KECS-CR-05-23

(주)LG CNS SafezoneIPS V3.0(SZ-4000) 인증보고서

인증번호 : KECS-NISS-0050-2006

2008년 8월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2006. 8.30	-	최초 작성
01	2007.10.26	-	권리변동(LG엔시스→LG CNS)
02	2008. 8.27	12p	인증효력유지내역 추가

본 문서는 (주)LG CNS의 SafezoneIPS V3.0(SZ-4000)에 대한 인증보고서이다.

인증기관

IT보안인증사무국

평가기관

한국정보보호진흥원

목 차

1. 요약 ····· 1
2. 식별정보 ····· 2
3. 보안정책 ····· 3
4. 가정사항 및 범위 ····· 3
   4.1 가정사항 ····· 3
   4.2 위협 대응범위 ····· 4
5. 제품정보 ····· 4
6. 설명서 ····· 5
7. 제품시험 ····· 5
   7.1 개발자 시험 ····· 5
   7.2 평가자 시험 ····· 6
8. 평가환경 ····· 7
9. 평가결과 ····· 7
10. 권고사항 ····· 10
11. 용어 정의 ····· 10
12. 참고문헌 ····· 11

1. 요약

본 보고서는 SafezoneIPS V3.0(SZ-4000)에 대한 정보보호시스템 공통평가기준(2005년 5월 21일 고시)(이하 '공통평가기준'이라 한다) EAL4 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과, 평가결과의 타당성 및 적합여부를 서술한다.

SafezoneIPS V3.0(SZ-4000)에 대한 평가는 한국정보보호진흥원에서 수행되었으며, 2005년 12월 9일에 평가 완료되었다. 본 보고서의 내용은 한국정보보호진흥원에서 제출한 평가보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 공통평가기준 3부의 EAL4 평가보증등급을 만족하여, 공통평가기준 1부 175항에 따라 "적합"한 것으로 평가하였다. 또한, 평가제품은 네트워크 침입방지시스템 보호프로파일 V1.1 (2005. 12. 21)을 만족한다.

SafezoneIPS V3.0(SZ-4000)은 내·외부 네트워크가 분리된 유일한 위치에 설치되어 통과하는 모든 네트워크 트래픽에 대하여 공격여부를 판단하여 유해트래픽인 경우는 차단하고 공격정보를 관리자에게 통보하는 침입차단 기능을 갖는 침입방지시스템으로, TOE는 다음의 보안기능을 제공한다:

- 침입탐지 및 침입대응 기능
- 관리자에 대한 식별 및 인증 기능
- 실행파일 및 환경설정 파일에 대한 무결성 점검 기능
- 보안속성 설정, 조회, 변경 등 보안관리 기능
- 감사기록 기능 및 고가용성 기능

인증기관은 평가자의 평가활동 및 시험절차를 점검하고, 기술적인 문제점 및 평가절차에 대한 지침을 제공하고, 각 평가단위 및 평가보고서의 내용을 검토하였다. 인증기관은 평가결과가 평가제품이 보안목표명세서에 서술된 모든 보안기능 요구사항 및 보증요구사항을 만족함을 보증함을 확인하였다. 따라서, 인증기관은 평가자의 관찰사항, 평가결과가 정확하고 타당하며, 적합여부 평가결과가 정확하다고 인증하였다.

인증 효력범위 : 본 인증보고서에 포함된 정보는 SafezoneIPS V3.0(SZ-4000)이 대한민국 정부기관에 의한 사용 승인 또는 품질보증을 의미하지 않는다.

2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가제품 식별정보

평가지침	정보보호시스템 평가인증지침 (2005. 5. 21) 정보보호시스템 평가인증 수행규정 (2005. 5. 7)
평가제품	SafezoneIPS V3.0(SZ-4000)
보호프로파일	네트워크 침입방지시스템 보호프로파일 V1.1 (2005. 12. 21)
보안목표명세서	SafezoneIPS V3.0(SZ-4000) 보안목표명세서 V1.00.02 (2005. 12. 05)
평가보고서	SafezoneIPS V3.0(SZ-4000) 평가보고서, 발행버전 1.01 (2005. 12. 09)
적합여부 **평가결과**	공통평가기준 2부 적합 EAL4 보증등급의 3부 적합
평가기준	정보보호시스템 공통평가기준 (2005. 5. 21) 최종해석(Final Interpretation) (2005. 6)
평가방법론	정보보호시스템 공통평가방법론 V2.2 최종해석(Final Interpretation) (2005. 6)
평가신청인	(주)LG CNS
개발업체	(주)LG CNS
평가자	한국정보보호진흥원 보안성평가센터 평가2팀 박순태, 안성수, 이승환, 송규철, 이성재(평가1팀)
인증담당자	IT보안인증사무국

