CR-14-89

nProtect UMS V3.5
인증보고서

인증번호 : CISS-0569-2014

2014년 12월

IT보안인증사무국

1. 제품 개요

nProtect UMS V3.5(이하 TOE)는 보안USB 메모리 내에 저장된 데이터에 대한 암호화 및 보안USB의 외부 반출을 통제하여 내부자산 유출을 방지하고 사용자 PC의 USB 포트에서 비인가 휴대용 저장매체에 대한 읽기/쓰기를 제어하는 소프트웨어 기반 보안USB 제품이다.

TOE는 사용자 PC에서 보안USB에 복사되는 모든 데이터를 암호화하고 보안USB의 외부 유출 시에도 인가된 사용자 이외의 접근을 통제할 수 있는 기능을 제공하며, 추가로 휴대용 저장매체로의 내부 자산의 유출 방지를 제공하는 매체제어 기능을 제공한다.

구 분		명 칭
TOE		nProtect UMS V3.5
TOE 구성요소	nProtect UMS Server	nProtect UMS Server V3.5.0.7
	nProtect UMS Console	nProtect UMS Console V3.5.0.7
	nProtect UMS Agent	nProtect UMS Agent V3.5.0.7
	nProtect Defenstick	nProtect Defenstick V3.5.0.6

[표 1] TOE 구성요소 구분

■ nProtect UMS Server (이하 'UMS Server')

UMS Server는 S/W 형태로 물리적으로 안전한 환경에 위치한 서버에 설치되며, 관리자 계정 관리와 조직 관리, Defenstick 관리, UMS Agent 정책 관리, 감사기록 조회에 대한 보안관리 기능을 제공한다.

■ nProtect UMS Console (이하 'UMS Console')

UMS Console는 S/W 형태로 UMS Server와 함께 배포되며, 관리자 PC의 웹 브라우저를 통해 UMS Console를 다운받은 후 UMS Console을 통해 UMS Server에 접속하여 보안관리를 수행할 수 있도록 기능을 제공한다.

■ nProtect UMS Agent (이하 'UMS Agent')

UMS Agent는 S/W 형태로 사용자 PC에 설치되며, UMS Server로부터 수신 받은 매체제어 정책을 적용하여 사용자 PC의 USB 포트에서 비인가 휴대용 저장매체에 대한 읽기/쓰기를 제어하는 기능을 제공한다.

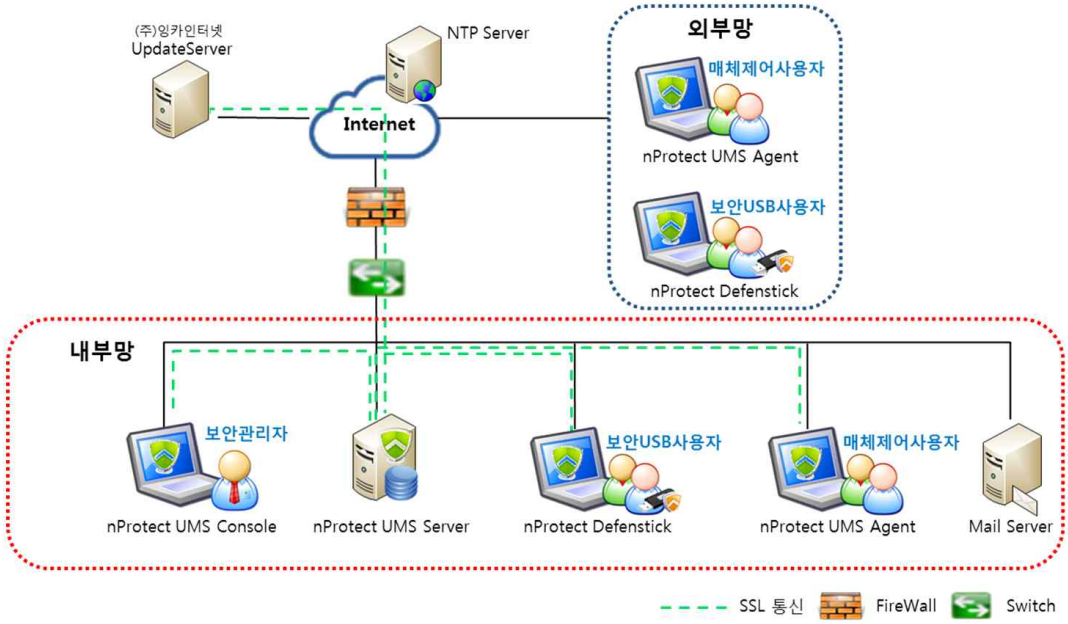
■ nProtect Defenstick (이하 'Defenstick')

