

기본상품 규격서

Chakra Max v4.5

(대표기능 : DB접근제어 솔루션)

1. 상품개요 및 구매조건

1.1 상품개요

본 규격서는 DB서버 접근에 대한 실시간 감사 및 접근제어를 통하여 중요한 데이터를 보호하는 DB접근제어 솔루션 Chakra Max v4.5 (이하 “본 솔루션” 이라 함)에 대하여 규정한다.

1.2 규격별 적용대상 및 범위, 사용기간

NO	물품분류번호	모델명	구매 단 위	라이선스 (적용대상)	SW라이선 스 (사용기간)	인도 조건	비고
	물품식별번호	제품규격		라이선스 (적용범위)			
1	43233205	Chakra Max v4.5	조	사이트	제한 없음	현장 설치도	
	26200804	Chakra Max v4.5 1~2Core		1~2코어			
2	43233205	Chakra Max v4.5	조	사이트	제한 없음	현장 설치도	
	26200805	Chakra Max v4.5 3~4Core		3~4코어			
3	43233205	Chakra Max v4.5	조	사이트	제한 없음	현장 설치도	
	26200806	Chakra Max v4.5 5~6Core		5~6코어			
4	43233205	Chakra Max v4.5	조	사이트	제한 없음	현장 설치도	
	26200807	Chakra Max v4.5 7~8Core		7~8코어			
5	43233205	Chakra Max v4.5	조	사이트	제한 없음	현장 설치도	
	26262804	Chakra Max v4.5 Manager License		Manager			

1.3 규격별 1조(copy)구매 시 SW라이선스 사용권리 및 사용기간

NO	물품식별 번호	모델명 및 제품규격	라이선스 적용대상 및 범위, 정책 등 (1조(copy)구매시)	
1	26200804	Chakra Max v4.5 1~2Core	라이선스 범위	해당제품은 1조구매시(1~2코어) 2 코어까지 사용할 수 있는 라이선스를 제공합니다.
			해당규격제품의 역할	관리대상 DB서버의 접근감사로깅 및 접근제어기능을 수행합니다.
			해당규격제품의 사용기간 구매	구매 시 사용기간에 제한이 없습니다.
2	26200805	Chakra Max v4.5 3~4Core	라이선스 범위	해당제품은 1조구매시(3~4코어) 4 코어까지 사용할 수 있는 라이선스를 제공합니다.
			해당규격제품의 역할	관리대상 DB서버의 접근감사로깅 및 접근제어기능을 수행합니다.
			해당규격제품의 사용기간 구매	구매 시 사용기간에 제한이 없습니다.
3	26200806	Chakra Max v4.5 5~6Core	라이선스 범위	해당제품은 1조구매시(5~6코어) 6 코어까지 사용할 수 있는 라이선스를 제공합니다.
			해당규격제품의 역할	관리대상 DB서버의 접근감사로깅 및 접근제어기능을 수행합니다.
			해당규격제품의 사용기간 구매	구매 시 사용기간에 제한이 없습니다.
4	26200807	Chakra Max v4.5 7~8Core	라이선스 범위	해당제품은 1조구매시(7~8코어) 8 코어까지 사용할 수 있는 라이선스를 제공합니다.
			해당규격제품의 역할	관리대상 DB서버의 접근감사로깅 및 접근제어기능을 수행합니다.
			해당규격제품의 사용기간 구매	구매 시 사용기간에 제한이 없습니다.

5	26262804	Chakra Max v4.5 Manager License	라이선스 범위	
			해당규격제품의 역할	관리대상 DB서버의 접근감사로깅 및 접근제어기능을 수행합니다.
			해당규격제품의 사용기간 구매	구매 시 사용기간에 제한이 없습니 다.

1.4 구매예시

예시1) 수요기관의 DB접근제어 대상 DB서버의 CPU가 1CPU 4코어라면,
Chakra Max v4.5 3~4Core 1조 구매

1.5 해당 규격별 제품은 기본 커스커마이징이 포함된 상품입니다

※기본 커스터마이징 범위는 수요기관과 납품업체가 상호협의

2. 제품 인증내역

분 류	인증 번호	인증 명칭	만료일자
GS인증 1등급	26-0080	Chakra Max v4.5	제한없음
CC인증	CISS-1356-2 025	Chakra Max v4.5	2030년 7월 24일