평가제품은 하드웨어 일체형 서버인 SafezoneIPS V3.0(SZ-4000)으로 이의 요구사항은 다음 [표 2]와 같다.

[표 2] SafezoneIPS V3.0(SZ-4000) 시스템 사양

항목		사양
SafezoneIPS 엔진	CPU	Intel 2.8GHz * 2개
	Memory	4GB
	인터페이스	서비스 포트 2개(Giga용 Port) * 2 관리용 포트 2개(10/100용 1개, 1000용 1개)
	HDD	73 GB
	운영체제	SZOS V1.0 (자체 OS)
관리콘솔	CPU	2.4Ghz 1개 이상
	Memory	1 GB 이상
	인터페이스	2 포트 이상
	HDD	72GB * 2개이상
	운영체제	MS Windows 2000 이상
	데이터 관리	MS SQL Server 2000 이상

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다:

침입방지 침입이 발생한 경우 침입을 시도하는 호스트의 접근은 차단해야 한다.

식별및인증 관리자는 TOE의 보안기능을 사용하기 전에 반드시 식별 및 인증 과정을 통과해야 한다.

무결성점검 TOE의 실행파일 및 환경설정 파일 등 중요 파일에 대해서는 무결성 점검 기능을 사용하여 주기적으로 불법적인 변경 여부를 점검해야 한다.

보안관리 안전한 통신을 통해 접근한 인가된 관리자만 보안관리 기능을 사용할 수 있다.

감사기록 모든 행동에 대한 책임을 추적하기 위해 보안관련 사건은 기록 및 유지되어야 하며, 기록된 데이터는 검토되어야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.물리적보안 TOE는 인가된 자만이 접근 가능한 물리적으로 안전한 환경에 위치한다.

A.보안유지 네트워크 구성 변경, 호스트의 증감, 서비스의 증감 등으로 내부 네트워크 환경이 변화될 때, 변화된 환경과 보안정책을 즉시 TOE 운영정책에 반영하여 이전과 동일한 수준의 보안을 유지한다.

A.신뢰된관리자 TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대하여 적절히 교육 받았고, 관리자 지침에 따라 의무를 수행한다.

A.운영체제보강 TOE에 의해 필요하지 않은 운영체제상의 서비스나 수단 등을 제거하는 작업과 운영체제상의 취약점에 대한 보강 작업을 수행하여 운영체제에 대한 신뢰성과 안전성을 보장한다.

A.유일한연결점 TOE는 네트워크상에 설치 운영되는 경우, 네트워크를 외부망과 내부망으로 분기해주며, 외부망과 내부망간의 모든 통신은 TOE를 통해서만 이루어진다.

A.안전한 TOE 외부서버 TOE가 제공하는 보안기능을 위해 TOE 외부에 존재하는 신뢰 된 시각 유지를 위한 NTP (Network Time Protocol) 서버와 최신 침입패턴규칙을 제공하는 업데이트 서버는 안전하다.

A.TIME TOE가 운영되는 IT 환경은 RFC 1305를 따르는 NTP 서버 또는 운영체제로부터 신뢰할 만한 Timestamp가 제공된다.

