국가 망 보안체계(N2SF) 가이드라인

정보 서비스 모델 4: 업무단말의 인터넷 이용

1. **N2SF 정의 :** 각 기관의 업무정보 정보시스템을 식별하고 업무 중요도에 따라 **기밀(Classified), 민감(Sensitive), 공개(Open) 등급으로 분류**하여 등급별로 차등적인 보안통제를 적용하는 보안 프레임워크.

2. **기대효과 :** 공공기관에서의 **생성형AI, 클라우드, SaaS 등 신기술 활용에 따른 보안성 확보 토대 제시.**

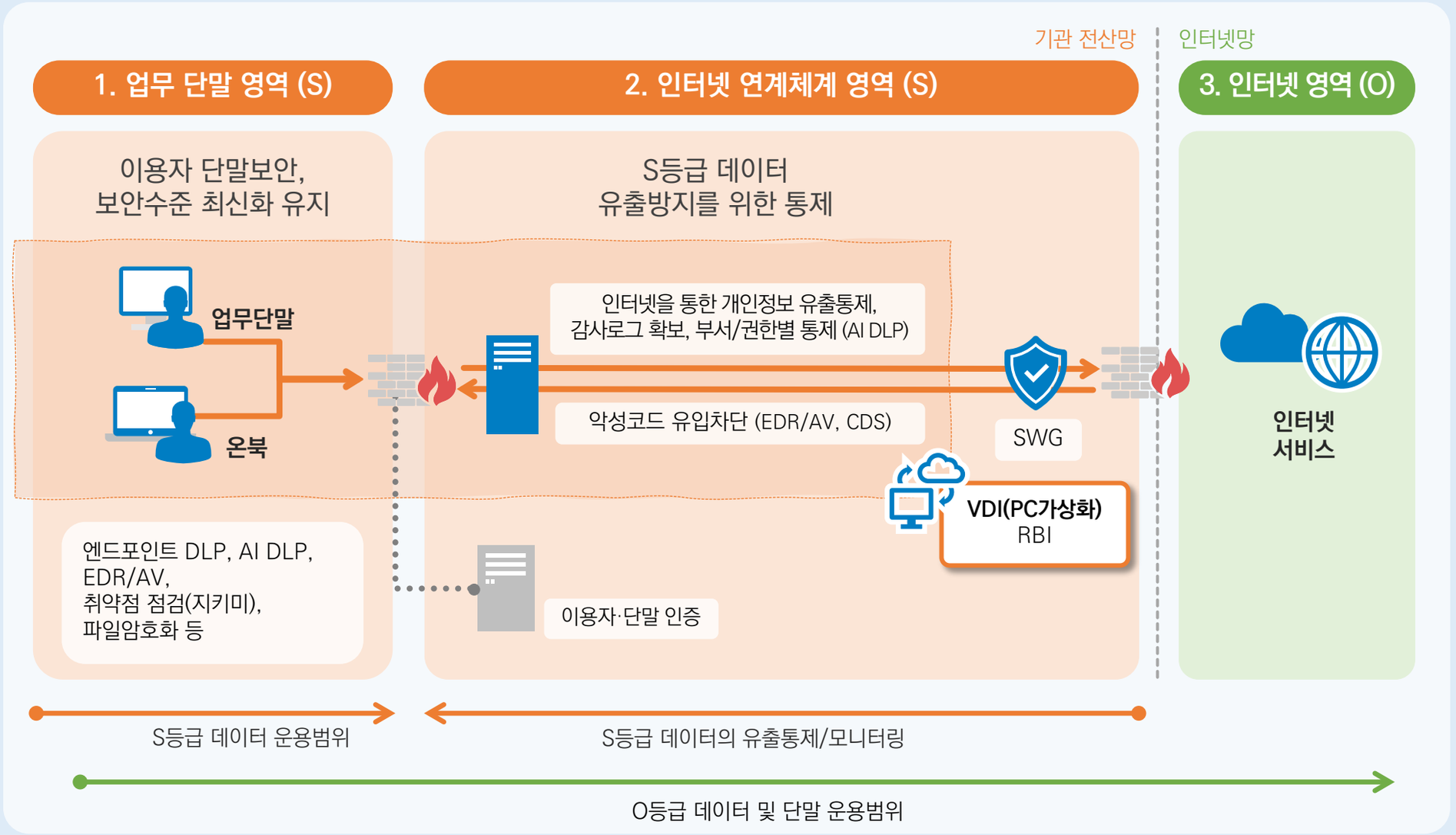
3. **11개 정보서비스 모델 해설서 제공 :**

   본 리포트는 〈모델4 : 업무단말의 인터넷 이용〉 대상으로 분석.

