정 관리 기능 및 ICAM 연계 모니터링	비정상 계정 활동 차단	PDP (ICAM), UEM, DLP
34	N2SF-LI-2	연계체계	로그인 실패 횟수 제한 정책 적용	임계 초과 시 계정 잠금	PDP (ICAM)
35	N2SF-LI-4	연계체계	계정 잠금 해제 시 추가 인증 적용	MFA 인증 완료 후 해제 허용	PDP (ICAM)
36	N2SF-IF-7	연계체계	데이터 분류 기준(C/S/O) 및 DLP 솔루션 적용	비인가 송신 탐지 및 차단	CDS, DLP
37	N2SF-IF-8	연계체계	중요 데이터 식별·분류·모니터링 솔루션 적용	민감 데이터 탐지 시 차단 조치	DLP, Web Filtering, DRM, 매체제어 솔루션
38	N2SF-IF-10	연계체계	PAM G/W 및 DLP 기반 허용 통신만 사용하도록 통제	중요정보 유출 시도 차단	방화벽(FW), Metwork IPS, WAF, DLP
39	N2SF-IF-14	연계체계	데이터 등급별 보안 솔루션 및 DLP 필터링 적용	AI 서비스 전송 정보 사전 통제	DRM, CDS
40	N2SF-IF-3	연계체계	DLP를 통한 데이터 흐름 통제	정책 위반 전송 차단	DLP, 문서중앙화 솔루션, EDR
41	N2SF-IF-5	인터넷 연계체계	민감 구간 간 정보 전송 차단	전송 시도 이력 로깅 및 감사 가능 상태 유지	CDS
42	N2SF-LP-4	연계체계	ICAM 기반 계정·권한 통합 관리	권한 부여 현황 주기 점검	PDP (ICAM)

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
43	N2SF-LP-4(4)	연계체계	다계층 보안 솔루션 연계 로깅	관리자 권한 사용 내역 주기 감사	PDP (ICAM), SIEM
44	N2SF-AC-1(5)	연계체계	ICAM을 통한 계정 관리 시스템화	계정 관리 이력 기록·보관	PDP (ICAM)
45	N2SF-EB-8	연계체계	물리적 보안 및 매체제어 장치 적용	인가되지 않은 장치 연결 차단	매체제어 솔루션
46	N2SF-LP-M1	연계체계	특별권한 사용자 승인 절차 수립	변경 이력 기록 및 주기 감사	PDP (ICAM)
47	N2SF-LP-M2	연계체계	최소권한 원칙 적용	권한 부여 현황 정기 검토	보안정책 및 관리적 보안
48	N2SF-AC-1(2)	연계체계	ICAM 기반 계정 상태 모니터링	비정상 계정 상태 탐지 시 조치	PDP (ICAM)
49	N2SF-AC-M1	연계체계	DLP·네트워크 보안 로그 저장	감사·추적 가능하도록 보관	PDP (ICAM), UEM
50	N2SF-AC-M2	연계체계	DLP·네트워크 보안 로그 저장	감사·추적 가능하도록 보관	PDP (ICAM), UEM, SIEM
51	N2SF-LI-M1	연계체계	로그인 실패·세션 무결성 모니터링	이상 탐지 시 관리자 보고 및 조치	PDP (ICAM)
52	N2SF-LI-M2	연계체계	로그인 실패·세션 무결성 모니터링	이상 탐지 시 관리자 보고 및 조치	PDP (ICAM)
53	N2SF-IF-M2	연계체계	정보흐름 통제 로그 및 이상 탐지 기능 적용	정책 미준수 사항 식별 및 개선	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
54	N2SF-IF-M3	연계체계	정보흐름 통제 로그 및 이상 탐지 기능 적용	정책 미준수 사항 식별 및 개선	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등
55	N2SF-IF-M4	연계체계	정보흐름 통제 로그 및 이상 탐지 기능 적용	정책 미준수 사항 식별 및 개선	DLP, NAC, SIEM
56	N2SF-IF-M5	연계체계	정보흐름 통제 로그 및 이상 탐지 기능 적용	정책 미준수 사항 식별 및 개선	보안정책 및 관리적 보안
57	N2SF-EB-M3	연계체계	외부 통신 로그 수집 및 행위 분석	이상 행위 탐지 시 차단	방화벽(FW), Network IPS, WAF, DLP, RBI, SIEM 등
58	N2SF-EB-M4	연계체계	외부 통신 로그 수집 및 행위 분석	이상 행위 탐지 시 차단	DLP, NDR
59	N2SF-EI-M1	연계체계	외부 인증수단 ICAM 연계 관리	인증 연동 현황 일괄 관리	PDP (ICAM), UEM, NAC
60	N2SF-SG-4	네트워크	방화벽(FW)을 통해 서버, DMZ, 업무 PC 네트워크 영역 분리	영역 간 통신은 정책 승인된 경우에만 허용	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
61	N2SF-SG-5	네트워크	방화벽(FW) 기반 서버, DMZ, 업무 PC 구간 분리	구간 분리 정책을 주기적으로 검토·갱신	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
62	N2SF-IF-9	네트워크	방화벽(FW), NMS 및 PDP(ICAM)–Network DLP 연동 적용	사용자와 생성형 AI 서비스 간 연결을 식별·인증하여 관리	SWG (유해사이트 차단), NAC

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
63	N2SF-EB-6	네트워크	Network DLP 를 통한 네트워크 트래픽 모니터링	정책 위반 데이터 흐름 탐지 시 즉시 차단	방화벽(FW), Web Filtering, EDR, SWG (유해사이트차단)
64	N2SF-WA-7	네트워크	WIPS 를 통한 무선 네트워크 위협 탐지	비인가 AP 및 단말 접속 차단	WIPS
65	N2SF-DU-2	네트워크	전송 구간 암호화(TLS, 안전한 암호 알고리즘) 적용	개인정보 및 인증정보 전송 시 암호화 강제	VPN (IPsec), TLS, HTTPS
66	N2SF-EB-M1	네트워크	인터넷 구간 전송 데이터 암호화 적용	암호화 미적용 트래픽 차단	VPN (IPsec), TLS, HTTPS
67	N2SF-IS-4	네트워크	방화벽(FW), DLP, 유해사이트 차단 및 내부 DNS 정책 적용	인가되지 않은 외부 서비스 접속 차단	VLAN, 방화벽(FW), NAC 기반 업무망·인터넷망 분리
68	N2SF-IF-1	네트워크	Routing, Subnet 기반 네트워크 흐름 통제	외부 공격은 보안장비로 차단, 내부→외부 트래픽은 DLP 로 통제	방화벽(FW), Network IPS, WAF, SWG, DLP, EDR
69	N2SF-IF-9	네트워크	방화벽(FW) ACL 및 서버 접근 IP 제한 정책 적용	허용 목록 외 접근 시도 차단 및 기록	SWG (유해사이트 차단), NAC
70	N2SF-EB-1	네트워크	외부 공개 서비스의 연결 접점 및 포트 정의	승인 및 취약점 점검 후 외부 연결 허용	Web Filtering, RBI, DLP, 방화벽(FW), SWG
71	N2SF-EB-2	네트워크	다계층 경계 보안(Anti-DDoS, IPS, 방화벽(FW), WAF) 적용	경계 트래픽을 상시 모니터링하고 이상 시 차단	방화벽(FW), Web Filtering, SWG (유해사이트 차단), RBI 솔루션 및 Proxy 서버, Gateway 네트워크 구성

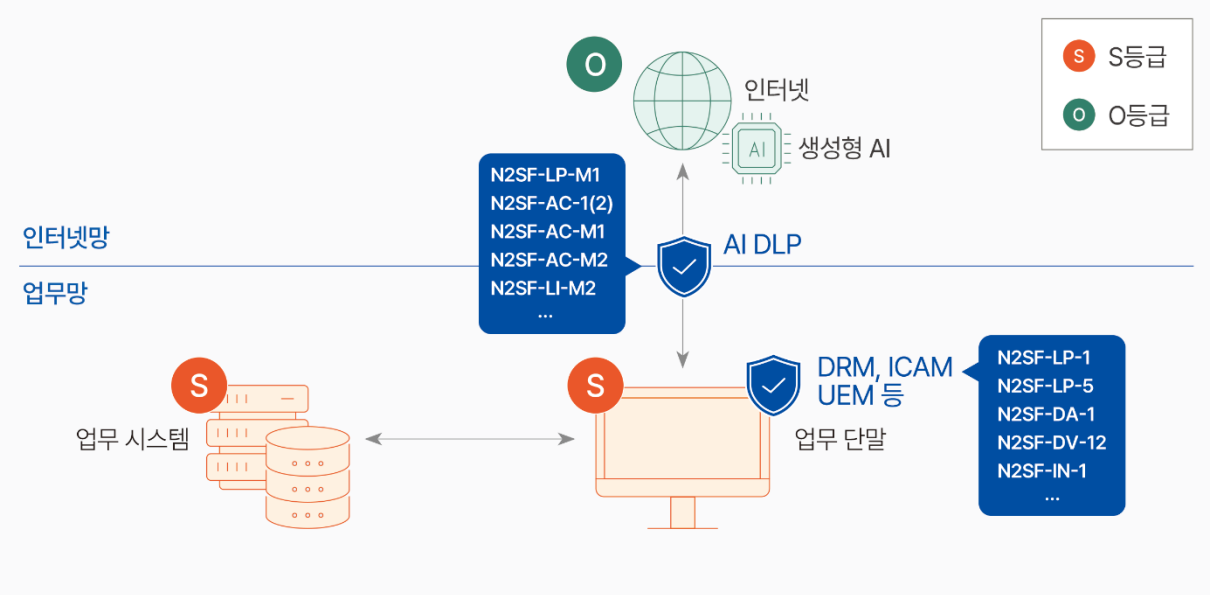
No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
72	N2SF-EB-3	네트워크	방화벽(FW) 계층 분리 및 화이트리스트 정책 적용	허용 포트·IP를 주기적으로 검토·갱신	PDP (ICAM), UEM, Web Filtering, NAC, RBI, SWG (유해사이트 차단)
73	N2SF-EB-5	네트워크	Proxy 서버를 통한 외부 통신 중계	내부 단말의 외부 직접 연결 차단	PDP (ICAM), UEM, RBI
74	N2SF-EB-6	네트워크	Network DLP 및 유해사이트 차단 솔루션 적용	중요정보 외부 유출 시도 탐지·차단 및 추적	방화벽(FW), Web Filtering, EDR, SWG (유해사이트차단)
75	N2SF-EB-14	네트워크	DNSSEC 기반 보안 DNS 서버 적용	비인가 DNS 서버로의 접근 차단	내 PC 지키미, 방화벽(FW), SWG (유해사이트 차단)
76	N2SF-EB-15	네트워크	VPN 우회 서비스 차단 정책 적용	우회 트래픽 탐지 및 차단	EDR, SWG (유해사이트 차단)
77	N2SF-IF-2	네트워크	SSL/TLS 프록시 및 복호화 DLP 적용	암호화 채널 내 정보 흐름 검사 수행	SSL/TLS Proxy, SSL 복호화 및 가시성
78	N2SF-IF-6	네트워크	Network DLP 또는 Proxy 기반 트래픽 검사	중요정보 탐지 시 차단	DLP
79	N2SF-EB-10	네트워크	Backend 네트워크 접근 제한 및 API 인증 적용	허용되지 않은 IP·도메인 접근 차단	보안정책 및 관리적 보안
80	N2SF-EB-11	네트워크	네트워크 보안 솔루션 이중화 구성	장애 발생 시 무중단 운영 유지	Anti-DDoS, 방화벽(FW), Network IPS, WAF 이중화 구성

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
81	N2SF-EB-13	네트워크	오류정보 전송에 대한 DLP 필터링 적용	오류정보 외부 발송 시 차단	DLP
82	N2SF-AC-M3	네트워크	네트워크 세션 활동 로깅	비정상 세션 탐지 및 주기적 감사	PDP (ICAM), UEM, SIEM
83	N2SF-EB-M5	네트워크	방화벽(FW) 기반 사고 대응 통제 체계 적용	침해 발생 시 외부 통신 즉시 차단	방화벽(FW)
84	N2SF-SG-6	관리	일반 사용자 기능과 관리·보안 목적 기능을 분리	일반 계정과 특수 목적 계정을 구분하여 운영	PDP (ICAM)
85	N2SF-IM-1	관리	개인정보 포함 문자열을 계정 식별자로 사용하지 않도록 기준 수립	계정 생성·운영 시 식별자 기준 준수 여부 점검	PDP (ICAM)
86	N2SF-LP-M1	관리	특수권한 계정에 대한 승인 기반 권한 부여 체계 적용	특수권한 계정을 분리 관리하고 변경 이력 점검	보안정책 및 관리적 보안
87	N2SF-DU-M3	관리	문서관리 정책 적용	정책에 따른 문서 생성·보관·폐기 절차 운영	보안정책 및 관리적 보안
88	N2SF-LI-1	관리	비밀번호 일방향 암호화 적용	비밀번호 일방향 암호화 적용	PKI
89	N2SF-IF-7	관리	업무정보에 대한 데이터 분류 및 DLP 솔루션 적용	비인가 정보 송신 시 차단	CDS, DLP
90	N2SF-IF-8	관리	중요 데이터 식별·분류·모니터링 솔루션 적용	민감 데이터 탐지 시 분류 및 차단	DLP, Web Filtering, DRM, 매체제어 솔루션
91	N2SF-LP-4(1)	관리	관리자 원격접속 제한 정책 적용	원격 관리자 접속 미허용 상태 유지	보안정책 및 관리적 보안
92	N2SF-DU-M3	관리	데이터 관리 정책 수립	데이터 관리 정책을 운영 절차에 반영	보안정책 및 관리적 보안
93	N2SF-IF-M1	관리	정보흐름 통제 정책 수립	통제 기준 및 예외 절차를 문서화·정기 갱신	보안정책 및 관리적 보안

(나) 자체정의 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	비고
1	N2SF-ORG1-1	단말	단말에서 생성·처리되는 업무정보의 등급이 변경될 수 있는 조건과 기준을 정의한 정보 등급 변화 정책을 수립	정보 등급 변화 정책을 문서화하여 운영 기준으로 적용하고, 관련 담당자가 정책을 준수하도록 관리	가이드라인 개선 방향
2	N2SF-ORG1-2	단말	단말에서 처리되는 업무정보의 등급 변경 이력을 기록·관리할 수 있는 관리 절차를 적용	정보 등급 변경 시 변경 전·후 등급과 변경 사유를 기록하고, 이력을 주기적으로 점검·관리	가이드라인 개선 방향

2.3 정보서비스 적용 기관 망 구성도 예시



수립한 보안 요구사항 및 보안통제 항목 구현 사항 등 산출물을 토대로 국가정보원 보안성 검토 신청 시, N2SF를 적용한 기관의 실제 망 구성도를 작성하여 첨부하여야 한다.

3. [모델 3] 업무환경에서 외부 클라우드 활용 업무협업 체계

본 정보서비스 모델은 기관 전산망 내 이용자 단말(업무 단말, 온북 등)을 통해 업무시스템에 접속하여 업무를 수행하는 환경에서, 업무 생산성·효율성 제고를 위해 이용자 업무 단말에서 외부 클라우드 업무협업 체계(SaaS)를 활용하는 모델이다.

※ (참고자료) N2SF 보안 가이드라인 1.0 - (부록2) 모델3 업무환경에서 외부 클라우드 활용 업무협업 체계

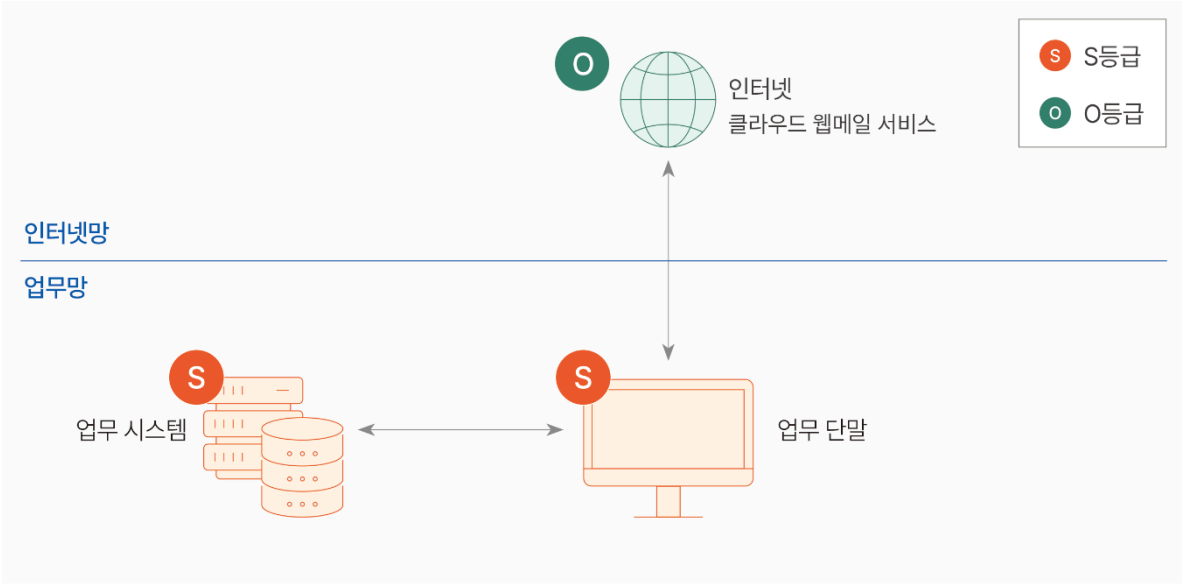
본 실증 사례는 업무 단말에서 외부 클라우드를 활용하기 위해 1개의 정보서비스 모델을 활용한다. 업무 단말이 외부 클라우드에 접속하여 데이터 입출력을 통한 업무 활용이 가능하도록 구현하는 데 중점을 둔다.

각 기관에서는 내부 업무환경과 외부 클라우드를 유기적으로 연계하여 업무 생산성·효율성을 제고하고자 할 때 참고할 수 있다.

3.1 정보서비스 유형 요약

정보서비스 유형 / 모델 No. (N2SF 가이드라인 기준)		모델 3 / 외부 클라우드 활용 업무협업 체계
정보서비스 개요	업무정보	① 직원 인사 정보 ② 시스템 구조 검토 회의록 ③ 연구 관련 통계(공개용) ④ 홍보용 사진
	정보시스템	① 업무 단말 ② 업무 시스템 ③ 클라우드 웹메일 서비스
	정보서비스 사용 시나리오	① 기관 정보를 외부 민간 클라우드 메일 서비스에 접속하여 첨부

위치/주체/객체 관점의 정보서비스 구조



- 위치: 업무망(S 등급), 주체: 업무 단말(S 등급), 객체: 클라우드 웹메일 서비스(O 등급)
- 업무망(S 등급)에서 업무 단말(S 등급)을 이용해 클라우드 웹메일 서비스(O 등급) 이용
- 업무 단말(S 등급)은 일차적으로 업무망 – 업무 시스템(S 등급)에 접속하여 식별, 인증 및 권한 확인 과정을 거친 후 클라우드 웹메일 서비스(O 등급)에 접속

보안통제 대상	① 업무 단말 ② 연계체계 ③ 클라우드 웹메일 서비스 연계 체계

3.2 최종산출물 서식

[1] 정보서비스 사용 시나리오별 정보시스템 식별

정보서비스 사용 시나리오별 정보시스템 식별

번호	사용 시나리오	관련 정보시스템	비고
1	기관 내 정보를 외부 민간 클라우드 웹메일 서비스에 접속하여 첨부		
1-1	업무 단말에서 외부 민간 클라우드 웹메일 서비스에 첨부	㉠ 업무 단말 ㉡ 클라우드 웹메일 서비스	

[2] 정보서비스 보안목표

국가정보원 보안성 검토 시 제출하는 문서중, 자체 보안대책에 대한 최종 산출물 서식 1번 「정보서비스 보안목표」는 아래와 같이 정리됨

No.	영역	보안 목표	비고
1	공통	정보서비스 모델 3. 외부 클라우드 활용 업무협업 체계	N2SF 가이드라인 1.0
2	업무 단말	업무망 연계를 위한 단말 보호	자체
3	연계체계	연계 시스템 간 전송 데이터의 무결성 확보	자체
4	네트워크	기관 내외부 통신 시 업무망 침해 피해 방지	자체

[3] C/S/O 등급분류

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 2번 「C/S/O 등급 분류표」는 아래와 같이 정리됨

No.	정보시스템		업무정보	
	명칭	C/S/O 등급	명칭	C/S/O 등급
1	업무 시스템	S	홍보용 사진 정보	O
			회의록	S
			연구 통계	O
			인사 정보	S
2	업무 단말	S	홍보용 사진 정보	O
			회의록	S
			연구 통계	O
			인사 정보	S
3	클라우드 웹메일 서비스	O	홍보용 사진 정보	O
			회의록	S
			연구 통계	O
			인사 정보	S

[4] 위협 식별 - 모델링 및 C/S/O 평가

기관의 정보서비스 구성요소에 따라 유스케이스별로 모델링 및 C/S/O 보안등급을 나누어 평가하며, 「정보 생산·저장」 보안원칙과 「정보 이동」 보안원칙을 적용하여 보안대책의 필요성을 평가한다.

N2SF 보안 가이드라인*에서 본 정보서비스는 기관 전산망 영역에 위치하는 **업무시스템(위치, S등급)**, **이용자 단말(주체, S등급)** 및 **인터넷 영역에 위치하는 이용자 단말(주체, O등급)**, **외부 클라우드 활용 업무협업 체계(객체, O등급)**로 구성되며, O등급의 이용자 단말, 업무 협업체계에서 S등급 업무정보가 생산·저장(활용), 이동하지 않도록 보안 원칙을 제시하고 있다. 아래 제시하는 실증 사례 및 N2SF 보안 가이드라인에 대하여 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 유연하게 참고하여 보안 원칙을 수립하여야 한다.

* N2SF 보안 가이드라인 1.0 – (부록2) 모델3 외부 클라우드 활용 업무협업 체계

사례: 기관 정보를 외부 민간 클라우드 메일 서비스에 접속하여 첨부

(1) 행정망에서 인터넷망 클라우드 웹메일 서비스에 데이터 첨부

<table>
<tr><th>구분</th><th>결과 및 설명</th><th>보안대책
필요여부</th></tr>
<tr><td>「위치-주체-객체」 모델
C/S/O 평가</td><td>
<table>
<tr><th>구분</th><th>C 등급</th><th>S 등급</th><th>O 등급</th></tr>
<tr><td>위치
Domain</td><td></td><td>업무 시스템</td><td></td></tr>
<tr><td>주체
Subject</td><td></td><td>업무 단말</td><td></td></tr>
<tr><td>객체
Object</td><td></td><td></td><td>클라우드 웹메일
서비스</td></tr>
</table>
행정망(S 등급)에서 업무단말(S 등급)을 이용해 인터넷망 DPG 허브(S 등급)를 이용하여 클라우드 웹메일 서비스에 접속하는 경우, 위치, 주체, 객체는 모두 S 등급에 해당
</td><td>아니오</td></tr>
<tr><td>「정보 생산·저장」
보안원칙</td><td>
<table>
<tr><th>~에서 생산·저장</th><th>C 정보</th><th>인사, 회의록 정보</th><th>연구 통계,
홍보용 사진 정보</th></tr>
<tr><td>C 시스템</td><td>●</td><td>●</td><td>●</td></tr>
<tr><td>업무 시스템</td><td>+</td><td>●</td><td>●</td></tr>
<tr><td>클라우드
웹메일서비스</td><td>+</td><td>+ ⃠</td><td>●</td></tr>
</table>
클라우드 웹메일 (O 등급)은 O 등급 이하인 공개 정보만을 생산 및 저장할 수 있으므로 인사 및 시스템 구조 정보(S 등급)를 다룰 경우 보안 원칙에 위배됨
</td><td>예</td></tr>
<tr><td>「정보 이동」 보안원칙</td><td>
<table>
<tr><th>~정보가 ~로 이동</th><th>C 시스템</th><th>업무 시스템</th><th>클라우드 웹메일
서비스</th></tr>
<tr><td>C 정보</td><td>●</td><td>+</td><td>+</td></tr>
<tr><td>인사, 회의록
정보</td><td>●</td><td>●</td><td>+ ⃠</td></tr>
<tr><td>연구통계,
홍보용사진정보</td><td>●</td><td>●</td><td>●</td></tr>
</table>
클라우드 웹메일 (O 등급)은 O 등급 이하인 공개 정보만을 주고받을 수 있으며, 따라서 인사 및 시스템 구조 정보(S 등급)를 주고받을 경우 보안원칙에 위배됨
</td><td>예</td></tr>
</table>

[5] 보안요구사항 및 보안통제

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 3번 「보안 요구사항 및 보안통제」는 아래와 같이 작성할 수 있다.

