부록 1

Draft

국가 망 보안체계 보안 가이드라인

보안통제 항목 해설서

2025. 1

국가정보원

NSR 국가보안기술연구소

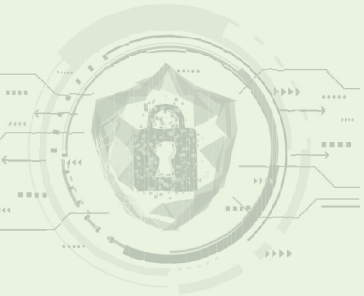
부록 1

Draft

국가 망 보안체계
보안 가이드라인

보안통제 항목 해설서

2025. 1



국가 망 보안체계
보안 가이드라인
보안통제 항목 해설서

부록 1

문서이력

개정일	버전	내역	비고
2025.1.	Draft	「국가 망 보안체계 보안 가이드라인_보안통제 항목 해설서」 발간	

CONTENTS

제4장 통제

제5장 데이터

제6장 정보자산

보안통제 항목 종합

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
권한	최소권한 Least Privilege (LP)	NNSF-LP-1	정보시스템 접근 권한 정의	업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.	●	●	
		NNSF-LP-2	보안통제 권한 제한	보안통제 권한은 정보보안담당관(자) 또는 이에 준하는 관리권한을 부여받은 인원에게만 부여한다.	●	●	●
		NNSF-LP-3	보안통제 계정 노출 방지	보안통제 권한 목적으로 사용되는 계정과 이외 기능에 사용되는 계정은 중복 사용하지 않도록 보안통제 권한 계정의 노출을 방지한다.	●	●	●
		NNSF-LP-4	원격접속을 통한 관리자 권한 접속제한	기관 네트워크 내부에서 관리자 권한 접속이 제한되는 경우 등 불가피한 상황에서만 한시적으로 기관 네트워크 외부에서의 관리자 권한 접속을 허용하며, 목적이 달성된 경우 외부에서의 관리자 권한 접속을 즉시 차단한다.	–	●	●
		NNSF-LP-5	관리자 권한 제한	정보시스템 관리자 권한은 관리자 및 운영자 등 최소한의 인원에게만 부여한다.	●	●	
		NNSF-LP-6	기관 이외 인원의 관리자 권한 제한	기관 구성원 이외 인원에게 관리자 권한은 부여하지 않으며, 다만 정보보안 감사, 사이버보안 실태평가, 사고 조사 및 진단·점검 등에 필요한 경우 외부 인원에게 관리자 권한을 한시적으로 부여할 수 있다.	●	●	●
		NNSF-LP-7	사용자에게 부여된 관리자 권한 관리	사용자에게 관리자 권한이 부여된 경우 주기적으로 지속 필요 여부를 검토하고 불필요한 경우 권한을 삭제한다.	–		
		NNSF-LP-8	코드 실행권한 제한	코드는 필요한 권한으로만 실행되도록 제한하고, 사용자 권한으로 실행되는 코드가 관리자 영역으로 접근되지 않도록 차단한다.	●	●	●
		NNSF-LP-9	관리자 권한 실행 로깅 및 감사	관리자 권한 기능 실행 내역은 로깅하고 주기적인 사용 내역 감사를 실시한다.	●	●	●
	신원검증 Identity Verification (IV)	NNSF-IV-1	관리자 승인	정보시스템 사용자 계정(대민서비스 등 서비스 이용자 계정 제외) 부여를 위한 계정 등록 절차에 정보시스템 관리자(정보화담당관 또는 이에 준하는 관리자)의 승인을 포함한다.	●	●	
		NNSF-IV-2	신원 증거 제출	개인은 신원을 증명할 수 있는 증거를 등록 기관에 제출한다.	●	●	
		NNSF-IV-3	신원 증거 검증	제출된 신원 증거를 검증한다.	●	●	

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
권한	신원검증 Identity Verification (IV)	NNSF-IV-4	대면 신원 증거 검증	대면으로 신원 증거를 검증한다.	●		
		NNSF-IV-5	외부 신원 검증 수용	동등한 수준의 보증을 제공하는 외부(기관 또는 업체 등)에서의 신원 검증 결과를 수용한다.	●	●	●
	식별자관리 Identifier Management (IM)	NNSF-IM-1	공개된 식별자의 계정 사용 금지	정보시스템 계정 식별자로 개인의 공개된 식별자 사용을 금지한다.	●		
		NNSF-IM-2	사용자 상태 식별	개인과 조직의 구별, 사용자 상태(활성, 비활성, 임시계정 등)를 식별하고 관리한다.	●	●	
		NNSF-IM-3	기관 간 상호 관리	기관 간 식별자 관리를 위해 인증정보 관리기관, 외부 연동 정보시스템 관리기관 등과 주기적으로 관련 정보를 공유한다.			
		NNSF-IM-4	상호(쌍, Pairwise) 가명 식별자	사용자의 익명성 보장이 필요한 경우 사용자 간 식별을 위해 식별 정보가 없는 상호(쌍, Pairwise) 가명 식별자를 제공한다.	●	●	
		NNSF-IM-5	속성 유지관리 및 보호	안전하게 보호조치가 된 저장소에서 고유하게 식별된 각 개인, 그룹, 장치 또는 서비스에 대한 속성을 유지 및 관리한다.	●		
	계정관리 Account Management (AC)	NNSF-AC-1	계정 관리 자동화	정보시스템 계정관리를 효율화하고 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정관리를 수행한다.			
		NNSF-AC-2	계정 상태 모니터링	계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.	●	●	
		NNSF-AC-3	계정 자동 비활성화	계정 사용 기간이 종료되거나 일정 기간동안 사용하지 않은 계정은 자동으로 비활성화한다.	●	●	●
		NNSF-AC-4	감사 활동 자동화	계정 사용과 관련된 감사 활동을 자동화한다.			
		NNSF-AC-5	계정 자동 로그아웃	비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.	●	●	●
		NNSF-AC-6	불필요한 관리자 권한 계정 제거	관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.	●	●	●
		NNSF-AC-7	공유 및 그룹 계정 사용 제한	공유 및 그룹 업무가 필요한 경우로 제한하여 공유 및 그룹 계정을 사용한다.	●	●	
		NNSF-AC-8	의심스러운 계정 모니터링	미등록 계정 접속 시도 및 비정상적인 시간대 접속 등 의심스러운 계정에 대해 모니터링한다.	●		
		NNSF-AC-9	위험에 노출된 계정 비활성화	정보시스템의 취약점 노출 등 위험이 발생되면 일정 시간 동안 위험에 노출된 계정은 비활성화한다.	●	●	●

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
인증	다중요소 인증 Multi-Factor Authentication (MA)	NNSF-MA-1	관리자 계정 다중요소 인증 (MFA, Multi-factor Authentication)	관리자 권한 인증 수행 시 다중요소 인증을 적용한다. *다음의 인증요소 중2가지 이상을 조합하여 활용 (1)지식기반 요소: 사용자가 설정한 정보 (비밀번호, PIN, 패턴, 보안질문 등) (2)소유기반 요소: 사용자에게 발급한 장치 (OTP, 기관 지급 인증장치 등) 또는 계정 사용자가 소유하고 있으며 기관이 승인한 장치 이용(SMS, 모바일 공무원증, 모바일OTP 등) (3)생체기반 요소: 사용자 고유 생체정보 (지문, 홍채, 얼굴, 정맥 등)	●	●	●
		NNSF-MA-2	사용자 계정 다중요소 인증 (MFA, Multi-factor Authentication)	지정되지 않은 접속 경로 또는 사전 승인되지 않은 단말을 통한 사용자 계정에 대해 다중요소 인증을 적용한다.	●	●	
		NNSF-MA-3	다중요소 인증 장치 분리	다중요소 인증시에는 인증을 요청한 장치와 물리적으로 분리된 별도의 장치(수단 등)를 활용하여 인증을 수행한다.	●	●	
		NNSF-MA-4	다중요소 인증 (MFA, Multi-factor Authentication) 경로 분리	다중요소 인증시에는 인증을 요청한 장치의 통신 경로와 분리된 별도의 통신 경로를 통해 인증을 수행한다.	●		
	외부연계 External Integration (EI)	NNSF-EI-1	외부 자격증명 수단 활용	안전성 및 신뢰성을 검증받은 외부 기관 (또는 업체 등)에서 발급한 자격증명 수단을 활용한다.	●	●	
		NNSF-EI-2	외부 인증 수단 활용	안전성 및 신뢰성을 검증받은 외부의 인증 수단을 활용한다.	●	●	
	식별 Identification (ID)	NNSF-ID-1	단말 무결성 검증	단말 내 신뢰 가능한 모듈(TPM 등)을 통한 구성정보(BIOS 설정정보, Disk 설치 정보 등) 등을 확인한다.	●	●	
		NNSF-ID-2	정보서비스 식별 및 제한	인증절차를 통해 사전 승인한 정보서비스만을 활용하도록 제한한다.	●		
	인증보호 Authentication Protection (AU)	NNSF-AU-1	계정 인증 재전송 공격 방지	불법적인 계정 인증을 시도하는 재전송 공격 방지 대책을 적용한다.	●	●	●
		NNSF-AU-2	통합인증(SSO, Single Sign-On)	통합인증 기능 적용 시 불법적인 계정 로그인 시도에 대한 기술적 대책을 적용한다.	●	●	
		NNSF-AU-3	생체 인증 공격 방지	생체 데이터를 암호화 하여 저장 및 전송하며, 변조 여부를 탐지할 수 있는 메커니즘을 사용한다.	●	●	●
		NNSF-AU-4	비밀번호 보안수준 점검	자동화된 도구를 이용하여 비밀번호 정책에 적합하게 설정·유지되고 있는지 점검한다.			

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
인증	인증보호 Authentication Protection (AU)	NNSF-AU-5	대체 보안수단 강구	보안 기능을 구현 또는 제공하는 주요 수단을 사용할 수 없거나 손상되었을 상황을 대비한 대체 보안수단을 강구한다.	●		
		NNSF-AU-6	공개키 기반구조(PKI) 인증서	신뢰할 수 있는 공개 키 인프라(PKI)를 통해 발급된 인증서 사용을 인증서 유효기간 동안 관리하고 보호한다.	●	●	●
	인증정책 Authentication Policy (AP)	NNSF-AP-1	기관 발급 증명수단 인증 활용	기관에서 발급한 자격 증명수단(모바일 공무원증 등)을 활용하여 사용자를 인증한다.	●	●	
		NNSF-AP-2	인증 프로파일 활용	정의된 사용자 프로파일을 사용하여 인증표준화 및 관리를 수행한다.			
		NNSF-AP-3	특정상황에서의 다중요소 인증 (MFA, Multi-factor Authentication)	특정 상황 또는 조건에서는 다중요소 인증을 적용하여 사용자를 인증한다.	●	●	
		NNSF-AP-4	그룹 계정 사용자 인증	그룹 계정 인증 시 해당 그룹 계정에 포함된 사용자를 식별할 수 있는 인증수단을 적용하여 사용자 인증을 추가로 수행한다.			
		NNSF-AP-5	재인증	주기적 또는 특정 상황·조건에서는 사용자에게 재인증을 요구한다.	●	●	
		NNSF-AP-6	동시 중복 인증 차단	정보서비스 특성을 반영하여 동시 중복인증을 차단한다.	●	●	
	인증수단 Authentication Method (AM)	NNSF-AM-1	암호모듈 기반 인증	관련 법규, 정책 및 규정 등을 준수한 암호모듈 인증체계를 적용한다.	●	●	●
		NNSF-AM-2	비밀번호 기반 인증	숫자·문자·특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.	●	●	
		NNSF-AM-3	공개키 기반 인증	신뢰할 수 있는 인증 기관(CA)을 통해 발급된 인증서의 유효성을 검증하고, 인증서의 발급, 갱신, 폐지 등을 관리한다.	●	●	●
		NNSF-AM-4	초기 인증수단 변경	정보시스템 구성요소 배포·설치 전 기본(초기) 인증수단을 변경한다.	●	●	●
		NNSF-AM-5	인증수단 보호	정보시스템의 보안수준에 준하여 인증수단을 보호한다.	●	●	
		NNSF-AM-6	암호화 되지 않은 인증수단 내장 금지	암호화되지 않은 인증수단이 응용프로그램 또는 스크립트 등에 내장되거나 기능키 등에 삽입되지 않아야 한다.	●	●	●
		NNSF-AM-7	캐시된 인증수단 재사용 차단	캐시된 인증수단이 세션 유효 시간이 만료된 이후에 재사용되는 되는 것을 차단한다.	●	●	

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
인증	인증수단 Authentication Method (AM)	NNSF-AM-8	공개키 기반 저장소 관리	네트워크, 운영체제, 브라우저, 응용프로그램을 포함하여 모든 정보시스템에 설치된 PKI 저장소에 대해 관리방안을 수립한다.	●	●	
	로그인 Login (LI)	NNSF-LI-1	유효한 인증정보 노출 방지	인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.	●	●	●
		NNSF-LI-2	로그인 실패에 따른 접속 제한	정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.	●	●	●
		NNSF-LI-3	로그인 실패에 따른 인증요소 추가	정의한 횟수 이상 연속적으로 로그인을 실패한 경우 추가 인증수단(생체인증, OTP, ARS 등)을 적용한다.	●	●	
		NNSF-LI-4	계정 잠금 해제 인증요소 추가	계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.	●	●	●
		NNSF-LI-5	정보시스템 사용 알림	로그인(사용자 인증 성공) 후 사용자 화면에 정보시스템(서비스 등)에 관한 정보를 알림으로 표시하고, 사용자가 명확하게 인지한 상황에서 표시를 종료하도록 적용한다.	●		
		NNSF-LI-6	직전 로그인 정보 알림	로그인(사용자 인증 성공) 후 사용자 화면에 사용자의 직전 로그인 정보를 사용자가 확인할 수 있도록 표시한다.	●	●	
		NNSF-LI-7	실패 로그인 정보 알림	로그인(사용자 인증 성공) 후 사용자 화면에 사용자의 로그인 실패 정보를 사용자가 확인할 수 있도록 알림을 표시힌다.	●	●	
		NNSF-LI-8	로그인 이력 정보 제공	로그인(사용자 인증 성공) 후 사용자 화면에 로그인 성공 이력 정보를 제공한다.	●	●	
		NNSF-LI-9	계정 정보 변경 알림	로그인(사용자 인증 성공) 후 사용자 계정 관련 정보 변경 이력이 존재하는 경우, 일정 기간동안 사용자에게 해당 내용 알림을 표시한다.	●	●	
		NNSF-LI-10	로그인 부가 정보 제공	로그인(사용자 인증 성공) 후 이전에 성공한 로그인과 관련된 부가정보(접속위치, 단말 종류 등)를 제공한다.	●	●	
분리 및 격리	분리 Segregation (SG)	NNSF-SG-1	하드웨어 기반 분리	서로 다른 영역이 구분되도록 하드웨어를 통해 분리하고, 보안통제를 적용한다.	●	●	
		NNSF-SG-2	운영체제(OS) 기반 분리	서로 다른 영역이 구분되도록OS를 통해 분리하고, 보안통제를 적용한다.	●	●	●
		NNSF-SG-3	소프트웨어 기반 분리	서로 다른 영역이 구분되도록 소프트웨어를 통해 분리하고, 보안통제를 적용한다.	–	–	●