Defenstick은 보안USB H/W에 탑재되어 배포되며, 사용자 데이터 복사 시 암호화되어 인가된 사용자만이 복호화하여 데이터를 읽을 수 있도록 기능을 제공한다.

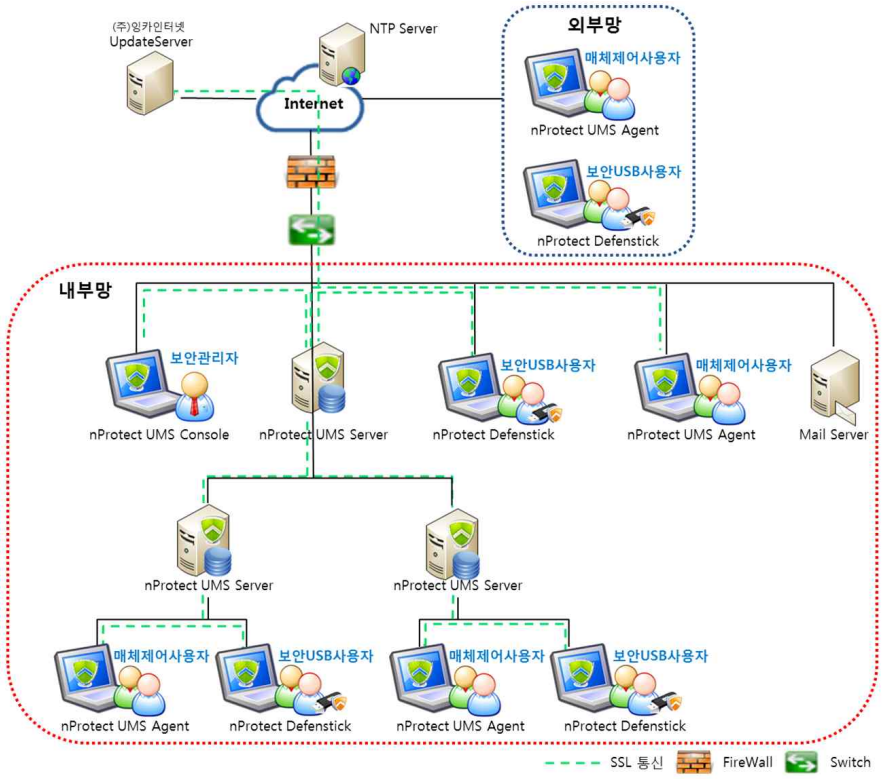
TOE는 아래의 [그림 1], [그림 2]와 같이 침입차단시스템 내에 설치되어 운영되며, 보안USB 메모리 내에 저장된 데이터에 대한 암호화 및 보안USB의 외부 반출을 통제하여 내부자산 유출을 방지하고 사용자 PC의 USB 포트에서 비인가 휴대용 저장매체에 대한 읽기/쓰

기를 제어하는 기능을 제공한다.

TOE의 운영환경은 [그림 1]과 같이 UMS Server가 단일 서버로 설치되어 운영되는 단일 서버 운영환경과 [그림 2]와 같이 다수의 UMS Server가 계층화로 설치되어 운영되는 계층화 서버 운영환경으로 구분된다.



[그림 1] TOE 운영환경-단일 서버



[그림 2] TOE 운영환경-계층화 서버

TOE의 운영을 위해 요구되는 외부 IT실체는 아래 [표 2]와 같다.

외부 IT 실체	TOE에 의해 요구되는 이유
㈜잉카인터넷 Update Server	TOE 최신의 실행코드를 갱신하기 위해 ㈜잉카인터넷의 Update Server가 요구된다.
NTP Server	TOE 운영에 따른 감사 데이터 생성 시 정확한 시간 정보 생성을 위해 신뢰할 수 있는 타임스탬프를 제공하는 NTP 서버가 요구된다.
Mail Server	감사 데이터 손실 예측 시 대응행동 및 잠재적인 보안 위반 탐지 시 대응행동으로서, 등록된 관리자의 메일 주소로 경보 메일을 발송하기 위한 메일 서버가 요구된다.