※ 보안 가이드라인에 없는 신규 자체정의 보안통제 항목: N2SF-SAAS

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
1	업무 단말	이용자 단말 보안성 유지	N2SF-LP-1
			N2SF-DA-1
			N2SF-DA-2
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-8
			N2SF-IN-10
			N2SF-IN-16
			N2SF-SG-2
			N2SF-SG-3
		이용자 단말 사용 보안	N2SF-AM-2
			N2SF-AM-9
			N2SF-DV-8
		이용자 단말 네트워크 보안	N2SF-SG-4
			N2SF-SG-5
			N2SF-SG-6
			N2SF-IF-9
			N2SF-EB-6
			N2SF-SN-1

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-WA-7
			N2SF-BC-1
			N2SF-DT-1
		이용자 단말 데이터 보호	N2SF-DU-2
		업무협업 체계(SaaS) 이용자 및 단말 관리	N2SF-LP-M1
			N2SF-EB-M1
			N2SF-DU-M3
2	SaaS 연계 체계	SaaS 연계체계 이용자 및 단말 인증	N2SF-AC-1
			N2SF-AC-1(1)
			N2SF-AC-1(2)
			N2SF-AC-1(4)
			N2SF-AC-3
			N2SF-AC-3(2)
			N2SF-DA-3
			N2SF-LI-1
			N2SF-LI-2
			N2SF-LI-4
		비인가 네트워크 연결 차단	N2SF-IS-4
			N2SF-IF-1
			N2SF-IF-9
			N2SF-EB-1
			N2SF-EB-2
			N2SF-EB-3
			N2SF-EB-6

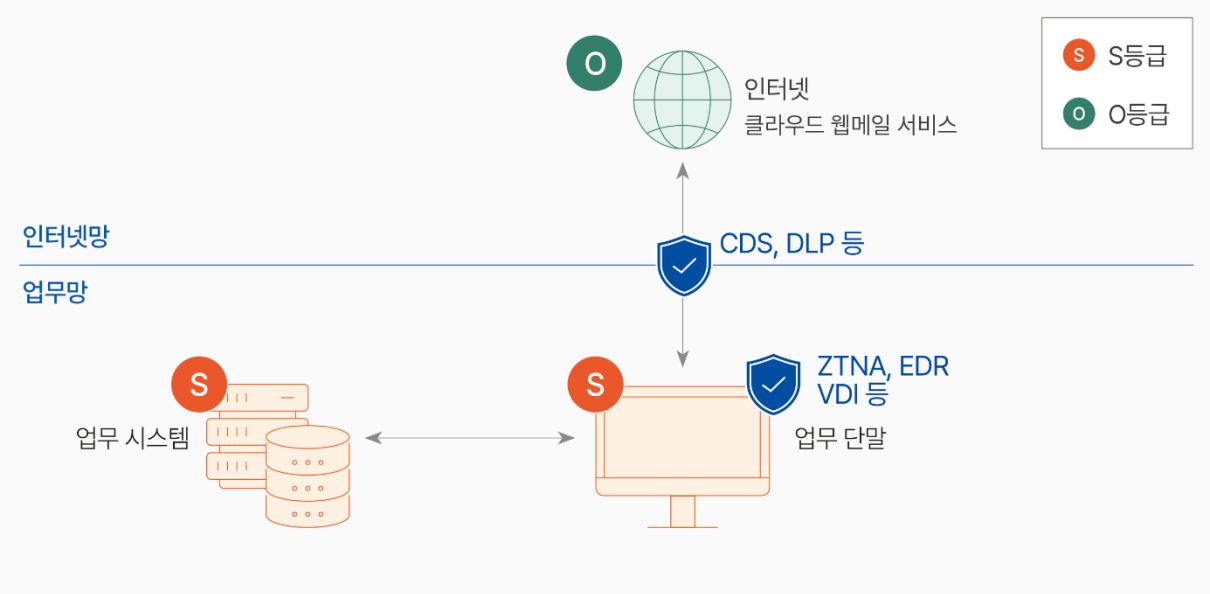
No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-EB-15
		기관 전산망과 업무협업 체계(SaaS) 전용선 수준 연결	N2SF-RA-5
			N2SF-IF-6
			N2SF-RA-2
			N2SF-RA-6
			N2SF-IF-15
		업무협업 체계(SaaS) 활용 시 데이터 보호	N2SF-IF-7
			N2SF-IF-8
			N2SF-IF-2
			N2SF-IF-6
			N2SF-IF-10
			N2SF-IF-14
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3
		연계체계 보안성 유지	N2SF-EB-13
			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-DV-4
			N2SF-IN-1(1)

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-11
		연계체계 운용 관리	N2SF-IF-M1
			N2SF-IF-M4
			N2SF-LP-M1
			N2SF-LP-M2
			N2SF-AC-1(2)
			N2SF-AC-M2
			N2SF-AC-M3
			N2SF-LI-M2
			N2SF-IF-M2
			N2SF-IF-M3
			N2SF-IF-M5
			N2SF-EB-M3
			N2SF-EB-M5
		가상화 인프라 구성요소 통합 관리 및 상태 감시	N2SF-SAAS-1
			N2SF-SAAS-1
		연계체계 전용선 수준 연결	N2SF-CD-1
		연계체계 보안성 유지	N2SF-DV-10
		연계체계 운용 관리	N2SF-IS-2
3	연계체계	연계체계 인증 정보 보호	N2SF-AU-5
			N2SF-AU-5(1)
		연계체계 보안성 유지	N2SF-EB-12

[6] 보안통제 구현계획

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 4번 「보안통제 구현계획표」는 아래와 같이 작성할 수 있다.

보안통제적용 정보서비스 구성도



보안통제 항목 단계별 보안 흐름

1	내부망 중요정보 생성·저장·반출 과정에 대한 데이터 보호
2	내부망 사용자·단말의 인증·접근·네트워크·단말 보안 통제
3	연계구간 트래픽·API·콘텐츠에 대한 다단계 보안 검증
4	서비스/워크로드 보안
5	각 기관별 보안 정책 및 이벤트에 대한 중앙 보안관리

(가) 보안통제 구현계획

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
1	N2SF-LP-1	업무 단말	ZTNA로 사용자단말 인증 후 애플리케이션 단위 최소권한 접근 통제	데이터 식별 결과를 접근통제 정책과 연계해 일관되게 적용 가능해야 함	ZTNA
2	N2SF-DA-1	업무 단말	UEM으로 단말 고유정보를 수집해 중앙 정책서버에 등록	단말 행위 기반 탐지와 중앙 정책 관리가 가능해야 함	UEM
3	N2SF-DA-2	업무 단말	ZTNA 디바이스 인증 정책으로 단말 기반 서비스 접근 제어	기존 네트워크 구조 변경 없이 정책 기반 통제가 가능해야 함	ZTNA
4	N2SF-IN-1(1)	업무 단말	UEM으로 단말 자산 및 패치 관리 수행	취약 요소를 지속 식별하고 자동 보완이 가능해야 함	UEM
5	N2SF-IN-5	업무 단말	ZTNA 정책으로 운영관리 포트 및 서비스 접근 통제	단말 행위 기반 탐지와 중앙 정책 관리가 가능해야 함	ZTNA
6	N2SF-IN-6	업무 단말	ZTNA Posture Check로 단말 설정 변경 탐지 및 통제	사전 진단 결과가 탐지·대응 체계로 연계되어야 함	ZTNA
7	N2SF-IN-8	업무 단말	ZTNA Agent로 단말 상태 점검 및 실행 제어	단말 행위 기반 탐지와 중앙 정책 관리가 가능해야 함	ZTNA
8	N2SF-IN-10	업무 단말	ZTNA Agent로 소프트웨어 설치 통제	인증·계정·권한을 통합 정책으로 관리할 수 있어야 함	ZTNA
9	N2SF-IN-16	업무 단말	APT/EDR로 악성코드 행위 기반 탐지 및 차단	실시간 탐지 기능을 운영 부담 없이 유지 가능해야 함	APT, EDR
10	N2SF-SG-2	업무 단말	OS 기반 논리적 분리 정책 적용	별도 솔루션 추가 없이 기존 통제로 충족 가능해야 함	단말 물리적 분리
11	N2SF-SG-3	업무 단말	OS 기반 업무/인터넷 환경 분리 운영	별도 솔루션 추가 없이 기존 통제로 충족 가능해야 함	단말 물리적 분리
12	N2SF-AM-2	업무 단말	ZTNA 인증 정책으로 비밀번호 정책 적용	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	ZTNA

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
13	N2SF-AM-9	업무 단말	ZTNA MFA 설정으로 추가 인증 적용	사용자 경험 저하 없이 단계적 적용이 가능해야 함	ZTNA
14	N2SF-DV-8	업무 단말	ZTNA 디바이스 제어 정책으로 하드웨어/설정 변경 통제	사용자 개입 없이 정책 일괄 적용이 가능해야 함	ZTNA
15	N2SF-SG-4	업무 단말	방화벽(FW) ACL 로 네트워크 분리 및 접근 통제	기존 네트워크 구조 변경 없이 정책 기반 통제가 가능해야 함	방화벽(FW)
16	N2SF-SG-5	업무 단말	CDS 로 데이터 전송 정책 및 승인 기반 통제	기존 네트워크 구조 변경 없이 정책 기반 통제가 가능해야 함	CDS
17	N2SF-SG-6	업무 단말	인증, 감사 및 데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 애플리케이션 실행 등 사용자 기능을 분리한다	API 흐름을 단일 지점에서 통제·가시화할 수 있어야 함	API Gateway
18	N2SF-IF-9	업무 단말	IPS/IDS 로 이상 트래픽 탐지 및 차단	네트워크 접근 제어를 자동화해 운영 복잡도를 낮춰야 함	IPS/IDS
19	N2SF-EB-6	업무 단말	IPS/IDS 필터링 정책으로 경계 트래픽 통제	데이터 행위와 네트워크 이상을 상관 분석할 수 있어야 함	IPS/IDS
20	N2SF-SN-1	업무 단말	ZTNA 세션 정책으로 인증 기반 세션 통제	인증·계정·권한을 통합 정책으로 관리할 수 있어야 함	ZTNA
21	N2SF-WA-7	업무 단말	ZTNA 네트워크 정책으로 무선/API 접근 통제	무선 환경 변화에 자동 대응 가능해야 함	ZTNA
22	N2SF-BC-1	업무 단말	블루투스/외부 인터페이스 차단	단말 상태 기반 정책 적용이 가능해야 함	매체제어
23	N2SF-DT-1	업무 단말	ZTNA API 접근제어 정책 적용	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	ZTNA
24	N2SF-DU-2	업무 단말	DRM 으로 문서 암호화 및 권한 기반 접근 통제	데이터 위치와 형식에 관계없이 일관된 보호 정책을 적용·유지할 수 있어야 함	DRM

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
25	N2SF-LP-M1	업무 단말	ZTNA 최소권한 정책으로 서비스 접근 통제	일반·특권 계정 통제를 분리해 관리해야 함	ZTNA
26	N2SF-EB-M1	업무 단말	SIEM/SOAR로 로그 수집 및 이상행위 분석	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	SIEM/SOAR
27	N2SF-DU-M3	업무 단말	DRM으로 데이터 암호화 및 사용 통제	정책 변경·배포를 중앙에서 일관되게 관리해야 함	DRM
28	N2SF-AC-1	SaaS 연계 체계	SIEM/SOAR로 ICAM 이벤트 수집·상관분석 및 이상행위 탐지	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	SIEM/SOAR
29	N2SF-AC-1(1)	SaaS 연계 체계	ICAM으로 계정·권한 정책 관리 및 인증·인가 정책 적용	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	ICAM
30	N2SF-AC-1(2)	SaaS 연계 체계	ICAM 인증 정책으로 인증정보 보호 및 접근 통제	다양한 보안 이벤트를 통합 분석할 수 있어야 함	ICAM
31	N2SF-AC-1(4)	SaaS 연계 체계	ZTNA 인증·접근 정책으로 로그인 실패 시 접근 제한	인증 절차 단순화와 보안 수준을 동시에 유지해야 함	ZTNA
32	N2SF-AC-3	SaaS 연계 체계	ICAM으로 계정·권한 관리 및 인증 정책 적용	다양한 보안 이벤트를 통합 분석할 수 있어야 함	ICAM
33	N2SF-AC-3(2)	SaaS 연계 체계	ICAM 인증 정책으로 계정 접근 통제	다양한 보안 이벤트를 통합 분석할 수 있어야 함	ICAM
34	N2SF-DA-3	SaaS 연계 체계	단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증	네트워크 접근 제어를 자동화해 운영 복잡도를 낮춰야 함	NAC
35	N2SF-LI-1	SaaS 연계 체계	ZTNA 정책으로 네트워크 격리 기반 접근 통제	특권 행위에 대한 통제·추적이 가능해야 함	ZTNA
36	N2SF-LI-2	SaaS 연계 체계	ZTNA 정책으로 정보흐름 동적 통제	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	ZTNA

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
37	N2SF-LI-4	SaaS 연계 체계	ZTNA 정책으로 출발지/목적지 인증 및 접근 통제	사용자 경험 저하 없이 단계적 적용이 가능해야 함	ZTNA
38	N2SF-IS-4	SaaS 연계 체계	방화벽(FW) 정책으로 데이터 전송 검사 및 승인 통제	기본 경계 통제를 안정적으로 유지해야 함	방화벽(FW)
39	N2SF-IF-1	SaaS 연계 체계	SIEM/SOAR로 외부 위협 통신 이상행위 탐지	사용자·단말 상태 기반 접근 제어가 가능해야 함	SIEM/SOAR
40	N2SF-IF-9	SaaS 연계 체계	IPS/IDS로 이상 트래픽 탐지 및 차단	네트워크 접근 제어를 자동화해 운영 복잡도를 낮춰야 함	IPS/IDS
41	N2SF-EB-1	SaaS 연계 체계	방화벽(FW) 정책으로 데이터 전송 흐름 통제	트래픽 제어와 접근 통제를 연계 운영해야 함	방화벽(FW)
42	N2SF-EB-2	SaaS 연계 체계	방화벽(FW) 정책으로 경계 구간 트래픽 통제	승인된 서비스만 허용	방화벽(FW)
43	N2SF-EB-3	SaaS 연계 체계	방화벽(FW) 정책으로 데이터 전송 승인 기반 통제	트래픽 제어와 접근 통제를 연계 운영해야 함	방화벽(FW)
44	N2SF-EB-6	SaaS 연계 체계	IPS/IDS 필터링 정책으로 경계 트래픽 통제	데이터 행위와 네트워크 이상을 상관 분석할 수 있어야 함	IPS/IDS
45	N2SF-EB-15	SaaS 연계 체계	IPS/IDS 룰셋으로 비정상 트래픽 탐지·차단	네트워크 행위 이상을 상관 분석할 수 있어야 함	IPS/IDS
46	N2SF-RA-5	SaaS 연계 체계	ZTNA 정책으로 API 최소권한 접근 통제	원격 접속 시 보안 정책을 일관되게 적용해야 함	ZTNA
47	N2SF-IF-6	SaaS 연계 체계	DRM으로 데이터 암호화 및 권한 통제	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	DRM
48	N2SF-RA-2	SaaS 연계 체계	ZTNA 인증 정책으로 API 접근 통제	원격 접속 시 보안 정책을 일관되게 적용해야 함	ZTNA
49	N2SF-RA-6	SaaS 연계 체계	ZTNA 정책으로 API 인증 및 접근 제어	원격 접속 시 보안 정책을 일관되게 적용해야 함	ZTNA

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
50	N2SF-IF-15	SaaS 연계 체계	ZTNA 정책으로 전용 통신망 기반 접근 통제	외부로부터 정보흐름을 보호할 수 있는 전용 통신망(전용회선, 가상사설망 등)을 구성한다.	ZTNA
51	N2SF-IF-7	SaaS 연계 체계	CDS 데이터 유형 식별자를 확인하여 전송 통제	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	CDS
52	N2SF-IF-8	SaaS 연계 체계	DRM 으로 데이터 암호화 및 사용 통제	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	DRM
53	N2SF-IF-2	SaaS 연계 체계	암호화된 정보의 내용을 확인하기 위하여 정보를 복호화	가시성 확보와 성능 영향 간 균형을 유지해야 함	SSL 암복호화
54	N2SF-IF-6	SaaS 연계 체계	DRM 으로 데이터 암호화 및 권한 통제	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	DRM
55	N2SF-IF-10	SaaS 연계 체계	ZTNA 정책으로 암호화된 정보흐름 통제	사용자·데이터·연계 통제를 통합 운영해야 함	ZTNA
56	N2SF-IF-14	SaaS 연계 체계	DRM 으로 데이터 암호화 및 권한 통제	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	DRM
57	N2SF-IF-3	SaaS 연계 체계	임베디드된 데이터 내부에 인가되지 않은 다른 종류의 데이터 삽입 차단	도메인 간 정보 이동을 정책적으로 제어할 수 있어야 함	EDR
58	N2SF-EB-13	SaaS 연계 체계	IPS/IDS 정책으로 경계 트래픽 탐지·차단	웹 접근 통제를 단계적으로 적용할 수 있어야 함	IPS/IDS
59	N2SF-LP-4	SaaS 연계 체계	SIEM/SOAR 로 비정상 요청 및 세션 탐지·차단	권한 상승과 사용을 분리 관리해야 함	SIEM/SOAR
60	N2SF-LP-4(1)	SaaS 연계 체계	SIEM/SOAR 로 콘텐츠/AI 응답 검증 이상행위 탐지	권한 상승과 사용을 분리 관리해야 함	SIEM/SOAR
61	N2SF-LP-4(4)	SaaS 연계 체계	SIEM/SOAR 로 콘텐츠 검증 및 이상행위 탐지	다양한 보안 이벤트를 통합 분석할 수 있어야 함	SIEM/SOAR
62	N2SF-AC-1(5)	SaaS 연계 체계	ICAM 인증 정책으로 계정 보호 및 접근 통제	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	ICAM

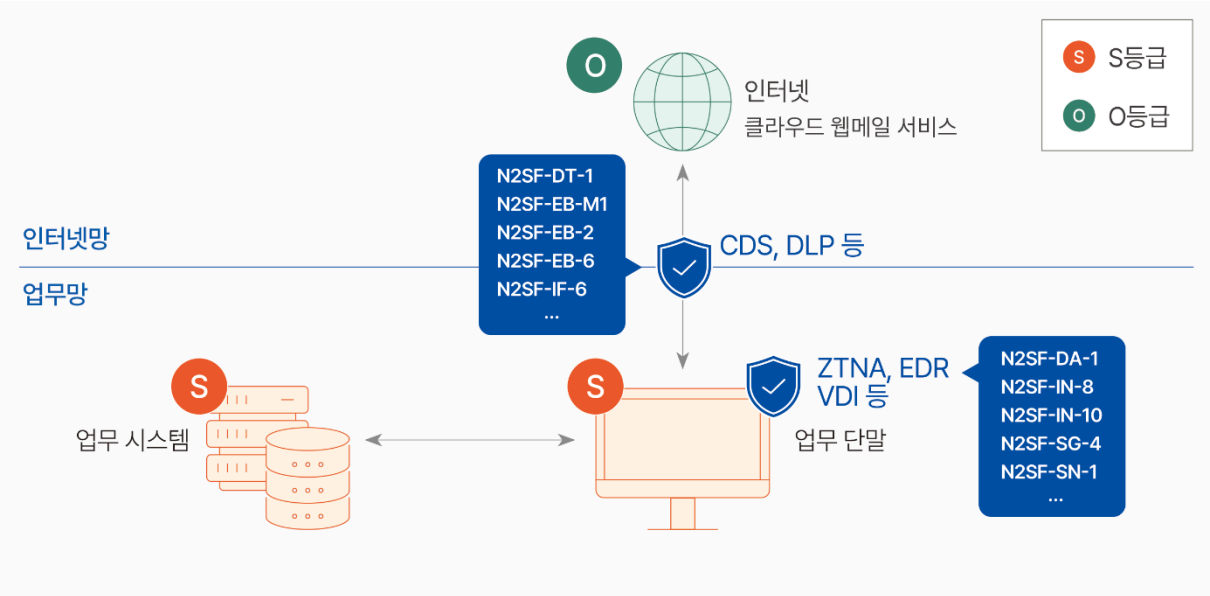
No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
63	N2SF-AC-3(1)	SaaS 연계 체계	SIEM/SOAR로 콘텐츠/응답 이상행위 탐지	계정 이벤트와 보안 로그를 연계 분석해야 함	SIEM/SOAR
64	N2SF-EB-8	SaaS 연계 체계	ZTNA 정책으로 API 인증 및 접근 통제	별도 솔루션 추가 없이 기존 통제로 충족 가능해야 함	ZTNA
65	N2SF-EB-10	SaaS 연계 체계	ZTNA 정책으로 관리자 권한 계정 접근 제한	경계·웹·API 구간을 다계층 구조로 연속 보호할 수 있어야 함	ZTNA
66	N2SF-EB-11	SaaS 연계 체계	SIEM/SOAR로 위험 계정 탐지 및 비활성화 대응	별도 솔루션 추가 없이 기존 통제로 충족 가능해야 함	SIEM/SOAR
67	N2SF-DV-4	SaaS 연계 체계	ZTNA 정책으로 운영관리 포트 접근 차단	정보 사용 맥락을 고려한 통제가 가능해야 함	ZTNA
68	N2SF-IN-1(1)	SaaS 연계 체계	UEM으로 단말 자산 및 패치 관리 수행	취약 요소를 지속 식별하고 자동 보완이 가능해야 함	UEM
69	N2SF-IN-5	SaaS 연계 체계	ZTNA 정책으로 운영관리 포트 및 서비스 접근 통제	단말 행위 기반 탐지와 중앙 정책 관리가 가능해야 함	ZTNA
70	N2SF-IN-6	SaaS 연계 체계	ZTNA Posture Check로 단말 설정 변경 탐지 및 통제	사전 진단 결과가 탐지·대응 체계로 연계되어야 함	ZTNA
71	N2SF-IN-11	SaaS 연계 체계	서비스 신뢰성 통제는 운영정책으로 관리	장애·사고 발생 시 서비스 영향 최소화를 고려한 신속한 복구가 가능해야 함	서버보안
72	N2SF-IF-M1	SaaS 연계 체계	SIEM/SOAR로 세션 감사 및 이상행위 탐지	정책 변경·배포를 중앙에서 일관되게 관리해야 함	SIEM/SOAR
73	N2SF-IF-M4	SaaS 연계 체계	SIEM/SOAR로 세션 감사 및 이상행위 탐지	다양한 보안 이벤트를 통합 분석할 수 있어야 함	SIEM/SOAR
74	N2SF-LP-M1	SaaS 연계 체계	ZTNA 최소권한 정책으로 서비스 접근 통제	일반·특권 계정 통제를 분리해 관리해야 함	ZTNA
75	N2SF-LP-M2	SaaS 연계 체계	SIEM/SOAR로 정책 변경 및 정보흐름 이상 탐지	다양한 보안 이벤트를 통합 분석할 수 있어야 함	SIEM/SOAR

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
76	N2SF-AC-1(2)	SaaS 연계 체계	ICAM 인증 정책으로 인증정보 보호 및 접근 통제	다양한 보안 이벤트를 통합 분석할 수 있어야 함	ICAM
77	N2SF-AC-M2	SaaS 연계 체계	ZTNA 정책으로 특수권한 사용자 접근 통제	로그 무결성과 장기 보관이 가능해야 함	ZTNA
78	N2SF-AC-M3	SaaS 연계 체계	SIEM/SOAR로 비정상 요청 및 세션 탐지	다양한 보안 이벤트를 통합 분석할 수 있어야 함	SIEM/SOAR
79	N2SF-LI-M2	SaaS 연계 체계	ICAM 인증 정책으로 계정 상태 모니터링	다양한 보안 이벤트를 통합 분석할 수 있어야 함	ICAM
80	N2SF-IF-M2	SaaS 연계 체계	SIEM/SOAR로 세션 감사 및 이상행위 탐지	다양한 보안 이벤트를 통합 분석할 수 있어야 함	SIEM/SOAR
81	N2SF-IF-M3	SaaS 연계 체계	SIEM/SOAR로 세션 감사 및 이상행위 탐지	정책 변경·배포를 중앙에서 일관되게 관리해야 함	SIEM/SOAR
82	N2SF-IF-M5	SaaS 연계 체계	SIEM/SOAR로 세션 감사 및 이상행위 탐지	다양한 보안 이벤트를 통합 분석할 수 있어야 함	SIEM/SOAR
83	N2SF-EB-M3	SaaS 연계 체계	SIEM/SOAR로 정보흐름 로그 수집 및 분석	접근 행위와 보안 이벤트를 함께 분석해야 함	SIEM/SOAR
84	N2SF-EB-M5	SaaS 연계 체계	SIEM/SOAR로 통제 이행 점검 및 감사 수행	기존 네트워크 구조 변경 없이 정책 기반 통제가 가능해야 함	SIEM/SOAR
85	N2SF-AU-5	연계체계	ICAM 인증 설정 기준 및 변경통제 정책 적용	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	ICAM
86	N2SF-AU-5(1)	연계체계	UEM으로 보안설정 및 구성요소 관리	기존 계정 체계와 연계한 중앙 관리가 가능해야 함	UEM
87	N2SF-EB-12	연계체계	ZTNA 정책으로 관리자 계정 접근 통제	외부 노출 자산을 지속적으로 식별·관리해야 함	ZTNA

(나) 자체정의 보안통제 구현계획

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건
1	N2SF-SAAS-1	정보시스템 (컨테이너·클라우드 환경)	CNAPP, CSPM, CWPP, KSPM, K8s Network Policy 기반으로 컨테이너 및 클라우드 워크로드 보안 상태를 통합 관리	클라우드 자산, 설정, 워크로드 보안 상태를 지속적으로 점검하고 정책 위반 및 취약 상태를 자동 탐지·통제할 수 있어야 함
2	N2SF-SAAS-2	정보시스템 (API 기반 서비스)	API Gateway, WAAP(API Protection), Service Mesh, IAM/SSO, SIEM 연계를 통해 API 통신 및 서비스 접근 보안 정책을 통합 관리	API 접근·인증·통신 정책을 단일 정책 체계에서 적용하고 위협 탐지 정보를 관제 시스템과 연계하여 가시성과 추적성을 확보할 수 있어야 함

3.3 정보서비스 적용 기관 망 구성도 예시



수립한 보안 요구사항 및 보안통제 항목 구현 사항 등 산출물을 토대로 국가정보원 보안성 검토 신청 시, N2SF를 적용한 기관의 실제 망 구성도를 작성하여 첨부하여야 한다.

