CR-16-06

nProtect Enterprise V3.5
인증보고서

인증번호 : CISS-0687-2016

2016년 1월

IT보안인증사무국

1. 제품 개요

1.1 TOE 유형

nProtect Enterprise V3.5(이하 TOE)은 운영체제 및 어플리케이션의 보안 취약점을 악용하여 발생하는 침해사고를 예방하기 위해 PC 등 단말의 보안 패치파일을 자동으로 설치 및 관리해 주는 패치관리시스템(Patch Management System, 이하 'PMS')이다.

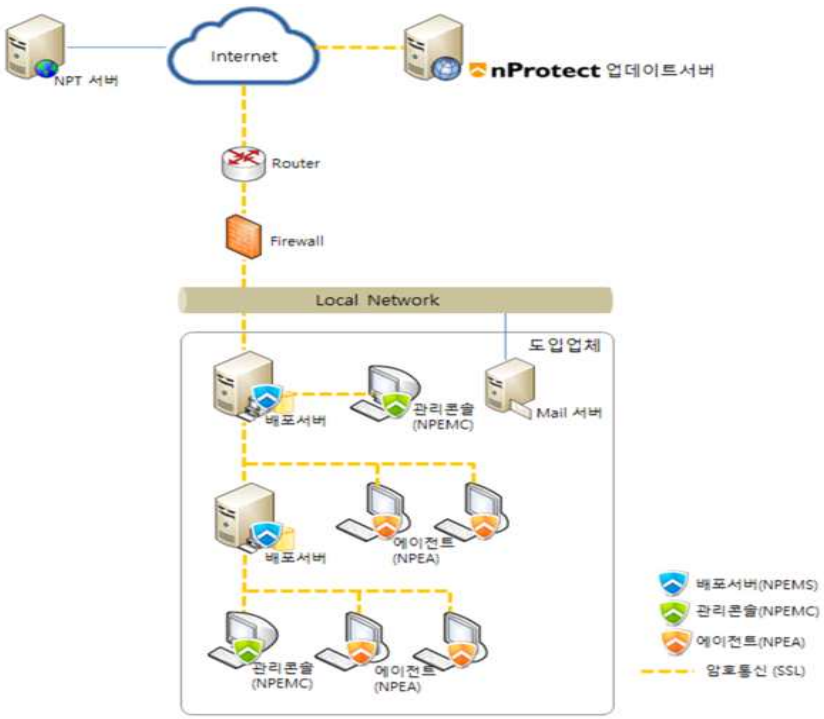
1.2 TOE 식별 및 구성요소

TOE 구성요소에 대한 식별정보는 [표 1]과 같다.

제품명	nProtect Enterprise V3.5
TOE 식별	nProtect Enterprise V3.5
TOE 구성요소 및 상세버전	nProtect NPEMS V3.5.0.9 nProtect NPEMC V3.5.0.9 nProtect NPEA V3.5.0.9