[표 2] TOE 운영을 위한 외부 실체

UMS Server, UMS Console, UMS Agent가 설치되어 운영되는 시스템의 최소 요구사항은 아래 [표 3]과 같다.

TOE	구분	최소 요구사항
UMS Server	CPU	Intel® QuadCore 3.0 GHz 이상
	RAM	8 GB 이상
	HDD	500 GB 이상
	NIC	1000 Mbps Ethernet 1개
UMS Console	CPU	Intel® DualCore 2.4 GHz 이상
	RAM	2 GB 이상
	HDD	160 GB 이상
	NIC	100/1000 Mbps Ethernet 1개
UMS Agent	CPU	Intel® DualCore 2.4 GHz 이상
	RAM	2 GB 이상
	HDD	160 GB 이상
	NIC	100/1000 Mbps Ethernet 1개

[표 3] TOE 구성요소 시스템의 최소 요구사항

UMS Server, UMS Console, UMS Agent, Defenstick이 동작되는 운영체제는 아래 [표 4]와 같다.

TOE	운영체제
UMS Server	Windows Server 2008 R2 Enterprise (64 bit)
	CentOS 6.4 (64 bit)
UMS Console	Windows 7 Professional SP1 (32/64 bit)
	Windows 8 Pro (32/64 bit)
UMS Agent	Windows Vista Business SP2 (32/64 bit)
	Windows 7 Professional SP1 (32/64 bit)
	Windows 8 Pro (32/64 bit)
Defenstick	Windows Vista Business SP2 (32/64 bit)
	Windows 7 Professional SP1 (32/64 bit)
	Windows 8 Pro (32/64 bit)

[표 4] TOE 구성요소의 운영체제

UMS Server, UMS Console, UMS Agent, Defenstick이 정상적으로 운영되기 위해 필요한 소프트웨어 요구사항은 아래 [표 5]와 같다.

TOE	소프트웨어	용도
UMS Server	MySQL 5.1.73	TSF 데이터, 감사 데이터 저장소
	NTAS middleware 3.0	UMS Server 동작을 위한 라이브러리 SDK
	Java VM 1.7.0_45	UMS Server Java 바이트코드를 수행할 수 있는 플랫폼 구성을 위한 Java Virtual Machine
UMS Console	Internet Explorer 8.0 이상	UMS Console 파일 다운로드를 위한 도구
	NTAS Frame Builder 3.0	UMS Console 동작을 위한 라이브러리 SDK
	Java VM 1.7.0_45	UMS Console Java 바이트코드를 수행할 수 있는 플랫폼 구성을 위한 Java Virtual Machine
UMS Agent	OpenSSL 1.0.1j	UMS Server와 암호화 통신을 위한 라이브러리
	nProtect Crypto V1.1	TSF 데이터, 사용자 패스워드 암호화를 위한 검증필 암호모듈
Defenstick	OpenSSL 1.0.1j	UMS Server와 암호화 통신을 위한 라이브러리
	nProtect Crypto V1.1	TSF 데이터 및 사용자 데이터, 사용자 패스워드 암호화를 위한 검증필 암호모듈

[표 5] TOE 구성요소의 소프트웨어 요구사항

Defenstick은 S/W 형태로 보안USB 하드웨어에 탑재되어 배포되며, 보안USB 하드웨어 모델은 비-TOE에 해당한다. Defenstick 보안USB 하드웨어 사양은 아래 [표 6]과 같다.

TOE	모델명	하드웨어 사양		
Defenstick	Defenstick	제품 사진		
		크기(mm)	30 * 17 * 7	
		무게(g)	3	
		색상	흰색 / 검정	
		인터페이스	USB 2.0 (USB 1.1 Compatible)	
		용량	8 GB, 16 GB, 32 GB	
		USB컨트롤러칩	SMI3257ENBA	
		전송속도 (1 GB 이상)	읽기	10 MB/s 이상
			쓰기	4 MB/s 이상

[표 6] Defenstick 보안USB 하드웨어 사양

TOE는 UMS Server, UMS Console, UMS Agent, Defenstick 및 설명서로 구성되어 있으며, TOE의 물리적 범위는 아래 [표 7]과 같다.