4. [모델 4] 업무 단말의 인터넷 이용

본 정보서비스 모델은 기관 전산망 내 이용자 단말(업무 단말, 온북 등)을 통해 업무시스템에 접속하여 업무를 수행하는 환경에서, 업무 생산성·효율성 제고를 위해 이용자 업무 단말에서 인터넷을 사용하는 모델이다.

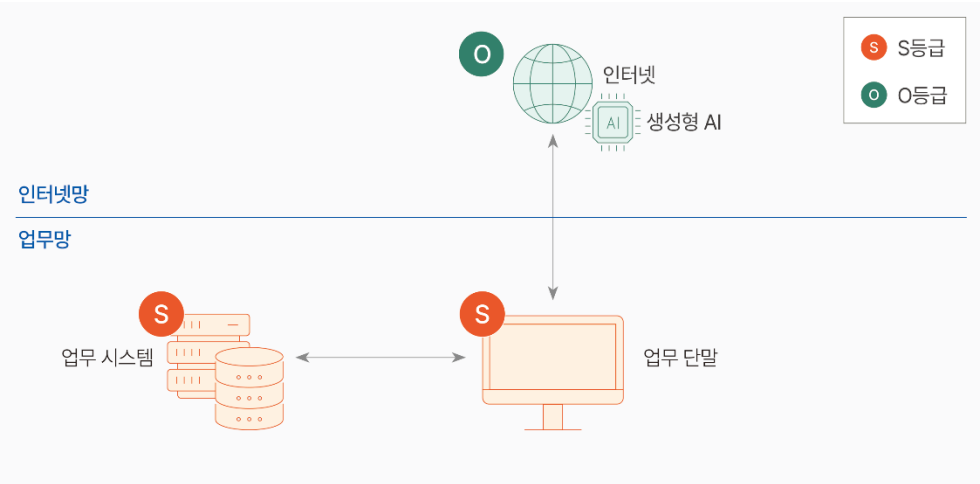
※ (참고자료) N2SF 보안 가이드라인 1.0 - (부록2) 모델4 업무 단말의 인터넷 이용

본 실증 사례는 업무 단말에서 인터넷을 이용하고 생성형 AI를 안전하게 사용하기 위해 2개의 정보서비스 모델을 활용한다. 외부 접속이 차단된 내부 업무망 환경에서 인터넷 검색 등 외부 서비스를 이용함으로써 업무 효율을 극대화하기 위해 외부 인터넷 자원 및 생성형 AI를 보안 규정 준수하여 현업에 도입하는 사례를 제시한다.

각 기관에서는 업무 단말의 인터넷 이용이 제한적인 환경에서 정보 검색, 생성형 AI를 통한 자료 요약 및 데이터 분석 등의 업무를 수행하고자 할 때 참고할 수 있다.

4.1 정보서비스 유형 요약

정보서비스 유형 / 모델 No. (N2SF 가이드라인 기준)		모델 2 / 업무환경에서 생성형 AI 활용 모델 4 / 업무 단말의 인터넷 이용
정보서비스 개요	업무정보	① 인터넷 수집자료 ② 인터넷 수집자료 취합문서 ③ 미공개 기관 고유업무정보 ④ 공개 기관 고유업무정보 ⑤ 연구 산출물 ⑥ 외부기관 연계데이터
	정보시스템	① 업무 단말 ② 업무 시스템 ③ 인터넷 서비스 ④ 생성형 AI 서비스 ⑤ 외부기관
	정보서비스 사용 시나리오	① 일반 인터넷 서비스 정보 수집 ② 생성형 AI 서비스 활용
위치/주체/객체 관점의 정보서비스 구조		



- 위치: 업무망(S 등급), 주체: 업무 단말(S 등급), 객체: 생성형 AI 서비스 (O 등급)
- 업무망(S 등급)에서 업무 단말 (S 등급)을 이용해 인터넷과 생성형 AI 서비스(O 등급) 이용
- 업무단말(S 등급)은 일차적으로 내부 시스템 – 업무 시스템 (S 등급) - 에 접속하여 식별, 인증 및 권한 확인 과정을 거친 후 인터넷 및 생성형 AI 서비스 (O 등급)에 접속

보안통제 대상	① 업무 단말 ② AI 연계체계 ③ 인터넷 연계체계 ④ 외부기관 연계체계 ⑤ 생성형 AI

4.2 최종산출물 서식

[1] 정보서비스 사용 시나리오별 정보시스템 식별

정보서비스 사용 시나리오별 정보시스템 식별

번호	사용 시나리오	관련 정보시스템
1	일반 인터넷 서비스 정보 수집	
1-1	업무 단말에서 인터넷 정보 검색 및 열람	㉮ 업무 단말 ㉯ 인터넷 서비스
2	생성형 AI 서비스 활용	
2-1	업무 단말에서 생성형 AI 서비스 활용	㉮ 업무 단말 ㉯ 생성형 AI 서비스

[2] 정보서비스 보안목표

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 1번 「정보서비스 보안목표」는 아래와 같이 정리됨

No.	영역	보안 목표	비고
1	공통	정보서비스 모델 2. 업무환경에서 생성형 AI 활용	N2SF 가이드라인 1.0
2		정보서비스 모델 4. 업무 단말의 인터넷 이용	N2SF 가이드라인 1.0
3	네트워크	업무영역과 별도로 연구망 구성 (연구망 침해 시 피해 전이 방지)	자체
4		망연계 보안 솔루션 도입	자체
5		심사목적에 필요한 인터넷 서비스로 접속 제한	자체
6	단말관리	인터넷과 연구시스템 동시연결 원천 차단	자체
7	자료	자체 파일 변환기를 사용하여 내부 생성 자료과 외부에서 다운로드 받은 자료를 구별함	자체

[3] C/S/O 등급분류

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 2번 「C/S/O 등급 분류표」는 아래와 같이 정리됨

No.	정보시스템		업무정보	
	명칭	C/S/O 등급	명칭	C/S/O 등급
1	업무 단말	S	인터넷 수집자료	O
			인터넷 수집자료 취합문서	S
			미공개 기관 고유업무정보	S
			공개 기관 고유업무정보	O
			연구 산출물	S
2	업무 시스템	S	인터넷 수집자료	O
			인터넷 수집자료 취합문서	S
			미공개 기관 고유업무정보	S
			공개 기관 고유업무정보	O
			연구 산출물	S
3	인터넷 서비스	O	인터넷 수집자료	O
4	생성형 AI 서비스	O	인터넷 수집자료	O
5	외부기관 연계데이터	O	외부기관 연계데이터	O

[4] 위협 식별 - 모델링 및 C/S/O 평가

기관의 정보서비스 구성요소에 따라 유스케이스별로 모델링 및 C/S/O 보안등급을 나누어 평가하며, 「정보 생산·저장」 보안원칙과 「정보 이동」 보안원칙을 적용하여 보안대책의 필요성을 평가한다.

N2SF 보안 가이드라인*에서 본 정보서비스는 기관 전산망 영역에 위치하는 **업무시스템(위치, S등급)**, **이용자 단말(주제, S등급)** 및 인터넷 영역에 위치하는 **인터넷 서비스(객체, O등급)**로 구성되며, O등급의 인터넷 서비스에서 S등급 업무정보가 생산·저장(활용), 이동하지 않도록 보안 원칙을 제시하고 있다. 아래 제시하는 실증 사례 및 N2SF 보안 가이드라인에 대하여 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 유연하게 참고하여 보안원칙을 수립하여야 한다.

* N2SF 보안 가이드라인 1.0 - (부록2) 모델4 업무 단말의 인터넷 이용

사례 1: 일반 인터넷 서비스 정보 수집

(1) 업무 단말에서 인터넷 정보 검색 및 열람

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C등급 / S등급 / O등급 위치 Domain: 업무 시스템 주체 Subject: 업무 단말 객체 Object: 인터넷 서비스 업무망(S 등급)에서 업무 단말(S 등급)을 이용해 인터넷 서비스(O 등급)를 이용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안대책 필요	예
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C정보 / 업무 단말 내 S업무 정보 / 인터넷 수집자료 C 시스템: ● ● ● 업무 단말: + ● ● 인터넷 서비스: + ⃠ + ● 인터넷 서비스(O 등급)는 O 등급 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)은 다룰 수 있으나, 그 외의 업무 단말 내 S 등급 업무정보를 다루는 경우 보안원칙에 위배됨	예
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / 업무 단말 / 인터넷 서비스 C 정보: ● + + 업무단말 내 S등급 업무정보: ● ● ⃠ + 인터넷 수집자료: ● ● ● 업무 단말(S 등급)이 인터넷 서비스(O 등급)에 접속하는 경우, 인터넷 수집자료(O 등급)와 같은 O 등급 업무정보만을 주고받을 수 있으며, 그 외 업무 단말 내 존재하는 S 등급 업무정보를 주고받는 경우 보안원칙에 위배됨.	예

사례 2: 생성형 AI 서비스 활용

(1) 업무 단말에서 생성형 AI 서비스 활용

<table>
<tr><th>구분</th><th>결과 및 설명</th><th>보안대책
필요여부</th></tr>
<tr><td>「위치-주체-객체」 모델
C/S/O 평가</td><td>
<table>
<tr><th>구분</th><th>C 등급</th><th>S 등급</th><th>O 등급</th></tr>
<tr><td>위치
Domain</td><td></td><td rowspan="2">업무망</td><td></td></tr>
<tr><td>주체
Subject</td><td></td><td rowspan="2">업무 단말</td><td></td></tr>
<tr><td>객체
Object</td><td></td><td></td><td>생성형 AI 서비스</td></tr>
</table>
업무망(S 등급)에서 업무 단말(S 등급)을 이용해 생성형 AI 서비스(O 등급)를 이용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안 대책 필요.
</td><td>예</td></tr>
<tr><td>「정보 생산·저장」
보안원칙</td><td>
<table>
<tr><th>~에서 생산·저장</th><th>C 정보</th><th>업무 단말 내
S 업무 정보</th><th>인터넷 수집자료</th></tr>
<tr><td>C 시스템</td><td>●</td><td>●</td><td>●</td></tr>
<tr><td>업무 단말</td><td>+</td><td>●</td><td>●</td></tr>
<tr><td>생성형 AI
서비스</td><td>+</td><td>⃠ +</td><td>●</td></tr>
</table>
생성형 AI 서비스(O 등급)는 O 등급인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)를 다룰 수 있으나, 그 외의 업무 단말 내 S 등급 업무정보를 다루는 경우 보안원칙에 위배됨.
</td><td>예</td></tr>
<tr><td>「정보 이동」 보안원칙</td><td>
<table>
<tr><th>~정보가 ~로 이동</th><th>C 시스템</th><th>업무 단말</th><th>인터넷 서비스</th></tr>
<tr><td>C 정보</td><td>●</td><td>+</td><td>+</td></tr>
<tr><td>업무 단말 내
S 등급 업무정보</td><td>●</td><td>●</td><td>⃠ +</td></tr>
<tr><td>생성형 AI
서비스</td><td>●</td><td>●</td><td>●</td></tr>
</table>
업무 단말(S 등급)이 생성형 AI 서비스(O 등급)에 접속하는 경우, 인터넷 수집자료(O 등급)와 같은 O 등급 업무정보만을 주고받을 수 있으며, 그 외 업무 단말 내 존재하는 S 등급 업무정보를 주고받는 경우 보안원칙에 위배됨.
</td><td>예</td></tr>
</table>

[5] 보안요구사항 및 보안통제

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 3번 「보안 요구사항 및 보안통제」는 아래와 같이 작성할 수 있다.

※ 보안 가이드라인에 없는 신규 자체정의 보안통제 항목: N2SF-ORG2

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
1	업무 단말	이용자 단말 보안성 유지	N2SF-LP-1	N2SF 모델 2번 N2SF 모델 4번
			N2SF-DA-1	
			N2SF-DA-2	
			N2SF-DV-12	
			N2SF-IN-1(1)	
			N2SF-IN-5	
			N2SF-IN-6	
			N2SF-IN-8	
			N2SF-IN-10	
			N2SF-IN-16	
		이용자 단말 사용 보안	N2SF-AM-2	N2SF 모델 2번 N2SF 모델 4번
			N2SF-AM-9	
			N2SF-DV-6	
			N2SF-DV-8	
		이용자 단말 네트워크 보안	N2SF-SG-4	N2SF 모델 2번 N2SF 모델 4번
			N2SF-SG-5	
			N2SF-SG-6	
			N2SF-IF-9	
			N2SF-EB-6	
			N2SF-SN-1	
			N2SF-WA-7	
			N2SF-BC-1	
			N2SF-DT-1	

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
		이용자 단말 데이터 보호	N2SF-DU-2	N2SF 모델 2 번 N2SF 모델 4 번
		이용자 계정 정보 보호	N2SF-IM-1	N2SF 모델 2 번
		생성형 AI 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1	N2SF 모델 2 번
			N2SF-EB-M1	
			N2SF-DU-M3	
		파일 직접 다운로드 차단	N2SF-CD-5	N2SF 모델 4 번
			N2SF-IN-16	
		인터넷 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1	N2SF 모델 4 번
			N2SF-EB-M1	
			N2SF-DU-M3	
		정보 등급 변화 정책 수립	N2SF-ORG2-1	자체정의 통제항목
		정보 등급 변화 내역 기록 및 관리	N2SF-ORG2-2	자체정의 통제항목
2	AI 연계체계	생성형 AI 서비스 이용자 및 단말 인증	N2SF-AC-1	N2SF 모델 2 번
			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	
		비인가 네트워크 연결 차단	N2SF-IS-4	N2SF 모델 2 번
			N2SF-IF-1	

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
			N2SF-IF-9	
			N2SF-EB-1	
			N2SF-EB-2	
			N2SF-EB-3	
			N2SF-EB-5	
			N2SF-EB-6	
			N2SF-EB-14	
			N2SF-EB-15	
		생성형 AI 서비스 활용 시 데이터 보호	N2SF-IF-2	N2SF 모델 2 번
			N2SF-IF-6	
			N2SF-IF-7	
			N2SF-IF-8	
			N2SF-IF-10	
			N2SF-IF-14	
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3	N2SF 모델 2 번
			N2SF-IF-5	
		연계체계 보안성 유지	N2SF-LP-4	N2SF 모델 2 번
			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-13	
			N2SF-DV-4	
			N2SF-DV-12	
			N2SF-IN-1(1)	

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
			N2SF-IN-5	
			N2SF-IN-6	
			N2SF-IN-11	
		연계체계 운용 관리	N2SF-LP-M1	N2SF 모델 2 번
			N2SF-LP-M2	
			N2SF-AC-1(2)	
			N2SF-AC-M1	
			N2SF-AC-M2	
			N2SF-AC-M3	
			N2SF-LI-M1	
			N2SF-LI-M2	
			N2SF-IF-M1	
			N2SF-IF-M2	
			N2SF-IF-M3	
			N2SF-IF-M4	
			N2SF-IF-M5	
			N2SF-EB-M3	
			N2SF-EB-M4	
			N2SF-EB-M5	
3	인터넷 연계체계	인터넷 서비스 이용자 및 단말 인증	N2SF-AC-1	N2SF 모델 4 번
			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	

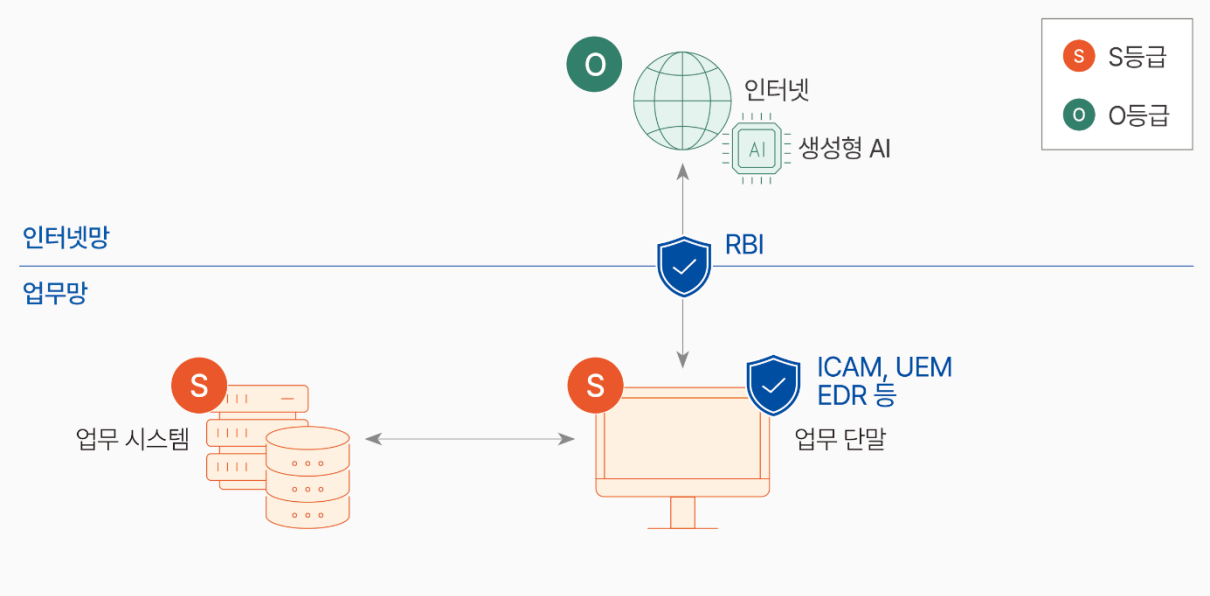
No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
			N2SF-LI-1	
			N2SF-LI-2	
			N2SF-LI-4	
		비인가 네트워크 연결 차단	N2SF-IS-4	N2SF 모델 4번
			N2SF-IF-1	
			N2SF-EB-1	
			N2SF-EB-2	
			N2SF-EB-3	
			N2SF-EB-5	
			N2SF-EB-6	
			N2SF-EB-14	
			N2SF-EB-15	
		인터넷 서비스 활용 시 데이터 보호	N2SF-IF-2	N2SF 모델 4번
			N2SF-IF-6	
			N2SF-IF-7	
			N2SF-IF-8	
			N2SF-IF-10	
			N2SF-IF-14	
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3	N2SF 모델 4번
			N2SF-IF-5	
		연계체계 보안성 유지	N2SF-LP-4	N2SF 모델 4번
			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	

No.	보안위험 발생지점	보안 요구사항	보안통제 항목	비고
			N2SF-EB-13	
			N2SF-DV-4	
			N2SF-DV-12	
			N2SF-IN-1(1)	
			N2SF-IN-5	
			N2SF-IN-6	
			N2SF-IN-11	
		연계체계 운용 관리	N2SF-LP-M1	N2SF 모델 4 번
			N2SF-LP-M2	
			N2SF-AC-1(2)	
			N2SF-AC-M1	
			N2SF-AC-M2	
			N2SF-AC-M3	
			N2SF-LI-M1	
			N2SF-LI-M2	
			N2SF-IS-6	
			N2SF-IF-M1	
			N2SF-IF-M2	
			N2SF-IF-M3	
			N2SF-IF-M4	
			N2SF-IF-M5	
			N2SF-EB-M3	
			N2SF-EB-M4	
			N2SF-EB-M5	
4	생성형 AI	생성형 AI 서비스 계정 관리	N2SF-EI-M1	N2SF 모델 2 번
		생성형 AI 서비스 활용 데이터 관리	N2SF-DU-M3	N2SF 모델 2 번

[6] 보안통제 구현계획

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 4번 「보안통제 구현계획표」는 아래와 같이 작성할 수 있다.

