

Endpoint Protector V5.0

인증보고서

인증번호 : ISIS-0834-2017

2017년 10월



IT보안인증사무국

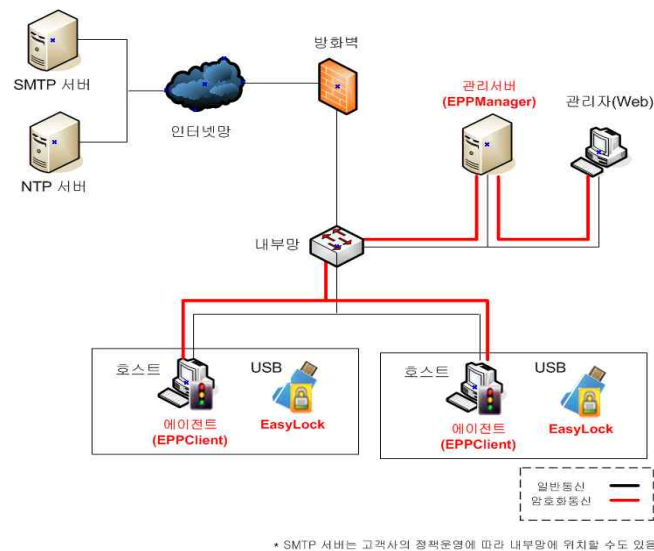
1. 제품 개요

Endpoint Protector V5.0(이하 TOE)은 사용자 PC(호스트)에 저장된 민감한 콘텐츠가 외부로 유출되는 것을 방지하기 위해 호스트와 연결된 휴대용 저장매체 및 인터페이스의 사용을 통제하고, 저장된 민감한 콘텐츠, 관리자지정 콘텐츠, 분석이 불가능한 콘텐츠에 대해 암호화를 수행하여 주는 호스트 자료유출방지 제품이다. TOE의 세부 식별자 및 배포형태는 [표 1]과 같다.

구분	식별자	유형	배포
TOE 명	Endpoint Protector V5.0	-	-
세부 식별자	Endpoint Protector V5.0.0.2		
TOE 구성요소	EPPManager V5.0.0.2	SW	CD
	EPPClient V4.9.0.1	EPPManager에 포함되어 배포	
	EasyLock V1.0.1.0		
설명서	Endpoint Protector V5.0 관리자설명서 V1.2	PDF	
	Endpoint Protector V5.0 사용자설명서 V1.0		
	Endpoint Protector V5.0 설치지침서 V1.1		

[표 1] TOE 및 구성요소 식별

TOE의 운영환경은 [그림 1]과 같다.



[그림 1] TOE 운영환경

TOE는 내부 네트워크에 설치되어 보안정책 설정 및 로그조회 등의 보안관리 기능을 수행하는 EPPManager V5.0.0.2와 호스트에 설치되는 EPPClient V4.9.0.1, 그리고 USB에 설치되는 EasyLock V1.0.1.0으로 구성된다.

EPPManager는 인가된 관리자가 TOE의 보안정책을 설정할 수 있는 보안관리 기능을 제공한다. TOE의 보안 정책 및 환경 설정 정보, 감사기록 등은 DBMS에 저장되어 관리된다. 잠재적인 보안 위반 사건 발생 시 EPPManager는 관리자에게 경고 메일을 전송한다. EPPClient는 EPPManager의 시간과 주기적으로 동기화하여 신뢰된 시간 정보를 생성하고, 이를 바탕으로 EPPManager로부터 전달받은 보안 정책을 실행하며, 운영에 따른 감사 데이터를 생성한 후 EPPManager로 전송한다. EasyLock은 호스트로부터 복사된 모든 데이터를 암호화하여 저장하는 기능을 제공한다.

관리자 PC와 Server, Server와 Agent간 전송되는 데이터는 암호통신 프로토콜을 통해 안전하게 전송된다. TOE의 운영을 위해 NTP 서버와 SMTP 서버가 요구된다.

TOE의 설치 및 운영에 필요한 소프트웨어 및 하드웨어의 요구사항은 다음과 같다.