   *이용자 단말(업무단말, 온북)에서의 인터넷 서비스 접속/이용을 위한 보안 요구사항 해설서로, 이를 통해 업무 생산성, 효율성, 활용성 향상을 기대할 수 있음.

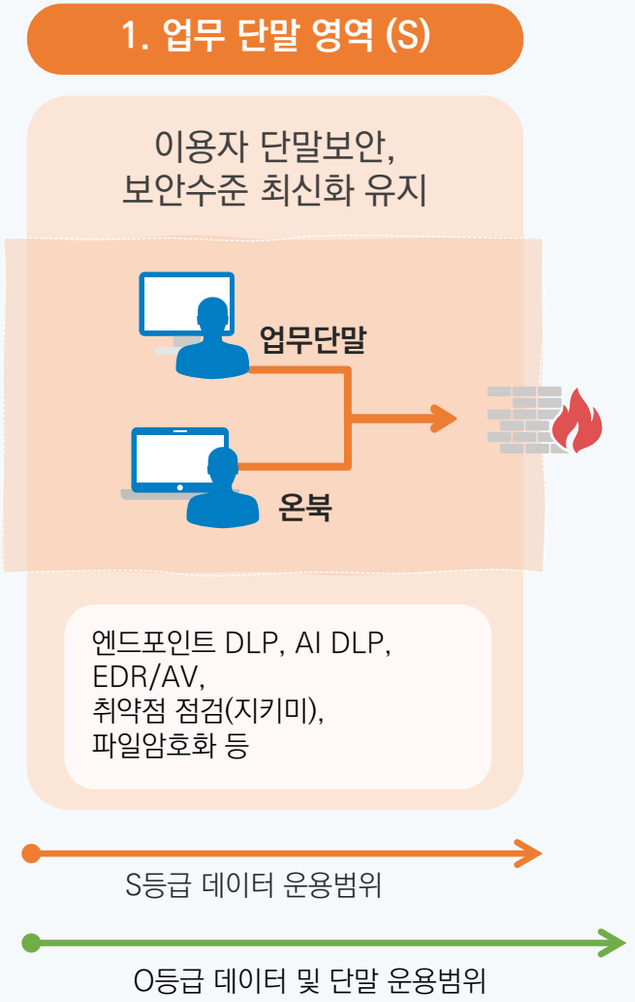
모델 4: 업무단말의 인터넷 이용

0. 기본 요약



모델 4: 업무단말의 인터넷 이용

1. 업무 단말 영역



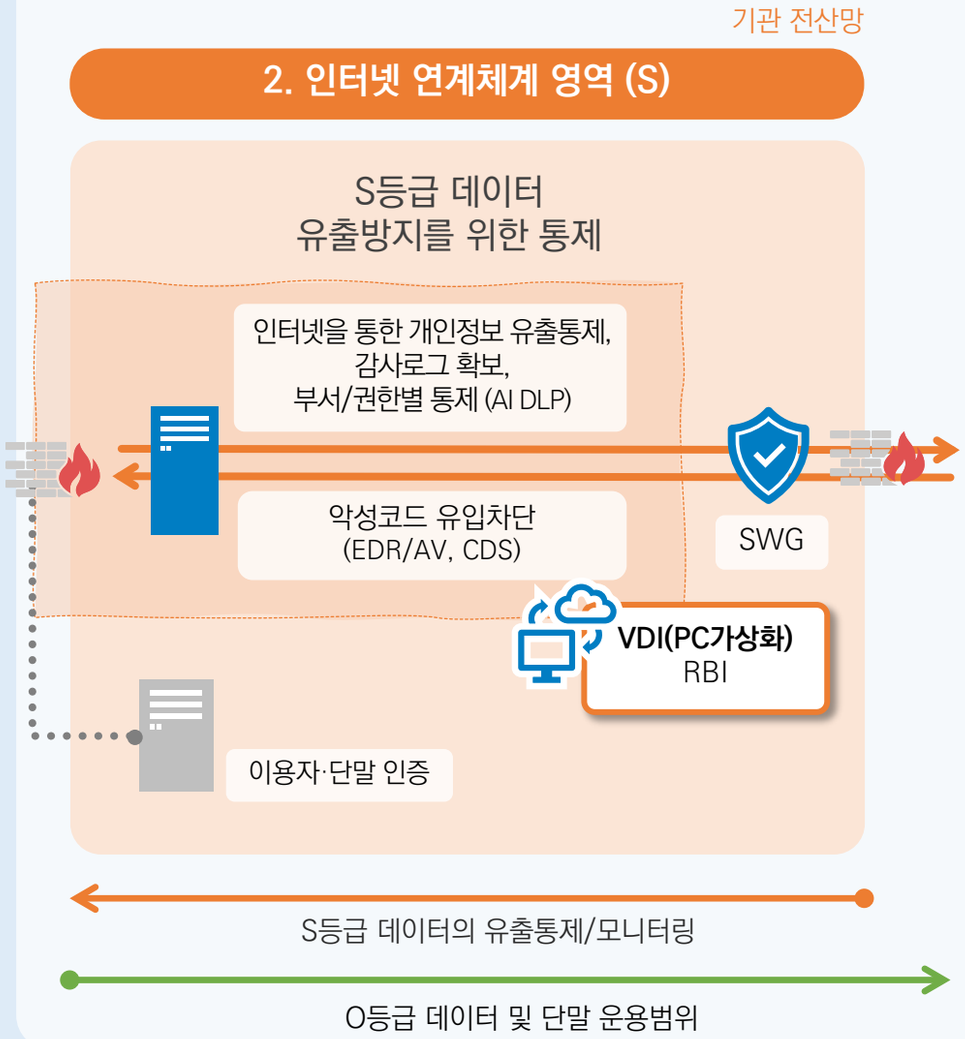
인터넷 이용을 허용하기 위해 이용자 단말(업무단말, 온북)에 적용해야 하는 보안조치

통제항목	기술적 보호조치
① 이용자 단말 보안성 유지	**엔드포인트DLP, VDI**(가상화) **내PC지키미, EDR/AV,** RBI
② 파일 직접 다운로드 차단	**SWG***(악성코드 배포사이트 차단)**, VDI,** RBI
③ 이용자 단말사용 보안	**내PC지키미, 엔드포인트DLP**
④ 이용자 단말 네트워크 보안	**엔드포인트 DLP, AI DLP** (네트워크), **SWG** (유해/비업무사이트 차단)**, VDI,** RBI
⑤ 이용자 단말 내 데이터 보호	**엔드포인트 DLP** (매체제어, 출력물보호, 파일암호화)
⑥ 인터넷 서비스 활용 이용자/단말관리 정책	**AI DLP** (네트워크), **엔드포인트 DLP**

*Secure Web Gateway

모델 4: 업무단말의 인터넷 이용

2. 인터넷 연계체계 영역



S등급 데이터는 통제하고
O등급 데이터는 허용하며
인터넷 서비스를 활용할 수 있도록
내부망에 적용해야 하는 보안조치

통제항목	기술적 보호조치
① 인터넷서비스 이용자/단말인증	**AI DLP,** 계정관리 (AD)
② 비인가 네트워크 연결차단	**SWG** (유해/비업무 사이트 차단), **VDI** (가상화), RBI
③ 인터넷 서비스 활용 시 데이터보호	**AI DLP,** CDS
④ 외부 비인가 접근, 악성콘텐츠 유입차단	**EDR/AV**, CDS
⑤ 연계체계 보안성 유지	관리적 조치
⑥ 연계체계 운용 관리	