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
분리 및 격리	분리 Segregation (SG)	NNSF-SG-4	IP체계 분리	서로 다른 영역 또는 정보자산(기능 등)별 IP체계를 분리하고, 보안통제를 적용한다.	●	●	●
		NNSF-SG-5	보안·운영관리 인프라 분리	보안·운영관리 인프라를 물리적으로 분리된 네트워크로 구성하여 이외 정보시스템과 분리한다.	●	●	●
		NNSF-SG-6	보안 기능과 사용자 기능 분리	인증, 감사 및 데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 어플리케이션 실행 등 사용자 기능을 분리한다.	●	●	●
	격리 Isolation (IS)	NNSF-IS-1	프로세스 격리	실행되는 각 프로세스(작업 또는 프로그램)가 다른 프로세스에 영향을 미치거나 간섭을 차단하기 위해 독립된 공간에서 실행한다.	●	●	
		NNSF-IS-2	정보시스템 운영·관리 기능 표출 제한	일반 사용자에게 정보시스템 관리와 관련된 기능 및 인터페이스 표출을 제한한다.	●	●	●
		NNSF-IS-3	어플리케이션 접근 통제	어플리케이션에 대한 접근을 통제하여 데이터의 무단 접근을 방지한다.	●	●	●
통제	정보흐름 Information Flow (IF)	NNSF-IF-1	정보흐름의 동적 통제	정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.			
		NNSF-IF-2	암호화된 정보흐름 통제	암호화된 정보의 내용을 확인하기 위하여 정보를 복호화하거나, 확인이 불가능한 암호화된 정보는 흐름을 차단하는 등의 조치를 적용한다.	●	●	●
		NNSF-IF-3	임베디드 데이터 삽입 차단	임베이드된 데이터 내부에 인가되지 않은 다른 종류의 데이터가 삽입되는 것을 차단한다.	●	●	
		NNSF-IF-4	메타데이터 활용 정보흐름 통제	메타데이터(소유자, 생성일시 등 기록), 이미지/영상/오디오용 메타데이터 등을 활용하여 정보흐름을 통제한다.			
		NNSF-IF-5	일방향 정보흐름 통제	쌍방 정보전송을 차단하고 일방향으로 정보흐름을 통제한다.	●		
		NNSF-IF-6	필터링 규칙 정보흐름 통제	보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.	●	●	●
		NNSF-IF-7	데이터 유형 식별자 통제	서로 다른 영역 간에 정보를 전송하는 경우 데이터 유형 식별자를 확인하여 전송 여부를 통제한다.	●	●	
		NNSF-IF-8	인가되지 않은 정보 전송 통제	인가되지 않은 정보가 포함되었는지 검사하고 보안정책에 따라 해당 정보의 전송을 차단한다.	●	●	

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
통제	정보흐름 Information Flow (IF)	NNSF-IF-9	출발지점과 도착지점 식별 및 인증	정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.	●	●	●
		NNSF-IF-10	정보 전송 방식 제한	정보 전송 시 특정하게 규정된 방식(기술)을 통해서만 가능하도록 제한한다.	●	●	
		NNSF-IF-11	데이터 전송 차단	서로 다른 정보시스템(또는 영역 등)으로의 접근은 허용하되 데이터 전송은 차단한다.	●		
		NNSF-IF-12	정보흐름 통제 기능 유지	독립적인 다수의 정보흐름 통제 체계를 구성하여 하나의 통제 체계가 무력화되더라도 정보흐름 통제 기능을 유지한다.			
	외부경계 External Boundary (EB)	NNSF-EB-1	연결 접점 제한	정보시스템의 외부 네트워크 연결 접점 수를 제한한다.	●	●	
		NNSF-EB-2	서비스별 외부 통신 통제	외부와 통신하는 서비스의 경계마다 통신흐름을 통제한다.	●	●	●
		NNSF-EB-3	화이트리스트 기반 통신 허용	기본적으로 모든 통신을 차단한 상태에서 필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용한다.	●	●	●
		NNSF-EB-4	분할 터널링 (Split Tunneling) 제한	인터넷 서비스와 원격접속을 통한 기관 네트워크를 동시에 이용하는 등 내·외부 통신을 동시 연결하는 분할 터널링 기법을 제한한다.	●	●	●
		NNSF-EB-5	통신 경유 (proxy) 강제화	인가된 정보시스템을 경유하여 통신하도록 통신경로를 강제화한다.	●		
		NNSF-EB-6	외부로의 사이버위협 통신 발신 제한	내부에서 외부 네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단하고, 발신자(사용자 및 정보자산 등)를 식별한다.	●	●	
		NNSF-EB-7	호스트 기반 경계 보호	정보시스템 구성요소에 호스트 기반 경계 보안체계를 적용한다.	●	●	
		NNSF-EB-8	운영관리용 포트의 물리적 연결 차단	운영관리용 포트에 인가되지 않은 장치의 포트 연결을 차단한다.	●	●	●
		NNSF-EB-9	전용 장치를 통한 관리자 권한 접속	전용 장치를 통해서만 네트워크를 경유하여 관리자 권한으로 접속한다.	●		
		NNSF-EB-10	정보시스템 구성요소 외부 노출 차단	정보시스템 운영관리 및 서비스를 제공하는 구성요소가 외부 노출되지 않도록 차단한다.	●	●	●

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
통제	외부경계 External Boundary (EB)	NNSF-EB-11	외부 경계 보호 기능 유지	외부 경계를 보호하는 정보자산(보안시스템 등) 장애 시에도 보호기능은 유지되도록 구성한다.	●	●	●
		NNSF-EB-12	외부 통신용 정보자산(장치) 설치 금지	외부 네트워크와 통신하는 인가되지 않은 정보자산(장치) 설치를 금지한다.	●	●	●
		NNSF-EB-13	오류정보 발신자 전송 제한	네트워크 규약에 따른 통신 오류 발생 시 발신자에게 피드백이나 경고를 통해 정보시스템 구성이나 취약점이 전송되지 않도록 한다.	●	●	
		NNSF-EB-14	개인 식별정보 보호	외부와 통신 시 개인을 식별하거나 특정 개인과 관련된 정보를 포함하는 경우 노출되지 않도록 조치한다.			
	원격접속 Remote Access (RA)	NNSF-RA-1	원격접속 모니터링 및 통제	원격접속을 모니터링하고 통제한다.	●	●	
		NNSF-RA-2	원격접속 세션 암호화	원격접속 세션의 기밀성과 무결성을 보호하기 위해 통신구간 암호화를 적용한다.	●	●	●
		NNSF-RA-3	원격접속 위치통제	보안관리 및 통제가 가능한 물리적 공간(위치) 또는 기술적 대책을 적용하여 원격접속을 허용한다.	●	●	
		NNSF-RA-4	관리자 권한 통제	원격접속을 통한 관리자 권한은 제한된 조건에서만 허용해야 하며, 관리자 권한으로 실행한 명령어 이력 등은 유지한다.	–	●	
		NNSF-RA-5	원격접속 정보 유출 방지	원격접속에 관한 정보를 무단으로 사용하거나 외부로 유출되는 것을 방지한다.	●	●	●
		NNSF-RA-6	원격접속 자동 종료 및 비활성화	일정시간 경과 등 조건에 따라 원격접속을 자동 종료하거나, 원격접속 목적이 달성된 경우 비활성화한다.	●	●	●
		NNSF-RA-7	원격 명령 신뢰성 검증	명령을 수행하기 전에 적절한 인증 체계 (암호화된 인증서, 보안 토큰, 또는 사용자 인증)를 적용하여 명령의 무결성과 출처를 검증한다.	●		
	세션 Session (SN)	NNSF-SN-1	로그아웃 세션 처리	로그아웃 또는 비정상 세션 종료 시 연결되었던 모든 세션의 식별자를 즉시 무효화하며, 더 이상 세션이 유효하지 않도록 한다.	●	●	●
		NNSF-SN-2	세션별 고유 식별자	각 사용자 세션마다 고유한 식별자를 활용하고, 고유한 식별자의 재사용을 방지한다.	●	●	●
		NNSF-SN-3	동시 접속 세션 제한	사용자 계정 또는 정보시스템 등을 기준으로 동시 세션 수를 제한한다.	●		

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
통제	세션 Session (SN)	NNSF-SN-4	세션 종료	세션 종료 요청이 있거나 세션 종료 조건 발생 시 자동으로 세션을 종료한다.	●	●	●
		NNSF-SN-5	사용자 기반 로그아웃	사용자 요청에 따라 로그아웃 할 수 있는 기능을 제공한다.			
		NNSF-SN-6	종료 메시지	사용자에게 종료되었다는 메시지를 표시한다.			
		NNSF-SN-7	로그인 유효시간 경과 경고 메시지	사용자에게 로그인 유효시간 경고 메시지를 표시한다.			
		NNSF-SN-8	네트워크 연결 해제	정상 세션 종료 또는 일정 시간 비활성 상태가 유지될 경우 네트워크 연결을 자동 해제한다.	●	●	
	무선망접속 Wireless Network Access (WA)	NNSF-WA-1	업무용 무선망 인증 및 암호화	사용자 인증, 기기(단말 등) 인증 및 무선통신 구간 암호화를 적용한다.	●	●	
		NNSF-WA-2	업무용 무선망 인증정보 보호	업무용 무선 통신망 서비스 식별 정보(SSID 등)를 경계지역 외부에서 확인할 수 없도록 적용하고, 무선 통신망 인증정보의 무단 사용 및 외부 유출을 방지한다.	●	●	
		NNSF-WA-3	업무용 무선망 신호 보호	무선 통신환경에 적합한 안테나를 선택하고 송수신 출력을 교신에 필요한 최저 출력으로 유지하여 경계지역 외부로 전파 되는 것을 방지한다.	●		
		NNSF-WA-4	비인가 무선장비 설치 차단	업무용 무선망 서비스에 비인가 무선장비가 설치되거나 가동되는 것을 탐지하고 운용되지 않도록 한다.	●	●	
		NNSF-WA-5	외부인 전용 무선망 구성	업무용 네트워크 또는 무선망과 분리하여 외부인 전용망을 구성한다.			
		NNSF-WA-6	무선망 관리기능 보호	무선망 관리기능은 무선망에 노출되지 않아야 하며, 지정된 관리자만 접속되도록 통제한다.	●	●	●
		NNSF-WA-7	비인가 무선망 접속 차단	인가되지 않은 무선망 접속을 차단한다.	●	●	●
	블루투스연결 Bluetooth Connection (BC)	NNSF-BC-1	블루투스 데이터 통신 제한	블루투스 장치 연결 시 키보드, 마우스, 오디오 등을 위한 입출력 기능 외 데이터 통신은 차단한다.	●	●	

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
데이터	암호 키 관리 Encryption Key Management (EK)	NNSF-EK-1	암호 키 설정	데이터 저장을 위해 암호 키를 생성하는 경우, 유형별 암호 키(대칭 키, 공개 키 등) 및 인증서를 키 관리 시스템(KMS)을 활용할 수 있다. 암호 키를 설정 시 C/S/O 보안등급별 암호화 강도, 암호 알고리즘(국산 암호, 국제 표준암호 등), 암호 키 유효기간 및 갱신, 암호 키와 서명용 키 분리, CRL(인증서 폐기 목록) 생성 주기 및 배포 경로 등을 설정 한다.	●	●	●
		NNSF-EK-2	암호 키 생성	KCMVP(Korea Cryptographic Module Validation Program) 인증을 받은 난수 발생기 또는 암호 모듈을 사용하며, 데이터의 보안 등급에 따라 소프트웨어 기반 TRNG(True Random Number Generator) 또는 하드웨어 기반 난수발생기를 사용한다.	●	●	
		NNSF-EK-3	암호 키 저장	암호 키는 암호화된 형태로 저장하거나 보안성이 요구되는 경우 보안 토큰 등을 사용하여 분리 보관한다.	●	●	●
		NNSF-EK-4	암호 키 사용	데이터 저장 규모 및 성능에 따라 암호화된 데이터베이스 또는 하드웨어 보안 모듈 (HSM: Hardware Security Module)를 활용하여 암호 키를 사용한다. 클라우드 환경에서 암호키를 안전하게 저장, 사용하기 위해 HSM을 활용할 수 있다.	●	●	
		NNSF-EK-5	암호 키 폐기	암호키는 복구 불가능한 상태로 안전하게 삭제하고 동일 암호 키가 재생성 및 재사용되지 않도록 조치한다. 그리고 CRL (인증서 폐기 목록) 관리해야 한다.	●	●	●
		NNSF-EK-6	전자서명 검증	데이터의 전송 및 저장 시 데이터 무결성 확인 및 암호화를 통한 데이터 보호를 위해 전자서명 생성 및 검증 키 관리, 표준화된 서명 검증 알고리즘과 서명용 인증서 관리, 전자서명 검증 기술을 적용한다.	●	●	●
	암호기술 적용 Encryption Technology Application (EA)	NNSF-EA-1	검증필 암호모듈 사용	국가정보원장이 안전성을 확인한 상용 암호모듈(검증필 암호모듈)을 사용한다.	●	●	●
		NNSF-EA-2	국가용 암호자재 및 장비 사용	국가정보원장이 개발하거나 안전성을 확인한 암호자재 또는 암호장비 등을 사용한다.	●		
		NNSF-EA-3	특수목적용 외국산 암호자재 및 장비 사용	외국기관 또는 외국군 등 특수목적 통신을 위해 외국산 암호자재 및 장비를 사용한다.	●	●	