보안통제적용 정보서비스 구성도



(가) 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
1	N2SF-DA-1	단말	UEM으로 단말 고유정보를 수집해 PDP(ICAM)에 사전 등록	접속 시 인증 절차 강제, 미등록 단말 접근 차단	PDP (ICAM), UEM
2	N2SF-DA-2	단말	PDP 및 RBI로 화이트리스트 기반 사이트 접속 정책 적용	비허용 사이트 접속 차단, 정책 주기 점검	PDP (ICAM), RBI, DLP, MDM
3	N2SF-DV-12	단말	내PC지키미 등 단말 보안/관리 도구 적용	설정/상태 준수 여부 정기 점검	내PC지키미, PMS, VDI

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
4	N2SF-IN-5	단말	내PC 지키미 및 UEM으로 단말 구성 변경 탐지	위험도 측정 후 수준별 대응(차단/격리/조치) 적용	내PC지키미, PDP (ICAM), VDI
5	N2SF-IN-6	단말	UEM 및 내PC지키미로 불필요 설치 소프트웨어 관리	불필요/미승인 SW 식별 및 제거·차단 정책 운영	UEM, 내PC지키미, PMS, VDI
6	N2SF-IN-8	단말	내PC 지키미 등으로 비인가 SW 설치·실행 모니터링	비인가 행위 탐지 시 차단, 이력 확인	내PC지키미
7	N2SF-IN-10	단말	내PC 지키미로 SW 설치 통제 정책 적용	승인 없는 설치 제한, 설치 이력 점검	내PC지키미
8	N2SF-IN-16	단말	백신으로 악성코드 탐지·차단 적용	엔진/패턴 최신화, 탐지 로그 점검	백신, EDR
9	N2SF-SG-2	단말	물리적으로 분리된 PC 사용	분리 정책 준수(용도/접근 범위) 관리	RBI, 가상화 솔루션
10	N2SF-SG-3	단말	물리적 분리 PC 환경 운영	지정 용도 외 사용 제한, 운영 상태 점검	RBI, 가상화 솔루션
11	N2SF-IS-1	단말	물리적으로 분리된 PC 사용	지정된 분리 단말에서만 업무 수행	RBI, 가상화 솔루션
12	N2SF-CD-5	단말	물리적 분리 PC 사용	분리 환경 유지 점검, 예외 사용 제한	RBI, 가상화 솔루션

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
13	N2SF-IN-16	단말	기존 백신을 활용한 악성코드 탐지·차단	탐지 시 차단 및 로그 확인·대응	백신, EDR
14	N2SF-DV-6	단말	매체제어 솔루션 적용	비인가 저장매체 사용 차단, 사용 이력 기록·점검	매체제어 솔루션
15	N2SF-DV-8	단말	윈도우 화면 보호기 설정 적용	내PC 지키미 등으로 설정 여부 월 단위 점검	윈도우 화면 보호기, 내PC 지키미
16	N2SF-SG-6	단말	일반 사용자 단말과 특권 사용자 단말 분리	역할별 단말 운영, 혼용 사용 금지	PDP (ICAM)
17	N2SF-DV-4	단말	매체제어 및 PC 보안 솔루션으로 단말 보호	안전 부팅 유지, 악성코드 유입·정보유출 통제	매체제어 솔루션
18	N2SF-DV-12	단말	안전한 펌웨어 업데이트 절차 적용	코드사이닝 등 무결성·인증 검증 시에만 허용	내PC 지키미, PMS, VDI
19	N2SF-IN-1(1)	단말	PC 관리솔루션으로 자산 목록 관리	자산 변경 시 갱신, 정기 점검	ITAM, 내PC 지키미, VDI, PMS
20	N2SF-IN-5	단말	PDP(ICAM) 기반 단말 등록 관리	인가 절차·인증 통과 단말만 등록 유지	내PC 지키미, PDP (ICAM), VDI
21	N2SF-IN-6	단말	UEM 및 PC 관리솔루션 기반 단말 관리	정책 준수 정기 점검, 미준수 시 조치	UEM, 내PC 지키미, PMS, VDI

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
22	N2SF-IN-11	단말	안전한 재기동 프로세스 운영	재기동 시 검증 절차로 무결성·신뢰성 확인	보안정책 및 관리적 보안
23	N2SF-IS-6	단말	물리적 분리 PC 사용	분리 환경 외 접근 제한, 운영 기준 준수 점검	SDP, SIEM/ SOAR
24	N2SF-IM-1	단말	개인정보 포함 문자열을 계정 식별자로 사용하지 않도록 기준 수립	계정 생성·운영 시 식별자 기준 준수 여부 점검	PDP (ICAM)
25	N2SF-LP-1	연계체계	외부 AI 서비스를 Business 유료 계정 기반으로 1인 1계정 운영	계정 운영정책 수립 및 ICAM을 통한 접근권한 관리	PDP (ICAM)
26	N2SF-IN-1(1)	연계체계	PDP(ICAM)을 통해 단말·사용자·서버·애플리케이션 등록 관리	등록 정보 최신성 유지 및 정기 점검	PDP (ICAM)
27	N2SF-AM-2	연계체계	PDP(ICAM) 기반 사용자 기본 인증 체계 적용	인증 정책 준수 여부 점검 및 미인증 접근 차단	PDP (ICAM)
28	N2SF-AM-9	연계체계	PDP(ICAM) 기반 사용자 소유기반 MFA 인증 적용	MFA 적용 대상·방식 관리 및 예외 통제	PDP (ICAM)
29	N2SF-IF-9	연계체계	방화벽(FW)·NMS 및 PAM G/W–DLP 연동으로 연결 식별	사용자–AI 서비스 연결 시 인증·식별 로그 관리	SWG (유해사이트 차단), NAC
30	N2SF-SN-1	연계체계	ICAM 및 PAM G/W로 세션 재연결 시 인증 재수행	세션 종료 후 재인증 강제 및 이력 점검	PDP (ICAM), UEM, DLP, RBI, DRM 등

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
31	N2SF-WA-7	연계체계	무선망에 WIPS 적용	비인가 AP·단말 접속 탐지 및 차단	WIPS
32	N2SF-DT-1	연계체계	UEM·PDP(ICAM)·PAM G/W로 권한 보유 여부 확인	권한 미보유 시 접근 차단 및 로그 관리	PDP (ICAM), UEM, NAC
33	N2SF-LP-M1	연계체계	일반/특별권한 계정을 ICAM에서 분리 관리	특별권한 사용 이력을 PAM G/W로 추적	PDP (ICAM)
34	N2SF-AC-1	연계체계	PDP(ICAM)을 통한 계정 관리 자동화	계정 생성·변경·삭제 절차 자동화 운영	PDP (ICAM)
35	N2SF-AC-1(1)	연계체계	계정 생명주기 및 권한 변경 자동화	생명주기 이벤트별 정책 적용 및 점검	PDP (ICAM)
36	N2SF-AC-1(2)	연계체계	PDP(ICAM)으로 계정 상태 모니터링	임시 생성·수정·활성화 상태 상시 점검	PDP (ICAM)
37	N2SF-AC-1(3)	연계체계	PDP(ICAM)을 활용한 계정 상태 관리	계정 상태 이상 시 관리자 조치	PDP (ICAM)
38	N2SF-AC-1(4)	연계체계	비활동 계정에 대해 강제 로그아웃 적용	비활동 시간 기준 설정 및 세션 종료	PDP (ICAM), 내PC지키미
39	N2SF-AC-3(2)	연계체계	AI 서비스 계정은 유료계정 관리 기능 활용	내부 시스템 계정은 ICAM으로 모니터링	PDP (ICAM), UEM, DLP

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
40	N2SF-DA-3	연계체계	UEM으로 단말 고유정보를 PDP(ICAM)에 사전 등록	등록 단말만 접근 허용 및 인증 절차 적용	PDP (ICAM), UEM, NAC
41	N2SF-DA-4	연계체계	ICAM 기반 접근권한 관리 및 통제 적용	DLP 연계로 접근 이력 기록·감사	PDP (ICAM), DLP
42	N2SF-LI-4	연계체계	계정 잠금 해제 시 추가 MFA 인증 적용	AI 서비스는 유료계정 관리 기능 준수	PDP (ICAM)
43	N2SF-IF-14	연계체계	AI 서비스 전송 정보에 단어 기반 필터링 적용	사전 정의된 정책에 따라 전송 차단	DRM, CDS
44	N2SF-IF-5	연계체계	본 사업 범위 외 항목 적용 제외	C등급 정보 미사용 환경 유지	CDS
45	N2SF-LP-4	연계체계	계정 및 권한을 ICAM에서 시스템화 관리	권한 부여·변경 이력 관리	PDP (ICAM)
46	N2SF-LP-4(1)	연계체계	최소 권한 및 접근제어	사용자 신원, 기기상태, 위치등을 판단하여 접근허용	PDP (ICAM)
47	N2SF-LP-4(4)	연계체계	AI 서비스 계정은 유료계정 관리 기능 사용	내부 시스템은 ICAM으로 사용 이력 추적	PDP (ICAM), SIEM
48	N2SF-AC-1(5)	연계체계	ICAM 기반 계정 관리 체계 운영	계정 관리 절차 표준화 및 점검	PDP (ICAM)

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
49	N2SF-AC-3(1)	연계체계	단말 위험 탐지 시 AI 서비스 연결 차단	비정상 계정 탐지 시 차단·조사	PDP (ICAM), UEM, NAC
50	N2SF-LP-M1	연계체계	AI 사용 권한을 ICAM·PAM G/W로 제어	권한 승인·회수 절차 운영	보안정책 및 관리적 보안
51	N2SF-LP-M2	연계체계	사용자 권한 부여·사용 현황 모니터링	ICAM·PAM G/W·DLP 로그 점검	PDP (ICAM)
52	N2SF-AC-1(2)	연계체계	PDP(ICAM) 기반 계정 상태 모니터링	계정 변경 상태 상시 점검	PDP (ICAM)
53	N2SF-AC-M1	연계체계	UEM·PDP(ICAM)·PAM·RBI로 자동 감사	감사 정책 자동화 및 결과 확인	PDP (ICAM), UEM
54	N2SF-AC-M2	연계체계	UEM·PDP(ICAM)·DLP로 감사 기록 관리	감사 로그 생성·보관·추적	PDP (ICAM), UEM, DLP, SIEM
55	N2SF-AC-M3	연계체계	RBI 사용 이력 및 데이터 전송 통제	중요·개인정보 전송 차단 및 점검	PDP (ICAM), UEM, RBI
56	N2SF-LI-M1	연계체계	로그인 실패·의심 패턴 실시간 탐지	관리자 알림 및 대응 절차 운영	PDP (ICAM)
57	N2SF-LI-M2	연계체계	ICAM 계정 사용 이력 점검	설정 변경·사용 이력 주기 검토	PDP (ICAM)

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
58	N2SF-IF-M5	연계체계	DLP 오류·비정상 행위 탐지 기능 적용	탐지 시 알림 및 조치	DLP
59	N2SF-EB-M3	연계체계	AI DLP 외부 통신 로그 저장	로그 주기적 검증 및 감사	DLP
60	N2SF-EB-M4	연계체계	PDP 정책엔진으로 이상행위 탐지	필요 시 정책 기반 차단 조치	PDP (ICAM)
61	N2SF-EI-M1	연계체계	외부 인증수단 ICAM 연계 관리	인증 연동 현황 일괄 관리	PDP (ICAM), UEM, NAC
62	N2SF-SG-4	네트워크	방화벽(FW)을 통해 서버·DMZ·업무 PC 영역 분리	영역 간 트래픽을 정책 기반으로 통제	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
63	N2SF-SG-5	네트워크	방화벽(FW)을 통해 서버·DMZ·업무 PC 영역 분리	분리 정책 유지 및 변경 시 검토	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
64	N2SF-EB-6	네트워크	PAM G/W로 외부 연결을 화이트리스트 방식으로 허용	비인가 목적지로의 트래픽 차단	방화벽(FW), Web Filtering, EDR, SWG (유해사이트 차단
65	N2SF-BC-1	네트워크	매체제어 솔루션으로 블루투스 통신 차단	무선 인터페이스 사용 상태 점검	매체제어 솔루션

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
66	N2SF-EB-M1	네트워크	DLP를 사용해 개인정보 전송 통제	개인정보 전송 탐지 시 차단 및 로그 관리	DLP
67	N2SF-AC-3	네트워크	보안솔루션 및 PDP(ICAM) 기반 계정 모니터링	의심 계정 탐지 시 대응 절차 수행	PDP (ICAM), UEBA, EDR SIEM
68	N2SF-LI-1	네트워크	RBI 로그인 등 인증 채널 암호화 유지	인증정보 평문 노출 방지	PDP (ICAM), PKI, RBI
69	N2SF-IS-4	네트워크	방화벽(FW)·AIDLP·유해사이트 차단 설정 적용	내부 DNS에 AI 서비스 등록 관리	VLAN, 방화벽(FW), NAC 기반 업무망·인터넷망 분리
70	N2SF-IF-1	네트워크	메인/DMZ 방화벽(FW)으로 네트워크 흐름 통제	PAM G/W·AIDLP 기능 연계 운영	방화벽(FW), Network IPS, WAF, SWG, DLP, EDR
71	N2SF-EB-1	네트워크	RBI로 특정 대상 사이트 연결 접점 제한	외부 연결 경로 수 최소화	Web Filtering, RBI, DLP, 방화벽(FW), SWG
72	N2SF-EB-2	네트워크	AI 서비스는 RBI 경유 접속만 허용	유해사이트 차단 솔루션 병행 운영	방화벽(FW), Web Filtering, SWG (유해사이트 차단), RBI 솔루션 및 Proxy 서버, Gateway 네트워크 구성

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
73	N2SF-EB-3	네트워크	UEM·PDP(ICAM)·RBI 기반 접속 통제	화이트리스트 기반 외부 접속 제공	PDP (ICAM), UEM, Web Filtering, NAC, RBI, SWG (유해사이트 차단)
74	N2SF-EB-5	네트워크	통제 대상 외부 서비스는 RBI 경유 접속	직접 인터넷 접속 차단	PDP (ICAM), UEM, RBI
75	N2SF-EB-6	네트워크	RBI 기반 인가 URL 접속 허용	비인가 URL 차단 및 DLP 연계	방화벽(FW), Web Filtering, EDR, SWG (유해사이트 차단)
76	N2SF-EB-14	네트워크	방화벽(FW)으로 인가된 DNS 시스템만 허용	비인가 DNS 접근 차단	내PC지키미, 방화벽(FW), SWG (유해사이트 차단)
77	N2SF-EB-15	네트워크	우회 통신 탐지용 보안 장비 연계	VPN·우회 트래픽 탐지 및 차단	EDR, SWG (유해사이트 차단)
78	N2SF-IF-2	네트워크	SSL/TLS 프록시로 암호화 채널 통제	복호화 가시성 제공 DLP 적용	SSL/TLS Proxy, SSL 복호화 및 가시성
79	N2SF-IF-6	네트워크	네트워크 DLP로 정보 필터링	중요 정보 외부 유출 차단	DLP
80	N2SF-IF-7	네트워크	DLP 기반 비인가 전송 차단	정책 위반 트래픽 탐지·차단	CDS, DLP

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
81	N2SF-IF-8	네트워크	DLP로 인가되지 않은 정보 필터링	중요 정보 유출 방지	DLP, Web Filtering, DRM, 매체제어 솔루션
82	N2SF-IF-10	네트워크	허용 사이트·프로토콜만 사용하도록 통제	DLP로 정책 위반 트래픽 차단	방화벽(FW), Network IPS, WAF, DLP
83	N2SF-IF-3	네트워크	DLP를 사용한 정보 흐름 통제	데이터 이동 내역 점검	DLP, 문서중앙화 솔루션, EDR
84	N2SF-EB-8	네트워크	물리적 보안관리 및 매체제어 적용	관리 포트에 비인가 장치 차단	매체제어 솔루션
85	N2SF-EB-10	네트워크	방화벽(FW)으로 외부→내부 접근 차단	네트워크 접근 정책 유지	Routing, Subnet, 방화벽(FW) 정책
86	N2SF-EB-11	네트워크	네트워크 보안장비로 외부 위협 대응	대응 체계 지속 운영	Anti-DDoS, 방화벽(FW), Network IPS, WAF 이중화 구성
87	N2SF-EB-13	네트워크	오류정보 발송 시 DLP 탐지 적용	오류 정보 외부 유출 차단	DLP
88	N2SF-IF-M1	네트워크	정보흐름 통제 정책 수립	통제 기준·예외 절차 문서화·갱신	보안정책 및 관리적 보안
89	N2SF-IF-M2	네트워크	RBI·보안장비 로그 저장	감사·추적 가능하도록 보관	방화벽(FW), Network IPS, WAF, DLP, SWG,

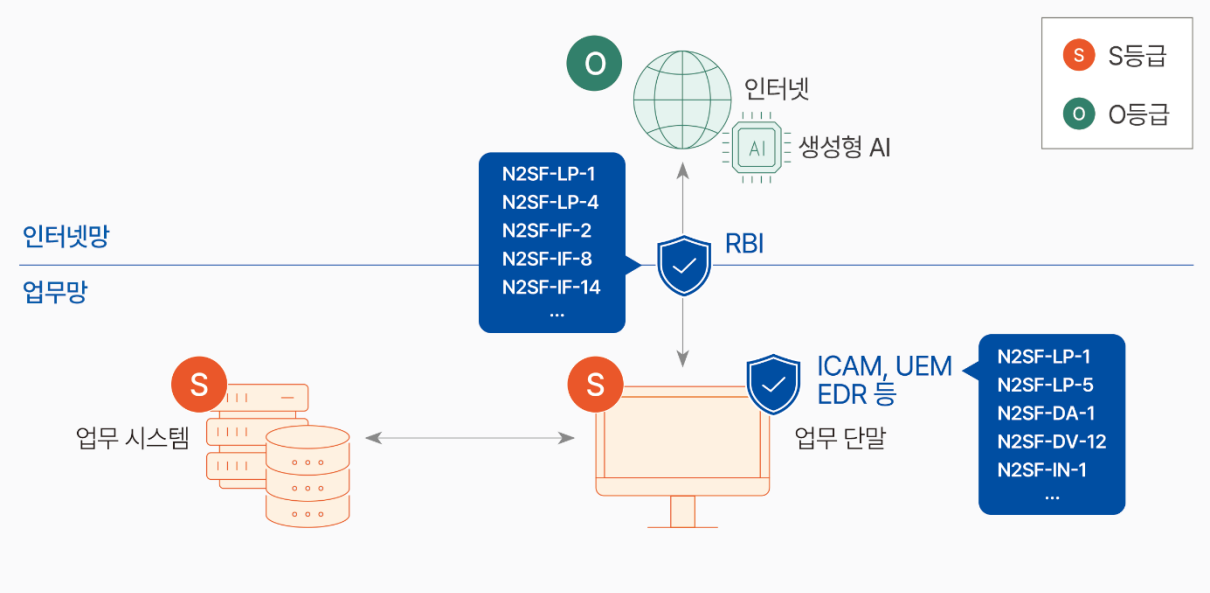
No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
					RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등
90	N2SF-IF-M3	네트워크	정보흐름 통제 적용 현황 점검	미준수 사항 식별 및 개선	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등
91	N2SF-IF-M4	네트워크	비정상 흐름 탐지 체계 적용	정책 우회 행위 탐지	DLP, NAC, SIEM
92	N2SF-EB-M5	네트워크	네트워크 방화벽(FW) 기반 대응	침해 시 외부 통신 즉시 차단	방화벽(FW)
93	N2SF-DU-2	시스템	중요·개인정보 암호화 저장	저장 데이터 암호화 상태 관리	DB 암호화, DRM
94	N2SF-DU-M3	관리	데이터 취급 정책 문서화	정책 시행 및 준수 여부 점검	보안정책 및 관리적 보안
95	N2SF-LI-2	관리	로그인 실패 횟수 제한 정책 적용	AI 서비스는 유료계정 정책 준수	PDP (ICAM)

(나) 자체정의 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	비고

1	N2SF-ORG2-1	단말	단말에서 생성·처리되는 업무정보의 등급이 변경될 수 있는 조건과 기준을 정의한 정보 등급 변화 정책을 수립	정보 등급 변화 정책을 문서화하여 운영 기준으로 적용하고, 관련 담당자가 정책을 준수하도록 관리	가이드라인 개선 방향
2	N2SF-ORG2-2	단말	단말에서 처리되는 업무정보의 등급 변경 이력을 기록·관리할 수 있는 관리 절차를 적용	정보 등급 변경 시 변경 전·후 등급과 변경 사유를 기록하고, 이력을 주기적으로 점검·관리	가이드라인 개선 방향

4.3 정보서비스 적용 기관 망 구성도 예시



수립한 보안 요구사항 및 보안통제 항목 구현 사항 등 산출물을 토대로 국가정보원 보안성 검토 신청 시, N2SF를 적용한 기관의 실제 망 구성도를 작성하여 첨부하여야 한다.

5. [모델 5] 공공데이터의 외부 AI 융합

본 정보서비스 모델은 국가·공공 클라우드와 AI 서비스의 융합을 통해 AI 모델 경량화, 파인튜닝, 오토 브라우징, 검색 증강 생성(RAG) 등을 수행하기 위한 보안 요구사항 및 대책을 제시한다.

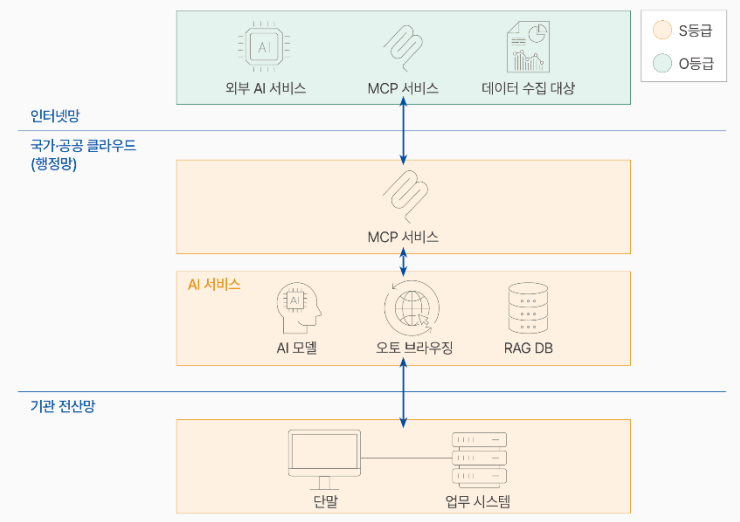
※ (참고자료) N2SF 보안 가이드라인 1.0 - (부록2) 모델5 공공데이터의 외부 AI 융합

본 실증 사례는 공공데이터와 외부 AI를 안전하게 연동하기 위해 1개의 정보서비스 모델을 활용한다. 국가·공공 클라우드 기반 AI 서비스를 바탕으로 구현된 모델이며, 업무정보 보안 등급에 따라 안전한 정보 연계를 구현하는 데 중점을 둔다. 특히 행정망에서 동작하는 AI 서비스와 외부 AI 서비스의 연동을 가정하여 별도 실증 시나리오(MCP(Model Context Protocol) 서비스 등)를 구성하여 보안 유효성을 검증한다.

각 기관에서는 국가·공공 클라우드 기반 AI 서비스 또는 유사 환경에서 외부 인터넷 자원(AI 서비스 등)을 안전하게 결합하고자 할 때 참고할 수 있다.

5.1 정보서비스 유형 요약

정보서비스 유형 / 모델 No.5 (N2SF 가이드라인 기준)		모델 5 / 공공 데이터의 외부 AI 융합
정보서비스 개요	업무정보	① 데이터 수집 로그 ② 데이터(학습 및 서비스 제공용) ③ 망중계 로그 ④ AI 플랫폼 운영 및 관리 로그 ⑤ MCP 서비스 운영 및 관리 로그 ⑥ 행정망 AI 서비스 보안 시스템 로그 ⑦ 행정망 AI 서비스 운영 및 관리시스템 로그
	정보시스템	① 업무 단말 ② 업무 시스템 ③ 행정망 AI 서비스 ④ 행정망 MCP 서비스 ⑤ 외부 AI/MCP 서비스(인터넷망)
	정보서비스 사용 시나리오	① 데이터 수집(학습 및 서비스 제공) ② 행정망 AI/MCP 서비스가 외부 AI/MCP 서비스 활용
위치/주체/객체 관점의 정보서비스 구조		



- AI 서비스는 기관 전산망(S 등급)으로부터 AI 서비스 요청을 받고, 필요 시 인터넷망 AI/MCP 서비스 이용
- 기관 전산망(S 등급)에서 사전 허용된 업무단말(S 등급), 업무시스템(S 등급)이 국가·공공 클라우드(S 등급) AI 서비스(S 등급)를 이용하며, AI 서비스에서 식별, 인증 및 권한을 확인함
- 위치: 국가·공공 클라우드(S 등급), 주체: AI 서비스(S 등급), 객체: AI/MCP 서비스(O 등급)

보안통제 대상	① 업무 시스템 ② 행정망 AI 서비스 ③ 행정망 MCP 서비스 연계체계 ④ 외부 AI/MCP 서비스 연계체계

5.2 최종산출물 서식

[1] 정보서비스 사용 시나리오별 정보시스템 식별

정보서비스 사용 시나리오별 정보시스템 식별

번호	사용 시나리오	관련 정보시스템
1	업무 시스템이 행정망 AI 서비스 이용	㉠ 업무 시스템 ㉯ 행정망 AI 서비스
2	행정망에서 학습 및 서비스 제공 목적 데이터 수집	
2-1	행정망에서 각 기관 인터넷 공개정보를 수집	㉠ 행정망 AI 서비스 ㉰ 각 기관 외부 인터넷 공개 데이터베이스
2-2	행정망에서 각 기관 행정망 공개정보를 수집	㉠ 행정망 AI 서비스 ㉰ 각 기관 업무망 공개 데이터베이스
2-3	행정망에서 AI 서비스 피드백 데이터를 수집	㉠ 행정망 AI 서비스 ㉯ 행정망 AI 서비스
3	행정망에서 외부 AI/MCP 서비스와 연계	
3-1	행정망에서 외부 AI 서비스와 연계	㉠ 행정망 AI 서비스 ㉱ 외부 인터넷 AI 서비스
3-2	행정망 MCP 서비스가 외부 AI/MCP 서비스와 연계	㉠㉡ 행정망 MCP 서비스 ㉱ 외부 인터넷 AI/MCP 서비스

[2] 정보서비스 보안목표

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 1번 「정보서비스 보안목표」는 아래와 같이 정리됨

No.	영역	보안 목표	비고
1	공통	정보서비스 모델 5. 공공 데이터의 외부 AI 융합	N2SF 가이드라인 1.0
2	네트워크	특정 외부 AI/MCP 서비스, 데이터 수집 대상으로 접속 제한	자체
3		네트워크 분리 및 비인가 연결 차단	자체
4		정보 유출 방지 및 외부로부터의 위협 유입 방지	자체

[3] C/S/O 등급분류

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 2번 「C/S/O 등급 분류표」는 아래와 같이 정리됨

No.	정보시스템		업무정보	
	명칭	C/S/O 등급	명칭	C/S/O 등급
1	행정망 AI 서비스	S	데이터 수집 로그	S
			수집 데이터 (학습 및 서비스 제공)	S
			망중계 로그	S
			AI 서비스 운영 및 관리 로그	S
			AI 서비스 보안 시스템 로그	S
			AI 서비스 운영 및 관리시스템 로그	S
2	행정망 MCP 서비스	S	MCP 서비스 운영 및 관리 로그	S

[4] 위협 식별 - 모델링 및 C/S/O 평가

기관의 정보서비스 구성요소에 따라 유스케이스별로 모델링 및 C/S/O 보안등급을 나누어 평가하며, 「정보 생산·저장」 보안원칙과 「정보 이동」 보안원칙을 적용하여 보안대책의 필요성을 평가한다.

N2SF 보안 가이드라인*에서 본 정보서비스는 **기관 전산망 영역(위치, S등급)**에 위치하는 **업무시스템(주체, S등급)**과 국가·공공 클라우드에 위치한 **행정망 AI 서비스(객체, S등급)**의 구성, **국가·공공 클라우드(위치, S등급)**에 위치한 **행정망 AI 서비스(주체, S등급)**, 인터넷망 영역에 위치하는 **외부 AI 서비스(객체, O등급) 및 MCP 서비스(객체, O등급)**로 구성되며, S등급 업무시스템, 행정망 AI 서비스에서만 S등급 업무정보가 생산·저장(활용), 이동하고, O등급의 외부 AI 서비스 및 MCP 서비스에서 S등급 업무정보가 생산·저장(활용), 이동하지 않도록 보안 원칙을 제시하고 있다. 아래 제시하는 실증 사례 및 N2SF 보안 가이드라인에 대하여 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 유연하게 참고하여 보안원칙을 수립하여야 한다.