TOE 구성요소	구분	사양
EPPManager	CPU	Intel Atom D525 2 Core 1.8 GHz 이상
	RAM	4 GB 이상
	HDD	1 TB 이상
	NIC	Intel Giga Lan Port * 2 이상
	OS	Linux Ubuntu Server V14.04.1(LTS, 64-bit)
EPPClient	CPU	Intel Pentium 4 1.5 Ghz 이상
	RAM	2 GB 이상
	HDD	500 GB 이상
	NIC	10/100Mbps * 1 이상
	무선NIC	802.11 a/b/g/n
	OS	Windows 10 Enterprise(32-bit) Windows 10 Enterprise(64-bit)
EasyLock	USB 용량	1 GB 이상
	호스트 OS	Windows 10 Enterprise(32-bit) Windows 10 Enterprise(64-bit)

[표 2] TOE의 설치 및 운영에 필요한 H/W 및 S/W 요구사항

EPPManager는 다음과 같은 제3자 제공 소프트웨어를 포함한다.

- ExtJS v6.2.1: 자바스크립트 라이브러리. 빠른 성능의 RIA (Rich Internet Application)를 구축할 수 있는 자바스크립트 프레임워크로써, 도표 구현 시 사용됨
- PHP V5.6.28: 텍스트, HTML, URL의 파싱이나 폼 처리 정규 표현식, 데이터 베이스(DB)와 사용자간의 원활한 커뮤니케이션 등을 목적으로 사용됨
- NGINX v1.10.3: 관리자가 웹 기반 보안관리 기능 제공을 위한 소프트웨어
- MySQL 5.5.57: EPPManager에 위치하며, 탐지/관리로그 및 정책데이터의 저장, 검색, 그리고 순서화 방법을 제공
- OpenSSL v1.0.2l: EPPManager와 EPPClient, EPPManager와 관리자 PC 간 전송데이터 암호화 기능 제공

EPPClient는 다음과 같은 제3자 제공 소프트웨어를 포함한다.

- SQLite 3.11: EPPClient의 TSF데이터 저장
- MagicCrypto V2.1.0: 호스트에서 검색된 민감한 콘텐츠 및 관리자 지정 콘텐츠에 대한 암호화 기능 제공
- OpenSSL v1.0.2l: EPPManager와 EPPClient 간 전송데이터 암호화 기능 제공

EasyLock은 다음과 같은 제3자 제공 소프트웨어를 포함한다.

- MagicCrypto V2.1.0: 호스트에서 USB 메모리로 이동 저장된 데이터에 대한 암호화 기능 제공

TOE에 포함된 검증필 암호모듈은 다음과 같다.

구분	내용
암호모듈명	MagicCrypto V2.1.0
검증번호	CM-118-2021.8
개발사	(주)드림시큐리티
검증일	2016년 8월 1일

[표 3] 검증필 암호모듈 정보

TOE의 보안관리를 위한 관리자 PC의 요구사항은 다음과 같다.

구분	사양
CPU	Intel Pentium4 2 GHz 이상
RAM	2 GB 이상
HDD	500 GB 이상
NIC	10/100 Mbps * 1 이상
운영체제	Windows 10 Home (64-bit) Windows 10 Pro (64bit)
소프트웨어	FireFox v53.0

[표 4] 관리자 PC의 H/W 및 S/W 요구사항

인증 효력에 관한 고지: 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

2. 주요 기능

TOE가 제공하는 일반적인 보안 특성은 다음과 같다.

■ 호스트 데이터 보호

TOE(EPPClient)가 휴대용 저장매체 및 인터페이스에 대해 적용하는 정책은 각각 [표 4] 및 [표 5]와 같다.

매체	통제정책
이동식 메모리	사용 허용/ 차단 민감한 콘텐츠 허용/차단
이동식 디스크 (외장하드, USB 메모리)	
CD/DVD/BD	사용 허용/ 차단
MTP(Media Transfer Protocol Device): Android v4.1 이상	
PTP(Photo Transfer Protocol Device): 스캐너 등 이미지 스캔장치	
iPhone (iPhone 4/6s/7plus)	
iPad (iPad 2/3/Air/Air2)	
iPod (iPod Nano/Shuffle4)	