모델 4: 업무단말의 인터넷 이용

3. 물리적 망분리 – VDI – RBI 비교

구분	물리적 망분리	VDI (PC 가상화)	RBI (브라우저 격리)
보안성	● 가장 높음	◎ 높음	○ 높음 (브라우저에 국한)
활용성	데스크탑 전체기능 활용. 카카오톡 등 상용메신저 사용, 유튜브 등 스트리밍 서비스 시청, 문서 편집, 웹검색 모두 가능	데스크탑 전체기능 활용. 카카오톡 등 상용메신저 사용, 유튜브 등 스트리밍 서비스 시청, 문서 편집, 웹검색 모두 가능	웹 브라우저를 통한 활용에 국한. 메신저, 문서 편집 불가, 유튜브 등 스트리밍 서비스 시청 제약
편의성	인터넷을 사용하기 위해서는 물리적으로 두대의 PC사이 망 전환 작업이 필요	소프트웨어적으로 구성되어 업무망과 인터넷망 전환이 손쉬움 소규모 Text 데이터의 경우(예:1Kb) 업무용 PC와 인터넷 PC 간 데이터 공유 용이 (예: 복사 및 붙여넣기)	소프트웨어적으로 구성되어 업무망과 인터넷망 전환이 손쉬움
인터넷 접속단말 제약성	본인 자리, 본인 PC에서만 인터넷 접속가능	사내 어느 PC에서나 인터넷 접속 가능	사내 어느 PC에서나 인터넷 접속 가능
단말 보호조치	(간소화된) AV + EDR + 내PC지키미	AV + EDR + 내PC지키미 보호조치 필요	AV + EDR + 내PC지키미 보호조치 필요

모델 4: 업무단말의 인터넷 이용

4. 보안 요구사항 별 기술적 보호조치 요약

영역	보안요구사항	기술적 보호조치
1. 업무 단말 영역	① 이용자 단말 보안성 유지	**엔드포인트DLP, VDI**(가상화), **내PC지키미, EDR/AV,** RBI
	② 파일 직접 다운로드 차단	**SWG**(악성코드 배포사이트 차단), **VDI,** RBI
	③ 이용자 단말사용 보안	**내PC지키미, 엔드포인트DLP**
	④ 이용자 단말 네트워크 보안	**엔드포인트 DLP, AI DLP** (네트워크), **SWG** (유해/비업무 사이트 차단), **VDI,** RBI
	⑤ 이용자 단말 내 데이터 보호	**엔드포인트 DLP** (매체제어, 출력물보호, 파일암호화)
	⑥ 인터넷 서비스 활용 이용자/단말관리 정책	**AI DLP** (네트워크), **엔드포인트 DLP**
2. AI 연계체계 영역	① 인터넷서비스 이용자/단말인증	**AI DLP,** 계정관리 (AD)
	② 비인가 네트워크 연결차단	**SWG** (유해/비업무 사이트 차단), **VDI** (가상화), RBI
	③ 인터넷 서비스 활용 시 데이터보호	**AI DLP,** CDS
	④ 외부 비인가 접근, 악성콘텐츠 유입차단	**EDR/AV**, CDS
	⑤ 연계체계 보안성 유지	관리적 조치
	⑥ 연계체계 운용 관리	

모델 4: 업무단말의 인터넷 이용

5. 업무단말 인터넷 활용 기술적 보호조치 퀵가이드

통제항목	기술적 보호조치
1. 엔드포인트 업무단말 악성코드 유입통제	AV/EDR
2. 엔드포인트 업무단말 개인정보 유출통제/매체제어/파일암호화	엔드포인트 DLP
3. 엔드포인트 업무단말 취약점 점검/PC보안	내PC지키미
4. 개인정보 유출 실시간 차단	AI DLP
5. 업무단말의 인터넷 이용 감사로그 확보	AI DLP
6. 사용자/부서별 외부 인터넷 접근통제	AI DLP, VDI, RBI
7. 네트워크 악성코드 유입통제	SWG, CDS
8. 네트워크 격리	VDI, RBI
9. 유해사이트, 불필요 서비스 차단 등 네트워크 접근통제	SWG
10. 사용자 인증	Active Directory, 강화된 인증 솔루션 (2팩터 인증)

국가 망 보안체계에 따른 체계적인 업무단말 인터넷 활용 및 적용 방안은
소만사 프라이버시 컨설팅을 통해 구현하실 수 있습니다
privacy@somansa.com

참고자료

[국가사이버안보센터] 국가 망 보안체계(N2SF) 보안가이드라인 1.0

· (본문) 국가 망 보안체계 보안 가이드라인 1.0

· (부록2) 정보서비스 모델 해설서(11종)

https://www.ncsc.go.kr/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=218023&pageIndex=1&searchCnd2=