* N2SF 보안 가이드라인 1.0 - (부록2) 모델5 공공 데이터의 외부 AI 융합

사례 1: 기관 전산망 내 업무 시스템에서 행정망 AI 서비스를 활용하는 경우

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C등급 / S등급 / O등급 위치 Domain / / 기관 전산망 / 주체 Subject / / 업무 시스템 / 객체 Object / / 행정망 AI 서비스 / 기관 전산망(S 등급)에 위치한 업무 시스템(S 등급)이 행정망 AI 서비스(S 등급) 활용 - 유스케이스 2-2: 행정망에서 각 기관 전산망 공개정보를 수집 - 유스케이스 2-3 은 행정망 내에서 AI 서비스 피드백 데이터를 수집하는 경우로 생략	아니오
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C정보 / 업무 정보 / 업무 정보 C 시스템 / ● / ● / ● 업무시스템 행정망 AI서비스 / + / ● / ● O시스템 / + / + / ● 업무 시스템(S 등급)이 행정망 AI 서비스(S 등급)를 이용해 S 등급 이하의 업무정보를 생산·저장하는 것은 보안원칙에 위배되지 않음	아니오
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / 업무 시스템 행정망 AI 서비스 / O 시스템 C 정보 / ● / + / + 업무정보 / ● / ● / + O정보 / ● / ● / ● 업무 시스템(S 등급) 내 S 등급 이하의 업무정보가 행정망 AI 서비스(S 등급)로 이동하는 것은 보안원칙에 위배되지 않음. 업무 시스템(S 등급) 내 S 등급 이하의 업무정보가 행정망 AI 서비스(S 등급) 외 활용 및 업무 시스템의 비인가 연결을 차단하도록 보안 통제 필요	아니오

사례2: 행정망 AI 서비스에서 인터넷망의 외부 AI 서비스, MCP서비스, 각 기관 공개 데이터베이스를 활용하는 경우

<table>
<tr><th>구분</th><th>결과 및 설명</th><th>보안대책
필요여부</th></tr>
<tr><td>「위치-주체-객체」
모델 C/S/O
평가</td><td>
<table>
<tr><th>구분</th><th>C 등급</th><th>S 등급</th><th>O 등급</th></tr>
<tr><td>위치
Domain</td><td></td><td>국가·공공
클라우드(행정망)</td><td></td></tr>
<tr><td>주체
Subject</td><td></td><td>행정망 AI/MCP
서비스</td><td></td></tr>
<tr><td>객체
Object</td><td></td><td></td><td>외부 AI/MCP 서비스,
각 기관 공개 데이터 베이스</td></tr>
</table>
국가·공공 클라우드(행정망)의 AI 서비스(S 등급), MCP 서비스(S 등급)가 외부 인터넷망의 외부 AI/MCP 서비스 및 각 기관 공개 데이터베이스(O 등급)를 활용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안대책 필요
- 유스케이스 2-1: 행정망에서 각 기관 인터넷 공개정보를 수집
- 유스케이스 3-1: 행정망 AI 서비스에서 외부 AI 서비스와 연계
- 유스케이스 3-2: 행정망 AI 서비스의 MCP 서비스가 외부 AI/MCP 서비스와 연계
</td><td>예</td></tr>
<tr><td>「정보 생산·저장」
보안원칙</td><td>
<table>
<tr><th>~에서 생산·저장</th><th>C 정보</th><th>S 정보</th><th>업무 정보</th></tr>
<tr><td>C 시스템</td><td>●</td><td>●</td><td>●</td></tr>
<tr><td>행정망 AI/MCP 서비스</td><td>+</td><td>●</td><td>●</td></tr>
<tr><td>외부 AI/MCP 서비스,
각 기관 공개 데이터 베이스</td><td>+</td><td>+ ⃠</td><td>●</td></tr>
</table>
행정망 AI/MCP 서비스(S 등급)는 S 등급 이하인 업무정보만을 생산 및 저장할 수 있으므로 외부 AI/MCP 서비스, 공개 데이터베이스(O 등급)를 포함해 행정망 AI/MCP 서비스 내 존재하는 S 등급 이하 업무정보를 다룰 수 있음.

외부 AI/MCP 서비스, 공개 데이터베이스(O 등급)에 행정망 AI/MCP 서비스의 업무정보를 업로드하지 않고 단순 질의/요청하는 경우, O 등급인 업무정보만을 생산 및 저장할 수 있으므로 외부 AI/MCP 서비스, 공개 데이터베이스 수집자료(O 등급)를 다룰 수 있음. 따라서 보안원칙에 위배되지 않아 보안대책 불필요

외부 AI/MCP 서비스, 공개 데이터베이스(O 등급)에 업무정보(S 등급)를 포함하여 질의/요청하는 경우, 외부 AI/MCP 서비스, 공개 데이터베이스(O 등급)는 O 등급인 업무정보만을 생산 및 저장할 수 있으므로 보안원칙에 위배됨. 따라서 외부 AI/MCP 서비스, 공개 데이터베이스 내 S 등급 업무정보를 생산 및 저장하지 않도록 연계 구간에 적절한 보안대책 필요.
</td><td>예</td></tr>
</table>

<table>
<tr><th>구분</th><th>결과 및 설명</th><th>보안대책
필요여부</th></tr>
<tr><td>「정보 이동」
보안원칙</td><td>
<table>
<tr><th>~정보가 ~로 이동</th><th>C 시스템</th><th>행정망 AI/MCP 서비스</th><th>외부 AI/MCP 서비스, 각기관공개데이터베이스</th></tr>
<tr><td>C 정보</td><td>●</td><td>+</td><td>+</td></tr>
<tr><td>업무정보</td><td>●</td><td>●</td><td>+ ⃠</td></tr>
<tr><td>O 정보</td><td>●</td><td>●</td><td>●</td></tr>
</table>
행정망 AI/MCP 서비스(S 등급)가 외부 AI/MCP 서비스, 공개 데이터베이스(O 등급)에 접속하는 경우, 단순 질의와 같은 O 등급 업무정보 만을 주고받을 수 있음. 따라서 S 등급의 업무정보를 포함하지 않고 단순 질의/요청하게 되는 경우 보안원칙에 위배되지 않아 보안대책 불필요

행정망 AI/MCP 서비스(S 등급)가 외부 AI/MCP 서비스, 공개 데이터베이스(O 등급)에 접속하는 경우, 단순 질의/요청과 같은 O 등급 업무정보만을 주고받을 수 있으며, 그 외 행정망 AI/MCP 서비스 내 존재하는 S 등급 업무정보를 주고받는 경우 보안원칙에 위배됨. 따라서 외부 AI/MCP 서비스, 공개 데이터베이스로 S 등급 업무정보를 이동하지 않도록 연계 구간에 적절한 보안대책 필요.

행정망 AI 서비스, MCP 서비스내 업무정보의 외부 AI, MCP 서비스 외 활용, 이용자 단말의 비인가 연결을 차단하도록 보안통제 필요</td><td>예</td></tr>
</table>

[5] 보안요구사항 및 보안통제

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 3번 「보안 요구사항 및 보안통제」는 아래와 같이 작성할 수 있다.

※ 보안 가이드라인에 없는 신규 자체정의 보안통제 항목: N2SF-AIP

No.	구성요소	보안 요구사항	보안통제 항목
1	업무 시스템	업무 시스템 보안성 유지	N2SF-LP-1
			N2SF-LP-5
			N2SF-DA-1
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5

No.	구성요소	보안 요구사항	보안통제 항목
			N2SF-IN-6
			N2SF-IN-8
			N2SF-IN-16
		업무 시스템 사용 보안	N2SF-DA-3(1)
			N2SF-AM-2
			N2SF-AM-9
			N2SF-DV-6
		업무 시스템 네트워크 보안	N2SF-DT-1
			N2SF-EB-6
			N2SF-IF-9
			N2SF-SG-4
			N2SF-SG-5
			N2SF-WA-7
		업무 시스템 데이터 보호	N2SF-DU-2
		행정망 AI 활용을 사전에 승인받은 지정 업무 시스템	N2SF-EB-1
			N2SF-EB-7
			N2SF-DA-2
2	행정망 MCP 서비스 연계체계	연계체계 접속 업무 시스템 인증 및 비인가 네트워크 연결 차단	N2SF-DA-3
			N2SF-IF-9
			N2SF-IF-M2
			N2SF-EB-3
			N2SF-DA-4
			N2SF-IS-4
			N2SF-SG-M1
			N2SF-SG-M4
			N2SF-SG-4
		행정망 연계체계 전용선 수준 연결	N2SF-CD-1

No.	구성요소	보안 요구사항	보안통제 항목
			N2SF-IF-10
			N2SF-IF-15
		행정망 연계체계 활용 시 데이터 보호	N2SF-IF-2
			N2SF-IF-6
			N2SF-IF-7
			N2SF-IF-8
			N2SF-IF-10
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3
			N2SF-IF-5
			N2SF-IF-8
		콘텐츠 유형 분류 및 필터링을 통한 유출방지	N2SF-CD-5
		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-DV-12
			N2SF-EB-10
			N2SF-EB-11
			N2SF-EB-13
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-11
		연계체계 운용 관리	N2SF-AC-M1
			N2SF-AC-M2

No.	구성요소	보안 요구사항	보안통제 항목
			N2SF-AC-M3
			N2SF-EB-M3
			N2SF-EB-M4
			N2SF-EB-M5
			N2SF-IF-M2
			N2SF-IF-M3
			N2SF-IF-M4
			N2SF-IF-M5
			N2SF-IS-2
			N2SF-SG-M2
			N2SF-SG-M3
			N2SF-SG-M4
			N2SF-SG-M5
			N2SF-LI-M1
			N2SF-LI-M2
			N2SF-LP-M1
			N2SF-LP-M2
3	행정망 AI 서비스	행정망 AI 인증 관리	N2SF-AC-3
			N2SF-DA-3
			N2SF-LI-1
			N2SF-SN-M1
			N2SF-SN-M2
		행정망 AI 데이터 관리	N2SF-IF-5
			N2SF-DT-1
			N2SF-DT-2
			N2SF-DU-M1
		행정망 AI	N2SF-AIP-01

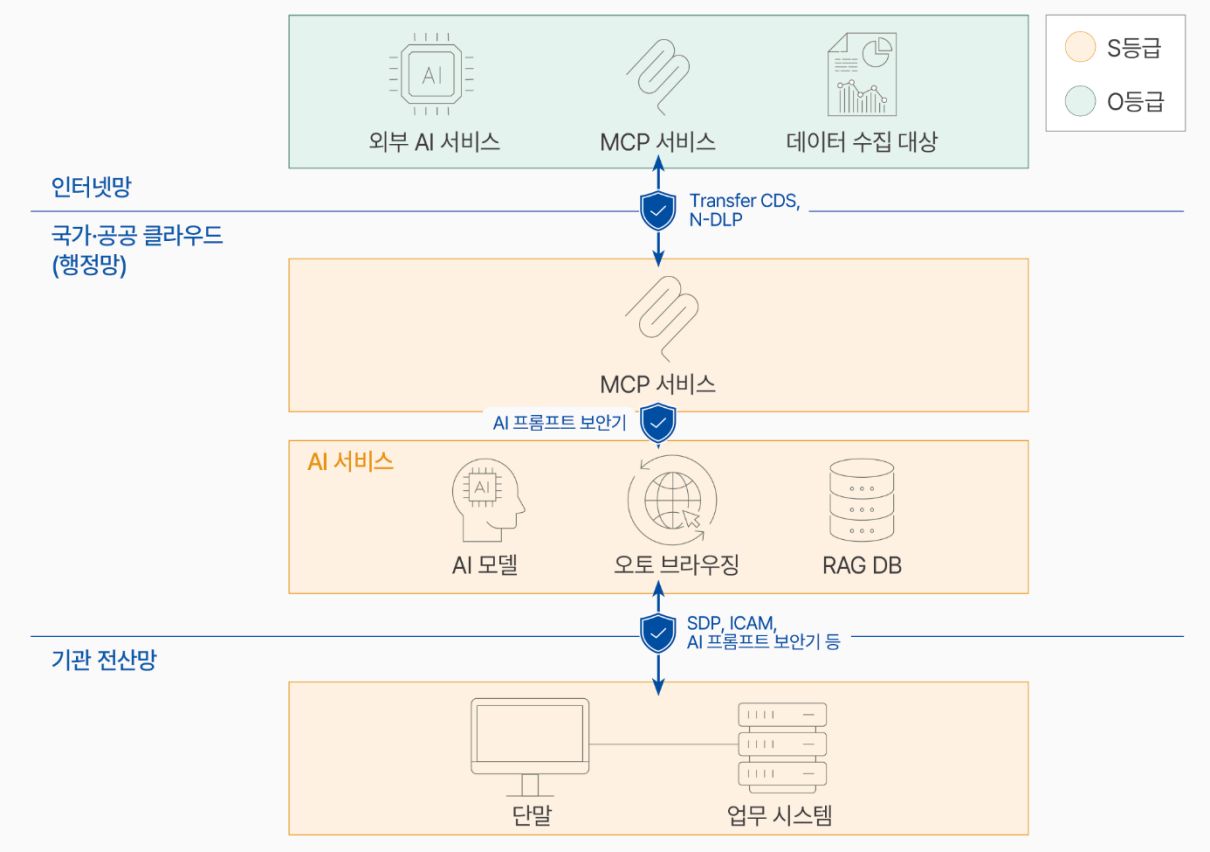
No.	구성요소	보안 요구사항	보안통제 항목
		서비스 사용 보안	
4	외부 AI/MCP 서비스 연계체계	비인가 네트워크 연결 차단	N2SF-IS-4
			N2SF-SG-4
			N2SF-IF-1
			N2SF-EB-1
			N2SF-EB-2
			N2SF-EB-3
			N2SF-EB-5
			N2SF-EB-6
			N2SF-EB-14
			N2SF-EB-15
		인터넷 서비스 활용 시 데이터 보호	N2SF-IF-2
			N2SF-IF-6
			N2SF-IF-7
			N2SF-IF-8
			N2SF-IF-10
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3
			N2SF-IF-5
		연계체계 보안성 유지	N2SF-LP-4
			N2SF-LP-4(1)
			N2SF-LP-4(4)
			N2SF-AC-1(5)
			N2SF-AC-3(1)
			N2SF-EB-10
			N2SF-EB-11
			N2SF-EB-13
			N2SF-DV-12

No.	구성요소	보안 요구사항	보안통제 항목
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-11
			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-6
			N2SF-SG-M2
		연계체계 운용 관리	N2SF-SG-M3
			N2SF-SG-M4
			N2SF-SG-M5
			N2SF-IF-M1
			N2SF-IF-M2
			N2SF-IF-M3
			N2SF-IF-M4
			N2SF-IF-M5
			N2SF-EB-M3
			N2SF-EB-M4
			N2SF-EB-M5

[6] 보안통제 구현계획

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 4번 「보안통제 구현계획표」는 아래와 같이 작성할 수 있다.

보안통제적용 정보서비스 구성도



(가) 보안통제 구현계획

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
1	N2SF-LP-1	업무 시스템	접근통제 시스템에 등록된 권한에 따른 접근 권한 부여	권한 부여·변경·회수 이력을 기록·보관하고 정기적으로 점검	ICAM, 관리자 시스템, 시스템접근통제, DB 접근통제
2	N2SF-LP-5	업무 시스템	접근통제 시스템에 등록된 권한에 따른 코드 실행 제한	코드 실행 권한은 승인된 계정에 한해 부여하고 실행 이력을 기록·감사	PAM, 서버보안, 시스템접근통제, DB 접근통제

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
3	N2SF-DA-1	업무 시스템	고유정보를 이용하여 PDP(ICAM)에 사전등록하고 접속 시 인증절차 이행	사전 등록된 시스템만 인증을 허용하고 미등록 시스템 접근은 차단	ICAM
4	N2SF-DV-12	업무 시스템	업무 시스템 보안/관리 솔루션을 통한 장치 펌웨어 업데이트 시 검증	승인·검증된 펌웨어만 적용하고 업데이트 이력을 기록·점검	서버보안, 서버백신, 클라우드 기능
5	N2SF-IN-1(1)	업무 시스템	업무 시스템 보안/관리 솔루션을 통한 정보시스템 구성요소 최신상태 확인	구성요소 최신 상태를 주기적으로 점검하고 미적용 항목은 보완 조치	서버보안, 서버백신, 클라우드 기능
6	N2SF-IN-5	업무 시스템	업무 시스템 보안/관리 솔루션을 통해 구성 변경을 탐지하고 대응방안 적용	인가되지 않은 설정 변경을 탐지하고 변경 발생 시 복구·조치 수행	서버보안, 서버백신, 클라우드 기능
7	N2SF-IN-6	업무 시스템	업무 시스템 보안/관리 솔루션을 통해 불필요 소프트웨어 등을 관리	불필요 소프트웨어 식별 후 제거·비활성화하고 예외 항목을 관리	서버보안, 서버백신, 클라우드 기능
8	N2SF-IN-8	업무 시스템	업무 시스템 보안/관리 솔루션을 통해 비인가 소프트웨어 설치·실행 모니터링 및 관리	비인가 소프트웨어 설치·실행 탐지 시 차단하고 관련 로그를 기록	서버보안, 서버백신, 클라우드 기능
9	N2SF-IN-16	업무 시스템	업무 시스템 Anti-Virus SW를 사용하여 악성코드 탐지 및 차단 시행	악성코드 탐지 시 격리·치료를 수행하고 탐지 이력을 점검	서버백신
10	N2SF-DA-3(1)	업무 시스템	인증서 등을 이용한 인증 수행	인증서 유효성 검증 및 만료 상태를 점검하고 인증 이력을 보관	인증서 관리
11	N2SF-AM-2	업무 시스템	PDP(ICAM) 기반으로 기본 인증 수행	기본 인증 정책을 중앙에서 관리하고 인증 실패 시 접근 차단	ICAM

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
12	N2SF-AM-9	업무 시스템	PDP(ICAM) 기반으로 소유 기반 MFA 인증 수행	MFA 적용 대상·방식을 관리하고 예외 승인 절차를 운영	ICAM
13	N2SF-DV-6	업무 시스템	관리통제 실행	승인되지 않은 장치 사용을 차단하고 사용 이력을 기록·점검	매체제어 솔루션
14	N2SF-DT-1	업무 시스템	데이터 전송 전 업무 시스템의 인증 및 권한을 PDP (ICAM) 전용 API 를 호출하여 확인하고 전송	전송 시 인증·권한 검증 결과를 확인하고 미인가 전송을 차단	ICAM
15	N2SF-EB-6	업무 시스템	네트워크패턴 분석을 통한 이상행위 모니터링	이상 네트워크 패턴 탐지 시 경고·차단하고 이벤트 로그를 분석	방화벽(FW), IPS, WAF 등 네트워크 보안장비
16	N2SF-IF-9	업무 시스템	방화벽(FW) 등을 이용한 출발지, 목적지 식별 및 관리	출발지·목적지 식별 정책을 유지하고 비인가 흐름을 차단·기록	방화벽(FW), IPS, WAF 등 네트워크 보안장비
17	N2SF-SG-4	업무 시스템	방화벽(FW) 등을 이용한 서브 네트워크 별도 구성 및 운영	서브 네트워크 분리 정책을 유지하고 구간 간 접근을 통제	방화벽(FW), 라우팅, GW, 클라우드 기능
18	N2SF-SG-5	업무 시스템	방화벽(FW) 등을 이용한 보안•운영관리 업무 시스템 분리	보안·운영관리 구간 분리 정책을 적용하고 예외 접근 이력을 관리	방화벽(FW), 라우팅, GW, 클라우드 기능
19	N2SF-WA-7	업무 시스템	비인가 무선망 접속 차단	비인가 무선 접속 탐지 시 차단하고 접속 시도를 기록·점검	WIPS
20	N2SF-DU-2	업무 시스템	데이터 암호화	저장 데이터 암호화를 강제하고 암호화 상태 및 키 관리를 점검	데이터 암호화 솔루션(FED/EDR)

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
21	N2SF-EB-1	업무 시스템	업무 시스템의 외부 네트워크 연결 접점(예: 포트, 인터페이스) 수를 최소화하고, 불필요하거나 사용하지 않는 접점은 비활성화	외부 접점 최소화 정책을 유지하고 미사용 포트·인터페이스를 비활성화	방화벽(FW), 라우팅, GW, 클라우드 기능
22	N2SF-EB-7	업무 시스템	업무 시스템에 호스트 기반 방화벽(FW), IDS/IPS, EDR 에이전트 등 적용	호스트 보안 에이전트 동작 상태를 점검하고 위협 탐지 시 차단	서버보안, 서버백신
23	N2SF-DA-2	업무 시스템	지정된 업무 시스템이 승인된 서비스를 이용하도록 접근 시마다 통제를 수행해 접점 제한	승인된 서비스만 이용 가능하도록 통제하고 비인가 접점은 차단	SDP, ICAM
24	N2SF-DA-3	네트워크	고유정보를 이용하여 PDP(ICAM)에 사전등록하고 접속 시 인증절차 이행	사전 등록된 자산만 네트워크 접근을 허용하고 인증 실패 시 차단	ICAM
25	N2SF-IF-9	네트워크	방화벽(FW) 등을 이용한 출발지, 목적지 식별 및 관리	출발지·목적지 기반 흐름 식별 정책을 적용하고 비인가 통신을 차단	방화벽(FW), IPS, WAF 등 네트워크 보안장비
26	N2SF-IF-M2	네트워크	방화벽(FW), IPS 등의 로그 기록 및 보존	로그를 중앙 저장하고 무결성·보관기간을 관리하여 감사 가능 상태 유지	방화벽(FW), IPS, WAF 등 네트워크 보안장비
27	N2SF-EB-3	네트워크	방화벽(FW)의 모든 차단 실행 후 허용 정책 추가, 주기적 관리	기본 차단 정책을 유지하고 허용 정책은 승인 후 반영하며 정기 검토	방화벽(FW), WAF
28	N2SF-DA-4	네트워크	업무 시스템 정보를 PDP (ICAM)에 등록하여 권한을 설정, 통제 적용하고 접근통제 솔루션 등을 활용해 접근 이력 기록, 감사	접근 이력을 기록·보관하고 권한 변경 내역을 정기적으로 감사	ICAM
29	N2SF-IS-4	네트워크	네트워크간 방화벽(FW) 이용한 트래픽 분리	네트워크 간 트래픽 분리 정책을 유지하고 비인가 구간 통신을 차단	방화벽(FW), 클라우드 기능

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
30	N2SF-SG-M1	네트워크	자산 분리 기준 정책 수립 및 클라우드 내 VM 구성으로 이행	자산 분리 기준을 문서화하고 VM 구성의 분리 상태를 정기 점검	클라우드 기능
31	N2SF-SG-M4	네트워크	업무 시스템 정보를 PDP (ICAM)에 등록하여 권한을 설정, 통제 적용하고 접근통제 솔루션 등을 활용해 접근 권한 관리 및 모니터링	등록 자산의 권한·접근 현황을 모니터링하고 이상 접근을 차단	ICAM, 시스템접근통제, DB 접근통제
32	N2SF-SG-4	네트워크	방화벽(FW) 등을 이용한 시스템/네트워크 IP 체계 분리	시스템·네트워크 IP 분리 정책을 유지하고 충돌·우회 여부를 점검	방화벽(FW), GW, 클라우드 기능
33	N2SF-IF-10	네트워크	허용된 방식만 사용하도록 통제	허용된 전송 방식만 사용하도록 제한하고 위반 시 차단·기록	PAM, 데이터 수집 솔루션
34	N2SF-CD-1	네트워크	지정된 방식을 사용하도록 통제	지정된 연계 방식만 허용하고 비인가 방식 사용 시 차단·로그 관리	데이터 수집 솔루션
35	N2SF-IF-15	네트워크	방화벽(FW) 등을 이용해 정보흐름을 통제하고, SDP mTLS 적용	mTLS 적용 상태와 방화벽(FW) 정책을 점검하고 비인가 흐름을 차단	방화벽(FW), SDP
36	N2SF-IF-2	AI 서비스	암호화 채널의 정보흐름 통제	암호화 채널만 허용하고 평문 통신은 차단	SSL
37	N2SF-IF-6	AI 서비스	정보흐름 통제	정보흐름 필터링 기준을 적용하고 위반 데이터 전송을 차단	필터링, 가드레일
38	N2SF-IF-7	AI 서비스	데이터 전송 통제	데이터 전송 정책 위반 시 차단하고 전송 이력을 기록	필터링, 가드레일
39	N2SF-IF-8	AI 서비스	비인가 정보흐름 통제	비인가 정보흐름 탐지 시 차단하고 민감정보 여부를 점검	필터링, 가드레일