[표 1] TOE 구성요소

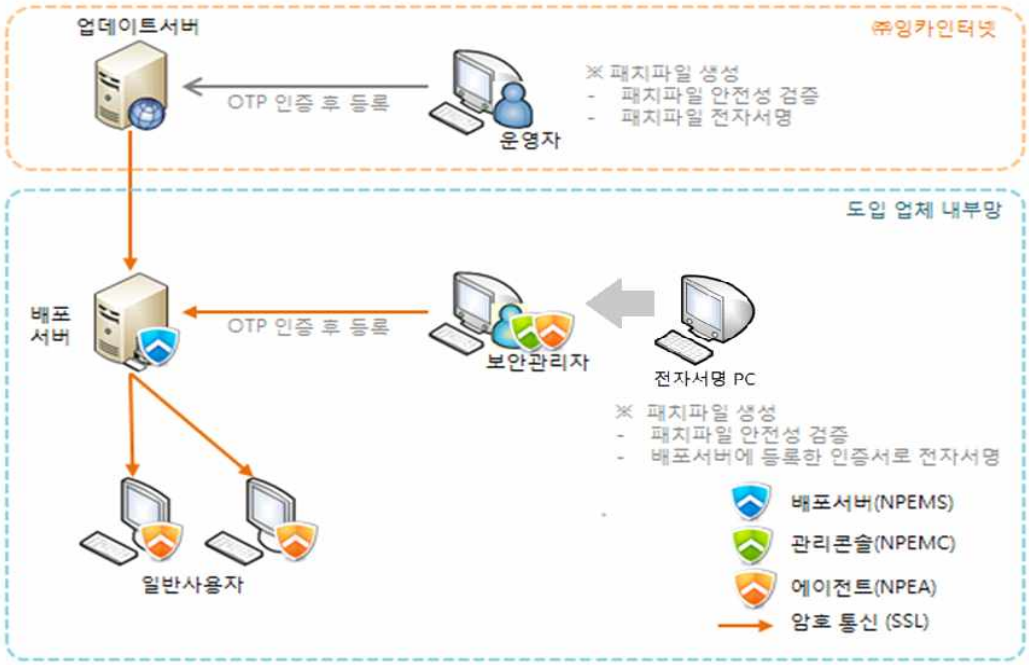
1.3 TOE 운영환경



[그림 1] TOE 운영 환경

TOE가 설치되어 운영되는 환경은 [그림1]과 같다.TOE는 패치배포 및 정책관리를 수행하는 배포서버(이하 NPEMS)와 관리자가 보안관리를 수행하는 관리콘솔(이하 NPEMC), 사용자 PC의 패치 설치/롤백을 수행하는 에이전트(이하 NPEA)로 구성된다.

NPEMS는 내부망의 물리적으로 안전한 환경에 위치하며, 필요에 따라 배포서버를 계층화 또는 복수화하여 구성할 수 있다. NPEMS는 업데이트 서버로부터 다운로드한 보안패치 파일과 인가된 관리자에 의해 등록된 보안패치 파일을 NPEA로 배포하고 NPEA에 대한 관리 기능을 수행한다. NPEMC은 신뢰할 수 있는 관리자의 PC에 구성되며, 관리자는 NPEMC를 통해 NPEMS에 접근하여 NPEA의 보안관리를 하고 감사데이터 조회를 수행한다. 관리자는 정책을 통해 NPEA에 패치파일 설치를 강제화 하거나 패치롤백을 수행할 수 있다. NPEA는 사용자PC에 구성되며, NPEMS로부터 패치파일을 제공받아 해당 단말에 설치하고, 전사적 패치정책의 적용을 위해 단말의 패치 정보를 NPEMS에 통보한다. 또한 관리자의 정책에 따라 매체제어기능과 PC방화벽 기능, 시스템 반출 기능을 수행한다.



[그림 2]패치파일 배포 경로

[그림 2]는 NPEMS에 저장되어 에이전트에 배포되는 패치파일의 배포경로를 나타낸다.

TOE 개발사인 ㈜잉카인터넷의 운영자는 [표 2]의 패치파일에 대한 안전성 검증 후 인터넷이 연결되지 않은 PC에서 전자서명을 수행하고, 전자서명 된 패치파일을 업데이트 서버에 OTP 인증 후 업로드한다. 패치파일 업로드 후 ㈜잉카인터넷의 운영자에게 업로드 알림 메일을 발송한다. NPEMS는 관리자에 의해 주기적 또는 수동으로 업데이트 서버로부터 전자서명된 패치파일을 다운로드 후, 관리자의 정책에 따라 패치파일을 NPEA로 배포한다. NPEA는 NPEMS로부터 내려받은 패치파일의 전자서명 검증 후 패치를 수행한다.