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
데이터	데이터전송 Data Transmission (DT)	NNSF-DT-1	전송 권한 확인	데이터가 전송되기 전에 이를 처리하는 개인이나 정보시스템이 적절한 권한을 보유하고 있는지 확인한다.	●	●	
		NNSF-DT-2	정보교환 중단	정보교환 대상 정보시스템 등에 대한 식별 및 통제가 확인되지 않을 경우 정보교환을 중단한다.	●	●	
		NNSF-DT-3	전송간 암호화 적용	물리적 보안수단에 의해 전송 간 보호되지 않는 경우 전송 구간에 대한 암호기술을 적용한다.	●	●	
		NNSF-DT-4	메시지 외부 암호화 보호	메시지 외부정보를 보호하기 위한 암호기술을 적용한다.			
		NNSF-DT-5	통신 패턴 은폐 또는 무작위화	통신패턴을 숨기거나 무작위화하는 암호기술을 적용한다.			
	데이터사용 Data Usage (DU)	NNSF-DU-1	오프라인 저장	중요 정보를 안전한 장소에 오프라인으로 보관하여 네트워크를 통한 무단 접근을 방지한다.	●	●	
		NNSF-DU-2	데이터 암호화 저장	데이터 대상 암호기술을 적용하여 기밀성을 보장한다.	●	●	●
		NNSF-DU-3	사용중 데이터 보호	검색, 연산, 분석 등 데이터 사용 과정에서 정보시스템 내 데이터를 보호하는 기술을 적용한다.	●	●	
		NNSF-DU-4	데이터 갱신 및 삭제	필요 시 데이터를 갱신하거나 생성하여 사용하고, 필요 목적이 종료되면 데이터는 삭제한다.	●	●	
정보자산	모바일단말 Mobile Device (MD)	NNSF-MD-1	모바일 코드 다운로드 및 실행 금지	허용되지 않은 모바일 코드 다운로드 및 실행을 금지한다.	●	●	
		NNSF-MD-2	자동 실행 금지	응용프로그램에서 모바일 코드의 자동 실행을 방지한다.			
		NNSF-MD-3	제한된 환경에서의 실행	모바일 코드를 제한된 환경(가상머신 등)에서만 실행하도록 제한한다.	●		
		NNSF-MD-4	민감정보 소통 제한	민감정보를 처리·저장·전송하는 경우 보안요건에 따른 기술적 조치가 적용되지 않은 일반적인 모바일 장비 사용을 제한한다.	●	●	
		NNSF-MD-5	모바일 장치 암호화 기술	모바일 장비 저장공간 암호화 또는 컨테이너 기반 저장공간 분리 및 암호화를 적용한다.	●	●	
		NNSF-MD-6	데이터 자동삭제 또는 초기화	특정 상황 또는 조건에 따라 단말 내부에 저장된 데이터를 자동 삭제하거나 초기화한다.	●	●	

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
정보자산	하드웨어 Device (DV)	NNSF-DV-1	하드웨어 무결성 검증	하드웨어 구성 요소의 무결성을 검증한다.	●	●	
		NNSF-DV-2	하드웨어 기반 펌웨어 보호 (Hardware-Based Protection)	펌웨어 구성요소 대상 하드웨어 기반 쓰기방지 기능을 활용한다.	●		
		NNSF-DV-3	하드웨어 장치(device) 사용 제한	정보자산 배포 또는 설치 전 특정 하드웨어 장치(USB포트, 무선통신 모듈 등)를 비활성화 또는 제거 등으로 사용을 제한한다.	●	●	
		NNSF-DV-4	포트 및 입출력 장치 제어	정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.	●	●	
		NNSF-DV-5	외부 정보자산 활용 정보처리 제한	외부 정보자산 등을 통한 정보의 처리, 저장 및 전송 등을 제한한다.	●		
		NNSF-DV-6	통신 기능이 포함된 저장장치 제한	통신기능이 포함된 저장장치를 사용을 제한한다.	●		
		NNSF-DV-7	기관 접속용 장치 제한	외부 정보자산(시스템 등)에서 기관 네트워크 접속이 가능한 장치 사용을 제한한다.	●		
		NNSF-DV-8	장치 자동 잠금	사용자가 일정시간 이상 정보시스템을 사용하지 않거나 방치할 경우 잠금 기능을 활성화하고, 화면에 표시되는 정보는 표출되지 않아야 한다.	●	●	●
		NNSF-DV-9	읽기전용 매체 활용 프로그램 실행	하드웨어 기반의 읽기 전용 매체에서 운영체제(OS) 로드 및 응용프로그램을 실행하여 실행환경의 무결성을 확보한다.	●		
		NNSF-DV-10	저장장치 연결 금지	정보시스템 기동 및 종료 또는 재시작하는 동안 쓰기 가능한 저장장치 연결을 금지한다.			
		NNSF-DV-11	읽기전용 매체 무결성 검증	읽기 전용 매체에 정보를 저장하기 이전 무결성을 검증한다.			
	정보시스템 구성요소 Information System Component (IN)	NNSF-IN-1	정보시스템 구성요소 최신상태 유지	정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성 요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.	●	●	
		NNSF-IN-2	구성요소 목록 현행화	정보시스템 구성 요소 설치, 제거, 또는 정보시스템 업데이트 시 목록을 갱신한다.	●	●	
		NNSF-IN-3	구성요소 목록 자동관리	자동화된 메커니즘을 통해 정보시스템 구성요소 목록의 최신성, 완전성, 정확성, 가용성을 유지한다.			

대항목	중항목	NNSF ID	소항목	보안통제설명	N²SF 우선 검토사항		
					C 기밀	S 민감	O 공개
정보자산	정보시스템 구성요소 Information System Component (IN)	NNSF-IN-4	비인가 구성요소 식별	정보시스템 내 비인가 하드웨어, 소프트웨어 및 펌웨어 구성 요소를 검사하여 식별한다.	●	●	●
		NNSF-IN-5	구성요소 목록 중앙관리	정보시스템 구성요소 목록을 통합관리하기 위한 중앙화된 저장소를 운용한다.			
		NNSF-IN-6	물리적 위치 식별	자동화된 메커니즘을 통해 정보시스템 구성요소의 물리적 위치를 식별한다.	●	●	
		NNSF-IN-7	변경 사항 테스트 및 검증	변경 사항을 최종 적용하기 전에 테스트 및 검증을 통해 안전성을 확보한다.	●	●	
		NNSF-IN-8	비인가 변경 방지	인가되지 않은 정보시스템 구성요소 변경을 방지한다.	●	●	●
		NNSF-IN-9	불필요한 구성요소 제거	필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.	●	●	●
		NNSF-IN-10	주기적인 구성요소 제거 상태 점검	주기적으로 사용하지 않은 기능, 포트, 프로토콜, 소프트웨어 및 서비스의 활성화 여부를 점검한다.	●	●	
		NNSF-IN-11	비인가 소프트웨어 실행 차단	허가되지 않은 소프트웨어(응용프로그램)이 실행되지 않도록 차단한다.	●	●	
		NNSF-IN-12	소프트웨어 기술지원 유지	개발자, 공급업체 또는 제조업체에서 기술지원이 종료된 구성요소는 교체하거나 지속적 기술지원이 가능하도록 조치한다.	●	●	●
		NNSF-IN-13	소프트웨어 설치 권한 제한	소프트웨어 설치 권한은 필요한 사용자에게만 부여한다.	●	●	
		NNSF-IN-14	재기동 서비스 신뢰성 확보	정보시스템 구성요소와 서비스가 재기동(재부팅) 할 때 소프트웨어와 데이터는 신뢰된 곳으로부터 획득한다.	●	●	●
		NNSF-IN-15	신뢰성이 보장된 구성요소 설치	신뢰할 수 있는 외부 기관·제조사 또는 기관이 자체 서명한 구성요소를 설치 및 활용한다.	●	●	●
		NNSF-IN-16	정보의 비지속성	정보시스템이 종료되거나 재부팅될 때 관련 정보(데이터 등)는 자동 삭제하여 유지되지 않도록 한다.	●	●	
		NNSF-IN-17	연결의 비지속성	일시적으로 사용된 연결은 사용이 종료되면 자동으로 연결을 끊어 연결이 유지되지 않도록 한다.	●	●	

제1장

권한

1. 최소 권한 (Least Privilege, LP)

정의

최소 권한은 사용자나 프로세스가 특정 업무를 수행하는 데 필요한 최소한의 권한만을 부여하는 보안 원칙으로, 내부 및 외부 위협으로부터 시스템을 보호하고, 내부 정보로의 불필요한 접근을 방지하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-LP-1	C S	정보시스템 접근 권한 정의
	업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.	
NNSF-LP-2	C S O	보안통제 권한 제한
	보안통제 권한은 정보보안담당관(자) 또는 이에 준하는 관리권한을 부여받은 인원에게만 부여한다.	
NNSF-LP-3	C S O	보안통제 계정 노출 방지
	보안통제 권한 목적으로 사용되는 계정과 이외 기능에 사용되는 계정은 중복 사용하지 않도록 보안통제 권한 계정의 노출을 방지한다.	
NNSF-LP-4	- S O	원격접속을 통한 관리자 권한 접속 제한
	기관 네트워크 내부에서 관리자 권한 접속이 제한되는 경우 등 불가피한 상황에서만 한시적으로 기관 네트워크 외부에서의 관리자 권한 접속을 허용하며, 목적이 달성된 경우 외부에서의 관리자 권한 접속을 즉시 차단한다.	
NNSF-LP-5	C S	관리자 권한 제한
	정보시스템 관리자 권한은 관리자 또는 운영자 등 최소한의 인원에게만 부여한다.	

NNSF ID	보안통제 항목 설명	
NNSF-LP-6	C S O	기관 이외 인원의 관리자 권한 제한
	기관 구성원 이외 인원에게 관리자 권한은 부여하지 않으며, 다만 정보보안 감사, 사이버보안 실태평가, 사고 조사 및 진단·점검 등에 필요한 경우 외부 인원에게 관리자 권한을 한시적으로 부여할 수 있다.	
NNSF-LP-7	-	사용자에게 부여된 관리자 권한 관리
	사용자에게 관리자 권한이 부여된 경우 주기적으로 지속 필요 여부를 검토하고 불필요한 경우 권한을 삭제한다.	
NNSF-LP-8	C S O	코드 실행권한 제한
	코드는 필요한 권한으로만 실행되도록 제한하고, 사용자 권한으로 실행되는 코드가 관리자 영역으로 접근되지 않도록 차단한다.	
NNSF-LP-9	C S O	관리자 권한 실행 로깅 및 감사
	관리자 권한 기능 실행 내역은 로깅하고 주기적인 사용 내역 감사를 실시한다.	

구현 방법 예시

- **역할 기반 접근 제어(RBAC) 적용**
  - 사용자의 역할에 따라 각기 다른 권한을 부여하고, 최소한의 권한만 설정하여 불필요한 권한 남용을 방지한다.
- **정기적인 권한 검토**
  - 모든 사용자의 권한을 정기적으로 검토하여, 더 이상 필요하지 않은 권한을 제거하거나 조정한다.
- **자동화된 권한 관리 도구 사용**
  - 권한 관리 도구를 사용하여 조직 내 권한 설정과 변경을 중앙에서 관리하고, 최소 권한 원칙을 자동으로 적용한다.
- **시스템 프로세스 권한 설정**
  - 시스템에서 실행되는 각 프로세스에 대해 필요한 권한만 부여하고, 과도한 시스템 자원 접근을 차단한다.
- **권한 분리**
  - 한 사용자가 많은 권한을 가지지 않도록 업무 및 권한을 분리하여 보안을 강화한다.

2. 신원 검증 (Identity Verification, IV)

정의

신원 증명은 시스템 접근을 위한 자격 증명을 설정할 목적으로 대상 사용자의 신원 정보를 수집, 검증 및 확인하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-IV-1	C S	관리자 승인
	정보시스템 사용자 계정(대민서비스 등 서비스 이용자 계정 제외) 부여를 위한 계정 등록 절차에 정보시스템 관리자(정보화담당관 또는 이에 준하는 관리자)의 승인을 포함한다.	
NNSF-IV-2	C S	신원 증거 제출
	개인은 신원을 증명할 수 있는 증거를 등록 기관에 제출한다.	
NNSF-IV-3	C S	신원 증거 검증
	제출된 신원 증거를 검증한다.	
NNSF-IV-4	C	대면 신원 증거 검증
	대면으로 신원 증거를 검증한다.	
NNSF-IV-5	C S O	외부 신원 검증 수용
	동등한 수준의 보증을 제공하는 외부(기관 또는 업체 등)에서의 신원 검증 결과를 수용한다.	

구현 방법 예시

- **신원 확인 절차 도입**
  - 계정 등록 시 사용자의 신원을 고유하게 식별할 수 있는 절차를 도입한다. 예를 들어, 정부 발급 신분증, 인증서, 생체 인식 등을 검증한다.

- **다단계 신원 검증 적용**
  - 중요한 시스템에 접근하는 사용자에게는 다단계 신원 검증을 적용하여 보안성을 강화한다.

- **신원 증거 수집 및 저장**
  - 사용자의 신원 증거를 안전하게 수집하고, 이를 암호화하여 저장한다. 수집된 정보는 개인정보 보호법을 준수하여 처리한다.

• **자동화된 신원 검증 시스템**

– 신원 검증 절차를 자동화하여 신원 확인 과정을 빠르고 정확하게 처리할 수 있도록 한다.

• **법적 요구사항 반영**

– 조직이 속한 국가나 지역의 법적 요구사항에 맞추어 신원 확인 절차를 설계하고 적용한다.

3. 식별자 관리 (Identifier Management, IM)

정의

식별자 관리는 기관의 IT 자산 및 인적 자원을 식별할 수 있는 고유한 식별자를 생성, 관리하여 접근 통제를 강화하고 인증 프로세스를 지원하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-IM-1	C	공개된 식별자의 계정 사용 금지
	정보시스템 계정 식별자로 개인의 공개된 식별자 사용을 금지한다.	
NNSF-IM-2	C S	사용자 상태 식별
	개인과 조직의 구별, 사용자 상태(활성, 비활성, 임시계정 등)를 식별하고 관리한다.	
NNSF-IM-3		기관 간 상호 관리
	기관 간 식별자 관리를 위해 인증정보 관리기관, 외부 연동 정보시스템 관리기관 등과 주기적으로 관련 정보를 공유한다.	
NNSF-IM-4	C S	상호(쌍, Pairwise) 가명 식별자
	사용자의 익명성 보장이 필요한 경우 사용자 간 식별을 위해 식별 정보가 없는 상호(쌍, Pairwise) 가명 식별자를 제공한다.	
NNSF-IM-5	C	속성 유지관리 및 보호
	안전하게 보호조치가 된 저장소에서 고유하게 식별된 각 개인, 그룹, 장치 또는 서비스에 대한 속성을 유지 및 관리한다.	

구현 방법 예시

• **권한 기반 식별자 할당**

– 특정 인원이 식별자를 할당할 수 있도록 권한을 부여하고, 이를 통해 모든 식별자가 적절하게 관리되도록 한다.

- **고유한 식별자 생성 규칙 설정**
  - 사용자, 장치, 역할 등의 식별자가 고유하게 생성될 수 있도록 규칙을 설정하고, 시스템에서 중복된 식별자가 생성되지 않도록 한다.
- **식별자 재사용 제한 설정**
  - 기존 사용된 식별자를 일정 기간 재사용하지 못하도록 시스템에서 제한하는 기능을 설정한다.
- **식별자 할당 로그 기록**
  - 모든 식별자 할당 및 변경 사항을 기록하여, 필요시 감사할 수 있도록 관리한다.
- **식별자 수명 주기 관리**
  - 사용자나 장치가 시스템에서 더 이상 사용되지 않으면, 해당 식별자를 비활성화하고 일정 기간 후에 재사용할 수 있도록 관리한다.