별첨 1. 보안통제

1) 업무단말(업무단말, 온북) 영역

목적 : 해킹/내부자 실수에 의한 단말기 내 정보탈취 및 악성코드 유입 사전예방

① 이용자 단말 보안성 유지

코드	보안통제항목	내용	기술적 보호조치
N2SF-LP-1	정보시스템 접근 권한 정의	업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.	**엔드포인트DLP** (그룹/서비스별 접근통제 정책 설정)
N2SF-DA-1	단말 무결성 검증	단말 내 신뢰 가능한 모듈(TPM 등)을 통한 구성정보(BIOS 설정정보, Disk 설치 정보 등) 등을 확인한다.	
N2SF-DA-2	정보서비스 식별 및 제한	인증절차를 통해 사전 승인한 정보서비스만을 활용하도록 제한한다.	
N2SF-DV-12	장치 펌웨어 업데이트 검증	펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.	**내PC지키미, VDI** (가상화), RBI
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.	
N2SF-IN-5	비인가 변경 방지	인가되지 않은 정보시스템 구성요소 변경을 방지한다.	
N2SF-IN-6	불필요한 구성요소 제거	필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.	

별첨 1. 보안통제

1) 업무단말(업무단말, 온북) 영역

목적 : 해킹/내부자 실수에 의한 단말기 내 정보탈취 및 악성코드 유입 사전예방

① 이용자 단말 보안성 유지

코드	보안통제항목	내용	기술적 보호조치
N2SF-IN-8	비인가 소프트웨어 실행 차단	허가되지 않은 소프트웨어(응용프로그램)가 실행되지 않도록 차단한다.	**내PC지키미** **VDI** (가상화) RBI
N2SF-IN-10	소프트웨어 설치 권한 제한	소프트웨어 설치 권한은 필요한 사용자에게만 부여한다.	
N2SF-SG-2	운영체제(OS) 기반 분리	하나의 시스템에 다수 OS가 존재하더라도, 각 운영체제는 서로 독립된 환경으로 분리되도록 구성한다.	
N2SF-SG-3	소프트웨어 기반 분리	소프트웨어 논리구조를 활용하여 기능이나 사용자의 실행 영역을 분리하며, 실행 파일 간 충돌이나 간섭을 차단한다.	
N2SF-IS-1	프로세스 격리	실행되는 각 프로세스(작업 또는 프로그램)가 다른 프로세스에 영향을 미치거나 간섭을 차단하기 위해 독립된 공간에서 실행한다.	
N2SF-IN-16	악성코드 감염 차단	악성코드 유입 및 실행 등으로 인한 악성코드 감염을 실시간 탐지하고 차단한다.	**EDR/AV**

별첨 1. 보안통제

1) 업무단말(업무단말, 온북) 영역

목적 : 해킹/내부자 실수에 의한 단말기 내 정보탈취 및 악성코드 유입 사전예방

② 파일 직접 다운로드 차단

코드	보안통제항목	내용	기술적 보호조치
N2SF-CD-5	파일 유형 기반 전송 정책	파일 확장자, MIME 타입, 내부 Magic Number 등을 기준으로 허용된 파일 유형만 송수신 허용하고 나머지는 격리 또는 삭제한다.	**SWG** (악성코드 배포사이트 차단) **VDI,** RBI
N2SF-IN-16	악성코드 감염 차단	악성코드 유입 및 실행 등으로 인한 악성코드 감염을 실시간 탐지하고 차단한다.	