[표 4] 휴대용 저장매체에 대한 정책

매체	통제정책
무선랜	사용 허용/차단
모뎀	
Bluetooth	
USB 포트	
Serial 포트	
네트워크 공유폴더	
Parallel 포트	
적외선 포트	
Internal Memory Card Reader	
Webcam (Microsoft LifeCam VX-3000)	
eSATA	
Additional Keyboard	
Additional Mouse	
로컬프린터	

[표 5] 외부 인터페이스에 대한 정책

TOE(EPPClient)는 호스트에서 매체 및 Application(웹브라우저, 이메일, 인스턴트 메시징, 클라우드 서비스/파일 공유, 소셜 미디어/기타)으로 콘텐츠가 전송될 시, 아래와 같은 경우에 콘텐츠 전송을 차단한다.

- 민감한 콘텐츠 흐름제어: 해당 콘텐츠의 속성값이 관리자가 지정한 콘텐츠 흐름 제어 정책의 속성값(신용카드/개인정보(이메일주소, 주민등록번호, 여권번호, 전화번호, 운전면허번호, 건강보험번호)의 정규식, 파일 확장자)과 일치할 경우
- 관리자 지정 콘텐츠 흐름제어: 해당 콘텐츠의 속성값이 관리자가 지정한 콘텐츠 흐름제어 정책의 속성값(관리자가 정의한 콘텐츠 키워드)과 일치할 경우
- 분석이 불가능한 콘텐츠 흐름제어: 해당 콘텐츠가 분석이 불가능한 콘텐츠(필터 대상 외 파일, DRM File, 암호화된 파일, 비번이 설정된 압축파일, 비정상 확장자를 가진 파일)일 경우

구분	세부 구분	프로토콜	통제 정책
파일전송 제어대상	웹브라우저	HTTP, HTTPS	파일 첨부 차단/허용, 민감 콘텐츠 파일 첨부 차단/허용
	- Chrome V57(32/64 bits)		
	이메일	SMTP	
	- Outlook 2016(Attachments)		
인스턴트 메시징	-		
- Skype 7.35.65.103			
- Kakao Messenger 2.5.5			

구분	세부 구분	프로토콜	통제 정책
	파일공유	-	
	- Naver Cloud 1.5.2		
	- BitTorrent 7.1		
	- Dropbox(Desktop) 24.4		
	- FTP Command	FTP	
	미디어	-	
	- EasyLock V1.0.1.0		
- iTunes 12.6.0.100			
- FileZilla 3.25.1	FTP		
- Clipboard	-	민감한 콘텐츠 복사 허용/차단	
구분	세부 구분	파일종류	
파일종류 필터대상	그래픽 파일	JPEG, PNG, BMP, TIFF	
	오피스 파일	Word, Excel, PowerPoint, TXT, PDF, HWP - MS Office 2016 - Hancom Office Neo	
	압축 파일	ZIP, ZIP/Password, RAR	
구분	세부 구분	필터 유형	
개인정보 콘텐츠 필터대상	신용카드	Amex, Diners, Discover, JCB, Mastercard, Visa	
	개인정보	이메일주소, 주민등록번호, 여권번호, 전화번호, 운전면허번호, 건강보험번호	

[표 6] 파일전송 제어 대상

TOE(EPPClient)는 호스트에 저장된 민감한 콘텐츠 및 관리자 지정 콘텐츠에 대해 해당 콘텐츠를 관리자 요청 시, 또는 정의된 주기마다 검색 후 설정에 의해 해당 콘텐츠를 암호화 처리하며, 인가된 관리자에 의한 복호화 및 편집 완료된 콘텐츠에 대한 재암호화 기능을 제공한다. TOE는 민감한 콘텐츠에 대한 완전 삭제 기능을 제공한다.