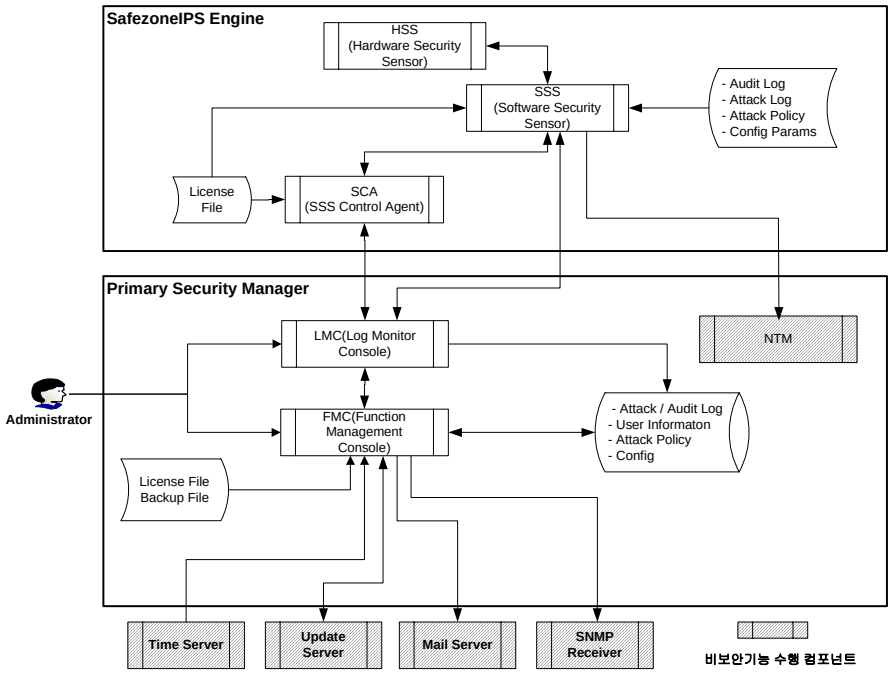
4.2 위협 대응범위

평가제품은 네트워크 트래픽에 대한 엄격한 통제를 요구하는 IT 환경에 적합한 수준의 보안위협에 대한 대처방법을 제공한다. 평가제품은 보안기능을 무력화하거나 우회하는 직접적인 물리적 공격에 대한 대처방법을 제공하고 있지 않다. 그러나, 평가제품과 연결된 네트워크에서 중간 수준의 전문지식, 자원, 동기를 가진 위협원에 의해 발생하는 논리적 공격에 대한 대처방법을 제공한다. 또한, 인가된 관리자로 가장하여 TOE에 접근하거나, 저장용량을 소진시키고, 서비스 공격·비정상적인 패킷 공격에 대한 대처방법을 제공한다. 연속적인 인증시도에 대한 대처와 제공되는 보안기능을 우회하는 할 수 없고, TSF 데이터의 무단변경에 대한 대처방법을 제공한다.

모든 보안목적 및 보안정책은 식별된 보안위협에 대한 대처방법을 제공할 수 있도록 서술되어 있다.

5. 제품정보

평가제품은 침입방지기능을 제공하며, 기본구조는 다음과 같다.



평가제품은 아래와 같은 주요 서브시스템으로 구성된다.

- **하드웨어 보안 센서(SY_HSS)**

외부에서 입력되는 패킷을 검사하고, 관리자가 설정한 보안정책에 따라 공격패킷을 차단하거나 전달한다. 침입탐지 대상사건에 대한 정보수집, 무결성공격 탐지, 정적공격 탐지, 상세차단, 차단예외 적용 등의 기능을 수행한다.

- **소프트웨어 보안 센서(SY_SSS)**

하드웨어 보안 센서의 운영 및 제어를 담당하며, 하드웨어 보안 센서에서 전달받은 데이터를 콘솔로 전달하는 기능을 수행하며, 2차 필터링 기능을 수행한다. DoS와 같은 형태의 동적공격 탐지, 이상트래픽 Ratelimit 공격 탐지, 침입탐지로그 및 하드웨어 보안 센서 운영로그생성기능을 수행한다.

- **소프트웨어 보안 센서 제어 에이전트(SY_SCA)**

소프트웨어 보안 센서의 동작(시동, 정지, 상태확인)을 제어하며, 소프트웨어 보안 센서를 주기적으로 확인하여 비정상적으로 종료하면 재시동을 수행한다.

- **로그 관리 콘솔(LMC)**

MS Windows 기반의 GUI 응용프로그램으로 엔진과의 인터페이스 및 SSS로부터 수신된 침입로그를 화면으로 출력한다.