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
40	N2SF-IF-10	AI 서비스	정보 전송 방식 제한	허용된 전송 방식만 사용하도록 제한하고 비허용 방식은 차단	HTTPS
41	N2SF-IF-3	AI 서비스	데이터 유입 시 악성코드 검사 실행	업로드 데이터에 대한 악성코드 검사 수행 후 이상 파일을 차단	Anti-Virus, 필터링
42	N2SF-IF-5	AI 서비스	데이터 유입 시 일방향 정보흐름 통제	일방향 정보흐름 정책을 적용하고 역방향 전송은 차단	망중계
43	N2SF-IF-8	AI 서비스	악성 콘텐츠 유입 차단	악성 콘텐츠 탐지 시 차단하고 탐지 이력을 점검	필터링, 가드레일
44	N2SF-CD-5	AI 서비스	파일 업로드 시 파일 유형 점검	허용된 파일 유형만 업로드 가능하도록 제한하고 예외 업로드를 차단	시큐어코딩 개발
45	N2SF-LP-1	행정망 (AI 서비스)	PDP (ICAM)에 등록하여 권한을 설정, 통제 적용하고 접근통제 솔루션 등을 활용해 권한에 따른 접근 권한 부여	권한별 접근 기준을 적용하고 권한 부여·변경 이력을 기록·점검	ICAM 관리자 시스템, 시스템접근통제, DB 접근통제
46	N2SF-LP-4	행정망 (AI 서비스)	PDP (ICAM)에 등록하여 권한을 설정, 통제 적용하고 접근통제 솔루션 등을 활용해 최소 인원에게 관리자 권한 부여	관리자 권한을 최소 인원에게만 부여하고 승인 이력을 관리	ICAM, 관리자 시스템, 시스템접근통제, DB 접근통제
47	N2SF-LP-4(1)	행정망 (AI 서비스)	원격접속을 통한 관리자 접속을 허용하지 않음	원격 관리자 접속 금지 정책을 유지하고 예외 허용 여부를 점검	-
48	N2SF-LP-4(4)	행정망 (AI 서비스)	PDF (ICAM), 접근통제 솔루션 등에서 관리자 권한 실행 내역을 로깅하고 주기적으로 검토	관리자 권한 실행 내역을 로깅하고 정기적으로 검토·감사	ICAM, 관리자 시스템, 시스템접근통제, DB 접근통제

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
49	N2SF-AC-1(5)	행정망 (AI 서비스)	ICAM, 접근통제 솔루션 등에서 유휴 계정 정리, 접근 제어	유휴 계정을 정기 정리하고 미사용 계정은 비활성화	ICAM, 관리자 시스템, 시스템접근통제, DB 접근통제
50	N2SF-AC-3(1)	네트워크	위험에 노출된 계정은 연결 차단	위험 계정 탐지 시 연결을 즉시 차단하고 차단 이력을 기록	ICAM, SDP
51	N2SF-DV-12	행정망 (AI 서비스)	클라우드 서비스에서 장치 펌웨어 업데이트 시 검증	장치 펌웨어 검증 후 적용하고 검증 결과를 기록·보관	클라우드 기능
52	N2SF-EB-10	행정망 (AI 서비스)	방화벽(FW) 등 접근통제 이용해 정보시스템 구성요소 외부 노출 차단	외부 노출 차단 정책을 적용하고 노출 포트·인터페이스를 정기 점검	방화벽(FW), 관리자시스템
53	N2SF-EB-11	네트워크	클라우드 공통보안서비스 (보안네트워크) 이중화 구성	이중화 구성 상태를 유지하고 장애 발생 시 전환 절차를 점검	클라우드 기능
54	N2SF-EB-13	AI 서비스	서비스 오류에 대한 응답 시 특정 내용보다는 일반화된 내용으로 응답하도록 설정	오류 응답 시 내부 정보가 노출되지 않도록 일반화된 메시지를 적용	시큐어코딩 개발
55	N2SF-IN-1(1)	행정망 (AI 서비스)	클라우드 ITSM 기능 적용해 정보시스템 구성 요소 최신 상태 유지	구성요소 최신 상태를 유지하고 미적용 항목은 자동 또는 수동 보완	클라우드 기능
56	N2SF-IN-5	행정망 (AI 서비스)	Logging&Audit을 통한 인가되지 않은 변경 추적 및 보안 감사	인가되지 않은 변경을 추적하고 변경 발생 시 검토·복구 수행	클라우드 기능
57	N2SF-IN-6	행정망 (AI 서비스)	비인가된 실행 파일이나 프로세스의 실행을 차단 및 경고	비인가 실행 파일·프로세스를 차단하고 차단 로그를 점검	서버보안, 서버백신
58	N2SF-IN-11	행정망 (AI 서비스)	재기동 시 클라우드 vTPM 이용	재기동 시 무결성 검증을 수행하고 실패 시 관리자 통보	클라우드 기능

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
59	N2SF-AC-M1	행정망 (AI 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	계정 관련 로그를 장기 보관하고 변경 이력을 감사 가능하게 유지	클라우드 기능, 시스템 접근통제, DB 접근통제, 관리자시스템
60	N2SF-AC-M2	행정망 (AI 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	접근·권한 변경 로그를 수집·보관하고 위변조 방지 조치를 적용	클라우드 기능, 시스템 접근통제, DB 접근통제, 관리자시스템
61	N2SF-AC-M3	행정망 (AI 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	사용자 활동 로그를 주기적으로 검토하고 이상 징후를 식별	클라우드 기능, 시스템 접근통제, DB 접근통제, 관리자시스템
62	N2SF-EB-M3	네트워크	Logging&Audit, 방화벽(FW) 등을 통한 로그 기록, 변경 추적 및 보안 감사	방화벽(FW)·로그 기록을 보존하고 변경 추적 및 감사 절차를 운영	클라우드 기능, 시스템 접근통제, DB 접근통제, 관리자시스템
63	N2SF-EB-M4	네트워크	ICAM 이용 이상행위 탐지 및 차단	이상행위 탐지 시 경고 또는 차단 조치를 수행하고 탐지 이력을 기록	ICAM
64	N2SF-EB-M5	네트워크	침해 발생 시 외부 통신 차단	침해 발생 시 외부 통신을 즉시 차단하고 사고 대응 절차를 연계	TMS 탐지센서(IPS), 방화벽(FW)
65	N2SF-IF-M2	네트워크	Logging&Audit, 방화벽(FW) 등을 통한 로그 기록, 변경 추적 및 보안 감사	정보흐름 관련 로그를 보존하고 주기적으로 감사·점검	방화벽(FW), 클라우드 기능
66	N2SF-IF-M3	네트워크	Logging&Audit, 방화벽(FW) 등을 통한 로그 기록, 변경 추적 및 보안 감사	변경 추적 로그를 검토하고 미준수 사항에 대해 개선 조치 수행	방화벽(FW), 클라우드 기능

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
67	N2SF-IF-M4	네트워크	실시간 로깅 및 비인가 흐름 탐지	실시간 로그 분석으로 비인가 흐름을 탐지하고 즉시 대응	방화벽(FW), SSL 복호화기, IPS, WAF 등
68	N2SF-IF-M5	네트워크	이상행위 탐지 및 보고	이상행위 탐지 결과를 보고하고 재발 방지 조치를 수행	방화벽(FW), SSL 복호화기, IPS, WAF 등
69	N2SF-IS-2	행정망 (AI 서비스)	정보시스템 운영, 관리 구성요소 외부 노출 차단	운영·관리 구성요소 외부 노출 차단 상태를 유지하고 예외 노출을 점검	방화벽(FW), WAF, 웹 어플리케이션 내 권한 제어, 접근통제, 권한관리
70	N2SF-SG-M2	행정망 (AI 서비스)	역할 기반 계정 및 권한 관리	역할 기반 계정·권한 정책을 유지하고 정기적으로 적정성을 검토	ICAM, 시스템접근통제, DB 접근통제, 관리자시스템, 웹어플리케이션
71	N2SF-SG-M3	행정망 (AI 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	분리 정책 관련 로그를 기록·보관하고 주기적으로 감사	시스템접근통제, DB 접근통제, 관리자시스템, 클라우드 기능
72	N2SF-SG-M4	행정망 (AI 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	접근 권한 및 분리 상태를 점검하고 이상 접근 시 조치	시스템접근통제, DB 접근통제, 관리자시스템, 클라우드 기능
73	N2SF-SG-M5	행정망 (AI 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	분리 위반 징후를 기록·감사하고 필요 시 차단 조치 수행	시스템접근통제, DB 접근통제, 관리자시스템, 클라우드 기능
74	N2SF-LI-M1	행정망 (AI 서비스)	로그인 실패, 의심스러운 로그인 시도 등을 모니터링하고 보고	로그인 실패·의심 로그인 시도를 모니터링하고 관리자에게 보고	ICAM, 시스템접근통제, DB 접근통제, 관리자시스템

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
75	N2SF-LI-M2	행정망 (AI 서비스)	로그인 관련 데이터들의 무결성을 주기적으로 점검 및 이상 여부 확인	로그인 관련 데이터의 무결성을 주기 점검하고 이상 여부를 확인	SDP, 시스템접근통제, DB 접근통제, 관리자시스템
76	N2SF-LP-M1	행정망 (AI 서비스)	특별권한 사용자 그룹 관리, 권한 부여 및 변경 통제	특별권한 사용자 그룹을 별도 관리하고 권한 변경 이력을 점검	PAM, 서버보안, 시스템접근통제, DB 접근통제
77	N2SF-LP-M2	행정망 (AI 서비스)	주요 사용자 최소 권한 부여, 권한 수준 정기적 검토	주요 사용자 권한을 정기 검토하여 불필요 권한을 회수	ICAM, 시스템접근통제, DB 접근통제, 관리자시스템
78	N2SF-AC-3	AI 서비스	ICAM 기반 의심스러운 계정 모니터링	의심 계정을 상시 모니터링하고 이상 행위 탐지 시 조사·조치 수행	ICAM, 시스템접근통제, DB 접근통제, 관리자시스템
79	N2SF-DA-3	AI 서비스	식별된 단말만 인증을 통해 접근 허용	식별된 단말만 접근을 허용하고 미등록 단말은 인증 단계에서 차단	SDP, ICAM
80	N2SF-LI-1	AI 서비스	암호화 통신	인증 채널 암호화를 유지하고 평문 인증 시도를 차단	HTTPS
81	N2SF-SN-M1	AI 서비스	세션 관리 정책 이행	세션 관리 정책을 적용하고 세션 만료·재인증 절차를 운영	SDP, ICAM, SSO
82	N2SF-SN-M2	AI 서비스	세션 로그 기록 및 주기적인 점검	세션 로그를 기록·보관하고 주기적으로 이상 여부를 점검	SDP, ICAM, 시스템접근통제, DB 접근통제, 관리자시스템
83	N2SF-IF-5	AI 서비스	데이터 유입 시 일방향 정보흐름 통제	일방향 정보흐름 정책을 유지하고 역방향 흐름 발생 시 차단	망중계
84	N2SF-DT-1	AI 서비스	권한 확인 및 통제	정보 전송 전 권한 확인을 수행하고 미인가 요청을 차단	SDP, ICAM, 시스템접근통제, DB 접근통제, 관리자시스템

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
85	N2SF-DT-2	AI 서비스	정보교환 대상 식별 및 통제	정보교환 대상 식별 기준을 적용하고 미식별·비인가 대상은 차단	SDP, ICAM, 시스템접근통제, DB 접근통제, 관리자시스템
86	N2SF-DU-M1	AI 서비스	최소한의 접근권한 부여, 주기적인 모니터링 및 관리	최소한의 접근권한을 유지하고 사용 현황을 주기적으로 점검	SDP, ICAM, 시스템접근통제, DB 접근통제, 관리자시스템
87	N2SF-AIP-01	AI 서비스	AI 모델에 대한 위협 차단	프롬프트·응답·콘텐츠 기반 위협을 탐지·차단하고 탐지 이력을 관리	AI 프롬프트 보안기(SSE, SWG, GenAI), 필터링, 가드레일
88	N2SF-IS-4	네트워크	네트워크간 트래픽 분리	네트워크 간 트래픽 분리 정책을 유지하고 비인가 통신을 차단	방화벽(FW)
89	N2SF-SG-4	네트워크	시스템/네트워크 IP 체계 분리	시스템·네트워크 IP 체계 분리 상태를 유지하고 충돌 여부를 점검	방화벽(FW)
90	N2SF-IF-1	네트워크	네트워크 트래픽 통제	네트워크 트래픽 흐름을 정책 기반으로 통제하고 이상 흐름을 차단	방화벽(FW), Routing, GW
91	N2SF-EB-1	네트워크	외부 접점 수 제한	외부 접점을 최소화하고 승인되지 않은 접점은 비활성화	망중계, Transfer CDS, Anti-DDoS
92	N2SF-EB-2	네트워크	외부 통신 경계 흐름 통제	외부 통신 경계 흐름을 통제하고 비인가 경로는 차단·기록	망중계, Transfer CDS, Anti-DDoS
93	N2SF-EB-3	네트워크	모든 차단 실행 후 허용 정책 추가, 주기적 관리	기본 차단 정책을 유지하고 허용 정책은 승인 후 반영·정기 점검	방화벽(FW)

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
94	N2SF-EB-5	네트워크	Proxy를 이용한 통신 경로 강제화로 외부 통신 시 Proxy를 경유하도록 설정	외부 통신은 반드시 Proxy를 경유하도록 강제하고 직접 통신을 차단	AI 프롬프트 보안기(SSE, SWG, GenAI)
95	N2SF-EB-6	네트워크	Proxy를 이용한 통신 경로 강제화로 외부로의 사이버 위협 발신 시 Proxy에서 차단	외부 위협 발신 탐지 시 Proxy에서 즉시 차단하고 이벤트를 기록	AI 프롬프트 보안기(SSE, SWG, GenAI)
96	N2SF-EB-14	네트워크	Proxy를 이용한 통신 경로 강제화로 인가된 DNS 서버 외 요청 차단	인가된 DNS 서버만 허용하고 비인가 DNS 요청은 차단	AI 프롬프트 보안기(SSE, SWG, GenAI)
97	N2SF-EB-15	네트워크	Proxy를 이용한 통신 경로 강제화로 VPN, Tor 등 우회 경로 사용 탐지 및 차단	VPN·Tor 등 우회 경로 사용을 탐지·차단하고 시도 이력을 관리	AI 프롬프트 보안기(SSE, SWG, GenAI)
98	N2SF-IF-2	MCP 서비스	암호화 채널의 정보흐름 통제	암호화 채널만 허용하고 비암호화 통신은 차단	AI 프롬프트 보안기(SSE, SWG, GenAI), 필터링, 가드레일
99	N2SF-IF-6	MCP 서비스	정보흐름 통제	필터링·가드레일 기준에 따라 정보흐름을 통제하고 위반 시 차단	AI 프롬프트 보안기(SSE, SWG, GenAI), 필터링, 가드레일
100	N2SF-IF-7	MCP 서비스	데이터 전송 통제	데이터 전송 정책 위반 시 차단하고 전송 로그를 기록	AI 프롬프트 보안기(SSE, SWG, GenAI), 필터링, 가드레일
101	N2SF-IF-8	MCP 서비스	비인가 정보흐름 통제	비인가 정보흐름 탐지 시 차단하고 민감정보 여부를 점검	AI 프롬프트 보안기(SSE, SWG, GenAI), 필터링, 가드레일

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
102	N2SF-IF-10	MCP 서비스	정보 전송 방식 제한	허용된 전송 방식만 사용하도록 제한하고 비허용 방식은 차단	HTTPS
103	N2SF-IF-3	네트워크	악성코드 검사 실행	악성코드 검사 수행 후 이상 파일·콘텐츠를 차단하고 결과를 기록	Transfer CDS, AI 프롬프트 보안기(SSE, SWG, GenAI)
104	N2SF-IF-5	네트워크	데이터 유입 시 일방향 정보흐름 통제	일방향 정보흐름 정책을 유지하고 역방향 전송을 차단	망중계
105	N2SF-LP-4	행정망 (MCP 서비스)	최소 인원에게 관리자 권한 부여	관리자 권한은 최소 인원에게만 부여하고 권한 현황을 정기 점검	ICAM, 시스템접근통제, DB 접근통제
106	N2SF-LP-4(1)	행정망 (MCP 서비스)	원격접속을 통한 관리자 접속을 허용하지 않음	원격 관리자 접속 금지 상태를 유지하고 예외 허용 여부를 점검	-
107	N2SF-LP-4(4)	행정망 (MCP 서비스)	관리자 권한 실행 내역을 로깅하고 및 주기적으로 검토	관리자 권한 실행 내역을 로깅하고 주기적으로 검토·감사	ICAM, 시스템접근통제, DB 접근통제
108	N2SF-AC-1(5)	행정망 (MCP 서비스)	유휴 계정 정리, 접근 제어	유휴 계정을 식별·정리하고 미사용 계정을 비활성화	ICAM, 시스템접근통제, DB 접근통제
109	N2SF-AC-3(1)	행정망 (MCP 서비스)	위험에 노출된 계정은 연결 차단	위험 계정 탐지 시 연결을 즉시 차단하고 차단 이력을 기록	ICAM, SDP
110	N2SF-EB-10	행정망 (MCP 서비스)	정보시스템 구성요소 외부 노출 차단	구성요소 외부 노출 차단 정책을 유지하고 노출 상태를 점검	방화벽(FW)
111	N2SF-EB-11	행정망 (MCP 서비스)	클라우드 공통보안서비스 (보안네트워크) 이중화 구성	이중화 구성을 유지하고 장애 발생 시 서비스 연속성을 보장	클라우드 기능

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
112	N2SF-EB-13	MCP 서비스	서비스 오류에 대한 응답 시 특정 내용보다는 일반화된 내용으로 응답하도록 설정	오류 응답 시 내부 정보가 노출되지 않도록 일반화 메시지를 적용	시큐어코딩 개발
113	N2SF-DV-12	행정망 (MCP 서비스)	클라우드 서비스에서 장치 펌웨어 업데이트 시 검증	펌웨어 업데이트는 검증 후 적용하고 검증 결과를 기록·보관	클라우드 기능
114	N2SF-IN-1(1)	행정망 (MCP 서비스)	클라우드 ITSM 기능 적용해 정보시스템 구성 요소 최신 상태 유지	정보시스템 구성요소 최신 상태를 유지하고 미적용 항목을 보완	클라우드 기능
115	N2SF-IN-5	행정망 (MCP 서비스)	Logging&Audit을 통한 인가되지 않은 변경 추적 및 보안 감사	인가되지 않은 변경을 추적하고 변경 발생 시 검토·복구 수행	클라우드 기능
116	N2SF-IN-6	행정망 (MCP 서비스)	비인가된 실행 파일이나 프로세스의 실행을 차단 및 경고	비인가 실행 파일·프로세스를 차단하고 차단 로그를 점검	서버보안, 서버백신
117	N2SF-IN-11	행정망 (MCP 서비스)	재기동 시 클라우드 vTPM 이용	재기동 시 무결성 검증을 수행하고 실패 시 관리자 통보	클라우드 기능
118	N2SF-LP-M1	행정망 (MCP 서비스)	특별권한 사용자 그룹 관리, 권한 부여 및 변경 통제	특별권한 그룹을 별도 관리하고 권한 부여·변경 이력을 점검	PAM, 서버보안, 시스템접근통제, DB 접근통제
119	N2SF-LP-M2	행정망 (MCP 서비스)	주요 사용자 최소 권한 부여, 권한 수준 정기적 검토	주요 사용자 권한 수준을 정기 검토하고 최소권한 상태를 유지	ICAM, 시스템접근통제, DB 접근통제
120	N2SF-AC-1(2)	행정망 (MCP 서비스)	계정 상태 모니터링	계정 상태를 상시 모니터링하고 이상 상태 발생 시 조치	ICAM, 시스템접근통제, DB 접근통제
121	N2SF-AC-M1	행정망 (MCP 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	로그 기록·변경 추적 내역을 장기 보관하고 감사 가능 상태 유지	시스템접근통제, DB 접근통제, 클라우드 기능

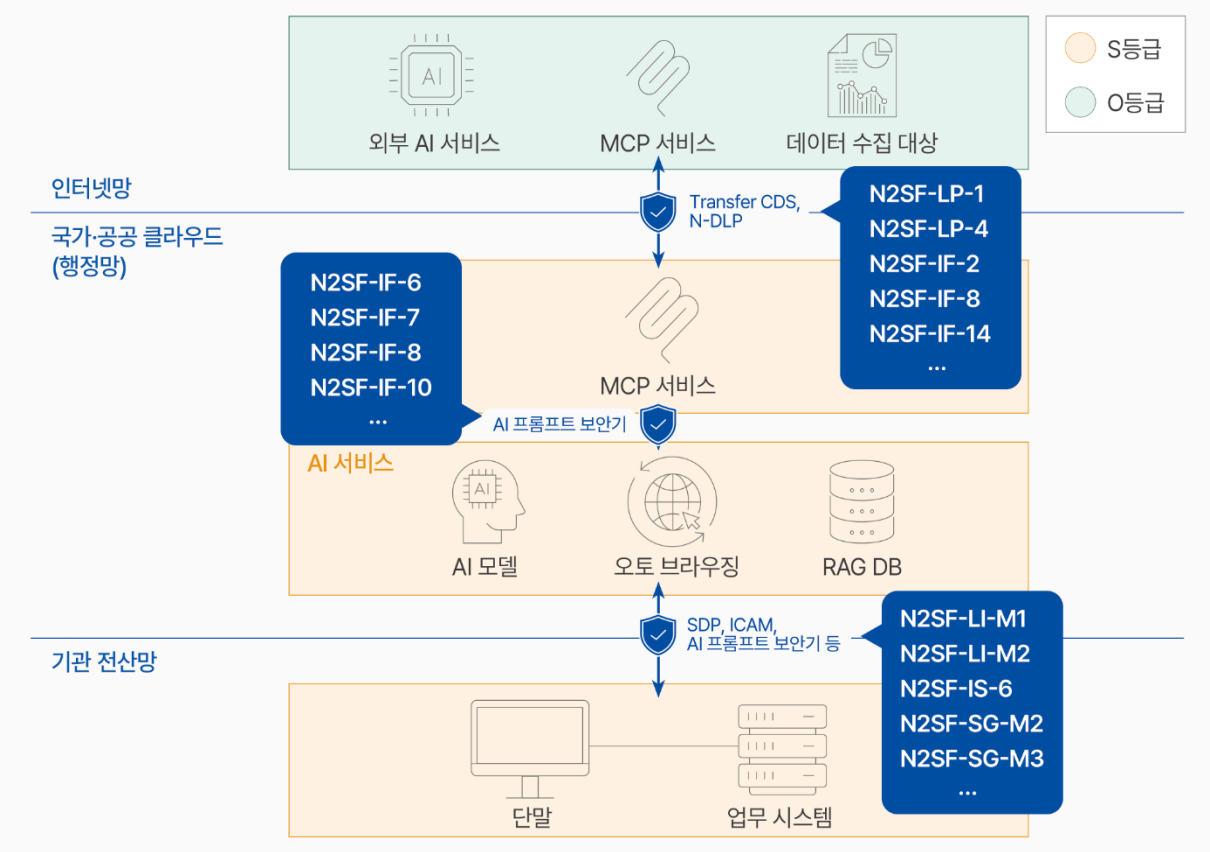
No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
122	N2SF-AC-M2	행정망 (MCP 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	감사 로그 무결성을 보장하고 접근·권한 변경 이력을 추적	시스템접근통제, DB 접근통제, 클라우드 기능
123	N2SF-AC-M3	행정망 (MCP 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	사용자 활동 로그를 기록·보관하고 이상 징후를 정기 분석	시스템접근통제, DB 접근통제, 클라우드 기능
124	N2SF-LI-M1	행정망 (MCP 서비스)	ICAM, 접근통제솔루션 등에서 로그인 실패, 의심스러운 로그인 시도 등을 모니터링하고 보고	로그인 실패·의심 로그인 시도를 탐지하고 관리자에게 보고	ICAM, 시스템접근통제, DB 접근통제
125	N2SF-LI-M2	행정망 (MCP 서비스)	로그인 관련 데이터들의 무결성을 주기적으로 점검 및 이상 여부 확인	로그인 데이터 무결성을 점검하고 이상 여부를 정기 확인	SDP, 시스템접근통제, DB 접근통제
126	N2SF-IS-6	행정망 (MCP 서비스)	통합보안관제로 격리 위반사항 대응	격리 위반사항 발생 시 통합보안관제를 통해 대응·조치 수행	통합보안관제
127	N2SF-SG-M2	행정망 (MCP 서비스)	역할 기반 계정 및 권한 관리	역할 기반 계정·권한 정책을 유지하고 정기적으로 적정성을 검토	SDP, 시스템접근통제, DB 접근통제
128	N2SF-SG-M3	행정망 (MCP 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	분리 정책 관련 로그를 기록·보관하고 정기적으로 감사	시스템접근통제, DB 접근통제, 클라우드 기능
129	N2SF-SG-M4	행정망 (MCP 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사	접근 권한 및 분리 상태를 점검하고 이상 접근 시 차단·조치	시스템접근통제, DB 접근통제, 클라우드 기능
130	N2SF-SG-M5	행정망 (MCP 서비스)	Logging&Audit, 접근통제솔루션 등을 통한 로그 기록, 변경 추적 및 보안 감사, 통합보안관제 수행	로그 기록·감사와 통합보안관제를 연계하여 분리 위반을 대응	시스템접근통제, DB 접근통제, 클라우드 기능, 통합보안관제

No.	보안통제 항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
131	N2SF-IF-M1	네트워크	정보흐름 통제 정책 수립 및 수행	정보흐름 통제 기준과 예외 절차를 문서화하고 정기적으로 갱신	AI 프롬프트 보안기(SSE, SWG, GenAI), 방화벽(FW), 라우팅
132	N2SF-IF-M2	네트워크	로그 기록, 변경 추적 및 보안 감사	로그를 기록·보관하여 변경 추적 및 보안 감사를 수행	방화벽(FW), 클라우드 기능
133	N2SF-IF-M3	네트워크	로그 기록, 변경 추적 및 보안 감사	변경 추적 로그를 정기 점검하고 미준수 사항에 대해 개선 조치	방화벽(FW), 클라우드 기능
134	N2SF-IF-M4	네트워크	방화벽(FW), SSL 복호화기, IPS 등 실시간 로깅 및 비인가 흐름 탐지, 통합보안관제 수행	실시간 로깅과 비인가 흐름 탐지를 수행하고 통합관제로 연계	방화벽(FW), SSL 복호화기, IPS, 통합보안관제
135	N2SF-IF-M5	네트워크	방화벽(FW), SSL 복호화기, IPS 등 실시간 로깅, 이상행위 탐지 및 보고, 통합보안관제 수행	이상행위를 탐지·보고하고 사고 대응 절차와 연계하여 조치	방화벽(FW), SSL 복호화기, IPS, 통합보안관제
136	N2SF-EB-M3	네트워크	Logging&Audit, 방화벽(FW) 등을 통한 로그 기록, 변경 추적 및 보안 감사	외부 통신 로그를 보관하고 변경 추적 및 감사 절차를 운영	방화벽(FW), 클라우드 기능
137	N2SF-EB-M4	네트워크	ICAM 이용 이상행위 탐지 및 차단, 통합보안관제 수행	ICAM 기반 이상행위를 탐지·차단하고 통합보안관제로 모니터링	ICAM, 통합보안관제
138	N2SF-EB-M5	네트워크	TMS 탐지센서(IPS), 방화벽(FW) 등 활용, 통합보안관제 수행	침해 징후 발생 시 방화벽(FW)·IPS 연계 차단 및 통합보안관제 대응 수행	방화벽(FW), SSL 복호화기, IPS, 통합보안관제

(나) 자체정의 보안통제 구현계획

No.	보안통제항목	적용대상	보안통제 적용방안	보안통제 구현·운영 요건
1	N2SF-AIP-01	AI 서비스	AI 프롬프트 보안기(SSE, SWG, GenAI), 필터링, 가드레일	AI 모델에 대한 보안위협을 탐지/차단할 수 있어야 함

5.3 정보서비스 적용 기관 망 구성도 예시



수립한 보안 요구사항 및 보안통제 항목 구현 사항 등 산출물을 토대로 국가정보원 보안성 검토 신청 시, N2SF를 적용한 기관의 실제 망 구성도를 작성하여 첨부하여야 한다.