4. 계정 관리 (Account Management, AC)

정의

계정 관리는 시스템 내에서 사용자와 관련된 계정을 생성, 관리, 모니터링, 비활성화 및 삭제 기능을 수행하여 불필요한 계정 사용을 방지하고, 비 인가된 사용자 접근을 통제하여 보안성을 유지하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-AC-1		계정 관리 자동화
	정보시스템 계정관리를 효율화하고 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정관리를 수행한다.	
NNSF-AC-2	C S	계정 상태 모니터링
	계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.	
NNSF-AC-3	C S O	계정 자동 비활성화
	계정 사용 기간이 종료되거나 일정 기간동안 사용하지 않은 계정은 자동으로 비활성화한다.	
NNSF-AC-4		감사 활동 자동화
	계정 사용과 관련된 감사 활동을 자동화한다.	

NNSF ID	보안통제 항목 설명	
NNSF-AC-5	C S O	계정 자동 로그아웃
	비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.	
NNSF-AC-6	C S O	불필요한 관리자 권한 계정 제거
	관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.	
NNSF-AC-7	C S	공유 및 그룹 계정 사용 제한
	공유 및 그룹 업무가 필요한 경우로 제한하여 공유 및 그룹 계정을 사용한다.	
NNSF-AC-8	C	의심스러운 계정 모니터링
	미등록 계정 접속 시도 및 비정상적인 시간대 접속 등 의심스러운 계정에 대해 모니터링한다.	
NNSF-AC-9	C S	위험에 노출된 계정 비활성화
	정보시스템의 취약점 노출 등 위험이 발생되면 일정 시간 동안 위험에 노출된 계정은 비활성화한다.	

구현 방법 예시

- **계정 승인 프로세스 도입**
  - 계정 생성 시, 기관에서 지정한 승인 절차를 거쳐야 하며, 승인 없이 계정을 생성하지 않도록 설정한다.

- **권한 및 접근 통제 설정**
  - 각 계정의 권한을 역할과 필요에 맞게 설정하고, 불필요한 접근을 제한한다.

- **정기적인 계정 사용 검토**
  - 계정 사용 상태를 주기적으로 검토하여, 사용되지 않는 계정을 비활성화 하거나 삭제한다.

- **계정 모니터링 시스템 도입**
  - 계정 사용을 실시간으로 모니터링하고, 의심스러운 계정 활동을 탐지할 수 있는 시스템을 도입한다.

- **계정 비활성화 기준 설정**
  - 사용자가 더 이상 기관에 필요하지 않거나 이동 및 퇴사할 경우, 계정을 자동으로 비활성화하는 정책을 시행한다.

제2장

인증

1. 다중요소 인증 (Multi-Factor Authentication, MA)

정의

다중요소 인증은 기관 내부 사용자의 정보시스템 등에 접근 시 사용자 인증을 위해 두 개 이상의 인증 요소를 사용하여 보안성을 강화하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-MA-1	C S O	관리자 계정 다중요소 인증(MFA, Multi-factor Authentication)
	관리자 권한 인증 수행 시 다중요소 인증을 적용한다. * 다음의 인증요소 중 2가지 이상을 조합하여 활용 (1) 지식기반 요소 : 사용자가 설정한 정보(비밀번호, PIN, 패턴, 보안질문 등) (2) 소유기반 요소 : 사용자에게 발급한 장치(OTP, 기관 지급 인증장치 등) 또는 계정 사용자가 소유하고 있으며 기관이 승인한 장치 이용(SMS, 모바일 공무원증, 모바일 OTP 등) (3) 생체기반 요소 : 사용자 고유 생체정보(지문, 홍채, 얼굴, 정맥 등)	
NNSF-MA-2	C S	사용자 계정 다중요소 인증(MFA, Multi-factor Authentication)
	지정되지 않은 접속 경로 또는 사전 승인되지 않은 단말을 통한 사용자 계정에 대해 다중요소 인증을 적용한다.	
NNSF-MA-3	C S	다중요소 인증 장치 분리
	다중요소 인증시에는 인증을 요청한 장치와 물리적으로 분리된 별도의 장치(수단 등)를 활용하여 인증을 수행한다.	
NNSF-MA-4	C	다중요소 인증(MFA, Multi-factor Authentication) 경로 분리
	다중요소 인증시에는 인증을 요청한 장치의 통신 경로와 분리된 별도의 통신 경로를 통해 인증을 수행한다.	

구현 방법 예시

- **다중요소 인증 시스템 구축**
  - 기관 사용자 식별 및 인증을 위한 다중요소 인증 시스템을 구축한다.
  - 사용자 인증에 대한 로그를 기록한다.

- **MFA 인증**
  - 사용자에 대한 1) 지식기반 요소, 2) 소유기반 요소, 3) 생체기반 요소 중 2개 이상의 요소를 조합하여 인증한다.
  - 지식기반 요소는 사용자가 설정한 패스워드, PIN, 패턴, 보안 질문 등의 정보를 인증 수단으로 사용한다.
  - 소유기반 요소는 기관이 사용자에게 발급한 OTP 등 장치 또는 사용자가 소유하고 있으며 기관이 승인한 장치인 모바일 공무원증, SMS 등을 인증 수단으로 사용한다.
  - 생체기반 요소는 지문, 홍채 인증 등 사용자 고유 생체정보를 활용하여 인증 수단으로 한다.

- **인증 장치 분리**
  - 사용자가 현재 인증을 위해 사용 중인 기본 단말 외 사용자 모바일 기기, 기관에서 지급한 OTP 기기, 기관에서 지급한 인증 토근 등을 인증 수단으로 활용한다.

- **인증 경로 분리**
  - 사용자가 현재 인증을 위해 사용 중인 인증 수단의 네트워크 경로 외 다른 경로를 활용하는 인증 수단을 MFA 인증에 활용한다. (예: 기관 내 유선 접속 단말을 통한 ID/Password 인증 수행 시 모바일(이동통신망), OTP 등을 통한 추가 인증 수행)

2. 외부 연계 (External Integration, EI)

정의

외부 연계 인증은 외부 기관 사용자에 대한 접근 시스템을 식별하고 시스템에 대한 접근 권한 부여하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-EI-1	C S	외부 자격증명 수단 활용
	안전성 및 신뢰성을 검증받은 외부 기관(또는 업체 등)에서 발급한 자격증명 수단을 활용한다.	
NNSF-EI-2	C S	외부 인증 수단 활용
	안전성 및 신뢰성을 검증받은 외부의 인증 수단을 활용한다.	

구현 방법 예시

• 타기관 또는 기타 기관 사용자 자격증명

- 모바일 공무원증 등 기관에서 신뢰할 수 있으며 기관 외 사용자 식별 및 자격증명이 가능한 수단을 인증 방법으로 사용한다.

• 외부 인증 수단 연계

- 기관 외 사용자에 대한 인증 수행 시 기관이 사전 승인한 외부 인증 시스템과 인증 프로파일을 활용한 연계를 통해 인증을 수행한다. (예: 이동통신사 인증 등)

• 외부 사용자 접속 시 정보 분리

- 외부 사용자에게 허용된 정보시스템에만 접속할 수 있도록 외부 사용자 단말의 네트워크 경로를 별도 설정한다.
- 외부 사용자의 정보 조회 시 익명화 등 업무정보를 필터링하여 제공한다.

3. 식별 (Identification, ID)

정의

식별은 기관 정보시스템 및 시스템 구성장비에 대한 비인가 단말의 접속을 차단하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-ID-1	C S	단말 무결성 검증
	단말 내 신뢰 가능한 모듈(TPM 등)을 통한 구성정보(BIOS 설정정보, Disk 설치 정보 등) 등을 확인한다.	
NNSF-ID-2	C	정보서비스 식별 및 제한
	인증절차를 통해 사전 승인한 정보서비스만을 활용하도록 제한한다.	

구현 방법 예시

- **접속 단말 정보 검증**
  - 단말 내 하드웨어 기반의 보안 모듈인 TPM 등을 통한 단말 내 구성 정보의 진단 결과를 수집하여, 단말 관리 시스템에서 관리하는 단말 구성 정보와 무결성 검증 후 접속을 허용한다.

- **비인가 소프트웨어 실행 차단**
  - 사용자 단말에서 업무 수행에 불필요한 비인가 소프트웨어 실행을 차단한다.

- **비인가 서비스 접속 차단**
  - 사용자 단말에서 업무 수행에 불필요한 서비스 접속을 차단한다.

4. 인증보호 (Authentication Protection, AU)

정의

인증보호는 계정 인증 보안 강화 및 불법적인 계정 로그인 시도 방지, 생체 인증 공격 방지, 대체 보안수단 강구 등 인증 과정에서의 보안성 강화 및 다양한 위협에 대응하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-AU-1	C S O	계정 인증 재전송 공격 방지
	불법적인 계정 인증을 시도하는 재전송 공격 방지 대책을 적용한다.	

NNSF ID	보안통제 항목 설명	
NNSF-AU-2	C S	통합인증(SSO,SingleSign-on)
	통합인증 기능 적용 시 불법적인 계정 로그인 시도에 대한 기술적 대책을 적용한다.	
NNSF-AU-3	C S O	생체 인증 공격 방지
	생체 데이터를 암호화 하여 저장 및 전송하며, 변조 여부를 탐지할 수 있는 메커니즘을 사용한다.	
NNSF-AU-4		비밀번호 보안수준 점검
	자동화된 도구를 이용하여 비밀번호 정책에 적합하게 설정·유지되고 있는지 점검한다.	
NNSF-AU-5	C	대체 보안수단 강구
	보안 기능을 구현 또는 제공하는 주요 수단을 사용할 수 없거나 손상되었을 상황을 대비한 대체 보안수단을 강구한다.	
NNSF-AU-6	C S O	공개키 기반구조(PKI) 인증서
	신뢰할 수 있는 공개키 인프라(PKI)를 통해 발급된 인증서 사용을 인증서 유효기간 동안 관리하고 보호한다.	

구현 방법 예시

- **재전송 공격 방지 대책 적용**
  - 인증 요청에 시간 정보를 포함시켜 제한된 시간 내에서만 유효성 보장, 난수 생성을 통한 매번 다른 인증값을 통한 요청, MFA 인증 상시 적용 등을 사용자 인증 시 수행한다.
- **계정 정보 보호 대책 적용**
  - MFA 인증, 재전송 공격 방지 적용, 비활성화 시 세션 종료 등을 사용자 인증 시 수행한다.
- **대체 보안 메커니즘 구현**
  - 시스템의 핵심 보안 기능이 손상될 가능성에 대비하여 보안 메커니즘을 정의하고 이를 구현한다.
- **대체 메커니즘 적용 프로세스 수립**
  - 기본 메커니즘이 손상되거나 사용할 수 없는 상황에서 즉시 대체 메커니즘이 적용될 수 있도록 절차를 수립하고 테스트한다.
- **대체 메커니즘의 주기적 점검**
  - 대체 보안 메커니즘을 정기적으로 점검하고 최신 보안 위협에 대응 할 수 있도록 업데이트한다.

• **인증서 발급 절차 수립**

- 기관에서 정의한 정책에 따라 PKI 인증서를 발급하는 절차를 수립하고, 필요한 경우 기관이 사전 승인한 서비스 제공자로부터 인증서를 획득한다.

• **루트 인증서 관리**

- 신뢰할 수 있는 루트 인증서만 신뢰 저장소에 포함되도록 관리하고, 만료된 인증서는 즉시 삭제한다.

• **자동화된 인증서 검증 시스템 도입**

- 인증서가 발급되고 저장소에 저장될 때, 자동으로 검증할 수 있는 시스템을 도입하여 인증서의 유효성을 보장한다.

5. 인증정책 (Authentication Policy, AP)

정의

인증정책은 기관 사용자 증명, 인증 프로파일, 그룹계정 사용자 인증 등 기관 내 사용자의 신원을 지속적으로 확인하고 보호하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-AP-1	C S	기관 발급 증명수단 인증 활용
	기관에서 발급한 자격 증명수단(모바일 공무원증 등)을 활용하여 사용자를 인증한다.	
NNSF-AP-2		인증 프로파일 활용
	정의된 사용자 프로파일을 사용하여 인증 표준화 및 관리를 수행한다.	
NNSF-AP-3	C S	특정상황에서의 다중요소 인증(MFA, Multi-factor Authentication)
	특정 상황 또는 조건에서는 다중요소 인증을 적용하여 사용자를 인증한다.	
NNSF-AP-4		그룹 계정 사용자 인증
	그룹 계정 인증 시 해당 그룹 계정에 포함된 사용자를 식별할 수 있는 인증수단을 적용하여 사용자 인증을 추가로 수행한다.	

NNSF ID	보안통제 항목 설명	
NNSF-AP-5	C S	재인증
	주기적 또는 특정 상황·조건에서는 사용자에게 재인증을 요구한다.	
NNSF-AP-6	C S	동시 중복 인증 차단
	정보서비스 특성을 반영하여 동시 중복인증을 차단한다.	

구현 방법 예시

• 기관 발급 자격 증명 수단

- 모바일 공무원증 등 기관에서 발급한 자격 증명을 사용자 인증 수단으로 활용할 수 있다.

• 특정 상황에 따른 추가 인증 설정

- 기관 외에서의 접근 시도, 사용자 개인정보 접근 등 특정 상황에서는 MFA 등 추가 인증을 요구하도록 설정한다.

• 사용자 자격 증명 변경 시 재인증

- 사용자 자격 증명 및 인증 수단 변경 시 해당 계정을 로그아웃 처리하고, 인증 절차를 다시 요구한다.

• 시스템 보안설정 변경 시 재인증

- 시스템 보안설정 변경 시 사용자 계정에 대한 보안 정책 적용을 위해 해당 계정을 로그아웃 처리하고, 인증 철자를 다시 요구한다.

• 특별권한 기능 실행 시 재인증

- 시스템 설정 변경 등 특별권한 명령 실행 시 현재 사용자 계정에 대한 재인증을 요구한다.

• 기타 기관이 지정한 상황에서의 재인증

- 그 외 기관이 필요하다고 지정한 상황에 대해 현재 사용자 계정에 대한 또는 사용자 계정 로그아웃 처리 후 재인증을 수행한다.

6. 인증수단 (Authentication Method, AM)

정의

인증수단은 시스템 접근에 사용되는 인증의 생성, 변경, 보호, 갱신 등을 관리하기 위한 통제 항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-AM-1	C S O	암호모듈 기반 인증
	관련 법규, 정책 및 규정 등을 준수한 암호모듈 인증체계를 적용한다.	
NNSF-AM-2	C S	비밀번호 기반 인증
	숫자·문자·특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.	
NNSF-AM-3	C S O	공개키 기반 인증
	신뢰할 수 있는 인증 기관(CA)을 통해 발급된 인증서의 유효성을 검증하고, 인증서의 발급, 갱신, 폐지 등을 관리한다.	
NNSF-AM-4	C S O	초기 인증수단 변경
	정보시스템 구성요소 배포·설치 전 기본(초기) 인증수단을 변경한다.	
NNSF-AM-5	C S	인증수단 보호
	정보시스템의 보안수준에 준하여 인증수단을 보호한다.	
NNSF-AM-6	C S O	암호화 되지 않은 인증수단 내장 금지
	암호화되지 않은 인증수단이 응용프로그램 또는 스크립트 등에 내장되거나 기능키 등에 삽입되지 않아야 한다.	
NNSF-AM-7	C S	캐시된 인증수단 재사용 차단
	캐시된 인증수단이 세션 유효 시간이 만료된 이후에 재사용되는 되는 것을 차단한다.	
NNSF-AM-8	C S	공개키 기반 저장소 관리
	네트워크, 운영체제, 브라우저, 응용프로그램을 포함하여 모든 정보시스템에 설치된 PKI 저장소에 대해 관리방안을 수립한다.	