구 분		명 칭	형태	배포
TOE 구성요소	UMS Server	nProtect UMS Server V3.5.0.7	S/W	CD
	UMS Console	nProtect UMS Console V3.5.0.7	S/W	온라인
	UMS Agent	nProtect UMS Agent V3.5.0.7	S/W	CD
	Defenstick	nProtect Defenstick V3.5.0.6	S/W	보안USB
설명서	운영설명서	nProtect UMS V3.5 관리자매뉴얼[관리서버] v1.5	PDF	CD
		nProtect UMS V3.5 사용자매뉴얼[에이전트] v1.4		
		nProtect UMS V3.5 사용자매뉴얼[보안USB] v1.4		
	설치지침서	nProtect UMS V3.5 관리자설치매뉴얼[관리서버] v1.4	PDF	CD
		nProtect UMS V3.5 사용자설치매뉴얼[에이전트] v1.4		

[표 7] TOE 물리적 범위

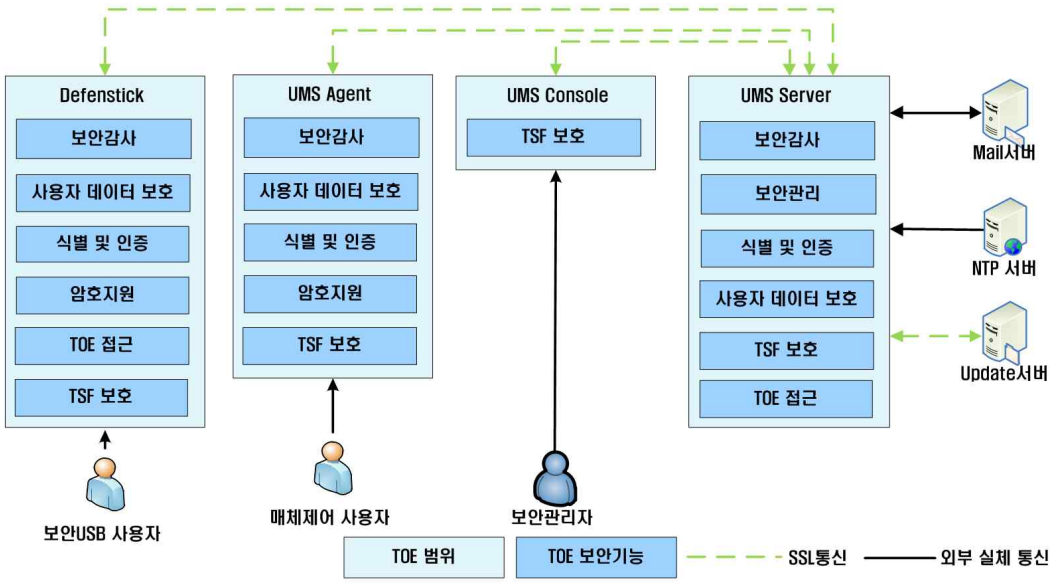
TOE는 검증필 암호모듈 의무 탑재 대상인 소프트웨어 기반 보안USB 제품으로서 [표 8]과 같이 검증필 암호모듈을 탑재하였다.

구분	내용
검증필 암호모듈 명	nProtect Crypto V1.1
검증번호	CM-79-2018.9
개발사	㈜잉카인터넷
검증일	2013년 9월 9일
효력만료일	2018년 9월 9일

[표 8] 탑재된 검증필 암호모듈

2. 주요 기능

TOE가 제공하는 일반적인 보안 기능은 [그림 3]과 같다.



[그림 3] 논리적 범위와 경계

[UMS Server]

■ 보안감사

UMS Server는 보안감사 대상 사건 발생 시 감사 데이터를 생성하고 잠재적인 위반 사항을 탐지하며, 인가된 관리자가 지정한 메일 주소로 경보 메일을 통해 보안 경보를 제공한다. 또한, 생성된 모든 감사 데이터를 안전하게 관리할 수 있도록 한다. 감사 데이터는 비 인가된 삭제를 방지하고, 임계치를 설정하여 이를 초과하는 경우 오래된 데이터를 덮어쓰기 함으로서 감사 저장소를 보호하는 기능을 제공한다.

