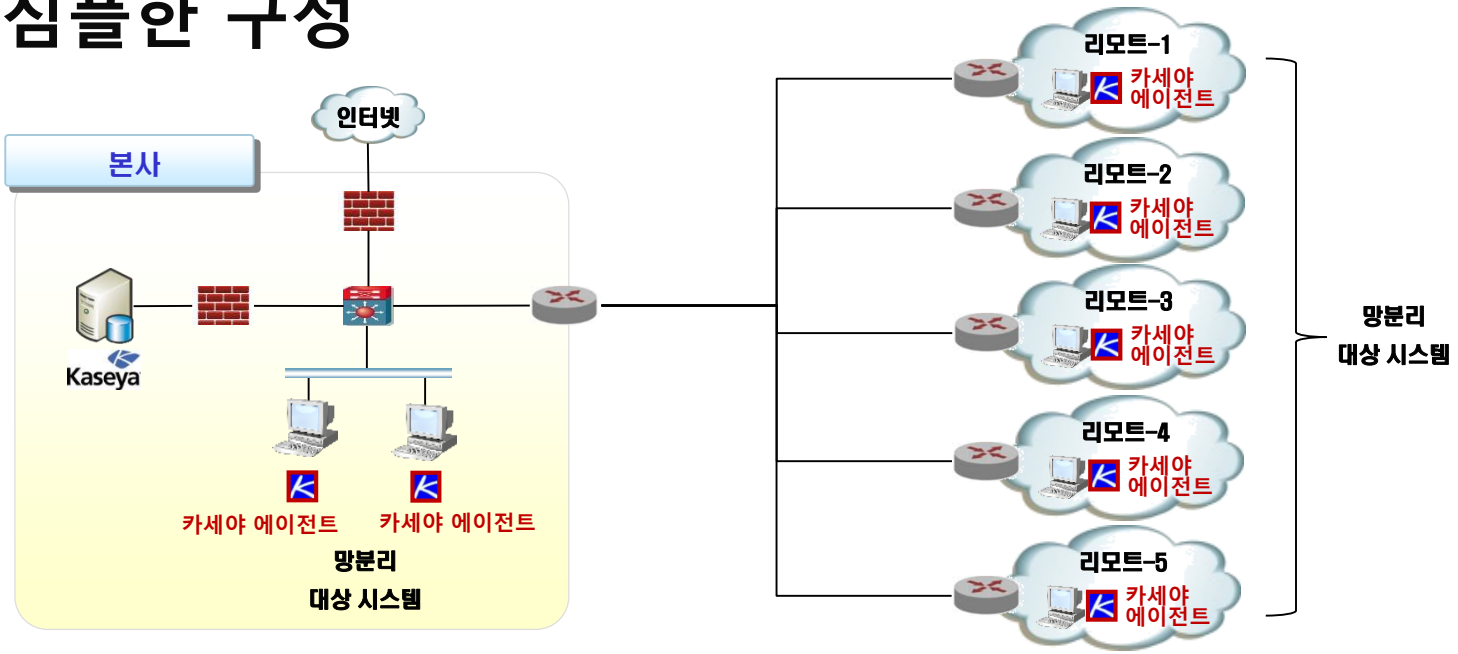
Kaseya

망분리 클라이언트 인프라 구축을 위한 카세야 관리 방안 제안 (1차 자료)

Flexible Configuration (유연한 구성)