구분	세부 구분	파일종류
파일종류 필터대상	그래픽 파일	JPEG, PNG, BMP, TIFF
	오피스 파일	Word, Excel, PowerPoint, TXT, PDF, HWP - MS Office 2016 - Hancom Office Neo
	압축 파일	ZIP, ZIP/Password, RAR
구분	세부 구분	필터 유형
개인정보 콘텐츠 필터대상	신용카드	Amex, Diners, Discover, JCB, Mastercard, Visa
	개인정보	이메일주소, 주민등록번호, 여권번호, 전화번호, 운전면허번호, 건강보험번호

[표 7] 검출 대상 민감한 콘텐츠

■ 보안감사

TOE는 각 보안기능에 대해 사건 일시, 사건 유형, 주체의 신원 정보 등을 포함하여 로그데이터를 생성하고, 안전하게 DB에 저장한다. TOE는 인가된 관리자에게 로그 데이터에 대한 조회 기능과 통계보고서를 생성 기능을 제공한다. TOE는 디스크 사용량의 사전경보 임계치 초과 시 및 포화 임계치 초과 시, 무결성 검사 실패 시와 같은 TOE 운용의 중요 사건 발생 시 관리자에게 경보메일을 통해 사건의 발생을 통보한다. TOE는 감사저장소의 용량이 사전 정의된 임계치에 도달 시 관리자에게 경보를 발송하며, 감사저장소의 용량이 사전 정의된 포화 임계치에 도달 시 오래된 로그데이터를 덮어 쓴다.

■ 식별 및 인증

TOE는 관리자에 대해 식별 및 인증기능을 제공한다. 이때, TOE는 입력되는 패스워드를 마스킹 처리한다. TOE는 식별 및 인증 실패 횟수가 지정된 한도에 도달 한 관리자 계정에 대해 정의된 시간동안 로그인을 지연한다. TOE는 관리자의 로그인 이후, 중복 로그인을 방지하는 기능을 제공한다.

■ TSF 보호

TOE는 TOE 운영에 기반이 되는 TOE의 주요 프로세스들이 정상적으로 동작하는지 여부에 대해 최초 구동 시와 구동이후 주기적으로 검사를 수행한다. 검사 결과 동작하지 않는 프로세스가 발견될 시 즉시 재 구동하여 TOE의 정상적인 운영 상태를 유지시키며, TOE의 TSF실행코드 및 TSF데이터에 대해 최초 구동 시, 구동 이후 주기적으로, 관리자가 원할 시 무결성 침해 여부를 검사하여 무결성 침해가 발견될 경우 관리자에게 경보메일을 발송한다.

■ 보안관리

TOE는 인가된 관리자(최고관리자 1개의 계정)에게 TOE의 모든 보안기능에 대한 관리 기능을 제공한다. 관리자는 TOE에 식별 및 인증 과정을 거쳐 접속한 후 보안 기능 관리, 보안 속성 관리, TSF데이터 관리를 수행할 수 있다. 보안관리를 위해 관리서버에 접속을 시도하는 최고관리자는 설정된 2개 이하의 IP에서만 접속할 수 있다.

■ USB 데이터 보호

TOE(EasyLock)는 호스트로부터 콘텐츠가 전송되었을 시 해당 콘텐츠를 암호화하여 저장한다.

■ 암호지원

TOE(EPPClient와 EasyLock)는 호스트 내에서 검색된 민감한 콘텐츠와 호스트로부터 전송된 콘텐츠를 보호하기 위해 암호키 생성 알고리즘과와 암호화 알고리즘을 사용하여 콘텐츠 암호화를 수행하며, 이전 암호키를 안전하게 파기한다.

3. 평가결과 요약

TOE에 대한 평가는 한국시스템보증(주)에서 수행하였다. 평가는 제품이 공통평가 기준 2부와 3부의 EAL2 평가보증등급을 만족하여, 공통평가기준 1부 305항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2017. 8. 24) 정보보호제품 평가인증 수행규정 (2017. 9. 12)
평가제품	Endpoint Protector V5.0
보호프로파일	없음
보안요구사항	호스트 자료유출방지 제품 보안요구사항 V1.0 매체제어 제품 보안요구사항 V1.0
보안목표명세서	Endpoint Protector V5.0 보안목표명세서 V1.4 (2017.10.16)
평가보고서	Endpoint Protector V5.0 평가결과보고서 V3.00 (2017.10.16)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R2
평가방법론	정보보호시스템 공통평가방법론 V3.1 R2
검증필 암호모듈	MagicCrypto V2.1.0 (주)드림시큐리티
평가신청인	(주)코소시스코리아
개발업체	(주)코소시스코리아
평가기관	한국시스템보증(주)