구현 방법 예시

- **기본 인증 수단 변경 절차 설정**
  - 시스템 설치 후 첫 사용 전에 기본 인증 수단을 반드시 변경하도록 설정한다.

- **주기적 비밀번호 변경 정책**
  - 사용자의 비밀번호는 일정 기간마다 주기적으로 변경하도록 정책을 수립한다.
- **암호화된 인증 수단 저장**
  - 비밀번호 및 인증서는 해시 또는 암호화된 형식으로 저장하여 보호한다.
- **인증 수단 손실 처리 절차 마련**
  - 분실된 인증 수단은 즉시 폐기하고 새로운 인증자를 발급하는 절차를 마련한다.
- **사용자 교육**
  - 사용자들에게 인증 수단 보호의 중요성과 분실 시 즉시 보고하는 절차를 교육한다.

7. 로그인 (Login, LI)

정의

로그인은 인증 피드백 보호, 로그인 시도 제한, 시스템 사용 알림, 인증 결과 처리 등 사용자 계정 인증 과정에서의 보안 위협 방지를 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-LI-1	C S O	유효한 인증정보 노출 방지
	인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.	
NNSF-LI-2	C S O	로그인 실패에 따른 접속 제한
	정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.	
NNSF-LI-3	C S	로그인 실패에 따른 인증요소 추가
	정의한 횟수 이상 연속적으로 로그인을 실패한 경우 추가 인증수단(생체인증, OTP, ARS 등)을 적용한다.	
NNSF-LI-4	C S O	계정 잠금 해제 인증요소 추가
	계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.	

NNSF ID	보안통제 항목 설명	
NNSF-LI-5	C	정보시스템 사용 알림
	로그인(사용자 인증 성공) 후 사용자 화면에 정보시스템(서비스 등)에 관한 정보를 알림으로 표시하고, 사용자가 명확하게 인지한 상황에서 표시를 종료하도록 적용한다.	
NNSF-LI-6	C S	직전 로그인 정보 알림
	로그인(사용자 인증 성공) 후 사용자 화면에 사용자의 직전 로그인 정보를 사용자가 확인할 수 있도록 표시한다.	
NNSF-LI-7	C S	실패 로그인 정보 알림
	로그인(사용자 인증 성공) 후 사용자 화면에 사용자의 로그인 실패 정보를 사용자가 확인할 수 있도록 알림을 표시한다.	
NNSF-LI-8	C S	로그인 이력 정보 제공
	로그인(사용자 인증 성공) 후 사용자 화면에 로그인 성공 이력 정보를 제공한다.	
NNSF-LI-9	C S	
	로그인(사용자 인증 성공) 후 사용자 계정 관련 정보 변경 이력이 존재하는 경우, 일정 기간동안 사용자에게 해당 내용 알림을 표시한다.	
NNSF-LI-10	C S	로그인 부가 정보 제공
	로그인(사용자 인증 성공) 후 이전에 성공한 로그인과 관련된 부가정보(접속위치, 단말 종류 등)를 제공한다.	

구현 방법 예시

• 로그인 시도 제한 보호조치

- 기관이 지정한 인증 기준 횟수 이상으로 사용자 인증 실패 시 해당 계정의 상태를 잠금으로 변경하여 일정 시간 또는 영구히 접속을 차단한다.
- 기관이 지정한 인증 기준 횟수 이상으로 사용자 인증 실패 시 해당 계정에 대한 기본 인증 수단 외 추가 요소 인증을 요구한다.
  - ▸ 예: 기본 비밀번호 외 OTP, 생체인증, ARS, SMS, 보안질문, 모바일 공무원증, 기관 지급 인증장치 등 추가 인증 수단 사용

• 시스템 알림 설정

- 사용자가 기관 정보시스템 등 시스템 로그인 전 또는 로그인 후 해당 사용에 대한 필요 내용을 인지할 수 있도록 알림 기능을 수행한다.

- 시스템 사용에 대한 필요 내용은 시스템 사용 조건, 권한, 정책 등 기관이 지정한 내용을 출력한다.

• 이전 로그인 정보 알림

- 사용자 로그인 후 접속 시간, 접속 위치(IP 주소) 등 기관이 지정한 직전 로그인 정보를 사용자 화면에 출력한다.

• 로그인 실패 정보 알림

- 사용자 로그인 후 이전 로그아웃 시점부터 현재 로그인 시점 사이의 로그인 실패 정보를 사용자가 확인할 수 있도록 알림을 수행한다.

• 로그인 정보 제공

- 사용자 로그인 후 사용자 화면에서 사용자가 이전 로그인 관련 정보를 확인할 수 있도록 기능을 제공한다.

• 계정 정보 변경 알림

- 비밀번호 변경, 계정 복구 관련 인증 방법 변경, 계정 권한 변경 등 사용자 계정 주요 정보가 변경된 경우, 변경 시점부터 기관이 지정한 일정 기간 사용자가 변경 내용을 확인할 수 있도록 알림을 수행한다.

제3장

분리 및 격리

1. 분리 (Segregation, SG)

정의

정보서비스 및 업무정보가 보안 등급에 따라 서로 다른 보안 도메인으로 구분되도록 하드웨어, 소프트웨어, 운영체제 분리 또는 인프라, 사용자 기능 분리를 통해 각 영역에 대한 보안을 강화하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-SG-1	C S	하드웨어 기반 분리
	서로 다른 영역이 구분되도록 하드웨어를 통해 분리하고, 보안통제를 적용한다.	
NNSF-SG-2	C S O	운영체제(OS) 기반 분리
	서로 다른 영역이 구분되도록 OS를 통해 분리하고, 보안통제를 적용한다.	
NNSF-SG-3	- - O	소프트웨어 기반 분리
	서로 다른 영역이 구분되도록 소프트웨어를 통해 분리하고, 보안통제를 적용한다.	
NNSF-SG-4	C S O	IP체계 분리
	서로 다른 영역 또는 정보자산(기능 등)별 IP체계를 분리하고, 보안통제를 적용한다.	
NNSF-SG-5	C S O	보안·운영관리 인프라 분리
	보안·운영관리 인프라를 물리적으로 분리된 네트워크로 구성하여 이외 정보시스템과 분리한다.	
NNSF-SG-6	C S O	보안 기능과 사용자 기능 분리
	인증, 감사 및 데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 어플리케이션 실행 등 사용자 기능을 분리한다.	

구현 방법 예시

• 물리적 분리: 사용자 기능과 시스템 관리 기능을 서로 다른 하드웨어에서 운영하는 방식이다.

▸ 예: 회사에서 일반 직원들이 사용하는 컴퓨터는 별도의 네트워크에 연결하고, 시스템 관리자들이 사용하는 서버 관리용 컴퓨터는 다른 네트워크에 연결, 이처럼 물리적으로 다른 장비를 사용하여 시스템 관리 기능과 사용자 기능을 분리.

• 논리적 분리: 물리적으로 같은 장비를 사용하더라도, 소프트웨어나 네트워크 설정을 통해 기능을 분리하는 방식이다.

- 한 대의 서버에서 일반 사용자는 특정 소프트웨어만 접근할 수 있고, 시스템 관리자는 별도의 관리자 모드로 로그인하여 서버를 관리할 수 있도록 설정한다. 예를 들어, 가상화 기술을 사용하여 한 대의 서버에서 여러 가상 컴퓨터를 운영하여 각 가상 컴퓨터에 다른 기능을 할당할 수 있다.

• 가상화 기술

- 가상화 기술을 사용하면 하나의 물리적 서버에서 여러 개의 가상 머신을 생성하고, 각 가상 머신을 서로 독립된 환경에서 운영할 수 있다. 이로 인해, 서로 다른 보안 도메인 간의 소프트웨어적 분리가 가능하다.
  ▸ 예: 한 회사에서 직원들의 업무 데이터를 처리하는 서버와 고객 데이터를 처리하는 서버를 물리적으로 분리하기 어렵다면, 가상화 기술을 사용해 한 서버 내에서 각각의 데이터를 처리하는 가상 머신을 생성하고, 이들 간의 통신을 차단하여 분리된 환경을 유지

• 컨테이너화(Containerization)

- 컨테이너 기술을 사용해 애플리케이션과 그 종속성을 독립된 환경에서 실행할 수 있다. 컨테이너는 운영체제 레벨에서 격리되며, 다른 컨테이너와는 독립적으로 운영된다.
  ▸ 예: 한 개발팀이 여러 애플리케이션을 운영할 때, 각 애플리케이션을 별도의 컨테이너에서 실행하여, 보안 도메인 간의 간섭을 방지하고, 각 애플리케이션에 맞는 보안 정책을 적용

• 접근 제어 목록(ACL) 및 방화벽 규칙

- 소프트웨어 기반의 접근 제어 목록(ACL)과 방화벽 규칙을 사용해 네트워크 트래픽을 제어하고, 보안 도메인 간의 통신을 제한할 수 있다.
  ▸ 예: 한 기업의 네트워크에서 민감한 데이터를 처리하는 서버와 일반 데이터를 처리하는 서버 간의 통신을 제한하기 위해 방화벽 규칙을 설정하고, ACL을 사용해 특정 IP 주소만 접근할 수 있도록 제한

• **가상화 보안 및 컨테이너 보안 적용**

– 가상화 환경의 경우 VM 간 횡적이동 공격을 방어하기 위한 서버백신, 호스트 방화벽, 호스트 IDS/IPS 등의 보안기술을 적용하고 컨테이너 환경의 경우 DevSecOps 환경 구성이 가능하도록 한다.

‣ 예: 컨테이너 환경을 구성하여 사용하는 경우 이미지 취약점(CVE) 점검, 이미지 악성코드 검사, 접근제어 보안 기능 등을 사용하여 DevSecOps 환경을 구성

2. 격리 (Isolation, IS)

정의

정보시스템은 각 프로세스를 독립된 공간에서 실행하여 상호 간섭을 차단하고, 일반 사용자에게 관리 기능 및 인터페이스의 노출을 제한하며, 애플리케이션 접근을 통제하여 데이터의 무단 접근을 방지하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-IS-1	C S	프로세스 격리
	실행되는 각 프로세스(작업 또는 프로그램)가 다른 프로세스에 영향을 미치거나 간섭을 차단하기 위해 독립된 공간에서 실행한다.	
NNSF-IS-2	C S O	정보시스템 운영·관리 기능 표출 제한
	일반 사용자에게 정보시스템 관리와 관련된 기능 및 인터페이스 표출을 제한한다.	
NNSF-IS-3	C S O	애플리케이션 접근 통제
	어플리케이션에 대한 접근을 통제하여 데이터의 무단 접근을 방지한다.	

구현 방법 예시

• 프로세스 격리를 위한 격리 기술

- 각 프로세스를 독립적인 가상 머신(VM) 또는 컨테이너(Container)에서 실행하여, 프로세스 간 간섭을 원천적으로 차단한다.
  - ▸ 예: Docker나 Kubernetes를 사용하여 애플리케이션을 격리
- 하드웨어 기반 메모리 보호(Memory Isolation) 기술을 활용하여 프로세스가 다른 프로세스의 메모리에 접근하지 못하도록 설정한다.
  - ▸ 예: Intel VT-x나 AMD-V 기술 활용

• 시스템 관리 기능 및 인터페이스 제한 기술

- 역할 기반 접근 제어(RBAC)를 통해 사용자 계정을 일반 사용자와 관리자 계정으로 분리하고, 일반 사용자에게는 시스템 관리 인터페이스와 기능(서버 설정, 네트워크 구성 등)에 접근 권한을 부여하지 않음
- 일반 사용자가 관리자용 인터페이스에 접근할 수 없도록 웹 애플리케이션에서 관리자 페이지 URL을 별도로 설정하고 인증

• 애플리케이션 접근 통제 기술

- 웹 애플리케이션 방화벽(WAF, Web Application Firewall)을 이용하여 애플리케이션 계층에서 발생하는 웹 트래픽을 감지하고 이를 통한 무단 접근을 차단한다.
  - ▸ 예: WAF를 사용하여 SQL Injection, XSS, Directory Traversal 등의 공격 방어
- 다단계 인증(MFA)을 적용하여 인증 절차를 강화하고 데이터 접근 권한을 최소 권한 원칙으로 설정한다.

제4장

통제

1. 정보흐름 (Information Flow, IF)

정의

정보시스템 간에 정보가 이동할 수 있는 경로에 대한 관리 제어를 통해 비정상 동작, 외부 공격, 암호화된 정보의 흐름, 일방향 데이터 전송 및 차단, 메타데이터 활용, 정보 전송 방식 제한, 보안 및 프라이버시 규칙 등을 통제하여 민감한 정보의 유출을 방지하고 안전한 정보흐름을 보장하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-IF-1		정보흐름의 동적 통제
	정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.	
NNSF-IF-2	C S O	암호화된 정보흐름 통제
	암호화된 정보의 내용을 확인하기 위하여 정보를 복호화하거나, 확인이 불가능한 암호화된 정보는 흐름을 차단하는 등의 조치를 적용한다.	
NNSF-IF-3	C S	임베디드 데이터 삽입 차단
	임베이드된 데이터 내부에 인가되지 않은 다른 종류의 데이터가 삽입되는 것을 차단한다.	
NNSF-IF-4		메타데이터 활용 정보흐름 통제
	메타데이터(소유자, 생성일시 등 기록), 이미지/영상/오디오용 메타데이터 등을 활용하여 정보흐름을 통제한다.	
NNSF-IF-5	C	일방향 정보흐름 통제
	쌍방 정보 전송을 차단하고 일방향으로 정보흐름을 통제한다	

NNSF ID	보안통제 항목 설명	
NNSF-IF-6	C S O	필터링 규칙 정보흐름 통제
	보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.	
NNSF-IF-7	C S	데이터 유형 식별자 통제
	서로 다른 영역 간에 정보를 전송하는 경우 데이터 유형 식별자를 확인하여 전송 여부를 통제한다.	
NNSF-IF-8	C S	인가되지 않은 정보 전송 통제
	인가되지 않은 정보가 포함되었는지 검사하고 보안정책에 따라 해당 정보의 전송을 차단한다.	
NNSF-IF-9	C S O	출발지점과 도착지점 식별 및 인증
	정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.	
NNSF-IF-10	C S	정보 전송 방식 제한
	정보 전송 시 특정하게 규정된 방식(기술)을 통해서만 가능하도록 제한한다.	
NNSF-IF-11	C	데이터 전송 차단
	서로 다른 정보시스템(또는 영역 등)으로의 접근은 허용하되 데이터 전송은 차단한다.	
NNSF-IF-12		정보흐름 통제 기능 유지
	독립적인 다수의 정보흐름 통제 체계를 구성하여 하나의 통제 체계가 무력화되더라도 정보흐름 통제 기능을 유지한다.	