- **기능 관리 콘솔(FMC)**

감사로그, 사용자, 보안정책 등 각종 보안속성을 관리하며, 관리자 식별 및 인증, 무결성 점검 기능, 백업 기능 등을 수행한다.

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다:

- SafezoneIPS V3.0(SZ-4000) 설치 지침서 Version 1.00.01, 2005년 12월 5일
- SafezoneIPS V2.0(SZ-4000) 관리자 설명서 Version 1.00.02, 2005년 12월 5일

7. 제품시험

7.1 개발자 시험

- **시험방법**

개발자는 제품의 보안기능을 고려하여 시험항목을 도출하였다. 각 시험항목은

시험서에 서술되어 있다. 시험서에 서술된 각 시험항목은 다음의 세부 항목을 포함하고 있다:

- 시험번호/시험자 : 시험항목 식별자 및 시험에 참여한 개발자
- 시험목적 : 시험 대상 보안기능 및 보안모듈을 포함하여 시험의 목적을 서술
- 시험환경 : 시험을 수행하기 위한 세부 시험환경
- 세부 시험절차 : 보안기능을 시험하기 위한 세부 절차
- 예상결과 : 시험절차를 수행하였을 때 나타날 것으로 예상되는 시험결과
- 실제결과 : 시험절차를 실제로 수행하였을 때 나타나는 시험결과
- 예상결과와 실제결과의 비교 : 예상결과 및 실제결과를 비교한 결과

평가자는 시험서의 시험환경, 시험절차, 시험범위 분석, 상세설계 시험 등 시험의 타당성을 평가하였다. 평가가는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 네트워크 구성, 평가제품, PC 및 서버 등 세부환경을 포함하고 있다. 또한, 각 시험항목을 시험하기 위해 필요한 응용서버 (웹서버, 메일서버 등) 및 평가도구 등 세부적인 시험환경을 서술하고 있다.

- **시험범위 분석/상세설계 시험**

세부 평가결과는 ATE_COV 및 ATE_DPT 평가결과에 서술되어 있다.

- **시험결과**

시험서는 각 시험항목의 예상결과 및 실제결과를 서술하고 있다. 실제결과는 실제 제품의 동작화면 뿐만 아니라 감사기록을 통해서도 확인할 수 있다.

7.2 평가자 시험

평가자는 개발자 시험과 동일한 평가환경 및 평가도구를 사용하여 평가제품을 설치하고 개발자가 제공한 시험항목 전체를 시험하였다. 평가자는 모든 시험항목에서 실제결과가 예상결과와 일치함을 확인하였다.

또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

평가자는 취약성 시험을 수행한 결과, 평가환경에서 어떠한 취약성도 악용 가능하지 않다는 점을 확인하였다.

평가자의 시험결과는 평가제품이 설계문서에 서술된 대로 정상적으로 동작됨을 보증하였다.

8. 평가환경

평가를 위한 네트워크는 내부와 외부를 분리하여 구성하였다. 아래의 하드웨어가 평가환경을 구성하는데 사용되었다:

- 컴퓨터 : 6대(내・외부용 및 관리콘솔용 컴퓨터 6대)
- CPU : 1.5GHz 이상
- RAM : 512MB 이상
- 하드디스크 : 10GB 이상

아래의 소프트웨어가 평가환경을 구성하는데 사용되었다:

- SUSE Linux 8.2
- Windows 2000 server, XP

평가제품에서 제공하는 모든 보안기능이 평가범위에 포함되며, 각 보안기능의 세부적인 보안속성 및 환경설정 방법에 따라 평가환경을 구성하였다.

9. 평가결과

평가는 공통평가기준, 공통평가방법론 및 최종해석(2005. 6)을 적용하였다. 평가는 평가제품이 공통평가기준 2부, EAL4 평가보증등급의 3부에 적합하다고 평가하였다. 자세한 평가결과는 평가보고서에 서술되어 있다.

- **보안목표명세서 평가 (ASE)**

평가자는 ASE 공통평가방법론 작업단위를 적용하여 평가하였다.

보안목표명세서 소개는 완벽하고 보안목표명세서의 다른 부분과 일관성이 있으며 보안목표명세서를 정확하게 식별하고 있다. TOE 설명은 TOE 목적 및 그 기능성을 이해할 수 있도록 설명하며, 조리 있고 완벽하며 내부적으로 일관성이 있으며, 보안목표명세서의 다른 부분과 일관성 있게 서술되어 있다.