③ 이용자 단말 사용 보안

코드	보안통제항목	내용	기술적 보호조치
N2SF-AM-2	비밀번호 기반 인증	숫자·문자·특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.	**내PC지키미**
N2SF-AM-9	소유기반 인증	생체인증, 모바일 인증 및 하드웨어 토큰 등을 활용한 인증체계를 적용한다.	2팩터 인증 (생체인증, 모바일 인증, OTP 등)
N2SF-DV-6	통신 기능이 포함된 저장장치 제한	**통신기능이 포함된 저장장치 사용을 제한**한다.	**엔드포인트 DLP** (매체제어) PC보안 솔루션
N2SF-DV-8	장치 자동 잠금	사용자가 **일정시간 이상 정보시스템을 사용하지 않거나 방치할 경우 잠금 기능을 활성화**하고, 화면에 표시되는 정보는 표출되지 않아야 한다.	**내PC지키미** 화면보호기 설정

별첨 1. 보안통제

1) 업무단말(업무단말, 온북) 영역

목적 : 해킹/내부자 실수에 의한 단말기 내 정보탈취 및 악성코드 유입 사전예방

④ 이용자 단말 네트워크 보안

코드	보안통제항목	내용	기술적 보호조치
N2SF-SG-4	IP체계	**서로 다른 영역 또는 정보자산(기능 등)별 IP체계를 분리**하고, 보안통제를 적용한다.	VDI (관리자망 망분리) RBI
N2SF-SG-5	보안·운영관리 인프라 분리	**보안·운영관리 인프라를 물리적으로 분리된 네트워크로 구성**하여 이외 정보시스템과 분리한다.	
N2SF-SG-6	보안 기능과 사용자 기능 분리	인증, 감사 및 **데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 애플리케이션 실행 등 사용자 기능을 분리**한다.	
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	**정보 전송 시** 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 **출발지점과 도착지점을 식별하고 인증**한다.	SWG (유해/비업무 사이트 차단)
N2SF-EB-6	외부로의 사이버위협 통신 발신 제한	내부에서 외부 **네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단**하고, **발신자(사용자 및 정보자산 등)를 식별**한다.	

별첨 1. 보안통제

1) 업무단말(업무단말, 온북) 영역

목적 : 해킹/내부자 실수에 의한 단말기 내 정보탈취 및 악성코드 유입 사전예방

④ 이용자 단말 네트워크 보안

코드	보안통제항목	내용	기술적 보호조치
N2SF-SN-1	로그아웃 세션 처리	로그아웃 또는 비정상 세션 종료 시 연결되었던 모든 세션의 식별자를 즉시 무효화하며, 더 이상 세션이 유효하지 않도록 한다.	SWG (유해/비업무 사이트 차단) **엔드포인트 DLP**
N2SF-WA-7	비인가 무선망 접속 차단	**인가되지 않은 무선망** 접속을 **차단**한다.	
N2SF-BC-1	블루투스 데이터 통신제한	**블루투스 장치 연결 시** 키보드, 마우스, 오디오 등을 위한 입출력 기능 외 **데이터 통신은 차단**한다.	
N2SF-DT-1	전송 권한 확인	**데이터가 전송되기 전**에 이를 처리하는 **개인이나 정보시스템**이 **적절한 권한**을 보유하고 있는지 확인한다.	**엔드포인트 DLP** **AI DLP** (그룹/서비스별 접근통제 정책설정, 개인정보유출 실시간 차단)

별첨 1. 보안통제

1) 업무단말(업무단말, 온북) 영역

목적 : 해킹/내부자 실수에 의한 단말기 내 정보탈취 및 악성코드 유입 사전예방

⑤ 이용자 단말 데이터 보호

코드	보안통제항목	내용	기술적 보호조치
N2SF-DU-2	데이터 암호화 저장	**데이터 대상 암호기술을 적용**하여 기밀성을 보장한다.	**엔드포인트 DLP** (개인/기밀정보 암호화)

⑥ 인터넷 서비스 활용 이용자 및 단말 관리

코드	보안통제항목	내용	기술적 보호조치
N2SF-LP-M1	특별권한 사용자 지정	일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.	**엔드포인트 DLP** **AI DLP** (권한별 계정설정, 개인정보 유출통제, 감사로그 저장)
N2SF-EB-M1	개인 식별정보 보호	외부와 통신 시 개인을 식별하거나 특정 개인과 관련된 정보를 포함하는 경우 노출되지 않도록 조치한다.	
N2SF-DU-M3	데이터 사용 정책 수립	데이터의 사용 목적, 접근 권한, 보존 기간, 폐기 절차 등을 포함하는 데이터 사용 정책을 문서화하고 전사적으로 적용 및 관리한다.	