구현 방법 예시

• 정보흐름의 탐지 및 동적 통제 기술

- 실시간 시스템 로그 및 네트워크 트래픽을 모니터링하여 비정상 행위를 탐지하여 정보흐름을 차단한다.
  - ▸ 예: 침입 탐지 시스템(IDS), 침입 방지 시스템(IPS), 보안관제솔루션 등
- DLP(Data Loss Prevention) 솔루션 등을 통해 보안 및 프라이버시가 포함된 데이터를 실시간으로 필터링하여 전송을 차단

• 일방향 정보흐름 통제 기술

- 물리적/논리적 망연계 솔루션을 통해 일방향 데이터 흐름만 허용하고 데이터 유형 식별자를 검사하여 인터넷망으로 내부 정보 유출을 방지한다.
  - ▸ 예: 물리적 일방향 전송장치(Data Diode), 보안 게이트웨이(Security Gateway), 망연계 시스템(CDS) 등

• **암호화된 정보흐름 통제 기술**

- KCMVP 인증을 받은 암호화 검증 기술을 사용하여 전송 중인 암호화 데이터를 복호화하여 보안정책에 맞는지 검사한다.
  - ▸ 예: DRM(Digital Rights Management) 솔루션 등
- 암호화 트래픽 가시성 확보를 위한 기술 적용을 통해 유해 트래픽을 감시한다.
  - ▸ 예: SSL 가시화 솔루션 등

• **고유 출발지점 및 도착지점 인증 기술**

- 디지털 인증서 및 다중요소 인증(MFA)를 이용하여 사용자, 기관, 응용 프로그램 등의 고유 ID를 기반으로 정보시스템 식별 및 인증을 수행한다.

2. 외부경계 (External Boundary, EB)

정의

정보시스템 경계에서는 외부 네트워크와의 연결 접점을 제한하고, 승인된 통신만 허용할 수 있도록 경계 보호 장치를 활용하여 트래픽을 필터링하며, 이를 통해 외부로부터의 무단 접근을 차단하고 내부 정보시스템 구성요소 및 데이터 유출 방지, 개인 식별 정보에 대한 보호조치를 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-EB-1	C S	연결 접점 제한
	정보시스템의 외부 네트워크 연결 접점 수를 제한한다.	
NNSF-EB-2	C S O	서비스별 외부 통신 통제
	외부와 통신하는 서비스의 경계마다 통신흐름을 통제한다.	
NNSF-EB-3	C S O	화이트리스트 기반 통신 허용
	기본적으로 모든 통신을 차단한 상태에서 필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용한다.	

NNSF ID	보안통제 항목 설명	
NNSF-EB-4	C S O	분할 터널링(Split Tunneling) 방지
	인터넷 서비스와 원격접속을 통한 기관 네트워크를 동시에 이용하는 등 내·외부 통신을 동시 연결하는 분할 터널링 기법을 제한한다.	
NNSF-EB-5	C	통신 경유(proxy) 강제화
	인가된 정보시스템을 경유하여 통신하도록 통신경로를 강제화한다.	
NNSF-EB-6	C S	외부로의 사이버위협 통신 발신 제한
	내부에서 외부 네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단하고, 발신자(사용자 및 정보자산 등)를 식별한다.	
NNSF-EB-7	C S	호스트 기반 경계 보호
	정보시스템 구성요소에 호스트 기반 경계 보안체계를 적용한다.	
NNSF-EB-8	C S O	운영관리용 포트의 물리적 연결 차단
	운영관리용 포트에 인가되지 않은 장치의 포트 연결을 차단한다.	
NNSF-EB-9	C	전용 장치를 통한 관리자 권한 접속
	전용 장치를 통해서만 네트워크를 경유하여 관리자 권한으로 접속한다.	
NNSF-EB-10	C S O	정보시스템 구성요소 외부 노출 차단
	정보시스템 운영관리 및 서비스를 제공하는 구성요소가 외부 노출되지 않도록 차단한다.	
NNSF-EB-11	C S O	외부 경계 보호 기능 유지
	외부 경계를 보호하는 정보자산(보안시스템 등) 장애 시에도 보호기능은 유지되도록 구성한다.	
NNSF-EB-12	C S O	외부 통신용 정보자산(장치) 설치 금지
	외부 네트워크와 통신하는 인가되지 않은 정보자산(장치) 설치를 금지한다.	
NNSF-EB-13	C S	오류정보 발신자 전송 제한
	네트워크 규약에 따른 통신 오류 발생 시 발신자에게 피드백이나 경고를 통해 정보시스템 구성이나 취약점이 전송되지 않도록 한다.	
NNSF-EB-14		개인 식별정보 보호
	외부와 통신 시 개인을 식별하거나 특정 개인과 관련된 정보를 포함하는 경우 노출되지 않도록 조치한다.	

구현 방법 예시

• 통신 모니터링 및 제어 기술

– 시스템 내·외부 경계에서 이루어지는 통신 흐름을 모니터링하고, 보안정책에 따라 차단 또는

허용한다. 승인되지 않은 통신이나 의심스러운 트래픽이 내부 네트워크에 영향을 주지 않도록 보장한다.

- ▸ 예: 방화벽을 통해 네트워크 트래픽을 실시간으로 모니터링하며, 비인가된 접근이나 악성 코드 전송 차단, 침입 탐지 솔루션을 (IDS/IPS)으로 이상 트래픽 탐지 및 차단 등

• 서브 네트워크(DMZ) 구현 기술

- 외부에서 접근 가능한 시스템(예: 웹 서버, 이메일 서버 등)을 내부 네트워크와 물리적 또는 논리적으로 분리된 DMZ 서브 네트워크에 배치한여 외부 공격이 내부 네트워크로 확산되는 것을 방지한다.
  - ▸ 예: DMZ에 웹 서버와 일방향 전송장치(Data Diode)를 함께 배치하여 외부로부터 들어오는 요청은 허용하되 내부 네트워크로의 불필요한 트래픽은 완전히 차단

• 외부 정보흐름 제어를 위한 경계 보호 기술

- 내·외부 네트워크 간의 연결은 경계 보호 솔루션(방화벽, 일방향 전송장치, 보안게이트웨이, 망연계솔루션 등)를 통해 이루어지며, 외부 연결은 보안 정책에 따라 관리되고 무단 접근은 차단된다.
  - ▸ 예: 보안 게이트웨이(Security Gateway)를 통해 정책 기반으로 외부 전송 데이터의 필터링 및 인증 수행, 일방향 전송장치(Data Diode)로 외부에서 내부로 유입되는 데이터에 대한 통제 수행

• 외부 네트워크 연결 통제 기술

- 외부경계에서 네트워크 연결 접점을 제한하여, 외부로부터 무단 접근 위험을 최소화한다.
  - ▸ 예: 외부로의 모든 트래픽은 방화벽을 통해 관리되며, 망연계솔루션(CDS)을 통해 다중 네트워크 간 연결을 관리하여 승인된 데이터만 전송

3. 원격접속 (Remote Access, RA)

정의

원격접속 환경에서의 기밀성과 무결성을 강화를 위한 접속 통제 및 통신구간 암호화, 관리자·사용자의 접속 위치 및 권한 사용에 제한, 무단 정보 유출 방지 및 일정 시간 이후 세션 자동 종료와 같은 안전한 원격접속을 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 항목 설명	
NNSF-RA-1	C S	원격접속 모니터링 및 통제
	원격접속을 모니터링하고 통제한다.	
NNSF-RA-2	C S O	원격접속 세션 암호화
	원격접속 세션의 기밀성과 무결성을 보호하기 위해 통신구간 암호화를 적용한다.	
NNSF-RA-3	C S	원격접속 위치 통제
	보안관리 및 통제가 가능한 물리적 공간(위치) 또는 기술적 대책을 적용하여 원격접속을 허용한다.	
NNSF-RA-4	- S	관리자 권한 통제
	원격접속을 통한 관리자 권한은 제한된 조건에서만 허용해야 하며, 관리자 권한으로 실행한 명령어 이력 등은 유지한다.C등급에서는 관리자 계정의 원격접속을 금지한다.	
NNSF-RA-5	C S O	원격접속 정보 유출 방지
	원격접속에 관한 정보를 무단으로 사용하거나 외부로 유출되는 것을 방지한다.	
NNSF-RA-6	C S O	원격접속 자동 종료 및 비활성화
	일정시간 경과 등 조건에 따라 원격접속을 자동 종료하거나, 원격접속 목적이 달성된 경우 비활성화한다.	
NNSF-RA-7	C	원격 명령 신뢰성 검증
	명령을 수행하기 전에 적절한 인증 체계(암호화된 인증서, 보안 토큰, 또는 사용자 인증)를 적용하여 명령의 무결성과 출처를 검증한다.	

구현 방법 예시

• 원격접속 모니터링 및 사용 제한 기술

- 원격 접속을 위한 장치를 제한하여, 관리자가 승인한 정보시스템에서만 접속 가능하도록 설정하며 보안 소프트웨어 설치 등 보안정책을 적용한다.
  - ▸ 예: 원격 접속을 승인받은 장치(온북, 업무용 단말 등)만 네트워크 접근이 가능하도록 NAC (Network Access Control)를 적용, VPN 클라이언트 소프트웨어를 설치할 때 기관 내부의 인증서가 포함된 이미지를 배포하여 비인가 장치 접근 차단

• 원격접속 인증 기술

- 원격 접속 요청은 사전에 정보보안담당관(자)의 승인을 받은 사용자 계정만 사용할 수 있게 하며 이력 관리가 필요하다.

▸ 예: 원격 접속 계정 승인 시 다중요소 인증(MFA)를 필수 설정해야 하며, 비밀번호, 보안 토큰, 생체 인증 또는 보안 질문의 조합 등을 포함

• VPN을 통한 원격 접근 보호 기술

– 안전한 원격 접속을 위해 VPN을 이용하고 SSL/TLS 등 암호화 프로토콜을 적용하여 데이터 전송의 안전성을 보장한다.

▸ 예: VPN 연결 시 Split Tunneling(분할 터널링)을 방지하여 모든 트래픽이 VPN 서버를 경유하도록 설정하고 VPN 사용 로그를 SIEM(Security Information and Event Management) 시스템에 통합하여 실시간 모니터링

• 원격접속 모니터링 및 세션 종료 기술

– 원격 접속 활동 로그를 모니터링하여 비활성 원격접속 세션에 대한 자동 종료 및 무단 접속 등 이상 행위 시 접속 차단을 수행한다.

4. 세션 (Session, SN)

정의

세션 관리 및 보안은 각 세션의 고유 식별자를 할당하여 비정상 종료나 비활성 상태 시 즉시 종료하고 사용자의 요청 또는 조건에 따라 동시 세션 수 제한, 자동 세션 종료, 알람 메시지 제공 등 세션의 보안통제를 통해 비인가 사용자 무단 접근과 정보 유출을 방지하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-SN-1	C S O	로그아웃 세션 처리
	로그아웃 또는 비정상 세션 종료 시 연결되었던 모든 세션의 식별자를 즉시 무효화하며, 더 이상 세션이 유효하지 않도록 한다.	
NNSF-SN-2	C S O	세션별 고유 식별자
	각 사용자 세션마다 고유한 식별자를 활용하고, 고유한 식별자의 재사용을 방지한다.	
NNSF-SN-3	C	동시 접속 세션 제한
	사용자 계정 또는 정보시스템 등을 기준으로 동시 세션 수를 제한한다.	

NNSF ID	보안통제 설명	
NNSF-SN-4	C S O	세션 종료
	세션 종료 요청이 있거나 세션 종료 조건 발생 시 자동으로 세션을 종료한다.	
NNSF-SN-5		사용자 기반 로그아웃
	사용자 요청에 따라 로그아웃 할 수 있는 기능을 제공한다.	
NNSF-SN-6		종료 메시지
	사용자에게 종료되었다는 메시지를 표시한다.	
NNSF-SN-7		로그인 유효시간 경과 경고 메시지
	사용자에게 로그인 유효시간 경고 메시지를 표시한다.	
NNSF-SN-8	C S	네트워크 연결 해제
	정상 세션 종료 또는 일정 시간 비활성 상태가 유지될 경우 네트워크 연결을 자동 해제한다.	

구현 방법 예시

• 사용자 세션 고유 식별자 활용 기술

- 각 세션에 고유한 식별자를 생성하여 추적 및 관리를 용이하게 하고 로그 아웃 및 비정상 세션 종료 시 식별자를 무효화하여 세션 탈취를 방지한다.
  - 예: 사용자가 로그인하면 UUID 기반의 고유 세션 ID를 생성하고, 이는 HTTPS 쿠키로 저장

• 동시 세션 수 제한 기술

- 동일한 계정으로 접속 가능한 세션 수를 제한하여 계정 공유나 비정상적인 사용을 방지한다.
  - 예: 기관 정책에 따라 한 사용자가 사용 가능한 동시 최대 세션 수만 허용되도록 설정하고, 초과 시 이전 세션을 자동 종료

• 세션 종료 및 알림 메시지 표시

- 사용자가 로그아웃하거나, 비활성 상태가 일정 시간 지속되면 세션을 종료하고 알림 메시지를 표시 후 네트워크 연결을 해제하도록 구현한다.
  - 예: 사용자가 기관에서 정의한 일정 시간 이상 입력이 없을 경우 자동으로 세션이 종료되도록 설정하고 종료 1분전, 종료 시점에 알림 메시지를 표출한 후 네트워크 연결 해제

• **로그아웃 기능**

– 사용자가 원하는 시점에 로그아웃할 수 있도록 명시적인 종료 기능을 제공하고 로그아웃 시 세션 ID를 무효화하고 HTTPS 연결을 종료한다.

5. 무선망 접속 (Wireless Network Access, WA)

정의

무선 통신망 보안은 사용자 및 기기 인증, 통신 구간 암호화, 송수신 출력 제어, 승인되지 않은 무선망 차단, 그리고 외부인 전용 무선망 분리 및 무선망 관리 기능 보호를 통해 무선망의 기밀성과 무결성을 유지하는 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-WA-1	C S	업무용 무선망 인증 및 암호화
	사용자 인증, 기기(단말 등) 인증 및 무선 통신 구간 암호화를 적용한다.	
NNSF-WA-2	C S	업무용 무선망 인증정보 보호
	업무용 무선 통신망 서비스 식별 정보(SSID 등)를 경계지역 외부에서 확인할 수 없도록 적용하고, 무선 통신망 인증정보의 무단 사용 및 외부 유출을 방지한다.	
NNSF-WA-3	C	업무용 무선망 신호 보호
	무선 통신환경에 적합한 안테나를 선택하고 송수신 출력을 교신에 필요한 최저 출력으로 유지하여 경계지역 외부로 전파 되는 것을 방지한다.	
NNSF-WA-4	C S	비인가 무선장비 설치 차단
	업무용 무선망 서비스에 비인가 무선장비가 설치되거나 가동되는 것을 탐지하고 운용되지 않도록 한다.	
NNSF-WA-5		외부인 전용 무선망 보호
	업무용 네트워크 또는 무선망과 분리하여 외부인 전용망을 구성한다.	
NNSF-WA-6	C S O	무선망 관리기능 보호
	무선망 관리기능은 무선망에 노출되지 않아야 하며, 지정된 관리자만 접속되도록 통제한다.	
NNSF-WA-7	C S O	비인가 무선망 차단
	인가되지 않은 무선망 접속을 차단한다.	