보안환경은 TOE와 TOE 보안환경에서 유도된 명확하고 일관된 보안상의 문제를 가정사항, 위협, 조직의 보안정책으로 정의하여 제공하고 있으며, 완전하고 일관성 있게 서술되어 있다. 보안목적은 식별된 위협을 만족시키며 식별된 조직의 보안정책을 달성하며, 서술된 가정사항을 만족시키고 있다.

IT 보안요구사항은 완전하고 일관성 있게 서술되어 있으며, 보안목적을 달성하기 위한 TOE의 개발에 알맞은 기반을 제공하고 있다. TOE 요약명세는 보안기능과 보증 척도를 정확하고 일관성 있게 정의하고, 서술된 TOE 보안요구사항을 만족하고 있다. 보안목표명세서는 수용하는 보호프로파일을 정확히 실체화하고 있다.

따라서, 보안목표명세서는 완전하고, 일관성 있고, 기술적으로 타당하며, 결과적으로 상응하는 TOE 평가의 기초자료로 사용하기에 적합하다.

- **형상관리 평가 (ACM)**

평가자는 ACM 공통평가방법론 작업단위를 적용하여 평가하였다. 형상관리 문서로부터 개발자가 구현 표현에 대한 수정을위해 자동화 도구를 사용하여 통제하고 있음을 확인하였다. 형상관리 문서로부터 개발자가 TOE 및 TOE와 관련된 형상항목을 명확하게 식별하고 있으며, 이러한 항목들을 변경하는 능력은 적절히 통제됨을 확인하였다. 형상관리 문서로부터 개발자가 최소한 TOE 구현의 표현, ST의 보증 컴포넌트에서 요구하는 평가증거물, 보안 결함에 대하여 형상관리를 수행함을 확인하였다.

따라서, 형상관리 문서는 소비자가 평가된 TOE를 식별하도록 해주며, 형상항목이 유일하게 식별됨을 보장하고 개발자가 TOE 변경을 통제 및 추적하기 위해 사용한 절차가 적절함을 보장한다.

- **배포 및 운영 평가 (ADO)**

평가자는 ADO 공통평가방법론 작업단위를 적용하여 평가하였다. 배포 문서는 TOE를 사용자 측에 배포하는 경우 TOE의 보안을 유지하고 TOE의 변경 및 대체를 탐지하기 위한 모든 절차를 서술하고 있다. TOE의 안전한 설치, 생성 시동을 위한 절차 및 단계는 문서화되어 있으며, 그 결과 TOE는 안전하게 환경이 구성됨을 확인하였다.

따라서, 배포 및 운영 문서는 개발자가 의도한 방식과 동일하게 TOE가 설치, 생성, 시동되며, TOE가 변경되지 않고 배포됨을 보장하기에 적절하다.

- **개발 평가 (ADV)**

평가자는 ADV 공통평가방법론 작업단위를 적용하여 평가하였다. 기능명세는 TOE 보안기능을 적절히 서술하고 있으며, TOE 보안기능이 보안목표명세서의 보안기능요구사항을 만족시키기에 충분함을 설명하고 있다. 또한, TOE 외부 인터페이스를 적절하게 서술하고 있다. 보안정책모델은 보안정책의 규칙과 특징을 기술하는데 명확하고 일관성이 있으며, 기능명세에 기술된 보안기능과 대응하도록 기술하고 있다.

기본설계는 TSF를 주요 구성 요소인 서브시스템으로 서술하고 있으며, 서브시스템의 인터페이스를 적절하게 서술하며, 기능명세를 정확하게 실현하고 있다. 상세설계는 TOE 보안기능의 내부 동작을 모듈과 모듈간의 상호관계 및 종속관계에 관하여 서술하고 있다. 상세설계는 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 기본설계를 정확하고 효과적으로 정교화하고 있다.

구현의 표현은 보안목표명세서의 보안기능요구사항을 만족하기에 충분하며, 상세설계를 정확하게 실현하고 있다. 표현의 일치성은 개발자가 보안목표명세서의 요구

사항을 기능명세, 기본설계, 상세설계, 구현의 표현으로 정확하게 완벽하게 구현했음을 보여준다.