배포파일 종류	패치대상 프로그램	버전
패치 파일 ※최초 설치파일 배포하지 않음	Windows 보안패치	Microsoft Windows 7 Professional SP1 x86, x64 Microsoft Windows 8.1 Pro x86, x64
	Internet Explorer	8,9,10,11
	MS Office	2007 SP3, 2010 SP2, 2013 SP1
	Adobe reader	10, 11
	Adobe acrobat reader	DC
	Adobe flash player	13, 14, 15, 16, 17, 18
	java jre	7, 8

[표 2] 업데이트 서버로부터 배포되는 파일 목록

TOE 도입기관의 관리자는 ㈜잉카인터넷으로부터 제공받는 패치파일 이외의 패치 파일을 배포하고자 할 경우, 패치파일에 대해 안전성을 검증 후 전자서명 한 패치파일을 배포할 수 있다. 관리자는 전자서명 검증을 위해 NPEMS에 도입기관의 인증서를 등록한 후, 물리적으로 안전한 전자서명 PC에서 패치파일의 안전성 검증하고 패치파일을 등록한 인증서로 전자서명한다. NPEMS에 패치파일 업로드 시 패치파일의 서명 검증 후 관리자 OTP 인증 절차를 거치며, 업로드 완료 후 TOE는 패치파일 업로드를 알리는 메일을 최고관리자에게 발송함으로써 파일 배포의 경각심을 일으킨다.

업데이트 서버와 NPEMS 간, TOE 구성 요소 간에는 안전한 SSL 통신(TLS 1.2)을 수행함으로써 전송데이터의 기밀성 및 비밀성을 보장한다.

또한 TOE는 Mail 서버와 연동하여 보안위반 사건 발생 시 등록된 관리자의 E-Mail 주소로 경보메일을 발송한다. TOE 운영 중 발생된 감사데이터는 DBMS에 저장된다.

2. TOE 범위

2.1 TOE 물리적 범위

TOE의 물리적 범위에 포함되는 요소는 [표 3]과 같다.

구성요소	Version	형태	배포방법
nProtect NPEMS	V3.5.0.9	S/W	CD
nProtect NPEMC	V3.5.0.9		
nProtect NPEA	V3.5.0.9		
nProtect Enterprise V3.5 관리자매뉴얼[관리서버]	1.1	PDF	
nProtect Enterprise V3.5 사용자매뉴얼[에이전트]	1.1		
nProtect Enterprise V3.5 관리자설치매뉴얼[관리서버]	1.1		
nProtect Enterprise V3.5 사용자자설치매뉴얼[에이전트]	1.1		

[표 3] TOE의 물리적 범위

또한, TOE에 포함되는 3rdParty 소프트웨어는 [표 4]와 같다.

구분	버전	비고
MySQL	5.1.73	TSF 데이터, 감사데이터 저장소
NTAS middleware	3.0	NPEMS 동작을 위한 라이브러리 SDK
Java SE Runtime Environment	1.7.0_45	Java 플랫폼 구성을 위한 Java Virtual Machine
NTAS Frame Builder	3.0	NPEMC 동작을 위한 라이브러리 SDK
OpenSSL	1.0.2e	에이전트 암호통신을 위한 라이브러리
nProtect Crypto	1.1	TSF데이터 암호화를 위한 검증필 암호모듈

[표 4] TOE 운영에 필요한 3rdParty 소프트웨어

비-TOE 하드웨어 및 소프트웨어는 다음과 같다. TOE 구성요소 중 '배포서버(NPEMS)' 설치 및 운영 위하여 필요한 사양은 [표 5]과 같다.

구분	세부 사양	
NPEMS	CPU	Intel(R) QuadCore CPU 3.0 GHz 이상
	RAM	8 GB 이상
	HDD	500GB
	NIC	1000 Mbps Ethernet 1개
	OS	Windows Server 2008 R2 Enterprise (64 bit) CentOS 6.4 (64 bit)

[표 5] NPEMS 운영환경 요구사양

TOE 구성요소 중 '관리콘솔(NPEMC)' 설치 및 운영을 위해 요구되는 세부 사양은 [표 6]와 같다.