3. 제품 권장사양 및 기능

3.1 구매한 S/W가 설치될 H/W제품 권장사양

NO	물품식별 번호	모델명 및 제품규격	권장사양	운영환경 (서버, 사용자)
1	26200804	Chakra Max v4.5 1~2Core	[Chakra Max Sever] Rocky Linux 9.x PetaSQL 2.0 [관리자용 Manager Program]	[Chakra Max Sever] CPU : Quad Core 3.0GHz 이상 Memory : 8GB 이상 DISK : 500GB 이상
2	26200805	Chakra Max v4.5 3~4Core		

3	26200806	Chakra Max v4.5 5~6Core	Windows 10 이상	[관리자용 Manager Program] CPU : Pentium(R) 3.40Ghz 이상 Memory : 4 GB 이상 DISK : 500GB 이상
4	26200807	Chakra Max v4.5 7~8Core		

4. SW구매시 제공되는 기능

4.1 기능 및 성능

Chakra Max는 DB사용자가 네트워크를 통하여 Chakra Max가 보호하는 DB로 접속하여 데이터를 생성, 변경 및 삭제하거나 데이터를 조회 시 이를 감시, 통제 및 감사 기능을 제공하는 네트워크 기반 DB접근통제 제품이다.

Chakra Max가 보호하는 보호대상 DB 서버의 종류는 다음과 같다.

- Oracle
- Sybase
- MS SQL
- My SQL
- Altibase
- Informix
- DB2 UDB
- Teradata z
- Tibero
- Cubrid
- PostGreSQL

또한, Chakra Max는 Telnet/SSH/FTP/R-Login/R-Command 등의 Remote 접속 감시를 지원 한다.

4.2 식별 및 인증

- Chakra Max 관리자 식별 및 인증 : ID 및 패스워드를 기반으로 식별 및 인증 수행하며, 패스워드 입력 시 보호를 위하여 "*" 출력
- 인증 피드백 및 인증 실패 대응 : 3회 연속 식별 및 인증 실패 시 인증을 지연하며, 접속한 관리자가 일정시간 동안 아무런 활동이 없으면 해당 세션을 잠그고 재 인증 수행

4.3 보안관리

- 로깅 정책 관리 : 생성하려는 로그를 선택
- Server 관리 : 보호대상 DB가 탑재된 서버 정보를 등록 및 관리
- DB 관리 : 보호대상 DB 정보를 등록 및 관리
- 보안정책 관리 : 보안정책을 설정 또는 해제하여 DB접속을 감시하고 위반사항에 대하여 대응
- 마스킹 정책 관리 : 중요 SQL 수행 결과에 대한 마스킹 여부 설정
- SQL Control : 일정기간 신규로 수집된 SQL을 검토하여 문제 SQL을 찾아 통제하고, 특정 톨에서 최초 접속 시 기본적으로 수행하는 SQL을 등록하여 보안정책에 영향을 받지 않도록 함
- 관리자 관리 : Chakra Max 관리자를 등록하고 권한을 부여
- 운영 관리 : Chakra Max 보안기능 수행에 필요한 기본 데이터 설정, 보안 엔진의 시동/중지 설정, 무결성 검사 설정 등

4.4 보안감사

- 감사 데이터의 생성 : 로깅 정책에 의거하여 통과하는 패킷, 패킷 처리시 집계한 통계 데이터, 보안사건 데이터 등을 시간 순으로 저장
- 감사 검토 : 저장된 감사 기록은 각종 조건 별로 검색이 가능하고 검색한 결과를 CSV 파일로 생성
- 감사 증적 보호 : 감사 저장소가 포화인 경우 관리자에게 통보 후 문제가 해결 될 때까지 보안기능을 일시 중단
- 보안경보 생성 : 감사 데이터 저장소가 일정한 용량을 초과하면 관리자에게 통보

4.5 DB데이터보호(Sniffing)

- 불법 접속/사용 탐지대상 사건 정보 수집 : 네트워크 상에서 보호대상 DB로 향하는 패킷을 수집
- 불법접속/사용 분석 : 수집한 패킷을 대상으로 보안정책에 기반하여 불법 접속, 사용사건 정보를 분석

- 불법접속/사용 대응 : 위반 사항 발견 시 지정된 경보 데이터 생성, 관리자에게 통보 등 대응 행동 수행

4.6 사용자 데이터보호(IP Forwarding)