- 심플한 구성



- 구성 설명
  - 중앙 카세야 관리 서버 구성
  - 망분리 대상 시스템에 경량 에이전트 구성

망분리 대상 시스템의 통합 관리 체계

보안 관리 극대화

- 필수 보안 SW 제어
- OS 보안 패치 제어
- Windows 사용자 계정 제어
- 매체 제어
- 업데이트 관리

데스크탑 표준화 자동화

- IE 브라우져 표준화
- IE 브라우져 옵션 설정
- Hosts 파일 표준화
- 바탕화면 표준화
- 업무용 단축아이콘 제어

HW/SW 자산 모니터링

- 모델명, 시리얼번호 관리
- 유연한 SW 배포/삭제/설치 방안 제시
- 커스텀 DB 필드 생성 및 별도 자산 관리 항목 추가

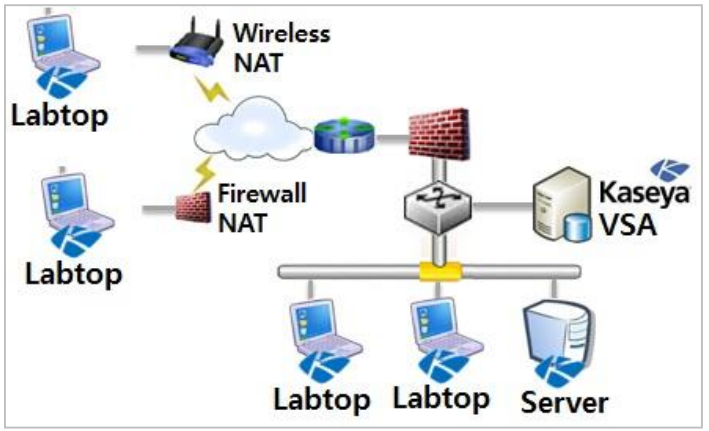
리모트 시스템 통제

- 별도 툴 없이, 원격 제어 기능 제공
- 원클릭 정책 적용
- 원격 시스템 전원 제어

제품 자체의 보안성 제공 (관리 제품으로 인한 보안 홀 제거)

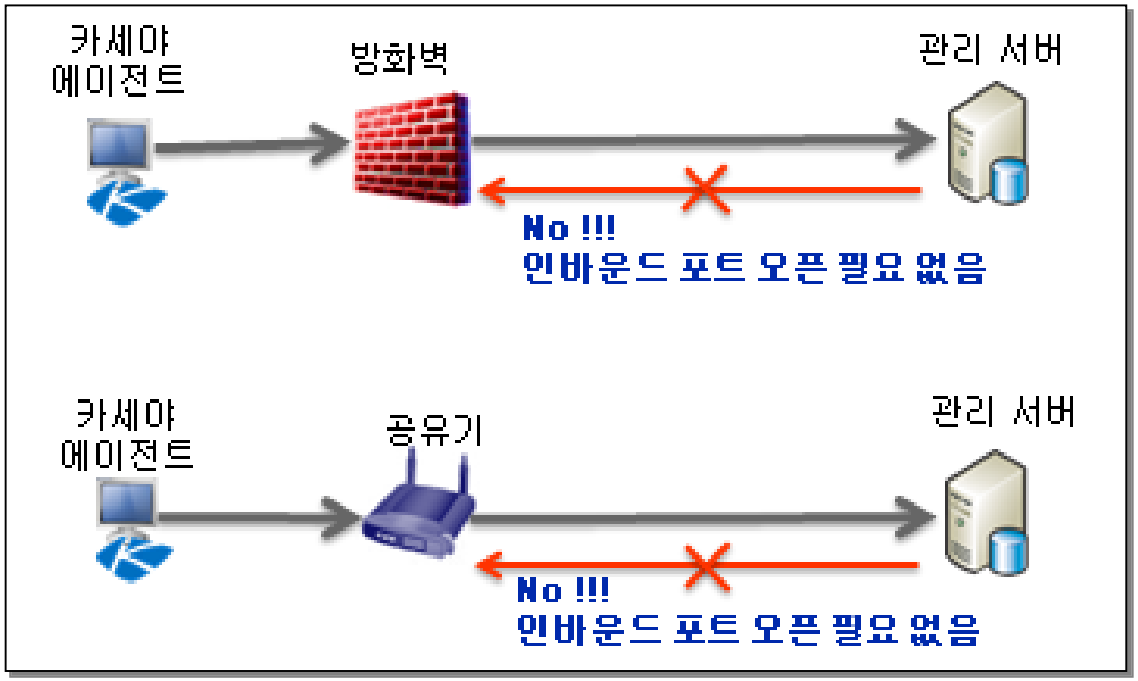
- 관리 통신 작동 방식
  - 카세야 특허 연결 알고리즘
  - 관리 대상 시스템으로 직접 접속 없음
  - 관리 서버를 통해서만 컨트롤

