IV

부록

사용된 보안통제항목에 대한 보충설명

사용된 보안통제항목에 대한 보충설명

#001	보안통제항목 카드				
N2SF-LP-1	권한	최소권한 (Least Privilege, LP)	C 기밀	S 민감	O 공개
	정보시스템 접근 권한 정의		●	●	
내용	업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.				
보안요구사항	이용자 단말 보안성 유지				
관련 정보자산	① 인터넷 단말				
보충설명	N2SF 기준으로도 인터넷 단말은 O등급의 자료만을 취급할 수 있으나, O등급 자료만 인터넷을 활용할 수 있도록 보안조치를 하는 경우 S등급 이상의 자료를 취급할 수 있도록 제시하고 있다. 다만, 이러한 경우에도 S등급 이상의 자료를 인터넷에서 활용할 수 있다는 의미는 아니다. 현재 우리 군에서는 전군 차원에서 정보 · 무기체계 軍 보안대책 가이드 상 기준에 의해 자료/정보 등급을 분류하고 있으므로, 인터넷 단말에서 취급할 자료/정보의 범주를 구분하여 군 관점에서의 등급을 분류할 수 있고, 분류된 결과는 부대보안심사위원회를 통해 결정하도록 정하고 있다. 이후 N2SF 기준의 정보등급과 대응시키는 방식으로 업무정보(데이터)를 식별할 필요가 있다.				
적용기술 · 방식	-				
참조정보	국방보안업무훈령	제12조의2, 제130조, 제131조, 별표16			
	국방사이버업무훈령	-			
	기타 (가이드 · 지침 등)	정보 · 무기체계 軍 보안대책 가이드 별표3			
비고	-				

#002	보안통제항목 카드				
N2SF-DA-1	인증	단말인증 (Device Authentication, DA)	C 기밀	S 민감	O 공개
	단말 무결성 검증		●	●	
내용	단말 내 신뢰 가능한 모듈(TPM 등)을 통한 구성정보(BIOS 설정정보, Disk 설치 정보 등) 등을 확인한다.				
보안요구사항	이용자 단말 보안성 유지				
관련 정보자산	① 인터넷 단말				
보충설명	단말 무결성 검증은 접속 단말 정보 수집 및 신뢰 점검을 위한 것으로, 인터넷 단말의 네트워크 허용 여부를 판단하는 기술적 보안조치를 위한 것이다. 즉, 단말의 무결성(펌웨어 변경, 보안 설정 위반 등)을 검사하여 무결성 검증을 통과한 경우에만 네트워크 접근을 허용하도록 네트워크 접근통제에 대한 보안대책을 강구해야 한다. 이 과정에서 단말 등록에 필요한 단말 고유식별자를 생성하기 위해 TPM, BIOS UUID, MAC 주소, 디지털 인증서 등의 정보나 측정값을 활용할 수 있다. 현재 우리 군에서는 네트워크 접속 장치 정보를 체계적으로 관리할 것과 미인증 장치의 네트워크 접속을 차단하도록 정하고 있어, 단말 무결성 검증 기술을 활용하여 단말 고유식별자를 생성한다.				
적용기술 · 방식	TPM 기반 무결성 검증, EDR, SIEM 연동				
참조정보	국방보안업무훈령	-			
	국방사이버업무훈령	NS-2-1-1, NS-2-1-2			
	기타 (가이드 · 지침 등)	보안통제항목 SC_N-04			
비고	-				

#003	보안통제항목 카드				
N2SF-DV-12	**정보자산**	하드웨어 (Device, DV)	C 기밀	S 민감	O 공개
	장치 펌웨어 업데이트 검증		●		
내용	펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.				
보안요구사항	이용자 단말 보안성 유지				
관련 정보자산	① 인터넷 단말				
보충설명	현재 우리 군은 보안적합성 검증 대상 ICT 제품(네트워크장비, 정보보호체계 등) 외에는 펌웨어 업데이트에 대해 특별한 제한을 두고 있지 않다. 그러나 N2SF에서는 C등급 자료를 취급하는 단말의 경우에도 펌웨어 업데이트 시 무결성을 검증하도록 정하고 있다. 인터넷 단말이 C등급의 자료를 취급하는 경우 하드웨어 기반의 쓰기방지 기능(Write Protection) 또는 보안 부팅 옵션으로 펌웨어의 무단 변경을 방지한다. 또한 펌웨어 업데이트 시에는 디지털 서명 검증 및 무결성 체크를 수행하며, 공인된 펌웨어만 허용되도록 한다.				
적용기술 · 방식	Write Protection, Signed Firmware Update, Secure Boot, 무결성 검증				
참조정보	**국방보안업무훈령**	-			
	국방사이버업무훈령	-			
	기타 (가이드 · 지침 등)	-			
비고	-				

#004	보안통제항목 카드				
N2SF-IN-1(1)	**정보자산**	정보시스템 구성요소 (Information System Component, IN)	C 기밀	S 민감	O 공개
	정보시스템 구성요소 최신상태 유지		●	●	
내용	정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트한다.				
보안요구사항	이용자 단말 보안성 유지				
관련 정보자산	① 인터넷 단말				
보충설명	현재 우리 군은 정보시스템을 구성함에 있어 보안대책 수립 · 검토 및 보안측정 시 구성 자산목록을 최신화하여 보안대책서에 반영하도록 정하고 있다. 또한, 각군 및 기관에서 소관 사이버자산에 대한 현황을 수시로 관리할 것과 관련 체계에 대한 정보를 최신화하고, 세부정보가 미비하거나 취약점 중요도가 높은 장비 · 체계는 원칙적으로 네트워크 접근을 제한할 것을 정하고 있다. 이처럼 인터넷 단말에 대한 정보는 면밀하게 파악 · 관리되어야 할 필요가 있고, 필요시 자동화 된 방식으로 접근통제가 가능하도록 네트워크장비나 정보보호체계에 등록 · 관리하여야 한다.				
적용기술 · 방식	ASM, 자동 자산 수집 에이전트, MAC/Serial 관리				
참조정보	**국방보안업무훈령**	제120조			
	국방사이버업무훈령	제45조, SM-5-1-1			
	기타 (가이드 · 지침 등)	보안대책서 SC_A			
비고	-				