- 정보 흐름 통제 및 차단 : Chakra Max를 통하여 DB접속을 요청하는 DB사용자의 IP 및 Port 정보를 바탕으로 접근 통제 수행
- 보안정책에 위반 사항이 없을 경우 대상 DB로 패킷을 전달하고 대상 DB로부터의 응답을 DB사용자에게 전달
- 위배 사항 발견 시 경보 데이터 생성, 관리자 통보, 해당 세션 강제 종료, 특정 패킷 Drop 등 보안정책에 정의된 대응 행동을 수행
- 정보흐름을 통제할 때 마스킹 정책을 조사하여 SQL 결과값 중 주요 정보는 마스킹하여 제공

4.7 무결성 검증

- 데이터 무결성 검증 : Chakra Max가 사용하는 보안설정 데이터에 대하여 최초 실행 시, 실행된 이후 주기적으로, 관리자 요청 시 무결성 검사를 수행하며, 검사 결과 비정상 수행 발견 시 관리자에게 통보 등 대응기능
- Chakra Max 실행코드에 대하여 최초 실행 시, 실행된 이후 주기적으로, 관리자 요청 시 무결성 검사를 수행하며, 검사 결과 비정상 수행 발견 시 관리자에게 통보 등 대응기능

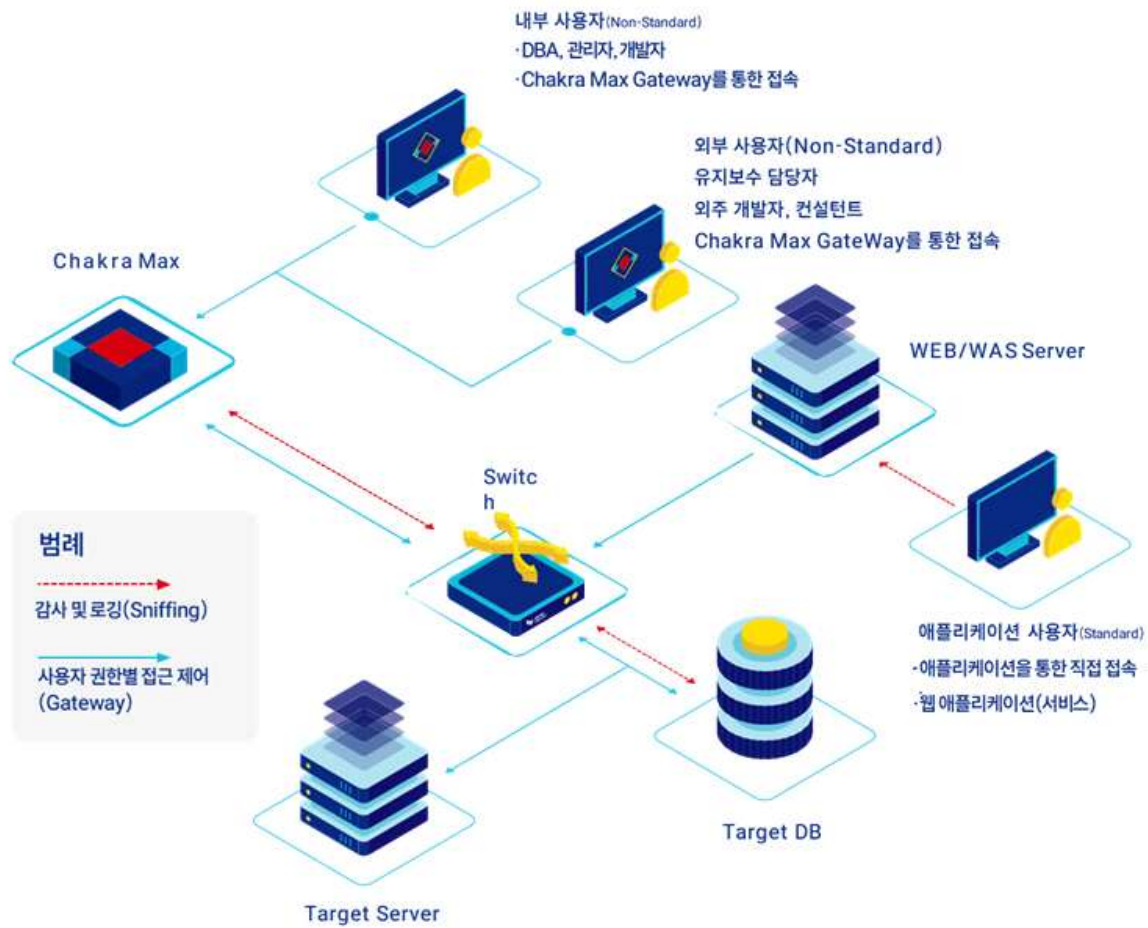
5. 서비스 구성 개념도

Chakra Max Server는 DB사용자와 DB서버의 네트워크 경로상에 존재하고, 사용자는 방화벽에 의해 DB서버로의 직접접속을 통제된다.