따라서, 개발에서 TOE 외부 인터페이스를 설명하는 기능명세, TOE 구조를 내부 서브시스템으로 설명하는 기본설계, TOE 구조를 내부 모듈로 설명하는 상세설계, 소스코드 수준의 설명인 구현의 표현, 이러한 TOE 표현방법의 일관성을 보장하기 위해 서로 대응시키는 표현의 일치성 문서는 TOE 보안기능을 제공하는 방법을 이해하기에 적절하다.

- **설명서 평가 (AGD)**

평가자는 AGD 공통평가방법론 작업단위를 적용하여 평가하였다. 관리자 설명서는 TOE를 안전한 방식으로 관리하는 방법을 서술하고 있다. 따라서, 설명서는 관리자 운영되는 TOE를 사용하는 방법을 적절하게 서술하고 있다.

- **생명주기 지원 평가 (ALC)**

평가자는 ALC 공통평가방법론 작업단위를 적용하여 평가하였다. 개발자의 개발환경에 대한 보안통제는 TOE를 안전하게 운영하기 위해 필요한 TOE 설계 및 구현의 비밀성 및 무결성을 제공하기에 적절함을 확인하였다. 개발자가 문서화된 TOE 생명주기 모델을 사용하고 있음을 확인하였다. 개발자가 일관성 있고 예측할 수 있는 결과를 낼 수 있는 잘 정의된 개발 도구를 사용했음을 확인하였다.

따라서, 생명주기 지원은 TOE 개발 전 과정에 사용된 보안절차 및 도구를 포함하여 TOE를 개발하고 유지보수 하는 동안 개발자가 사용하는 절차를 적절하게 서술하고 있다.

- **시험 평가 (ATE)**

평가자는 ATE 공통평가방법론 작업단위를 적용하여 평가하였다. 시험은 TOE 보안기능이 기능명세에 대하여 체계적으로 시험되었음을 확립하기에 충분하였다. 개발자가 기본설계에 대한 TOE 보안기능 시험을 수행하였음을 확인하였다. 개발자의 기능 시험서는 보안기능이 명세된 대로 수행함을 입증하기에 충분하였다. 평가자는 TSF 일부에 대한 독립적인 시험을 수행하여 TOE가 명세된 대로 동작함을 확인하였고, 개발자 시험에 대한 전수시험을 통하여 개발자가 수행한 시험에 대한 신뢰를 얻었다.

따라서, 시험에서 TOE 보안기능 일부를 독립적으로 시험함으로써 TOE 보안기능이 설계 문서 및 보안목표명세서에 명시된 TOE 보안기능요구사항에 따라서 동작함을 확인하였다.

- **취약성 평가 (AVA)**

평가자는 AVA 공통평가방법론 작업단위를 적용하여 평가하였다. 오용 분석에서 설명서가 오해되지 않고 불합리하지 않으며 상충되지 않음을 확인하였으며, 모든 운영모드에 대한 안전한 절차가 다루어졌으며, 설명서를 사용하면 TOE의 불안전한 상태를 방지 및 탐지할 수 있음을 확인하였다. 기능강도 선언은 보안목표명세서의

모든 확률 및 순열 메커니즘에 대하여 선언되었으며, 개발자의 기능강도 선언에 대한 분석은 정확함을 확인하였다.

취약성 분석서에는 TOE에 대해서 명백하게 알려진 취약성과 이에 대한 대응책을 기능 구현 또는 지침서나 설명서에 운용환경을 명시하는 등 대응책을 적절하게 서술하고 있으며, 평가자가 독립적인 취약성 분석을 수행하여 취약성 분석의 정확성을 확인하였다. 취약성 분석에서 TOE는 의도된 환경 내에서 낮은 수준의 공격 수준을 가진 공격자에 의해 악용 가능한 취약성을 가지지 않음을 확인하였다.

따라서, 개발자 및 평가자의 취약성 분석 및 평가자의 침투시험에 기반하여 의도한 환경 내에서 TOE에 악용 가능한 결함 및 약점이 존재하지 않음을 확인하였다.