구분	세부 사양	
NPEMC	CPU	Intel(R) DualCore 2.4 GHz 이상
	Memory	2GB 이상
	HDD	160GB 이상
	NIC	100/1000 Mbps Ethernet 1개
	OS	Windows 7 Professional SP1 (32/64 bit) Windows 8.1 Pro (32/64 bit)
	소프트웨어	Internet Explorer 11

[표 6] NPEMC 운영환경 요구사양

TOE 구성요소 중 '에이전트(NPEA)' 설치 및 운영을 위해 요구되는 세부 사양은 [표 7]와 같다.

구분	세부 사양	
NPEA	CPU	Intel(R) DualCore 2.4 GHz 이상
	Memory	2GB 이상
	HDD	160 GB 이상
	NIC	100/1000 Mbps Ethernet 1개
	운영체제	Windows 7 Professional SP1 (32/64 bit) Windows 8.1 Pro (32/64 bit)

[표 7] NPEA 운영환경 요구사양

TOE 운영에 필요한 외부 IT실체는 [표 8]와 같다. 다음의 외부 IT실체는 TOE 범위에 포함되지 않지만 TOE와 상호작용하는 인터페이스는 평가범위에 포함된다.

구분	용도
nProtect 업데이트 서버	㈜잉카인터넷에서 운영하는 패치파일 업데이트 서버
메일서버	경고 메일 전송을 위한 서버

[표 8] TOE와 운영에 필요한 외부 IT실체

2.2 TOE 논리적 범위

TOE의 논리적 범위는 총 8개의 서브시스템으로 구성되며 보안 감사, 암호 지원, 식별 및 인증, 보안 관리, TSF 보호, TOE 접근, 사용자데이터보호, 보안패치로 구성되어 있다. TOE가 제공하는 일반적인 보안 특성은 다음과 같다.

■ 보안감사

TOE는 TOE에서 발생하는 감사대상 사건에 대한 감사데이터를 생성하고, 인가된 관리자에게 모든 감사데이터 검토 및 시간/유형/주체별 등 분류하여 선택적 검토할 수 있는 기능을 제공한다. 감사사건 중 잠재적인 보안위반 사건에 대한 감사 사건에 대해 인가된 관리자에게 경보 메일을 발송한다. 생성된 감사데이터는 DBMS를 사용하여 저장하여 감사데이터 비인가된 삭제를 방지한다. 감사증적소 한도가 관리자가 설정한 한도 초과 시(50~80%, Default 80%) 관리자에게 경고메일을 발송하고, 감사 증적소 한도가 90%이상 초과 시 관리자에게 경고 메일 발송 및 가장 오래된 감사데이터를 삭제 후 저장하여 감사 데이터 보호를 수행한다.

■ 암호 지원

TOE는 검증필 암호모듈 nProtect Crypto V1.1에서 제공하는 ARIA-256bit 암호알고리즘을 사용하여 일반사용자 패스워드 및 TSF데이터를 암복호화하여 안전하게 관리한다.

■ 식별 및 인증

TOE는 TOE에 접근하는 관리자 및 에이전트 사용자에게 식별 및 인증을 제공하고, 패스워드 등록 시 보안성 기준을 만족하는지 검증한다. 관리자 및 사용자 인증 과정 시 입력되는 패스워드에 대한 마스킹 처리(‘●’) 가 되고, 식별 및 인증 실패 이유를 피드백하지 않는다. 관리자는 인증 실패횟수가 관리자 설정한도(1~5번, Default 3번)에 도달하면 관리자 설

정시간(5~60분 Default 5분)동안 인증이 지연된다. 에이전트 사용자는 인증 실패횟수가 관리자 설정한도(1~5번, Default 3번)에 도달하면 관리자가 인증 잠금 해제 시까지 인증이 지연된다.