- Chakra Max Server : DB접근 통제 기능을 수행하고, 감사데이터를 생성 및 조회 기능을 제공 하며, 관리자가 접속하여 관리 기능을 수행할 수 있도록 UI를 제공 한다.
- Chakra Max 관리자 : 웹 브라우저로 Chakra Max Server에 접속하여 Chakra Max가 보안 기능을 수행 할 수 있도록 관리 한다.
- 방화벽 : DB사용자와 DB서버 사이의 내부 방화벽은 DB사용자들이 Chakra Max Server를 경유하지 않고 DB서버에 우회 접근 하는 것 방지 한다.

Chakra Max는 Sniffing / IP Forwarding 기능과 이를 동시에 제공하는 Hybrid Mode 로 동작한다.

CHAKRA MAX 구성도



6. 공급 및 설치, 타시스템과의 연계 지원방안

6.1 공급 제품

구분	종류	비고
S/W	Chakra Max License V4.5	서버에 구성되는 Core License S/W
	Chakra Max Manager	관리자용 프로그램 (PC에 설치)
	Chakra Max Client	사용자용 프로그램 (PC에 설치) (IP Forwarding 사용시)

6.2 세부설치 방안

구분	내용	시간
서버용 S/W 설치	· Chakra Max License V4.5 구성 – Chakra Engine (Sniffing / IP Forwarding) 설치 – Repository DB 설치 – Report Module 설치 * 전용 Setup Tool을 이용하여 설치	30분
관리자용 프로그램 설치	· Chakra Max Manager 설치 – 모니터링, 정책관리, 로그조회 등의 관리자용 프로그램 – Windows PC용	10분
환경설정	· 대상 DBMS 등록 – 시스템 > 데이터베이스 메뉴로 동하여 등록 – 대상 DB서버의 IP, Service Port, SID/Service Name 등을 입력	
	· Sniffing용 Device 설정 (Sniffing 구성 시) – 시스템 > 환경설정 메뉴로 이동하여 등록 – 패킷미러가 구성된 스니핑 NIC Device를 지정	30분
	· 사용자 보안계정 등록 (IP Forwarding 구성 시) – 시스템 > 사용자 메뉴로 이동하여 등록 – 사용자별 DB접근제어용 보안 계정 생성	30분
사용자용 프로그램 설치	· Chakra Max Client 설치 (IP Forwarding 구성시) – 프로그램 설치 후 보안계정으로 로그인하여 DB 접속 – Windows PC용	10분
기능 테스트	· 세션 테스트 – 모니터 > 세션 메뉴로 이동하여 확인 – Sniffing : 패킷미러가 구성으로 분석된 DB Session 및 SQL 모니터링 상태 확인	120분

	- IP Forwarding : Chakra Max Client 프로그램을 실행하여 보안계정 로그인 후 DB에 접속, DB Session 및 SQL 모니터링 상태 확인 · 로그 조회 - 검색 > 데이터베이스 메뉴로 이동하여 확인 - 저장된 로그를 조회하여 기능 확인 · 보안정책 테스트 - 정책 > 보안정책 메뉴로 이동하여 확인 - 보안정책을 구성하여 경고/차단 기능 동작 확인 - 경고 정책, 마스킹 정책, 결재 정책, 전/후 데이터 저장 정책 구성 지원 · 레포트 테스트 - 보고서 메뉴로 이동하여 확인 - 제공되는 정형 레포트를 출력하여 확인	
--	--	--