별첨 1. 보안통제

2) 인터넷 연계체계 영역

목적 : 인가된 사용자의 인터넷 서비스 활용 보장, S등급 데이터 외부유출방지

① 인터넷 서비스 이용자 및 단말 인증

코드	보안통제항목	내용	기술적 보호조치
N2SF-AC-1	계정 관리 자동화	정보시스템 계정 관리를 효율화하고, 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정 관리를 수행한다.	AI DLP (그룹/서비스별 접근통제 정책설정, 개인정보유출 실시간 차단, 감사로그 저장, 이상징후 경보) 계정관리 (Active Directory)
N2SF-AC-1(1)	동적 계정 관리	사용자 상태(입사, 퇴사, 부서 이동 등)에 따라 계정 정보를 실시간으로 반영하고, 시스템 간 계정 동기화를 통해 계정 수명주기 관리를 자동화한다.	
N2SF-AC-1(2)	계정 상태 모니터링	계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.	
N2SF-AC-1(3)	계정 자동 비활성화	계정 사용 기간이 종료되거나 일정 기간 미사용된 계정은 자동으로 비활성화한다.	
N2SF-AC-1(4)	계정 자동 로그아웃	비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.	
N2SF-AC-3	의심스러운 계정 모니터링	비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.	

별첨 1. 보안통제

2) 인터넷 연계체계 영역

목적 : 인가된 사용자의 인터넷 서비스 활용 보장, S등급 데이터 외부유출방지

① 인터넷 서비스 이용자 및 단말 인증

코드	보안통제항목	내용	기술적 보호조치
N2SF-AC-3(2)	내부 사용자 모니터링	내부 사용자의 계정 사용 및 활동을 지속적으로 모니터링한다.	AI DLP (그룹/서비스별 접근통제 정책설정, 개인정보유출 실시간 차단, 감사로그 저장, 이상징후 경보) 계정관리 (Active Directory)
N2SF-DA-3	단말 식별 및 인증	단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증을 통해 시스템에 접근할 수 있도록 한다.	
N2SF-DA-4	인증된 단말의 접속 관리	인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.	
N2SF-LI-1	유효한 인증정보 노출 방지	인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.	
N2SF-LI-2	로그인 실패에 따른 접속 제한	정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.	
N2SF-LI-4	계정 잠금 해제 인증요소 추가	계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.	

별첨 1. 보안통제

2) 인터넷 연계체계 영역

목적 : 인가된 사용자의 인터넷 서비스 활용 보장, S등급 데이터 외부유출방지

② 비인가 네트워크 연결 차단

코드	보안통제항목	내용	기술적 보호조치
N2SF-IS-4	네트워크 격리	**내부망, 외부망, 보안망** 등 **네트워크 간에** **방화벽, 라우팅 제어 등으로 트래픽을 분리**하여 **정보 유출 또는 확산을 방지**한다.	**VDI** (논리적 망분리) RBI
N2SF-IF-1	정보흐름의 동적 통제	정보시스템의 **비정상 동작, 외부의 공격** 등 지정한 조건에 대하여 정보흐름을 **동적으로 통제**한다.	**SWG** (유해/비업무 사이트 차단)
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	**정보 전송 시** 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 **출발지점과 도착지점을 식별하고 인증**한다.	
N2SF-EB-1	연결 접점 제한	정보시스템의 외부 네트워크 연결 접점 수를 제한한다.	
N2SF-EB-2	서비스별 외부통신 통제	**외부와 통신하는 서비스**의 경계마다 **통신흐름을 통제**한다.	

별첨 1. 보안통제

2) 인터넷 연계체계 영역

목적 : 인가된 사용자의 인터넷 서비스 활용 보장, S등급 데이터 외부유출방지

② 비인가 네트워크 연결 차단

코드	보안통제항목	내용	기술적 보호조치
N2SF-EB-3	화이트리스트 기반 통신 허용	기본적으로 모든 통신을 차단한 상태에서 **필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용**한다.	SWG (유해/비업무 사이트 차단)
N2SF-EB-5	통신 경유(proxy) 강제화	**인가된 정보시스템을 경유하여 통신**하도록 **통신경로를 강제화**한다.	
N2SF-EB-6	외부로의 사이버위협 통신 발신 제한	내부에서 **외부 네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단**하고, 발신자(사용자 및 정보자산 등)를 식별한다.	
N2SF-EB-14	외부 DNS 통신 제한	**인가된 DNS 서버** 외의 요청을 차단한다.	
N2SF-EB-15	우회 통신 수단 탐지 및 차단	**VPN, Tor 등 우회 경로 사용을 탐지하고 차단**한다.	