구현 방법 예시

• 무선망 사용자 및 기기 인증 기술

- 무선망 접속 시 사용자 및 기기의 인증 절차를 수행한다.
  - ▸ 예: 사용자 ID와 비밀번호, 등록된 기기 MAC 주소를 기반으로 인증

• 무선망 암호화 적용 기술

- 무선망의 데이터 전송 시 암호화를 적용하여 기밀성을 유지한다.
  - ▸ 예: WPA3 암호화를 사용하여 통신 구간의 데이터를 보호

• 무선망 서비스 식별 정보(SSID) 보호 기술

- 업무용 무선망의 SSID Broadcast를 끄고, 연결 시 SSID를 수동으로 입력하여 SSID를 외부에서 감지할 수 없도록 비활성화

• 무선 신호 출력 조절을 통한 신호 보호 기술

- 외부로 무선 신호가 필요 이상으로 확산되지 않도록 송수신 출력을 제한하여 해킹 위험을 감소한다.
  - ▸ 예: 무선망 AP(Access Point) 중 신호 강도를 조정하여 불필요한 전파 확산을 방지하는 제품과 지향성 안테나를 사용하여 신호 확산 제어

• 외부인 전용 무선 네트워크 암호화 및 이력관리 기술

- 외부 방문자가 사용하는 무선망에도 암호화를 적용하고 사용 이력 관리
  - ▸ 예: 방문자 전용 Wi-Fi에 별도 VLAN을 구성하고, 사용 로그를 6개월간 보관

• 비인가 무선망 차단 기술

- 무선망 환경에서 비인가 AP를 탐지하고 차단한다.
  - ▸ 예: 무선망에 무선침입탐지(WIDS), 무선침입방지솔루션(WIPS)를 도입하여 승인되지 않은 AP를 식별하고 비인가 기기의 무선 접속을 차단

6. 블루투스 연결 (Bluetooth Connection, BC)

정의

정보시스템에서 블루투스 사용 시 키보드, 마우스와 같이 사용자 입력을 위한 HID(Human Interface Device) 프로파일과 데이터 전송을 위한 FTP(File Transfer Profile) 기반으로 동작하는 통신을 구분하여 정보유출 위협이 발생할 수 있는 데이터 통신을 제한하는 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-BC-1	C S	블루투스 데이터 통신 제한
	블루투스 장치 연결 시 키보드, 마우스, 오디오 등을 위한 입출력 기능 외 데이터 통신은 차단한다.	

구현 방법 예시

- **블루투스 데이터 통신 차단 기술**
  - 데이터 통신에 사용되는 블루투스 프로파일(FTP, SPP 등)을 차단하고, 입력 장치(HID)와 오디오 장치(HFP, A2DP)만 허용한다.
    - 예: 운영체제 또는 MDM(Mobile Device Management) 솔루션에서 블루투스 프로파일별 접근제어 설정
  - 블루투스 기기의 검색 모드를 제한된 검색 모드로 변경하여 외부 장치에서 블루투스 기기를 감지할 수 없도록 변경한다.

제5장

데이터

1. 암호 키 관리 (Encryption Key Management, EK)

정의

암호 키 관리는 암호 키의 생성, 배포, 저장, 사용 및 폐기 등 키의 전체 수명 주기를 안전하게 관리하기 위한 프로세스로 키의 무단 접근과 오용을 방지하고, 데이터 기밀성과 무결성을 유지하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-EK-1	C S O	암호 키 설정
	데이터 저장을 위해 암호 키를 생성하는 경우, 유형별 암호 키(대칭 키, 공개 키 등) 및 인증서를 키 관리 시스템(KMS)을 활용할 수 있다. 암호 키를 설정 시 C/S/O 보안등급별 암호화 강도, 암호 알고리즘(국산 암호, 국제표준암호 등), 암호 키 유효기간 및 갱신, 암호 키와 서명용키 분리, CRL(인증서 폐기 목록) 생성 주기 및 배포 경로 등을 설정 한다.	
NNSF-EK-2	C S	암호 키 생성
	KCMVP(KoreaCryptographic Module Validation Program) 인증을 받은 난수 발생기 또는 암호 모듈을 사용하며, 데이터의 보안 등급에 따라 소프트웨어 기반 TRNG(True Random Number Generator) 또는 하드웨어 기반 난수발생기를 사용한다.	
NNSF-EK-3	C S O	암호 키 저장
	암호 키는 암호화된 형태로 저장하거나 보안성이 요구되는 경우 보안 토큰 등을 사용하여 분리 보관한다.	
NNSF-EK-4	C S	암호 키 사용
	데이터 저장 규모 및 성능에 따라 암호화된 데이터베이스 또는 하드웨어 보안 모듈(HSM: Hardwaresecurity Module)를 활용하여 암호 키를 사용한다. 클라우드 환경에서 암호키를 안전하게 저장, 사용하기 위해 HSM을 활용할 수 있다.	

NNSF ID	보안통제 설명
NNSF-EK-5	C S O 암호 키 폐기
	암호키는 복구 불가능한 상태로 안전하게 삭제하고 동일 암호 키가 재생성 및 재사용되지 않도록 조치한다. 그리고CRL(인증서 폐기 목록) 관리해야 한다.
NNSF-EK-6	C S O 전자서명 검증
	데이터의 전송 및 저장 시 데이터 무결성 확인 및 암호화를 통한 데이터 보호를 위해 전자서명 생성 및 검증 키 관리, 표준화된 서명 검증 알고리즘과 서명용 인증서 관리, 전자서명 검증 기술을 적용한다.

구현 방법 예시

• 암호 키 관리 기술

- 암호 키는 키 관리 시스템(KMS)을 통해 안전하게 생성, 저장, 배포할 수 있다. 암호키와 서명용 키는 분리하여 관리해야 한다.
  - ▸ HSM 기반 KMS를 구축하여 암호 키 보안강도, 유효기간 및 정책 관리
  - ▸ 국산 인증 알고리즘 또는 국제표준 암호 알고리즘(AES 등) 사용
  - ▸ 암호 키를 HSM에 저장하거나, 보안 토큰(USB) 등을 사용해 분리 보관

• 키 접근 제어 기술

- 암호화 키에 접근할 수 있는 사람이나 시스템을 제한한다.
  - ▸ IAM(Identity Access Management)를 통해 키 접근 권한을 최소화

• 키 폐기

- 사용하지 않거나 만료된 키는 안전하게 삭제하거나 폐기하여 이후에 재사용될 가능성을 차단한다.

• 암호 키를 온프레미스에서 관리

- 외부 서비스 제공자가 데이터를 암호화하더라도, 암호 키는 조직의 자체 시설(온프레미스)에서 생성하고 관리한다.
  - ▸ 예: TPM(Trusted Platform Module)에 암호 키를 저장하여 물리적 보안

• 키 분할 및 분산 저장

- 암호화 키를 여러 부분으로 분할하여 각 부분을 다른 물리적 위치에 저장하여 한 곳에서 키가 탈취되더라도 전체 키를 얻지 못하게 한다.

2. 암호기술 적용 (Encryption Technology Application, EA)

정의

암호기술을 사용할 경우 보안등급과 용도에 따라 국가정보원장이 인증한 검증필 암호모듈 및 국가용 암호자재·장비를 사용하거나 특수목적용 암호자재·장비의 선택적 사용에 대한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-EA-1	C S O	검증필 암호모듈 사용
	국가정보원장이 안전성을 확인한 상용 암호모듈(검증필 암호모듈)을 사용한다.	
NNSF-EA-2	C	국가용 암호자재 및 장비 사용
	국가정보원장이 개발하거나 안전성을 확인한 암호자재 또는 암호장비 등을 사용한다.	
NNSF-EA-3	C S	특수목적용 외국산 암호자재 및 장비 사용
	외국기관 또는 외국군 등 특수목적 통신을 위해 외국산 암호자재 및 장비를 사용한다.	

구현 방법 예시

- **검증필 암호모듈 기술**
  - KCMVP 인증을 받은 암호모듈(국내 암호 알고리즘, AES 등)을 사용하여 데이터 암호화 및 복호화 수행한다.
  - 국가·공공기관 도입 기준으로 정보보안시스템, 양자암호통신장비, 암호가 주 기능인 제품군에 검증필 암호모듈 탑재를 요구한다.
    - 예: 정보보안시스템 유형(DB 암호화, 통합인증, 문서 암호화, 가상사설망, 소프트웨어 기반 보안 USB, 호스트 자료 유출 방지), 양자암호 통신장비 유형(양자키분배장비, 양자키관리장비, 양자통신암호화장비), 암호가 주 기능인 제품(메일/구간/디스크·파일 암호화, 하드웨어 구간 보안 토큰 등)

3. 데이터 전송 (Data Transmission, DT)

정의

데이터 전송은 시스템 간 데이터 및 정보를 안전하게 전송하기 위한 보안 요구사항을 명확히 하고, 이를 관리하는 절차를 포함한다. 이를 통해 전송 중인 정보가 허가되지 않은 사람이나 시스템에 의해 읽히거나 변경, 손상되지 않도록 전송 기밀성과 전송 무결성을 보호하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-DT-1	C S	전송 권한 확인
	데이터가 전송되기 전에 이를 처리하는 개인이나 정보시스템이 적절한 권한을 보유하고 있는지 확인한다.	
NNSF-DT-2	C S	정보교환 중단
	정보교환 대상 정보시스템 등에 대한 식별 및 통제가 확인되지 않을 경우 정보교환을 중단한다.	
NNSF-DT-3	C S	전송간 암호화 적용
	물리적 보안수단에 의해 전송 간 보호되지 않는 경우 전송 구간에 대한 암호기술을 적용한다.	
NNSF-DT-4		메시지 외부 암호화 보호
	메시지 외부정보를 보호하기 위한 암호기술을 적용한다.	
NNSF-DT-5		통신 패턴 은폐 또는 무작위화
	통신패턴을 숨기거나 무작위화하는 암호기술을 적용한다.	

구현 방법 예시

- **물리적 보호 방법**
  - 보호된 배포 시스템(PDS)은 기밀 정보를 전송할 때 사용하는 특별한 유선 또는 광섬유 통신 시스템이다. 이 시스템은 정보가 전송되는 동안 물리적으로 보호된 경로를 사용하여, 외부에서의 가로채기나 간섭을 방지한다.
    - 예: 군사 기밀 정보가 매우 안전한 물리적 네트워크를 통해 전송되는 경우, 보호된 배포 시스템을 사용

• 논리적 보호 방법(암호화)

- 정보가 전송되기 전에 암호화되어, 수신자가 암호를 해독할 때까지 읽을 수 없게 만든다.

• 암호화된 데이터 패킹

- 데이터를 전송하기 전에 암호화하여 패킹합니다. 이렇게 하면 패킹 과정에서 정보가 노출되거나 변조되는 것을 방지할 수 있다.

• 프로토콜 변환 시 암호화 유지

- 정보가 다른 통신 프로토콜로 변환될 때도 암호화 상태를 유지한다. 예를 들어, TLS로 암호화된 정보를 다른 프로토콜로 변환하면서도 암호화가 유지되도록 설계한다.

• 접근 제어 강화

- 전송 준비와 수신 과정에 접근할 수 있는 사용자를 최소화하고, 이들이 적절한 권한을 가지고 있는지 확인한다. 불필요한 접근을 제한하여 정보 노출 및 변조의 위험을 줄인다.

• 무작위화 기법

- 통신 패턴의 일관성을 줄이고, 통신 시 특정 시간대, 빈도, 패킷 길이 등을 무작위화하여 트래픽 분석을 통한 정보 노출을 방지한다.

• 통신 시간 무작위화

- 외부 서비스와의 통신이 일정한 간격이 아닌, 무작위적인 시간 간격으로 이루어지도록 설정한다.

• 통신 빈도 무작위화

- 패킷 전송의 빈도를 일정하지 않게 설정하여, 전송 패턴을 분석하기 어렵게 만든다.

• 패킷 길이 무작위화

- 전송되는 데이터 패킷의 크기를 일정하지 않게 무작위화하여, 패킷 분석을 통한 정보 노출을 방지한다.

• 트래픽 패딩(Traffic Padding)

- 무작위 데이터(패딩)를 통신에 추가하여 실제 데이터 전송량을 숨긴다.

4. 데이터 사용(Data Usage, DU)

정의

데이터 사용은 검색, 연산 또는 기타 데이터 처리 활동과 같이 데이터가 정보시스템 내부에서 사용되는 동안에도 데이터에 대한 보호조치를 구현하는 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-DU-1	C S	오프라인 저장
	중요 정보를 안전한 장소에 오프라인으로 보관하여 네트워크를 통한 무단 접근을 방지한다.	
NNSF-DU-2	C S O	데이터 암호화 저장
	데이터 대상 암호기술을 적용하여 기밀성을 보장한다.	
NNSF-DU-3	C S	사용중 데이터 보호
	검색, 연산, 분석 등 데이터 사용 과정에서 정보시스템 내 데이터를 보호하는 기술을 적용한다.	
NNSF-DU-4	C S	데이터 갱신 및 삭제
	필요 시 데이터를 갱신하거나 생성하여 사용하고, 필요 목적이 종료되면 데이터는 삭제한다.	

구현 방법 예시

- **오프라인 저장**
  - 민감한 정보는 필요시 오프라인 저장 장치에 저장하여 온라인 공격으로부터 보호할 수 있다.
    - 예: 중요한 파일을 외부 하드디스크 드라이브 등 백업 장치에 저장하고 이를 안전한 장소에 보관

- **데이터 암호화 및 프라이버시 보호 기술**
  - 암호화된 데이터에 대한 안전한 연산을 허용하고 처리 전반에 걸쳐 데이터의 기밀성을 유지한다.
    - 예: 동형암호, 안전 다자간 연산 등 데이터 암호기술

- **메모리 암호화**
  - 메모리 암호화를 활성화하여 데이터 사용 중에 메모리의 민감한 데이터를 보호하고 적절한

권한과 올바른 암호화 키가 있는 프로세스만 데이터를 읽을 수 있도록 한다.