6. [모델 8] 클라우드 기반 통합 문서체계

본 정보서비스 모델은 기관 내·외부에서 업무 단말, 모바일 단말, 원격 단말 등 단말 유형과 관계없이 통합문서체계를 활용하여 업무자료 생산·공유·협업을 수행하는 데 필요한 보안 요구사항 및 대책을 제시한다.

※ (참고자료) N2SF 보안 가이드라인 1.0 - (부록2) 모델8 클라우드 기반 통합 문서체계

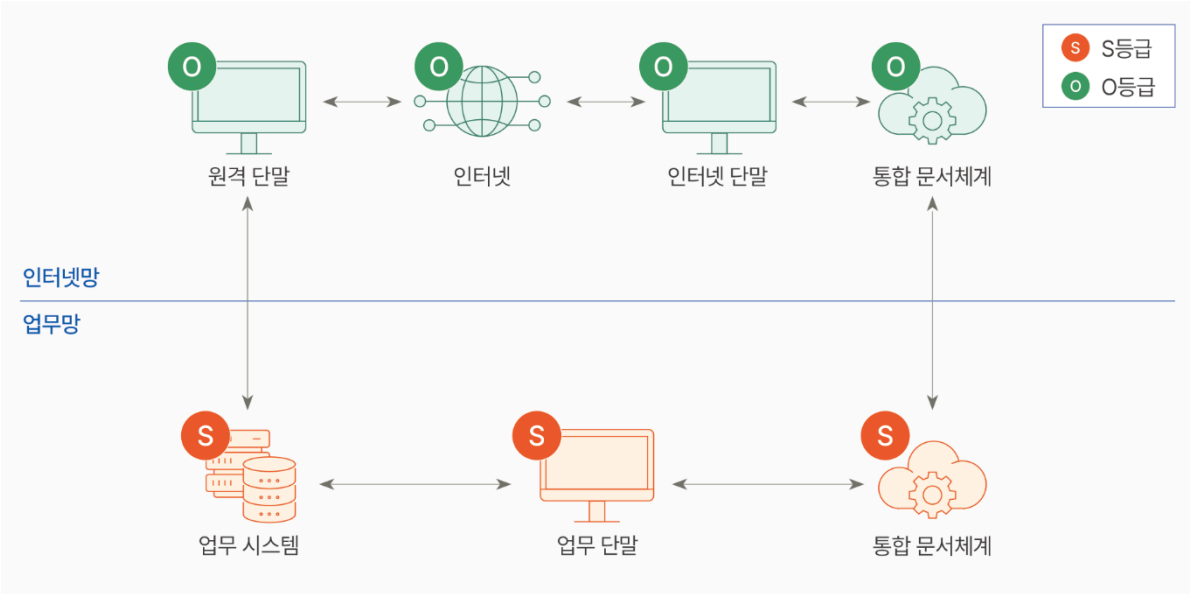
본 실증 사례는 클라우드 기반에서 문서를 안전하게 통합 관리하기 위해 1개의 정보서비스 모델을 활용한다. 기관 내·외부에서 기관 업무망에 구축된 클라우드 기반 문서 관리 시스템에 접속하여 업무 문서를 생성하고 열람이 가능하도록 구현하는 데 중점을 둔다. 이는 기존 망 분리 환경에서 분산되어 있었던 업무자료를 기관 내부 통합 문서체계로 일원화함으로써, 업무 단말과 인터넷 단말의 구분 없이 자료 생산·공유·협업이 가능하다.

각 기관에서는 망 분리된 환경에서도 물리적 제약 없이 내부 업무 시스템에 안전하게 접속하여 자료를 생산하고 공유하고자 할 때 참고할 수 있다.

6.1 정보서비스 유형 요약

정보서비스 유형 / 모델 No. 8 (N2SF 가이드라인 기준)		모델 8 / 클라우드 기반 통합문서체계
정보서비스 개요	업무정보	① 인터넷 수집자료 ② 인터넷 수집자료 취합문서 ③ 기관고유업무 산출물 ④ 타기관 업무요청 ⑤ 타기관 보고서
	정보시스템	① 업무망 단말 ② 인터넷망 단말 ③ 원격 단말 ④ 업무 시스템 ⑤ 업무망 문서중앙화 시스템 ⑥ 인터넷망 문서중앙화 시스템 ⑦ 인터넷 서비스
정보서비스 사용 시나리오		① 인터넷망과 업무망 간 파일 전송

위치/주체/객체 관점의 정보서비스 구조



- 인터넷망(O등급)에서 인터넷망 단말(O등급)을 이용해 업무망 문서중앙화시스템(통합문서체계, S등급)을 이용
- 인터넷망 단말(O등급)은 내부 인증시스템과 별개인 외부 인증 서비스를 이용
- 외부 인증 서비스는 식별 및 인증만 제공하며, 권한 할당은 없음
- 인터넷망 단말(O등급)은 일차적으로 외부 인증 서비스에 접속하여 식별, 인증을 거친 후 인터넷 수집자료(O등급)를 인터넷망 문서중앙화시스템(O등급)에 저장
- 인터넷망 문서중앙화시스템(O등급)은 주기적으로 업무망 문서중앙화시스템(S등급)으로 인터넷 수집자료(O등급) 일방향 통신 및 인터넷 수집자료(O등급)를 전송

보안통제 대상

① 업무망 단말
② 인터넷망 단말
③ 원격 단말
④ 문서중앙화시스템 연계체계
⑤ 문서중앙화시스템
⑥ 인터넷 연계체계

6.2 최종산출물 서식

[1] 정보서비스 사용 시나리오별 정보시스템 식별

정보서비스 사용 시나리오별 정보시스템 식별

번호	사용 시나리오	관련 정보시스템
1	인터넷망과 업무망 간 파일 전송	
1-1	인터넷망에서 업무망으로 파일 전송	㉠ 인터넷망 단말 ㉡ 업무망 문서중앙화시스템
1-2	업무망에서 인터넷망으로 파일 전송	㉠ 업무망 단말 ㉡ 인터넷망 문서중앙화시스템

[2] 정보서비스 보안목표

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 1번 「정보서비스 보안목표」는 아래와 같이 정리됨

No.	영역	보안 목표	비고
1	공통	정보서비스 모델 8. 클라우드 기반 통합 문서체계	N2SF 가이드라인 1.0
2	네트워크	업무영역과 별도로 기관 고유업무망 구성 (기관 고유업무망 침해 시 피해 전이 방지)	자체
3		업무목적에 필요한 인터넷 서비스만 접속	자체
4		인터넷에서 파일 다운로드 시 파일동적검사 실행	자체
5	단말관리	구름 OS 도입하여 인터넷과 업무 시스템 동시연결 원천 차단	자체
6		개인 구름 OS는 직원 개인과 일대일 매핑	자체
7		업무망 접속은 구름 OS 단말기로 제한	자체
8		업무망 단말 부팅 시 다중요소인증 실시	자체

[3] C/S/O 등급분류

국가정보원 보안성 검토 시 제출하는 문서 중, 자체 보안대책에 대한 최종 산출물 서식 2번 「C/S/O 등급 분류표」는 아래와 같이 정리됨

No.	정보시스템		업무정보		비고
	명칭	C/S/O 등급	명칭	C/S/O 등급	
1	업무망 단말	S	인터넷 수집자료	O	일시적으로 로컬파일로 존재
			인터넷 수집자료 취합문서	S	
			업무 산출물	S	
			타기관 업무요청	S	
			타기관 보고서	S	
2	인터넷망 단말	O	인터넷 수집자료	O	일시적으로 로컬파일로 존재
3	원격 단말	S	인터넷 수집자료	O	
			업무 시스템	S	
			업무망 문서중앙화 시스템	S	
			인터넷망 문서중앙화 시스템	O	
			인터넷 서비스	O	
4	업무 시스템	S	인터넷 수집자료	O	
			인터넷 수집자료 취합문서	S	
			기관 고유업무 산출물	S	
			타기관 업무요청	S	
			타기관 보고서	S	
5	업무망 문서중앙화 시스템	S	인터넷 수집자료	O	
			인터넷 수집자료 취합문서	S	
			기관 고유업무 산출물	S	
			타기관 업무요청	S	
			타기관 보고서	S	
6	인터넷망 문서중앙화 시스템	O	인터넷 수집자료	O	

[4] 위협 식별 - 모델링 및 C/S/O 평가

기관의 정보서비스 구성요소에 따라 유스케이스별로 모델링 및 C/S/O 보안등급을 나누어 평가하며, 「정보 생산·저장」 보안원칙과 「정보 이동」 보안원칙을 적용하여 보안대책의 필요성을 평가한다.

N2SF 보안 가이드라인*에서 본 정보서비스는 **인터넷 영역(위치, O등급)**에 위치하는 **이용자 단말(주체, O등급)**, 기관 전산망 영역에 위치하는 **통합문서체계(객체, S등급)**의 구성, **기관 전산망 영역(위치, S등급)**에 위치하는 **이용자 단말(주체, S등급)**, **통합문서체계(객체, S등급)**로 구성되며, O등급의 인터넷망 이용자 단말에서 S등급 업무정보가 생산·저장(활용), 이동하지 않고, S등급의 기관전산망 이용자 단말에서 S등급의 업무정보가 생산·저장(활용), 이동할 수 있도록 보안 원칙을 제시하고 있다. 아래 제시하는 실증 사례 및 N2SF 보안 가이드라인에 대하여 각 기관은 개별적으로 운영 중인 정보시스템의 특성과 네트워크 환경에 따라 유연하게 참고하여 보안원칙을 수립하여야 한다.

* N2SF 보안 가이드라인 1.0 - (부록2) 모델8 클라우드 기반 통합문서체계

사례: 인터넷망과 업무망 간 파일 전송

(1) 인터넷망에서 업무망으로 파일 전송

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C 등급 / S 등급 / O 등급 위치 Domain / 인터넷망 주체 Subject / 인터넷망 단말 객체 Object / 업무망 문서 중앙화시스템 인터넷망(O 등급)에서 인터넷망 단말(O 등급)을 이용해 업무망 문서중앙화 시스템(S 등급)을 이용하는 경우, 위치, 주체는 O 등급이나 객체가 S 등급에 해당하여 보안 대책 필요.	예
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C 정보 / S 정보 / 인터넷 수집자료 C 시스템 / ● / ● / ● 업무망 문서 중앙화시스템 / + / ● / ● 인터넷망 단말 / + / + / ● 인터넷망 단말(O 등급)은 O 등급인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)를 다룰 수 있음. 업무망 문서중앙화시스템(S 등급)은 S 등급 이하인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료(O 등급)를 다룰 수 있음.	아니오
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / 업무망 문서 중앙화시스템 / 인터넷망 단말 C 정보 / ● / + / + S 정보 / ● / ● / + 인터넷 수집자료 / ● / ● / ● 인터넷 단말(O 등급)이 업무망 문서중앙화시스템(S 등급)에 접속하는 경우, O 등급인 업무정보만을 주고받을 수 있으며, 따라서 인터넷 수집자료(O 등급)를 주고받아도 보안원칙에 위배되지 않음.	아니오

(2) 업무망에서 인터넷망으로 파일 전송

구분	결과 및 설명	보안대책 필요여부
「위치-주체-객체」 모델 C/S/O 평가	구분 / C 등급 / S 등급 / O 등급 위치 Domain: 업무망 주체 Subject: 업무망 단말 객체 Object: 인터넷망 문서 중앙화시스템 업무망(S 등급)에서 업무망 단말(S 등급)을 이용해 인터넷망 문서중앙화시스템(O 등급)을 이용하는 경우, 위치, 주체는 S 등급이나 객체가 O 등급에 해당하여 보안 대책 필요.	예
「정보 생산·저장」 보안원칙	~에서 생산·저장 / C 정보 / 인터넷 수집자료 취합문서, 연구산출물 / O 정보 C 시스템: ● / ● / ● 연구망 단말: + / ● / ● 인터넷망 문서 중앙화시스템: + / ⃠ + / ● 인터넷망 문서중앙화시스템(O 등급)은 O 등급인 업무정보만을 생산 및 저장할 수 있으므로 인터넷 수집자료 취합문서(S 등급), 연구 산출물(S 등급)을 포함한 S 등급 업무정보를 다룰 경우 보안원칙에 위배됨. 따라서 연계 구간에 적절한 보안 대책 필요.	예
「정보 이동」 보안원칙	~정보가 ~로 이동 / C 시스템 / 업무망 단말 / 인터넷망 문서 중앙화시스템 C 정보: ● / + / + 인터넷 수집자료 취합문서, 연구산출물: ● / ● / + ⃠ O 정보: ● / ● / ● 업무망 단말(S 등급)이 인터넷망 문서중앙화시스템(O 등급)에 접속하는 경우, O 등급인 업무정보만을 주고받을 수 있으며, 따라서 인터넷 수집자료 취합문서(S 등급)이나 연구 산출물(S 등급)을 포함한 S 등급 업무정보를 주고받는 경우 보안원칙에 위배됨. 따라서 연계 구간에 적절한 보안 대책 필요.	예

[5] 보안요구사항 및 보안통제

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 3번 「보안 요구사항 및 보안통제」는 아래와 같이 작성할 수 있다.

※ 보안 가이드라인에 없는 신규 자체정의 보안통제 항목: N2SF-ORG4

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
1	업무망 단말	업무 단말 보안성 유지	N2SF-LP-1
			N2SF-DA-1
			N2SF-DA-2
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-8
			N2SF-IN-10
			N2SF-IN-16
		업무 단말 사용 보안	N2SF-AM-2
			N2SF-AM-9
			N2SF-DV-6
			N2SF-DV-8
		업무 단말 네트워크 보안	N2SF-SG-4
			N2SF-SG-5
			N2SF-SG-6
			N2SF-IF-9
			N2SF-EB-6
			N2SF-SN-1
			N2SF-WA-7
			N2SF-BC-1
			N2SF-DT-1

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
		업무 단말 데이터 보호	N2SF-DU-2
		통합문서체계 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1
			N2SF-SG-M1
			N2SF-SG-M3
			N2SF-SG-M5
			N2SF-EB-M1
			N2SF-DU-M3
		업무망 단말 내 파일 저장 방지	N2SF-ORG4-1
2	인터넷망 단말	이용자 단말 보안성 유지	N2SF-LP-1
			N2SF-DA-1
			N2SF-DA-2
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-8
			N2SF-IN-10
			N2SF-IN-16
		이용자 단말 사용 보안	N2SF-AM-2
			N2SF-AM-9
			N2SF-DV-6
			N2SF-DV-8
		이용자 단말 네트워크 보안	N2SF-SG-4
			N2SF-SG-5
			N2SF-SG-6
			N2SF-IF-9
			N2SF-EB-6
			N2SF-SN-1

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-WA-7
			N2SF-BC-1
			N2SF-DT-1
		업무망 단말 내 파일 저장 방지	N2SF-ORG4-1
3	원격 단말	이용자 단말 보안성 유지	N2SF-LP-1
			N2SF-DA-1
			N2SF-DA-2
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-8
			N2SF-IN-10
			N2SF-IN-16
		이용자 단말 사용 보안	N2SF-AM-2
			N2SF-AM-9
			N2SF-DV-6
			N2SF-DV-8
		이용자 단말 네트워크 보안	N2SF-SG-4
			N2SF-SG-5
			N2SF-SG-6
			N2SF-IF-9
			N2SF-EB-6
			N2SF-SN-1
			N2SF-WA-7
			N2SF-BC-1
			N2SF-DT-1
		이용자 단말 데이터 보호	N2SF-DU-2

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
		통합문서체계 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1
			N2SF-SG-M1
			N2SF-SG-M3
			N2SF-SG-M5
			N2SF-EB-M1
			N2SF-DU-M3
		사전 지정한 사용자 및 전용 단말	N2SF-DA-3
			N2SF-DA-3(1)
			N2SF-DA-5
		전체 디스크 암호화 및 비인가 매체 차단	N2SF-DU-2
			N2SF-DV-3
			N2SF-DV-4
		콘텐츠 열람 시 워터마크 적용	N2SF-DU-M3
		원격 단말 사용 환경 보안	N2SF-ORG4-2
4	문서 중앙화시스템 연계체계	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
		비인가 네트워크 연결 차단	N2SF-IS-4
			N2SF-IF-1
			N2SF-IF-9

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-EB-1
			N2SF-EB-2
			N2SF-EB-3
			N2SF-EB-5
			N2SF-EB-6
			N2SF-EB-14
			N2SF-EB-15
		통합문서체계 서비스 활용 시 데이터 보호	N2SF-IF-2
			N2SF-IF-6
			N2SF-IF-7
			N2SF-IF-8
			N2SF-IF-10
			N2SF-IF-14
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3
			N2SF-IF-5
		연계체계 보안성 유지	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-13
			N2SF-DV-4
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-IN-6
			N2SF-IN-11
		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-IF-M1
			N2SF-IF-M2
			N2SF-IF-M3
			N2SF-IF-M4
			N2SF-IF-M5
			N2SF-EB-M3
			N2SF-EB-M4
			N2SF-EB-M5
		이용자 단말(모바일 단말, 원격 단말)과의 전용 통신망(또는 이에 준하는) 구성	N2SF-IF-11
			N2SF-EB-4
			N2SF-EB-5
			N2SF-EB-9
			N2SF-DA-3
			N2SF-DA-3(1)
		외부 단말 파일 다운로드 통제 및 콘텐츠 검증 및 암호화 송신	N2SF-DA-4
			N2SF-DA-5
			N2SF-IN-6
			N2SF-DV-5

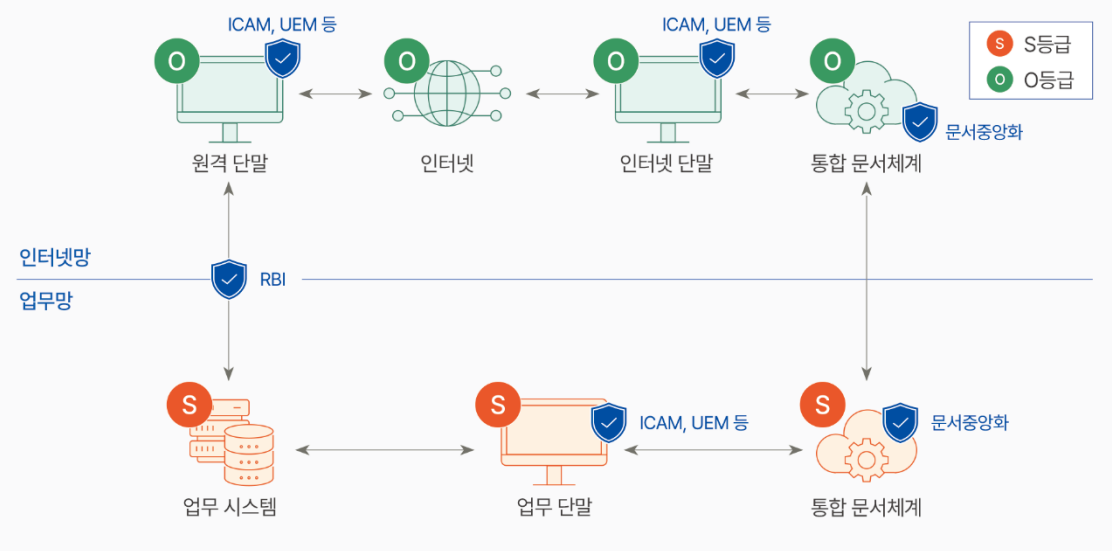
No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-CD-1
			N2SF-CD-2
5	인터넷 연계체계	업무 무관 유해사이트(게임, 도박 등) 및 비인가 사이트 접속 통제	N2SF-EB-1
			N2SF-EB-2
			N2SF-EB-14
			N2SF-EB-15
			N2SF-EB-M2
		외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3
			N2SF-IF-5
		연계체계 보안성 유지	N2SF-LP-4
			N2SF-LP-4(1)
			N2SF-LP-4(4)
			N2SF-AC-1(5)
			N2SF-AC-3(1)
			N2SF-EB-8
			N2SF-EB-10
			N2SF-EB-11
			N2SF-EB-13
			N2SF-DV-4
			N2SF-DV-12
			N2SF-IN-1(1)
			N2SF-IN-5
			N2SF-IN-6
			N2SF-IN-11
		연계체계 운용 관리	N2SF-LP-M1
			N2SF-LP-M2
			N2SF-AC-1(2)
			N2SF-AC-M1

No.	보안위험 발생지점	보안 요구사항	보안통제 항목
			N2SF-AC-M2
			N2SF-AC-M3
			N2SF-LI-M1
			N2SF-LI-M2
			N2SF-IF-M1
			N2SF-IF-M2
			N2SF-IF-M3
			N2SF-IF-M4
			N2SF-IF-M5
			N2SF-EB-M3
			N2SF-EB-M4
			N2SF-EB-M5
6	문서 중앙화시스템	문서 생산, 유통 범위·등급 설정, 자동 삭제 등 관리	N2SF-DU-2
			N2SF-DU-3
			N2SF-DU-4
			N2SF-DU-M2
			N2SF-DU-M3
			N2SF-EK-1
		단말 등급, 접속 위치 등에 따른 문서 접근통제	N2SF-DA-4
			N2SF-LP-1
			N2SF-DU-M1
		문서 작업 이력 기록 및 관리	N2SF-DU-M2
			N2SF-RA-1

[6] 보안통제 구현계획

국가정보원 보안성 검토 시 제출하는 문서 중, 국가 망 보안체계 보안 가이드라인 1.0의 최종 산출물 서식 4번 「보안통제 구현계획표」는 아래와 같이 작성할 수 있다.