별첨 1. 보안통제

2) 인터넷 연계체계 영역

목적 : 인가된 사용자의 인터넷 서비스 활용 보장, S등급 데이터 외부유출방지

③ 인터넷 서비스 활용 시 데이터 보호

코드	보안통제항목	내용	기술적 보호조치
N2SF-IF-2	암호화된 정보흐름 통제	**암호화된 정보의 내용을 확인하기 위하여 정보를 복호화하거나, 확인이 불가능한 암호화된 정보는 흐름을 차단**하는 등의 조치를 적용한다.	AI DLP (전송 데이터 원본저장, 파일 내 개인정보 포함 시 실시간 차단, 이상징후 탐지)
N2SF-IF-6	필터링 규칙 정보흐름 통제	**보안 및 프라이버시 등에 관한 필터링 규칙을 적용**하여 정보흐름을 통제한다.	
N2SF-IF-7	데이터 유형 식별자 통제	**서로 다른 영역 간에 정보를 전송하는 경우 데이터 유형 식별자를 확인하여 전송 여부를 통제**한다.	
N2SF-IF-8	인가되지 않은 정보 전송 통제	**인가되지 않은 정보가 포함되었는지 검사하고 보안정책에 따라 해당 정보의 전송을 차단**한다.	
N2SF-IF-10	정보 전송 방식 제한	정보 전송 시 특정 매체나 방식만 허용하고 나머지는 차단한다.	
N2SF-IF-14	보안등급 기반 흐름 통제	보안등급에 따라 정보 흐름을 제한하여 상위 등급에서 하위 등급으로의 부적절한 전송을 차단한다.	AI DLP CDS

별첨 1. 보안통제

2) 인터넷 연계체계 영역

목적 : 인가된 사용자의 인터넷 서비스 활용 보장, S등급 데이터 외부유출방지

④ 외부 비인가 접근 및 악성 콘텐츠 유입 차단

코드	보안통제항목	내용	기술적 보호조치
N2SF-IF-3	임베디드 데이터 삽입 차단	임베디드된 데이터 내부에 인가되지 않은 다른 종류의 데이터가 삽입되는 것을 차단한다.	EDR/AV
N2SF-IF-5	일방향 정보흐름 통제	일방향 전송 장치를 통해 단방향 정보 흐름만 허용하고 반대 방향 흐름을 차단한다.	CDS

*⑥연계체계 보안성 유지, ⑦연계체계 운용관리는 기본적 관리 보안조치에 해당되므로 생략

별첨 2.

C/ S / O 등급 분류체계

등급	분류기준	비고
기밀 (C)	▸ 제1호: 법률상 비밀·비공개로 규정 ▸ 제2호: 안보·국방·통일·외교 관련 공개 시 국익 저해 ▸ 제3호: 공개 시 국민 생명·신체·재산보호에 현저한 지장초래 ▸ 제4호: 진행 중 재판 및 범죄예방·수사·공소·형집행·교정 관련 정보로, 공개 시 현저한 직무수행 곤란 및 피고인 재판권 침해	정보 공개법 공공 데이터 법
민감 (S)	**▸ 제5호: 감사·감독·검사·시험·입찰계약·기술개발·인사관리 및 의사결정·내부검토 관련 정보로, 공개 시 공정한 업무수행, 연구개발 등에 현저한 지장** **▸ 제6호: 성명·주민번호 등 개인정보로, 공개 시 사생활 침해** **▸ 제7호: 법인·단체·개인의 경영상·영업상 비밀로, 공개 시 이익 침해** ▸ 제8호: 공개 시 부동산투기, 매점매석으로 특정인에게 이익·불이익	
	▸ 기 타: 로그 및 임시백업 등	
공개 (O)	▸ 기밀(C)·민감(S) 정보 이외의 정보	
	▸ 관련 법령 등에서 규정하는 요건을 충족한 비공개 정보 또는 기간의 경과 등으로 비공개 필요성이 소멸된 정보	