■ 보안 관리

TOE 관리자는 관리콘솔을 통해 보안관리를 수행하며, 관리자는 최고관리자와 보조관리자로 구분되며, 각 관리자 역할에 따라 기능이 분리되고 제한된다. 보조관리자는 패치관리 정책만 생성하고, TOE 운영에 필요한 중요 설정 정보에 대해 관리 및 패치관리 정책 생성/배포하는 기능은 최고관리자에게 제공한다. 또한 최고관리자가 등록한 2개 IP 주소의 관리콘솔에서만 관리접속이 가능하도록 접속 제한한다.

■ TSF 보호

배포서버와 관리콘솔은 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 검사 기능을 제공한다. 에이전트는 시동 시 및 관리자 요구 시, 정규 운영 동안 주기적으로, 일반 사용자 요구시 프로세스의 상태를 확인하는 자체 시험을 수행하고 무결성 점검 대상인 TSF 데이터 및 TSF 실행 코드에 대한 무결성 검사 기능을 제공한다. 업데이트서버와 배포서버간, TOE구성요소간 SSL 통신을 통해 전송되는 데이터에 대한 기밀성 및 무결성을 보장한다. 에이전트의 무결성 훼손 시 온라인 상태일 경우, 무결성이 훼손된 TSF데이터를 자동 복구한다.

■ TOE 접근

관리콘솔에 접속한 인가된 관리자의 비활동 시간(1~10분, Default 5분)후에 상호작용하는 세션이 잠기고, 에이전트의 패치관리 예외 및 시스템반출 가능 사용시 에이전트 사용자 비활동 시간(1~10분, Default 5분)후에 상호작용하는 세션이 종료된다. 관리자 로그인 이후 다른 단말에서 동일계정 및 동일권한으로 로그인 시도 시 이전 접속을 종료하고 신규 접속 허용한다.

■ 보안패치

TOE는 인가된 관리자에 의해 설정된 패치파일을 에이전트가 설치된 사용자 단말에 강제 설치하고 수행한 패치 결과를 서버로 전송한다. 인가된 관리자 정책 및 사용자 요청 시 롤백 기능을 제공한다. 또한 패치 오류 등의 예외사항 발생 시 주기적으로 자동 재설치를 시도한다.

■ 사용자데이터보호

TOE는 인가된 관리자의 방화벽 정책에 따라 TCP/UDP 프로토콜을 IP/Port 기준으로 제어하며, 프로세스 별, 타겟 도메인 별로 네트워크 접근을 통제하는 기능을 수행한다. TOE는 인가된 관리자의 매체제어 정책에 따라 휴대용 저장매체(이동식 디스크, 이동식 메모리, 플로피 디스크, CD/DVD, 네트워크 공유폴더)에 대해 기본적으로 읽기/쓰기를 차단하며, 정책에 따라 일부 매체에 대해 읽기 통제를 수행한다. 키보드/마우스에 대해서는 사용 여부를 통제한다. 또한 시스템반출 승인 요청을 통해 승인권한을 가진 사용자가 신청한 내역을 확인하고 에이전트가 설치된 단말 시스템의 반출입을 관리할 수 있는 기능을 수행한다.

3. 평가결과 요약

TOE에 대한 평가는 한국정보보안기술원에서 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 Enterprise V3.5
보호프로파일	없음
보안요구사항	패치관리시스템 보안요구사항 V1.0
보안목표명세서	nProtect Enterprise V3.5 보안목표명세서 V1.3
평가보고서	nProtect Enterprise V3.5 평가결과보고서 V1.20
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R2
평가방법론	정보보호시스템 공통평가방법론 V3.1 R2
검증필 암호모듈	해당사항 없음
평가신청인	㈜잉카인터넷
개발업체	㈜잉카인터넷
평가기관	한국정보보안기술원