10. 권고사항

- 본 제품은 최초 설치시 관리자 비밀번호가 고정되어 있으므로, 설치 완료후 반드시 비밀번호를 변경해야 한다.
- 임계값 설정에 따라 탐지하는 동적공격 정책은 대응 규칙이 적용되기까지 시간이 소요되어 공격 패킷이 보호망에 유입될 수 있으므로, 보호망의 트래픽 특성을 고려한 제품 튜닝 과정을 통해 적절한 임계값을 설정하여야 한다.
- 최신의 보안위반사건목록을 유지하기 위하여 라이브업데이트 기능을 통하여 갱신할 수 있으며, 네트워크 사용량이 상대적으로 적은 시간대(예: 늦은 밤 시간대, 주말)로 갱신 주기를 설정하는게 효율적이다.
- 본 제품은 감사기록 저장공간 소진으로 임계치에 도달하는 경우 관리자 통보 기능을 제공하나 관리자는 통보 기능에만 의존하지 말고 지속적으로 저장공간 사용량을 점검하고 감사기록 저장공간을 확보해야 한다.

11. 용어 정의

아래의 약어가 본 보고서에서 사용되었다.

CR	Certification Report
EAL	Evaluation Assurance Level
IT	Information Technology
KECS	Korea IT security Evaluation and Certification Scheme
TOE	Target of Evaluation

아래의 용어가 본 보고서에서 사용되었다.

TOE	평가의 대상인 IT제품이나 시스템 및 이와 관련된 설명서
감사기록	TOE의 보안에 관련된 사건의 기록을 저장하는 감사데이터

사용자	TOE 외부에서 TOE와 상호 동작하는 모든 실체, 사용자, 외부 IT 실체 등
인가된 관리자	TOE 보안정책에 따라 TOE를 안전하게 관리하는 인가된 사용자
인가된 사용자	TOE 보안정책에 따라 기능을 실행할 수 있는 사용자
신원	인가된사용자를 식별하는 유일한 표현
인증데이터	사용자의 신원을 증명하기 위하여 사용되는 정보
외부 IT 실체	TOE 외부에서 TOE와 상호 작용하는 안전하거나 안전하지 않은 모든 IT 제품이나 시스템
자산	TOE의 보안대책으로 보호되는 정보 및 자원
침입방지시스템	외부로부터 공격을 탐지하고 차단하여 보호대상 네트워크(즉, 내부망)로 공격의 영향이 미치지 않도록 하는 정보보호제품

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증보고서를 작성하였다:

[1] 정보보호시스템 공통평가기준 (2005. 5. 21)
[2] 정보보호시스템 공통평가방법론 V2.2
[3] 네트워크 침입방지시스템 보호프로파일 V1.1 (2005. 12. 21)
[4] 정보보호시스템 평가·인증 지침 (2005. 5. 21)
[5] 정보보호시스템 평가·인증업무 수행 규정 (2005. 5. 7)
[6] SafezoneIPS V3.0(SZ-4000) 보안목표명세서 V1.00.02 (2005. 12. 5), (주)LG CNS
[7] SafezoneIPS V3.0(SZ-4000) 평가보고서, 발행버전 1.01 (2005. 12. 9)

※ 인증효력유지 내역

1. SafezoneIPS V3.0(SZ-4000) 변경승인(2008. 8. 27)

· 변경사항

구 분	인증제품	변경승인제품
모델명	SZ-4000	SZ-4000P
CPU	Intel Xeon 2.8 GHz × 2	Xeon 하퍼타운 ES5420 2.5 GHz (Quad Core) × 2
Main Memory	4GB	4GB
HDD	146GB	250GB
NIC	서비스 : 4 Ports(Giga) 관리용 : 2 Ports (10/100용 1, 1000용 1)	서비스 : 8 Ports(Giga) 관리용 : 2 Ports(10/100/1000)

· 검토결과

인증제품의 CPU, HDD, NIC 등 H/W 요구사항 변경 후 인증효력유지를 신청한 SafezoneIPS V3.0(SZ-4000) 제품에 대해 보안영향분석서, 보안기능 및 취약성 분석 시험을 통한 시험결과 TOE의 보안기능 및 보증 범위에 영향을 미치지 않는 것으로 확인되어 이를 승인함