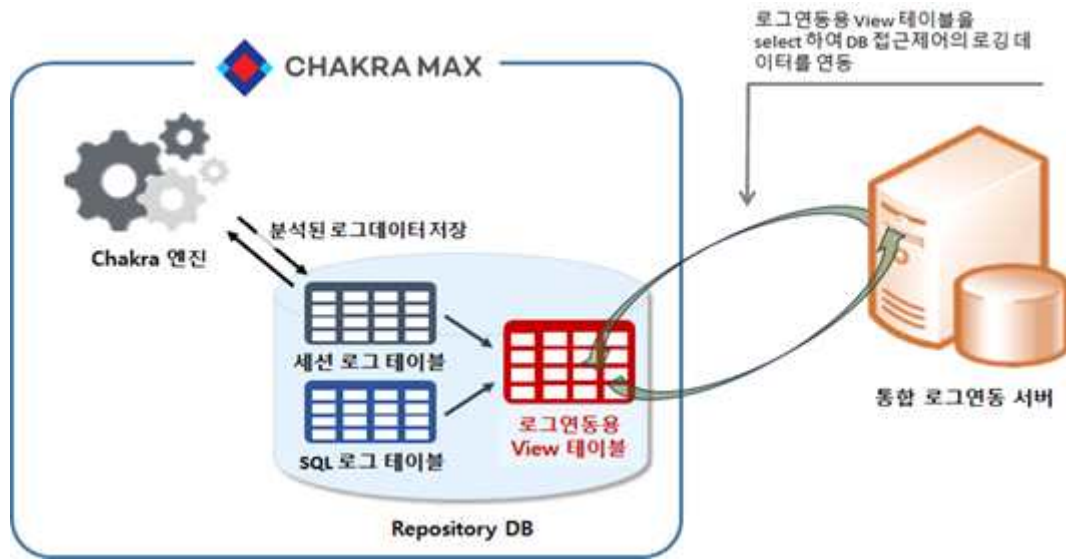
6.3. 타 시스템과의 연계 방안

Chakra Max는 타 시스템과의 연계를 위한 방안을 제공합니다.

● 로그연동

Chakra Max에서 분석하여 저장된 Repository DB에 저장된 로그 데이터를 (DBSession / SQL 로그, 경고/차단내역 등) View 테이블로 제공하며 통합로그서버와 같은 로그 데이터가 필요한 서버에서 제공된 View 테이블을 select하여 연동합니다.

7. 제품 구성 및 납품 방법



7.1 제품 구성

구분	종류	수량	비고
제품 인증서	소프트웨어 사용권 증서	1부	
제품 메뉴얼	소프트웨어 설치,사용설명서	1부	

7.2 납품 방법

납품 일정 및 장소, 방법 등은 구매 기관과 협의하여 진행합니다.

8. 검사 및 시험

Chakra Max는 제품의 신뢰성을 보장하기 위해 개발 및 릴리즈 과정에서 다음의 시험을 실시한다.

생명주기 단계에 따른 시험의 종류 및 절차는 다음과 같다.

단계	시험의 종류	시험 책임
구현	단위 테스트	개발 담당자
	통합 테스트	자동 Build 시스템에 의한 자동 테스트
	시스템 테스트	개발팀
검수	검수 테스트	QM실(QA팀)

[표 3-2] 단계별 시험종류 및 책임

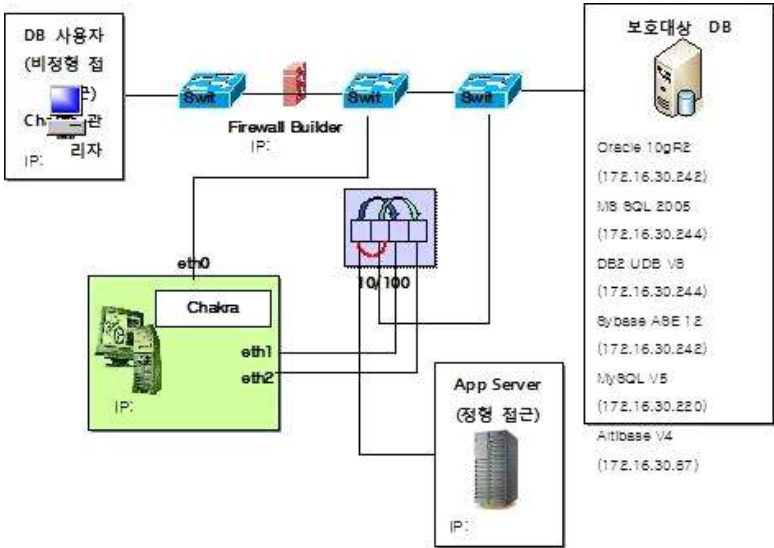
개발자는 각자의 개발 기능에 대해 local 환경에서 개별 검증(단위테스트)을 한다.

개발자가 형상관리 시스템에 개발 소스를 update(또는 add)하면 빌드 검증 툴인 BuildBot이 주어진 스케줄에 의해 컴파일 오류검증 및 자동 테스트를 한다. 테스트 시 오류가 발견되면 담당자 및 관련자에게 오류 메일이 발송된다.