■ 보안관리

UMS Server는 보안USB 정책 관리를 통해 Defenstick에 대한 접근통제 정책을 전달하며, 매체제어 정책 관리를 통해 UMS Agent가 설치된 사용자 PC에 연결된 휴대용 저장매체에 대한 접근통제 정책을 전달한다. 추가적으로, 시스템 반출관리를 통해 UMS Agent가 설치된 시스템의 반출입을 관리할 수 있는 기능을 제공한다.

■ 식별 및 인증

UMS Server는 보안 관리 기능을 이용하려는 관리자를 모든 행동 이전에 식별 및 인증을 수행하며, 연속된 인증 실패 처리 기능에 따라 안전한 식별 및 인증 기능을 제공한다.

■ 사용자 데이터 보호

UMS Server는 인가된 관리자가 설정한 보안관리자 접근통제 정책에 따라 보안관리자 인증 시 UMS Server에 대한 접근을 통제하는 기능을 제공한다.

■ TSF 보호

UMS Server는 SSL 통신을 통해 물리적으로 분리된 UMS Console, UMS Agent, Defenstick간 전송되는 데이터에 대한 기밀성 및 무결성을 보장하며, UMS Server는 안전한 상태를 유지하고 보안기능이 정상적으로 동작함을 보장하기 위해 시동 시 및 관리자 요구 시, 정규 운영 동안 주기적으로 프로세스의 상태를 확인하는 자체 시험을 수행하고 무결성 점검 대상인 TSF 데이터 및 TSF 실행 코드에 대한 무결성 검사를 수행한다. 또한, UMS Console을 통해 UMS Server에 로그인하는 보안관리자에 대한 인증정보 재사용 시도를 탐지 및 차단한다.

■ TOE 접근

UMS Server는 보안관리자가 일정시간(1~10분, Default: 5분) 사용하지 않을 경우, 세션을 잠기는 기능을 제공한다.

[UMS Console]

■ TSF 보호

UMS Console은 SSL 통신을 통해 물리적으로 분리된 UMS Server간 전송되는 데이터에 대한 기밀성 및 무결성을 보장한다. 또한, UMS Console은 안전한 상태를 유지하고 보안기능이 정상적으로 동작함을 보장하기 위해 시동 시 및 관리자 요구 시, 정규 운영 동안 주기적으로 프로세스의 상태를 확인하는 자체 시험을 수행하고 무결성 점검 대상인 TSF 데이터 및 TSF 실행 코드에 대한 무결성 검사를 수행한다.

[UMS Agent]

■ 보안감사

UMS Agent는 사용자 PC에 연결된 휴대용 저장매체에서 발생되는 모든 행동을 감사 데이터로 생성하며, UMS Server에 실시간으로 전송한다. UMS Server와 통신이 불가능한 경우 UMS Agent내 설치 폴더에 암호화하여 감사 데이터를 저장하며, UMS Server와 통신이 연결되었을 때 전송한다. 저장된 감사 데이터는 인가된 사용자라도 변경 및 삭제가 불가능하다.

■ 사용자 데이터 보호

UMS Agent는 UMS Server로부터 전달받은 매체제어 접근통제 정책에 따라 UMS Agent가 설치된 사용자 PC에 연결된 휴대용 저장매체(플로피디스크, 네트워크 공유폴더, DVD/CD-RW, 이동식저장장치)에 대해 쓰기 차단을 강제하며, 매체제어 접근통제 정책에 따라 휴대용 저장매체에 대한 읽기를 허용하거나 차단한다.

■ 식별 및 인증

UMS Agent는 사용자에 대해 모든 행동 이전에 식별 및 인증을 수행하며, 연속된 인증 실패 처리 기능에 따라 안전한 식별 및 인증 기능을 제공한다.

■ 암호지원

Defenstick은 보안USB사용자가 사용자 영역에 파일 복사를 시도 시 검증필 암호모듈인 nProtect Crypto V1.1에서 제공하는 ARIA-256bit/CBC모드로 암호화해서 저장한다. 암호키 등의 정보는 Defenstick의 숨김 영역에 저장되어 안전하게 관리된다.