• 신뢰할 수 있는 실행 환경(TEE)

- TEE 또는 보안 엔클레이브(security enclave)를 사용하여 민감한 연산을 격리하고 보호된 처리 영역 내에서 데이터를 안전하게 유지하며 무단 액세스 또는 도청으로부터 데이터를 보호한다.

• 액세스 제어 및 모니터링

- 데이터 액세스 및 처리 작업에 대한 액세스 제어 및 실시간 모니터링을 구현하고 승인된 애플리케이션과 사용자만 실제 사용 중인 데이터를 처리할 수 있도록 제한한다.

• 부채널 공격 완화

- 중요한 데이터에 액세스하기 위한 데이터 처리 중에 주 경로가 아닌 부수적인 경로로 데이터를 관찰 가능한 특성을 악용하는 부채널 공격(side channel attack)의 위험을 줄이기 위해 상시 실행, 임의 지연 등의 부채널 공격 완화 기술을 적용한다.

• 검색 시 데이터 마스킹

- 데이터 마스킹 기술을 적용하여 검색 작업 중에 데이터를 부분적으로 가리는 기법을 적용하여 필요한 데이터 쿼리를 허용하는 동시에 중요한 세부 정보를 보호한다.

제6장

정보자산

1. 모바일 단말 (Mobile Device, MD)

정의

모바일 단말은 시스템에서 허용 및 금지할 모바일 코드와 모바일 코드 기술을 정의하고 허용할 모바일 코드와 모바일 코드 기술의 사용 제한 사항과 구현 가이드를 수립하여 내부 혹은 외부에서 모바일 단말의 사용 인가, 모니터링을 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-MD-1	C S	모바일 코드 다운로드 및 실행 금지
	허용되지 않은 모바일 코드 다운로드 및 실행을 금지한다.	
NNSF-MD-2		자동 실행 금지
	응용프로그램에서 모바일 코드의 자동 실행을 방지한다.	
NNSF-MD-3	C	제한된 환경에서의 실행
	모바일 코드를 제한된 환경(가상머신 등)에서만 실행하도록 제한한다.	
NNSF-MD-4	C S	민감정보 소통 제한
	민감정보를 처리·저장·전송하는 경우 보안요건에 따른 기술적 조치가 적용되지 않은 일반적인 모바일 장비 사용을 제한한다.	
NNSF-MD-5	C S	모바일 장치 암호화 기술
	모바일 장비 저장공간 암호화 또는 컨테이너 기반 저장공간 분리 및 암호화를 적용한다.	
NNSF-MD-6	C S	데이터 자동삭제 또는 초기화
	특정 상황 또는 조건에 따라 단말 내부에 저장된 데이터를 자동 삭제하거나 초기화한다.	

구현 방법 예시

• 허용되는 모바일 코드와 허용되지 않는 코드 정의

- 안전하게 사용할 수 있는 모바일 코드(허용되는 코드)와 위험한 코드(허용되지 않는 코드)를 명확히 정의한다. 이렇게 하면, 사용자가 알 수 없는 위험한 코드를 실행하지 않도록 예방할 수 있다.
- 허용 목록 및 차단 목록 작성: 허용되는 모바일 코드(예: 신뢰할 수 있는 웹사이트에서 사용하는 JavaScript)와 허용되지 않는 코드(예: 의심스러운 출처의 Java 애플릿)를 구분하여 목록으로 관리한다..
- 기술적 차단: 보안 소프트웨어를 사용하여 허용되지 않은 코드가 시스템에서 실행되지 않도록 차단한다.

• 모바일 코드의 승인, 모니터링 및 제어

- 시스템에서 사용되는 모바일 코드는 사전에 승인받아야 하며, 사용 중에도 지속적으로 모니터링되고 제어되어야 한다. 이를 통해, 안전한 코드만이 실행되도록 보장할 수 있다.
- 전자서명 요구: 모바일 코드를 실행하려면, 신뢰할 수 있는 출처의 전자서명이 있는지 확인한다. 이를 통해, 신뢰할 수 없는 출처에서 온 코드는 실행되지 않도록 한다.
- 실시간 모니터링: 시스템이 실행 중일 때, 모바일 코드의 활동을 실시간으로 모니터링하여 이상한 행동을 감지하고 이를 차단한다.

• 모바일 기기 사용 제한과 승인

- 특정 시스템이나 네트워크에 모바일 기기를 연결할 때, 이를 허용할지 여부를 결정하고, 허용 시에는 사용 제한을 부과할 수 있다.
  - ▸ 예: 사전 승인된 모바일 기기 및 MDM 설치 시 업무정보 접근 허용

• 단말 정보 삭제

- 기관이 지정한 인증 기준 횟수 이상으로 모바일 단말을 통한 사용자 인증 연속 실패 시 중요 정보 취급·접근 단말의 경우 단말 완전 초기화를 수행하고, 개인 사용자 소유 단말의 경우 단말에 저장된 기관 관련 정보를 삭제한다.

2. 하드웨어 (Device, DV)

정의

하드웨어 보안 항목은 정보시스템과 하드웨어의 무결성을 유지하기 위해, 펌웨어 및 하드웨어 구성 요소 검증, 그리고 실행 환경의 무결성 보장을 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-DV-1	C S	하드웨어 무결성 검증
	하드웨어 구성 요소의 무결성을 검증한다.	
NNSF-DV-2	C	하드웨어 기반 펌웨어 보호(Hardware-Based Protection)
	펌웨어 구성요소 대상 하드웨어 기반 쓰기방지 기능을 활용한다.	
NNSF-DV-3	C S	하드웨어 장치(Device) 사용 제한
	정보자산 배포 또는 설치 전 특정 하드웨어 장치(USB포트, 무선통신 모듈 등)를 비활성화 또는 제거 등으로 사용을 제한한다.	
NNSF-DV-4	C S	포트 및 입출력 장치 제어
	정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.	
NNSF-DV-5	C	외부 정보자산 활용 정보처리 제한
	외부 정보자산 등을 통한 정보의 처리, 저장 및 전송 등을 제한한다.	
NNSF-DV-6	C	통신 기능이 포함된 저장장치 제한
	통신기능이 포함된 저장장치를 사용을 제한한다.	
NNSF-DV-7	C	기관 접속용 장치 제한
	외부 정보자산(시스템 등)에서 기관 네트워크 접속이 가능한 장치 사용을 제한한다.	
NNSF-DV-8	C S	장치 자동 잠금
	사용자가 일정시간 이상 정보시스템을 사용하지 않거나 방치할 경우 잠금 기능을 활성화하고, 화면에 표시되는 정보는 표출되지 않아야 한다.	
NNSF-DV-9	C	읽기 전용 매체 활용 프로그램 실행
	하드웨어 기반의 읽기 전용 매체에서 운영체제(OS) 로드 및 응용프로그램을 실행하여 실행환경의 무결성을 확보한다.	
NNSF-DV-10		저장장치 연결 금지
	정보시스템 기동 및 종료 또는 재시작하는 동안 쓰기 가능한 저장장치 연결을 금지한다.	
NNSF-DV-11		읽기 전용 매체 무결성 검증
	읽기 전용 매체에 정보를 저장하기 이전 무결성을 검증한다.	

구현 방법 예시

• 무결성 검증 도구 사용

- 개발자는 조직이 하드웨어 구성 요소의 무결성을 확인할 수 있는 도구를 제공해야 하며, 이를 통해 구성 요소의 변조 여부를 정기적으로 검증한다.

• 일련번호 검증

- 개발자가 제공한 검증 가능한 일련번호를 사용하여 각 하드웨어 구성 요소의 진위 여부를 확인하고, 복제된 하드웨어가 사용되지 않도록 방지한다.

• 복제 방지 라벨 사용

- 하드웨어 구성 요소에 복제하기 어려운 라벨을 부착하여, 하드웨어가 무단으로 교체되거나 변조되지 않았는지 확인한다.

• 하드웨어 기반의 쓰기 보호 칩 사용

- 특정 하드웨어 구성 요소에 쓰기 보호 칩을 적용하여, 펌웨어를 수정하지 못하도록 한다. 이 칩은 하드웨어적으로 쓰기 명령을 막아, 펌웨어가 원치 않게 변경되는 것을 방지한다.

• 물리적 비활성화 또는 제거

- PC의 USB 포트나 다른 포트를 물리적으로 막아 사용하지 못하게 USB 포트 등을 물리적으로 막는 캡을 사용하여 포트를 사용할 수 없도록 한다.
- CD/DVD 드라이브와 같은 입출력 장치를 물리적으로 제거하여 시스템에서 사용하지 못하게 한다.

• 논리적 비활성

- 운영체제나 보안 소프트웨어에서 특정 포트나 장치를 비활성화하도록 특정 소프트웨어를 활용하여 USB 포트를 사용하지 못하도록 설정하여, USB 드라이브를 연결해도 인식되지 않게 한다.

• 비활성 시간 설정:

- 컴퓨터나 장치에서 사용자가 일정 시간 동안 아무 작업도 하지 않으면, 시스템이 자동으로 잠금 상태로 전환(예: 화면 보호기능)되도록 설정한다.

• **CD-R 또는 DVD-R 사용**

- 운영체제 및 애플리케이션을 CD-R이나 DVD-R과 같은 읽기 전용 디스크에 저장하고 시스템을 부팅 및 운영체제와 애플리케이션을 실행한다.
- 이렇게 하면 운영체제가 설치된 후에는 수정할 수 없으므로, 악성코드나 해킹 시도로부터 안전하게 보호할 수 있다.

• **OTP-ROM 사용**

- 일회성 프로그램 가능 읽기 전용 메모리(OTP-ROM)에 운영체제를 저장하고, 이 메모리에서 운영체제를 로드하여 실행한다. OTP-ROM은 한 번 기록된 후에는 변경할 수 없으므로, 시스템의 무결성을 유지하는 데 유용하다.

3. 정보시스템 구성요소 (Information System Component, IN)

정의

정보시스템의 구성요소는 중앙화된 저장소를 통해 목록화하고, 설치·제거·업데이트 시 이를 정기적으로 갱신, 자동화된 메커니즘으로 최신성, 완전성, 정확성을 유지하여 불필요한 기능, 포트, 프로토콜, 소프트웨어를 비활성화 또는 제거하기 위한 통제항목이다.

보안통제 항목

NNSF ID	보안통제 설명	
NNSF-IN-1	C S	정보시스템 구성요소 최신상태 유지
	정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성 요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.	
NNSF-IN-2	C S	구성요소 목록 현행화
	정보시스템 구성 요소 설치, 제거, 또는 정보시스템 업데이트 시 목록을 갱신한다.	
NNSF-IN-3		구성요소 목록 자동관리
	자동화된 메커니즘을 통해 정보시스템 구성요소 목록의 최신성, 완전성, 정확성, 가용성을 유지한다.	
NNSF-IN-4	C S O	비인가 구성요소 식별
	정보시스템 내 비인가 하드웨어, 소프트웨어 및 펌웨어 구성 요소를 검사하여 식별한다.	

NNSF ID	보안통제 설명	
NNSF-IN-5		구성요소 목록 중앙관리
	정보시스템 구성요소 목록을 통합관리하기 위한 중앙화된 저장소를 운용한다.	
NNSF-IN-6	C S	물리적 위치 식별
	자동화된 메커니즘을 통해 정보시스템 구성요소의 물리적 위치를 식별한다.	
NNSF-IN-7	C S	변경 사항 테스트 및 검증
	변경 사항을 최종 적용하기 전에 테스트 및 검증을 통해 안전성을 확보한다.	
NNSF-IN-8	C S O	비인가 변경 방지
	인가되지 않은 정보시스템 구성요소 변경을 방지한다.	
NNSF-IN-9	C S O	불필요한 구성요소 제거
	필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.	
NNSF-IN-10	C S	주기적인 구성요소 제거 상태 점검
	주기적으로 사용하지 않은 기능, 포트, 프로토콜, 소프트웨어 및 서비스의 활성화 여부를 점검한다.	
NNSF-IN-11	C S	비인가 소프트웨어 실행 차단
	허가되지 않은 소프트웨어(응용프로그램)이 실행되지 않도록 차단한다.	
NNSF-IN-12	C S O	소프트웨어 기술지원 유지
	개발자, 공급업체 또는 제조업체에서 기술지원이 종료된 구성요소는 교체하거나 지속적 기술지원이 가능하도록 조치한다.	
NNSF-IN-13	C S	소프트웨어 설치 권한 제한
	소프트웨어 설치 권한은 필요한 사용자에게만 부여한다.	
NNSF-IN-14	C S O	재기동 서비스 신뢰성 확보
	정보시스템 구성요소와 서비스가 재기동(재부팅) 할 때 소프트웨어와 데이터는 신뢰된 곳으로부터 획득한다.	
NNSF-IN-15	C S O	신뢰성이 보장된 구성요소 설치
	신뢰할 수 있는 외부 기관·제조사 또는 기관이 자체 서명한 구성요소를 설치 및 활용한다.	
NNSF-IN-16	C S	정보의 비지속성
	정보시스템이 종료되거나 재부팅될 때 관련 정보(데이터 등)는 자동 삭제하여 유지되지 않도록 한다.	
NNSF-IN-17	C S	연결의 비지속성
	일시적으로 사용된 연결은 사용이 종료되면 자동으로 연결을 끊어 연결이 유지되지 않도록 한다.	

구현 방법 예시

• 불필요한 소프트웨어 및 서비스 제거

- 시스템에서 사용되지 않거나 불필요한 소프트웨어와 서비스를 제거하여 공격 표면을 줄인다.

• 포트 및 프로토콜 비활성화

- 사용되지 않는 네트워크 포트와 프로토콜을 비활성화하여 무단 접근 경로를 차단한다.

• 기능 제한 구성

- 시스템 구성 요소별로 단일 기능만 수행하도록 제한하고, 여러 기능이 동시에 동작하지 않도록 설정한다.

• 네트워크 스캐닝 도구 사용

- 네트워크 스캐닝 도구를 활용하여 시스템에서 열려 있는 포트나 불필요하게 실행 중인 서비스를 확인하고, 이를 기반으로 보안 설정을 최적화한다.

• 침입 탐지 시스템 활용

- 침입 탐지 및 방지 시스템을 사용하여, 금지된 기능이나 프로토콜이 활성화되는 것을 실시간으로 감지하고 차단한다.

• P2P 파일 공유 통제

- P2P 파일 공유 기술이 조직 내에서 무단으로 사용되지 않도록 해당 기술 사용을 제한하거나 금지하는 정책을 수립하고, 그 사용 내역을 기록한다.

• 자동화된 결함 탐지 및 보고 시스템 도입

- 시스템 내에서 발생하는 결함을 자동으로 탐지하고, 이를 정보보안 담당자에게 보고하는 시스템을 도입한다.

• 보안 패치 테스트 프로세스

- 보안 패치나 업데이트를 설치하기 전에, 별도의 테스트 환경에서 업데이트가 제대로 동작하는지, 예상치 못한 부작용은 없는지 검증하는 프로세스를 구축한다.

국가 망 보안체계
보안 가이드라인

보안통제 항목 해설서

부록 1