보안통제적용 정보서비스 구성도



(가) 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
1	N2SF-BC-1	단말	매체제어 솔루션을 적용하여 단말의 블루투스 통신을 통제	블루투스 기능을 기본 비활성화하고, 예외 사용 시 승인 절차를 거쳐 허용	매체제어 솔루션
2	N2SF-DA-1	단말	UEM 기반으로 단말 고유정보를 PDP(ICAM)에 사전 등록	등록되지 않은 단말은 인증 단계에서 자동 차단	PDP (ICAM), UEM
3	N2SF-DA-2	단말	RBI 를 적용하여 사용자 접속 사이트를 화이트리스트 기반으로 제한	사전 승인된 사이트만 접속 가능하도록 정책을 구성·운영	PDP (ICAM), RBI, DLP, MDM
4	N2SF-DA-3	단말	UEM 기반 단말 인증 정보를 PDP(ICAM)과 연계	인증 실패 단말은 네트워크 접근을 제한	PDP (ICAM), UEM, NAC
5	N2SF-DA-3(1)	단말	단말 식별 정보 기반 접근 통제를 수행	단말 변경·위험 탐지 시 재등록 및 재인증 절차 적용	PDP (ICAM), UEM, NAC
6	N2SF-DA-4	단말	ICAM 을 활용하여 단말 접근권한을 중앙에서 관리	접근 로그를 수집·보관하고 정기 감사에 활용	PDP (ICAM), DLP

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
7	N2SF-DA-5	단말	ICAM·UEM 연계를 통해 검증된 단말만 접속 허용	비인가 단말은 자동 격리 또는 차단	PDP (ICAM), UEM
8	N2SF-DV-12	단말	단말 보안·패치 관리 도구를 통해 단말 상태를 관리	최신 패치 미적용 단말은 경고 또는 접속 제한	내PC지키미, PMS
9	N2SF-DV-3	단말	OS 및 단말 통제 솔루션을 통해 장치 사용을 제한	정책 위반 장치 기능은 자동 차단	내PC지키미, 매체제어 솔루션
10	N2SF-DV-4	단말	매체제어·PC 보안 솔루션으로 단말 입출력 및 네트워크 통제	안전부팅 적용 및 악성코드 유입 시 자동 차단	매체제어 솔루션, PC 보안 솔루션
11	N2SF-DV-5	단말	문서중앙화 솔루션으로 단말 내 정보 저장을 제한	로컬 저장 시도를 탐지하고 즉시 차단	문서중앙화 솔루션
12	N2SF-DV-6	단말	단말 통제 솔루션으로 장치 기능을 관리	정책 위반 장치 사용 이력 기록 및 조치	매체제어 솔루션, UEM
13	N2SF-DV-8	단말	화면 보호기 정책을 적용하여 장시간 미사용 시 화면 잠금	설정 여부를 정기 점검하여 미적용 단말 조치	윈도우 화면 보호기, 내PC지키미, UEM
14	N2SF-IN-10	단말	중앙 관리 기반 소프트웨어 설치 정책 적용	비인가 소프트웨어 설치·실행 차단	내PC지키미, UEM
15	N2SF-IN-11	단말	안전한 재기동 절차를 통해 시스템 무결성 확보	재기동 시 구성요소 검증 및 서명 확인	보안정책 및 관리적 보안
16	N2SF-IN-16	단말	백신 기반 악성코드 탐지 및 차단	실시간 탐지 정책 유지 및 주기적 업데이트	백신, EDR
17	N2SF-IN-5	단말	PDP(ICAM) 기반 인가 절차를 통해 단말 등록 관리	인가되지 않은 변경 사항 발생 시 경고	내PC지키미, PDP (ICAM), UEM
18	N2SF-IN-6	단말	단말 관리·패치 도구로 서비스 상태 관리	불필요한 서비스 자동 식별 및 비활성화	UEM, 내PC지키미, PMS
19	N2SF-IN-8	단말	단말 보안 솔루션으로 비인가 SW 실행 통제	실행 시도 로그를 수집·분석	내PC지키미, UEM

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
20	N2SF-IS-1	단말	OS 기반 논리적 분리 환경을 적용	업무·외부 환경 간 데이터 직접 이동 차단	RBI, VDI: Cloud 환경
21	N2SF-IS-4	단말	방화벽(FW)·NAC·OS 분리를 통해 단말 환경 분리	환경 간 접근 시 인증 절차 재수행	VLAN, 방화벽(FW), NAC 기반 업무망·인터넷망 분리,
22	N2SF-IS-6	단말	논리적 분리 OS 환경을 운영	분리 정책 위반 시 자동 차단	SIEM, EDR
23	N2SF-SG-2	단말	보안 OS 기반 단말 사용 정책 적용	비인가 OS 사용 시 접속 제한	VDI (논리적 분리)
24	N2SF-SG-3	단말	보안 OS 기반 단말 사용 정책 유지	OS 무결성 점검 정기 수행	VDI (논리적 분리)
25	N2SF-SG-4	단말	망분리 솔루션 및 OS 분리 운영	업무용·외부용 OS 간 직접 통신 차단	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
26	N2SF-SG-6	단말	일반 사용자 단말과 특권 사용자 단말 분리	특권 단말은 별도 보안 정책 적용	PDP (ICAM)
27	N2SF-AC-1	연계체계	PDP(ICAM) 기반 계정관리 자동화 체계 적용	계정 생성·변경·삭제를 자동 처리하고 수동 개입 최소화	PDP (ICAM)
28	N2SF-AC-1(1)	연계체계	PDP(ICAM) 기반 계정 생명주기 관리	계정 상태 변화 시 권한 변경 이력을 자동 기록	PDP (ICAM)
29	N2SF-AC-1(2)	연계체계	PDP(ICAM)을 통한 계정 상태 모니터링	활성·휴면·임시 계정을 실시간 점검	PDP (ICAM)
30	N2SF-AC-1(3)	연계체계	PDP(ICAM) 기반 계정 상태 추적	비정상 상태 계정에 대해 관리자 알림 수행	PDP (ICAM)
31	N2SF-AC-1(4)	연계체계	ICAM·애플리케이션 연계 계정 관리	비활동 시간 초과 시 RBI를 통해 강제 로그아웃	PDP (ICAM), RBI

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
32	N2SF-AC-1(4)	연계체계	기존 시스템과 ICAM 통합 계정 관리	장시간 미사용 세션을 자동 종료	PDP (ICAM), 내 PC 지키미, UEM
33	N2SF-AC-1(5)	연계체계	ICAM 기반 계정 관리 시스템화	계정 현황을 중앙에서 일관되게 관리	PDP (ICAM)
34	N2SF-AC-3	연계체계	보안솔루션 및 ICAM 연계 계정 모니터링	의심 계정 발생 시 관리자 검토 및 조치	PDP (ICAM), UEBA, EDR SIEM
35	N2SF-AC-3(1)	연계체계	UEM·ICAM 기반 계정 위험 연계 통제	단말 위험 탐지 시 계정 연결 즉시 차단	PDP (ICAM), UEM, NAC
36	N2SF-AC-3(2)	연계체계	ICAM 을 통한 내부 계정 상시 모니터링	내부 계정 활동 로그를 주기적으로 점검	PDP (ICAM), UEM, DLP
37	N2SF-AC-M1	연계체계	UEM·ICAM 기반 자동 감사 체계 적용	감사 대상 이벤트 자동 수집 및 관리	PDP (ICAM), UEM
38	N2SF-AC-M2	연계체계	UEM·ICAM 연계 감사 로그 관리	감사 로그를 생성·보관하고 위변조 방지	PDP (ICAM), UEM, SIEM
39	N2SF-AC-M3	연계체계	시스템 로그 기반 사용 이력 관리	로그를 주기적으로 검토하여 이상 여부 확인	PDP (ICAM), UEM, SIEM
40	N2SF-SG-M5	업무 시스템	분리정책 위반 시, 경고, 세션 차단등을 자동 수행	자동감시-경고-차단-기록등 3 단계 업무 자동 수행	ICAM, SOAR
41	N2SF-AM-2	연계체계	PDP(ICAM) 기반 기본 인증 체계 적용	사용자 인증 정책을 중앙에서 일관되게 운영	PDP (ICAM)
42	N2SF-AM-9	연계체계	ICAM 기반 소유기반 MFA 인증 적용	MFA 미적용 계정은 접근 제한	2 Factor 인증 (생체인증, 모바일 인증, OTP 등)
43	N2SF-DT-1	연계체계	UEM·ICAM 연계 권한 검증 체계 적용	권한 미보유 사용자의 접근을 즉시 차단	PDP (ICAM), UEM, NAC
44	N2SF-IF-M5	연계체계	ICAM 기반 예외 상황 대응 체계 마련	예외 발생 시 승인·조치 이력 기록	보안정책 및 관리적 보안

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
45	N2SF-IN-1(1)	연계체계	PDP(ICAM)을 통한 자산(단말·사용자·서버) 등록 관리	등록되지 않은 자산 접근 차단	ICAM, 내PC지키미, UEM, VDI, PMS
46	N2SF-LI-1	연계체계	인증 채널 암호화 정책 적용	암호화 미적용 채널 접속 차단	PDP (ICAM)
47	N2SF-LI-2	연계체계	로그인 실패 제한 정책 운영	실패 횟수 초과 시 계정 잠금	PDP (ICAM)
48	N2SF-LI-M1	연계체계	로그인 실패·의심 패턴 탐지 체계 적용	실시간 탐지 후 관리자 알림	PDP (ICAM)
49	N2SF-LI-M2	연계체계	ICAM 기반 계정 사용 이력 점검	계정 설정·사용 이력을 정기 검토	PDP (ICAM)
50	N2SF-LP-1	연계체계	ICAM 기반 접근권한 중앙 관리	권한 부여·변경 시 승인 절차 적용	PDP (ICAM)
51	N2SF-LP-4	연계체계	계정·권한 시스템화 관리	역할 기반 권한 원칙(RBAC) 유지	PDP (ICAM)
52	N2SF-LP-4(1)	연계체계	RBI 기반 제한된 서버 접근 환경 구성	관리자·사용자 접근을 RBI로 제한	RBI
53	N2SF-LP-4(4)	연계체계	ICAM 기반 관리자 사용 이력 추적	관리자 명령·접속 로그를 감사에 활용	PDP (ICAM), SIEM
54	N2SF-LP-M1	연계체계	ICAM 기반 권한관리 자동화	권한 변경 시 자동 기록 및 검증	PDP (ICAM)
55	N2SF-LP-M2	연계체계	ICAM·RBI 연계 권한 사용 현황 모니터링	이상 권한 사용 시 즉시 조치	PDP (ICAM)
56	N2SF-SN-1	연계체계	ICAM·RBI 연계 세션 관리 체계 적용	세션 종료 후 재접속 시 재인증	PDP (ICAM), UEM, DLP, RBI, DRM 등
57	N2SF-WA-7	연계체계	WIPS 기반 무선망 보호 체계 적용	비인가 무선 AP·단말 탐지 및 차단	WIPS

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
58	N2SF-CD-1	네트워크	망연계 솔루션을 통한 네트워크 간 데이터 연계 통제	연계 경로·전송 대상·방식에 대한 사전 정의 및 승인	망연계 솔루션 (CDS)
59	N2SF-CD-2	네트워크	다단계 보안 레이블 적용을 통한 정보보안	전송 정보에 대한 보안등급 태깅후, 기준에 부합되는 경우에만 전달	DLP, FDR
60	N2SF-CD-5	네트워크	망연계 솔루션 기반 데이터 흐름 제어	비인가 전송 시 자동 차단 및 로그 기록	CDS, SWG, RBI
61	N2SF-EB-1	네트워크	업무망·인터넷망 망분리 및 네트워크 보안 솔루션 적용	외부 연결 접점 최소화 및 정책 기반 관리	Web Filtering, RBI, DLP, 방화벽(FW), SWG
62	N2SF-EB-10	네트워크	방화벽(FW) 등 네트워크 보안장비 적용	외부에서 내부로의 직접 접근 전면 차단	Routing, Subnet, 방화벽(FW) 정책
63	N2SF-EB-11	네트워크	네트워크 경계 보안장비 운영	외부 위협 대응 정책 상시 유지 및 점검	Anti-DDoS, 방화벽(FW), Network IPS, WAF 이중화 구성
64	N2SF-EB-13	네트워크	오류 정보 전송 통제 정책 적용	DLP 기반 오류 메시지 탐지 및 발신 차단	DLP
65	N2SF-EB-14	네트워크	DNS 접근 통제 정책 적용	인가된 DNS 서버만 사용하도록 강제	내 PC 지키미, UEM 방화벽(FW), SWG (유해사이트 차단)
66	N2SF-EB-15	네트워크	UEM·ICAM·RBI 연계 우회통신 탐지	비인가 터널링 탐지 시 즉시 차단	EDR, SWG (유해사이트 차단)

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
67	N2SF-EB-2	네트워크	네트워크 보안 솔루션 기반 접근 제어	정책 위반 트래픽 차단 및 로그 기록	방화벽(FW), Web Filtering, SWG (유해사이트 차단), RBI 솔루션 및 Proxy 서버, Gateway 네트워크 구성
68	N2SF-EB-3	네트워크	RBI 기반 내부 시스템 접근 통제	허용된 시스템만 접속 가능하도록 제한	PDP (ICAM), UEM, Web Filtering, NAC, RBI, SWG (유해사이트 차단)
69	N2SF-EB-4	네트워크	VPN 및 RBI 기반 원격접속 체계 적용	인증된 사용자만 제한적 접속 허용	VPN, RBI
70	N2SF-EB-5	네트워크	RBI 기반 외부 접근 통제 및 문서중앙화 연계	내부 저장 시 문서중앙화 솔루션 강제	PDP (ICAM), UEM, RBI
71	N2SF-EB-6	네트워크	방화벽(FW) 등 보안솔루션 기반 네트워크 통제	이상 트래픽 발생 시 즉시 차단	방화벽(FW), Web Filtering, EDR, SWG (유해사이트 차단)
72	N2SF-EB-8	네트워크	물리적 보안 및 매체제어 장치 적용	운영 포트에 비인가 장치 연결 차단	매체제어 솔루션
73	N2SF-EB-9	네트워크	보안 OS 기반 내부·외부 OS 분리	OS 간 직접 통신 차단	VDI, Secure OS
74	N2SF-EB-M1	네트워크	문서 검사 솔루션 기반 개인정보 보호	개인정보 포함 전송 시 자동 차단	DLP, 문서검사 솔루션
75	N2SF-EB-M3	네트워크	외부 통신 로그 수집 및 관리	VPN 등 외부 통신 로그 정기 검증	방화벽(FW), Network IPS, WAF, DLP, RBI, SIEM 등

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
76	N2SF-EB-M4	네트워크	정책엔진 기반 이상행위 탐지	이상 행위 탐지 시 자동 차단 또는 경고	DLP, NDR
77	N2SF-EB-M5	네트워크	침해 대응 네트워크 차단 절차 마련	침해 발생 시 외부 통신 즉시 차단	방화벽(FW)
78	N2SF-IF-1	네트워크	메인·DMZ 방화벽(FW) 흐름 통제	정책 기반 트래픽 흐름 관리	방화벽(FW), Network IPS, WAF, SWG, DLP, EDR
79	N2SF-IF-10	네트워크	허용 사이트·프로토콜 기반 통신 통제	문서중앙화 연계로 정보유출 방지	방화벽(FW), Network IPS, WAF, DLP
80	N2SF-IF-11	네트워크	문서중앙화 망 분리 운영	업무망·인터넷망 간 데이터 직접 이동 차단	문서중앙화 솔루션
81	N2SF-IF-14	네트워크	정보취급 환경 분리 운영	망·OS·저장 영역 간 분리 정책 유지	DRM, CDS
82	N2SF-IF-2	네트워크	SSL/TLS 가시성 기반 트래픽 통제	암호화 트래픽 검사 및 정책 적용	SSL/TLS Proxy, SSL 복호화 및 가시성
83	N2SF-IF-5	네트워크	망연계 솔루션 기반 데이터 흐름 제어	전송 이력 기록 및 감사 활용	CDS
84	N2SF-IF-6	네트워크	문서 검사·문서중앙화 솔루션 적용	문서 이동·반출 흐름 통제	문서 검사/문서 중앙화 솔루션
85	N2SF-IF-7	네트워크	망연계 기반 데이터 흐름 관리	비인가 흐름 탐지 및 차단	CDS
86	N2SF-IF-8	네트워크	문서 검사 솔루션 적용	문서 내 민감정보 탐지 및 차단	DLP, Web Filtering, DRM, 매체제어 솔루션
87	N2SF-IF-9	네트워크	NAC 기반 네트워크 인증 적용	단말 인증 및 문서 접근 권한 검증	SWG (유해사이트 차단), NAC
88	N2SF-IF-M1	네트워크	정보흐름 통제 정책 수립	통제 기준·예외 절차 문서화 및 정기 갱신	보안정책 및 관리적 보안

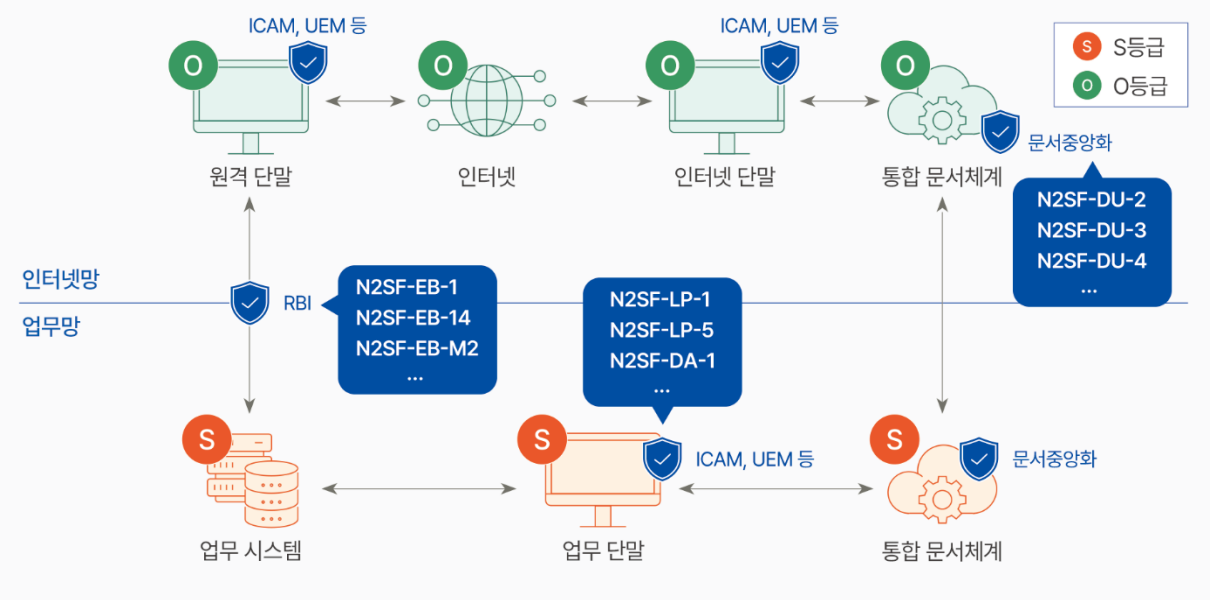
No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
89	N2SF-IF-M4	네트워크	보안 우회·비정상 흐름 탐지 체계	우회 시도 탐지 시 관리자 알림	DLP, NAC, SIEM
90	N2SF-SG-4	네트워크	망분리 솔루션 및 OS 분리 운영	업무용·외부용 환경 간 통신 차단	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
91	N2SF-SG-5	네트워크	방화벽(FW) 기반 영역 분리	서버·DMZ·업무 PC 영역 간 접근 통제	방화벽(FW), VLAN/NAC 기반 단말 구역 분리, 망분리 솔루션
92	N2SF-DU-2	시스템	중요·개인정보 암호화 저장 정책 적용	저장 시 암호화 강제 및 키 관리	DB 암호화, DRM
93	N2SF-DU-3	시스템	단말 보안 솔루션 적용	백신·패치 상태 정기 점검	PC 보안 솔루션, UEM
94	N2SF-DU-4	시스템	문서중앙화 데이터 자동 삭제 정책	인터넷망 데이터 1일 주기 삭제	문서중앙화 솔루션
95	N2SF-DU-M1	시스템	내부 시스템 접근권한 관리	권한 주기적 검토 및 조정	PDP (ICAM)
96	N2SF-DU-M2	시스템	시스템 사용 이력 점검 체계 적용	이상 징후 발견 시 즉각 대응	UEBA, SIEM
97	N2SF-DU-M3	시스템	데이터 관리 정책 수립	정책 문서화 및 전사 적용	보안정책 및 관리적 보안
98	N2SF-EK-1	시스템	문서중앙화 자체 암호화 기능 활용	암호화 설정 상시 유지	문서 중앙화 솔루션
99	N2SF-IF-3	시스템	문서중앙화 운영 및 첨부 이력 관리	첨부·반출 기록 로깅	문서 중앙화 솔루션
100	N2SF-IF-M2	시스템	시스템 사용 로그 관리	로그 보관 및 감사 활용	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건	적용 보안 솔루션
101	N2SF-IF-M3	시스템	시스템 사용 로그 관리	로그 무결성 유지 및 점검	방화벽(FW), Network IPS, WAF, DLP, SWG, RBI, DRM, NAC, EDR, 매체제어 솔루션 및 SIEM 등
102	N2SF-LI-4	시스템	계정 잠금 해제 시 MFA 적용	추가 인증 완료 후 잠금 해제	PDP (ICAM)
103	N2SF-RA-1	통합문서 체계	문서작업이력 기록 및 관리	실시간 모니터링을 통한 보안 통제	VDI, SIEM, NMS, ICAM
104	N2SF-SG-M1	관리	내부 보안 정책 수립	정책 승인·배포·이행 관리	보안정책 및 관리적 보안
105	N2SF-SG-M3	관리	주기적 보안점검 수행	취약점 발견 시 조치 및 이력 관리	보안정책 및 관리적 보안

(나) 자체정의 보안통제 구현계획

No.	보안통제 항목	적용 대상	보안통제 적용방안	보안통제 구현·운영 요건
1	N2SF-ORG4-1	단말	단말 내 데이터가 로컬 저장소에 상시 잔존하지 않도록 로컬파일 생성 및 저장을 제한	단말 내 생성된 파일을 주기적으로 자동 삭제하거나 세션 종료 시 로컬 저장 데이터를 초기화하도록 운영
2	N2SF-ORG4-2	단말	단말 접속이 허용된 사용환경(OS, 네트워크, 위치 등)을 사전에 정의하고 승인된 환경에서만 접속을 허용	승인되지 않은 단말 환경에서 접속 시 자동 차단하고, 환경 변경 시 재승인 절차를 적용하여 관리

6.3 정보서비스 적용 기관 망 구성도 예시



수립한 보안 요구사항 및 보안통제 항목 구현 사항 등 산출물을 토대로 국가정보원 보안성 검토 신청 시, N2SF를 적용한 기관의 실제 망 구성도를 작성하여 첨부하여야 한다

04

참고자료

KISA 한국인터넷진흥원

1. 참고자료

No.	목록	게시일
1	국가 망 보안체계 가이드라인 1.0	2025.9
1-1	(부록 1) 보안통제 항목 해설서	2025.9
1-2	(부록 2) 정보서비스 모델 해설서(11 종)	2025.9
1-2-1	모델 1. 인터넷 단말의 업무 활용성 제고	2025.9
1-2-2	모델 2. 업무환경에서 생성형 AI 활용	2025.9
1-2-3	모델 3. 외부 클라우드 활용 업무협업 체계	2025.9
1-2-4	모델 4. 업무 단말의 인터넷 이용	2025.9
1-2-5	모델 5. 공공 데이터의 외부 AI 융합	2025.9
1-2-6	모델 6. 연구 목적 단말의 신기술 활용	2025.9
1-2-7	모델 7. 개발 환경 편의성 향상	2025.9
1-2-8	모델 8. 클라우드 기반 통합문서체계	2025.9
1-2-9	모델 9. 모바일 업무환경 정보 연계	2025.9
1-2-10	모델 10. 무선 업무환경 운용 체계	2025.9
1-2-11	모델 11. 정보 연계를 위한 CDS 구성	2025.9
2	국가 망 보안체계 이해 및 활용 안내	2026.3

국가 망 보안체계(N2SF)
실증 사례집

인 쇄 2026 년 4 월

발 행 2026 년 4 월

발행처 한국인터넷진흥원
전라남도 나주시 진흥길 9

KISA 한국인터넷진흥원