■ TSF 보호

UMS Agent는 SSL 통신을 통해 물리적으로 분리된 UMS Server간 전송되는 데이터에 대한 기밀성 및 무결성을 보장한다. 또한, UMS Agent는 안전한 상태를 유지하고 보안기능이 정상적으로 동작함을 보장하기 위해 시동 시 및 관리자 요구 시, 사용자 요구 시 프로세스의 상태를 확인하는 자체 시험을 수행하고 무결성 점검 대상인 TSF 데이터 및 TSF 실행 코드에 대한 무결성 검사를 수행한다. 또한, UMS Agent는 무결성 오류 발생으로 인해 UMS Server와 통신되지 않는 상태에서 자동으로 오프라인 모드의 매체제어 정책을 적용하며, UMS Server와 재 연결

시 무결성이 훼손된 UMS Agent 파일을 자동 복구하고, 온라인 모드의 매체제어 정책을 재적용한다.

[Defenstick]

■ 보안감사

Defenstick은 보안USB 사용자의 데이터 복사 이벤트 및 기타 보안USB 메모리에서 발생되는 모든 행동을 감사 데이터로 생성하며, UMS Server로 실시간으로 전송한다. UMS Server와 통신이 불가능한 경우 보안USB 메모리의 보안영역에 감사 데이터를 저장하며, UMS Server와 통신이 연결되었을 때 전송한다. 저장된 감사 데이터는 인가된 보안USB 사용자라도 변경 및 삭제가 불가능하다.

■ 사용자 데이터 보호

Defenstick은 UMS Server로부터 전달받은 보안USB 접근통제 정책에 따라 사용자 PC에 연결된 Defenstick 내 데이터 영역에 대한 접근을 허용하거나 차단하며 관리자에 의해 UMS Server 보안관리를 통해 분실로 등록된 보안USB가 PC에 접속 시 분실정보가 Defenstick 내에 기록되어 더 이상 사용할 수 없도록 하며, 보안USB 메모리 내의 사용자 데이터에 접근이 불가능하게 된다. 또한, 연속된 인증 실패 사건(5회)이 발생하면 보안USB메모리 내의 데이터를 초기화하는 기능을 제공한다.

■ 식별 및 인증

Defenstick은 사용자에 대해 모든 행동 이전에 식별 및 인증을 수행하며, 연속된 인증 실패 처리 기능에 따라 안전한 식별 및 인증 기능을 제공한다.

■ 암호지원

Defenstick은 보안USB사용자가 사용자 영역에 파일 복사를 시도 시 검증필 암호모듈인 nProtect Crypto V1.1에서 제공하는 ARIA-256bit/CBC모드로 암호화해서 저장한다. 암호키 등의 정보는 Defenstick의 숨김 영역에 저장되어 안전하게 관리된다.

■ TOE 접근

Defenstick은 보안탐색기 사용시 비 인가된 사용자의 불법 정보 유출을 방지하기 위해는 최초 보안USB 인증 이후 1시간이 경과하면 세션을 종료하는 기능을 제공한다.

■ TSF 보호

Defenstcik은 SSL 통신을 통해 물리적으로 분리된 UMS Server간 전송되는 데이터에 대한 기밀성 및 무결성을 보장한다.

3. 평가결과 요약

TOE에 대한 평가는 한국시스템보증에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL2 평가보증등급을 만족하여, 공통평가기준 1부 305항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2013. 8. 8) 정보보호제품 평가인증 수행규정 (2012. 11. 1)
평가제품	nProtect UMS V3.5
보호프로파일	없음
보안요구사항	소프트웨어 기반 보안USB 제품 보안요구사항 V1.0
보안목표명세서	nProtect UMS V3.5 보안목표명세서 v1.4
평가보고서	nProtect UMS V3.5 평가결과보고서 V2.0
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R2
평가방법론	정보보호시스템 공통평가방법론 V3.1 R2
검증필 암호모듈	nProtect Crypto V1.1 ㈜잉카인터넷
평가신청인	㈜잉카인터넷
개발업체	㈜잉카인터넷
평가기관	한국시스템보증