개발팀은 운영 시스템 환경에서 종합 테스트(시스템 테스트)를 실시하고 문제가 없을 시 QM실(QA팀)에 검수 요청한다.

개발팀에서 검수 요청을 받으면, QM실의 QA팀은 검수팀을 구성하고 검수 테스트를 실시 한다. 검수 테스트 과정에서 발견되는 Bug는 Warevalley Collaboration System에 등록하여 수정 보완 한다.

Chakra Max 시험 환경 및 시험 범위는 다음과 같다.



[그림] 시험환경 구성

[표] 시험 범위

구분	주요 기능
식별 및 인증	Login
	Logout
보안관리	운영관리 - Chakra Max Server 관리
	운영관리 - Chakra Max Server 환경 설정
	보호대상 Server 관리
	보호대상 DB 관리
	Logging 정책 관리
	보안정책 관리
	암호화 정책 관리

	관리자 관리
보안감사	데이터 생성
	DB Session Monitor
	SQL Monitor
	Alert Monitor
	Log Analyzer
	Logging Directory 용량 위험범위 경고
DB 데이터/사용자 데이터 보호	Alert
	Session 차단
	데이터 마스킹
	Safe SQL
	New SQL
	Backup
무결성 검증	데이터 무결성
	실행코드 무결성

시험 방법은 Chakra Max 시험서에 명시 된 절차에 의해서 수행 된다.

Chakra Max 시험서의 시험 구성은 다음과 같다.

- 시험 목적
- 시험 환경
- 시험 선행 조건
- 시험 절차
- 예상 시험결과
- 실제 시험결과

내/외부 고객이나 개발자에 의한 제품의 기능 변경 요청은 Warevalley Collaboration System을 통하여 등록 한다.

등록된 요구사항은 형상위원회를 통하여 수용 여부를 결정하고, 수용 결정 한 사항은 개발팀장이 개발담당자를 할당하여 작업을 진행 하도록 한다.

개발자는 작업이 완료되면 Warevalley Collaboration System을 통하여 feed back하고, 구현물은 형상관리 시스템을 통하여 등록한다.

개발팀장은 구현된 기능을 검토하여 외부 배포가 필요 시 검수를 요청 후, 검수 통과 시 외부에 배포 한다.

9. 유지관리 서비스

- 구매 후 1년간 무상하자보수와 기본 유지관리 서비스를 포함하고

있음

무상하자보수 내용			설 명
항목	세부항목	지원범위	
기술 지원	장애발생 후 복구 (응답시간)	4시간이내	- 시스템 장애 시 대응 시간, 장애 처리 절차 등
	정기점검	방문 분기 1회	- 시스템의 장애를 사전에 예방하기 위하여 정기적으로 지원하는 정기점검, 정기성능 조율 서비스 - 제품의 점검 및 유지관리 이력관리, 시스템 사용자 관리지원 - 유지관리 작업 보고서 작성, 시스템 운영 보고서 작성
	일상지원	전화, e-mail	- 콜센터 운영, 사이트운영, 전화/email 등을 통한 장애접수, 질의응답
	이전 설치	이전 1회	- 제품의 이전설치 지원
제품 지원	업데이트 및 패치	원격지원	- 기존 SW 제품의 기능을 보완 및 새로운 기술의 적용이나 운영체제의 변화 등으로 발생하는 불일치 조정
	마이너 업그레이드	방문지원	- 기존 SW 제품을 향상시키기 위하여 새로운 버전으로 교체하는 서비스(4.0 →4.1, 버전의 소수점 변화)
교육 지원	운영자 교육	1회	- 제품 운영을 위한 운영자 교육
	사용자 교육	1회	- 제품 사용을 위한 사용자 교육

10. 보안 준수

제품 설치 등을 위해 구매 기관 방문 시에는 구매 기관의 보안 규정을 준수합니다.

11. 저작권 및 사용권

공급된 소프트웨어의 저작권은 기본적으로 공급사에 있으며 구매 기관은 해당 소프트웨어에 대한 사용권만을 가집니다.

12. 담당자 연락처

홈페이지	http://www.warevalley.com
이메일 상담	sales-kr@warevalley.com
고객센터	Tel. 02-1660-1675
팩스	Fax. 02-743-3023
주소	서울시 마포구 잔다리로81, 효산빌딩