- 제품 자체 보안성 아키텍쳐
  - 오직 단방향 통신만 허용
    (에이전트 ➔ 서버)
  - Only One 통신 포트
  - 에이전트 자체 "오픈된 서비스 포트 없음"
  - 모든 통신 데이터 자체 암호화
  - **CC 인증 – EAL2+**



- 네트워크 구성 독립성 제공
  - 로밍 보안 에이전트 기술
  - 네트워크 구성에 영향 받지 않으며, 위치에 상관없이, 정책 적용의 연속성 제공

에이전트 자체 포트 오픈 방지



- 대부분의 Agent 기반 관리 솔루션의 보안 취약점으로 작용될 수 있는, Agent 자체의 서비스 포트 오픈 부분을 원천적으로 봉쇄
  ➔ **에이전트 자체 보안성 강화**

- Agent에서 관리서버로 가는 세션만 형성되는 단방향 통신 체제 기반으로 작동

에이전트 성능 리소스 최소화 방안

Non-Driver 기반

o Windows 서비스
레벨에서 작동
o 타 SW 충돌보고 ➔ 0%
o 설치 소요 시간 ➔ 10초
o 설치 완료 이후,
리부팅 없이 즉시 작동

평균 리소스 사용

o 설치 파일 사이즈 ➔ 1.6MB
o 설치 이후, 평균 메모리 점유
➔ 3~6MB

o 단, 특정 시스템 작업 정책적용 시, 시스템 작업에 의한 메모리/CPU 점유는 다소 발생 할 수 있으나, 작업 완료 이후 정상 조치 됨
(예 – 디스크조각모음, 백신 검사 수행 등..)

대역폭 조절 기능

o 에이전트 자체적으로 트래픽 최대 대역폭 소비 제한 기능 (Bandwidth 제한 기능)
o SW/파일 배포 작업시 조절 기능 제공

제품 시장 반응

[CC 인증]

CESG

CRP264 – Kaseya Virtual System Administrator

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.

Sponsor:	Kaseya International Ltd	Developer:	Kaseya International Ltd
Product and Version:	Kaseya Virtual System Administrator Version 6.2.1.0		
Platform:	Multiple		
Description:	The Kaseya Virtual System Administrator provides IT managers with the capability to monitor, manage, and maintain distributed IT networks.		
CC Version:	Version 3.1		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL2 Augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
FIPS 140-2	Level 1 Crypto Module Validation is covered by the following FIPS 140-2 validation certificates numbers: ***(TBD)***.		
CC Certificate:	P264	Date Certified:	16 February 2012

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

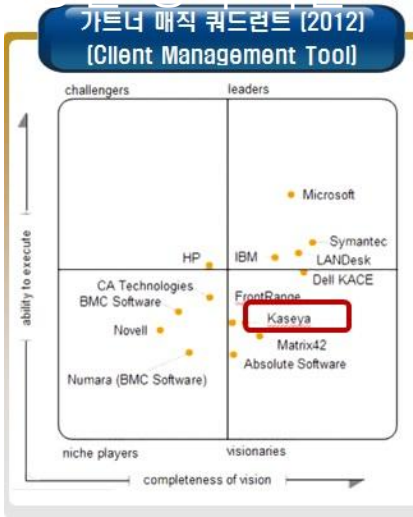
The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

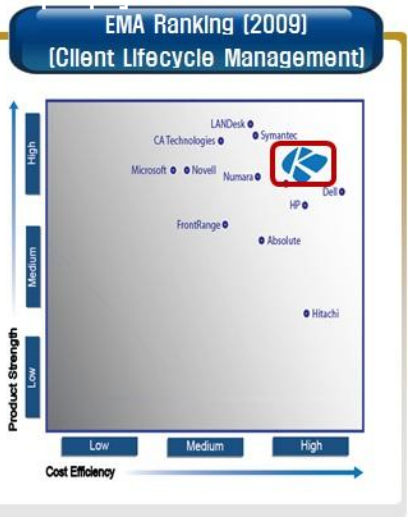
The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo　　CC logo　　SOGIS MRA logo

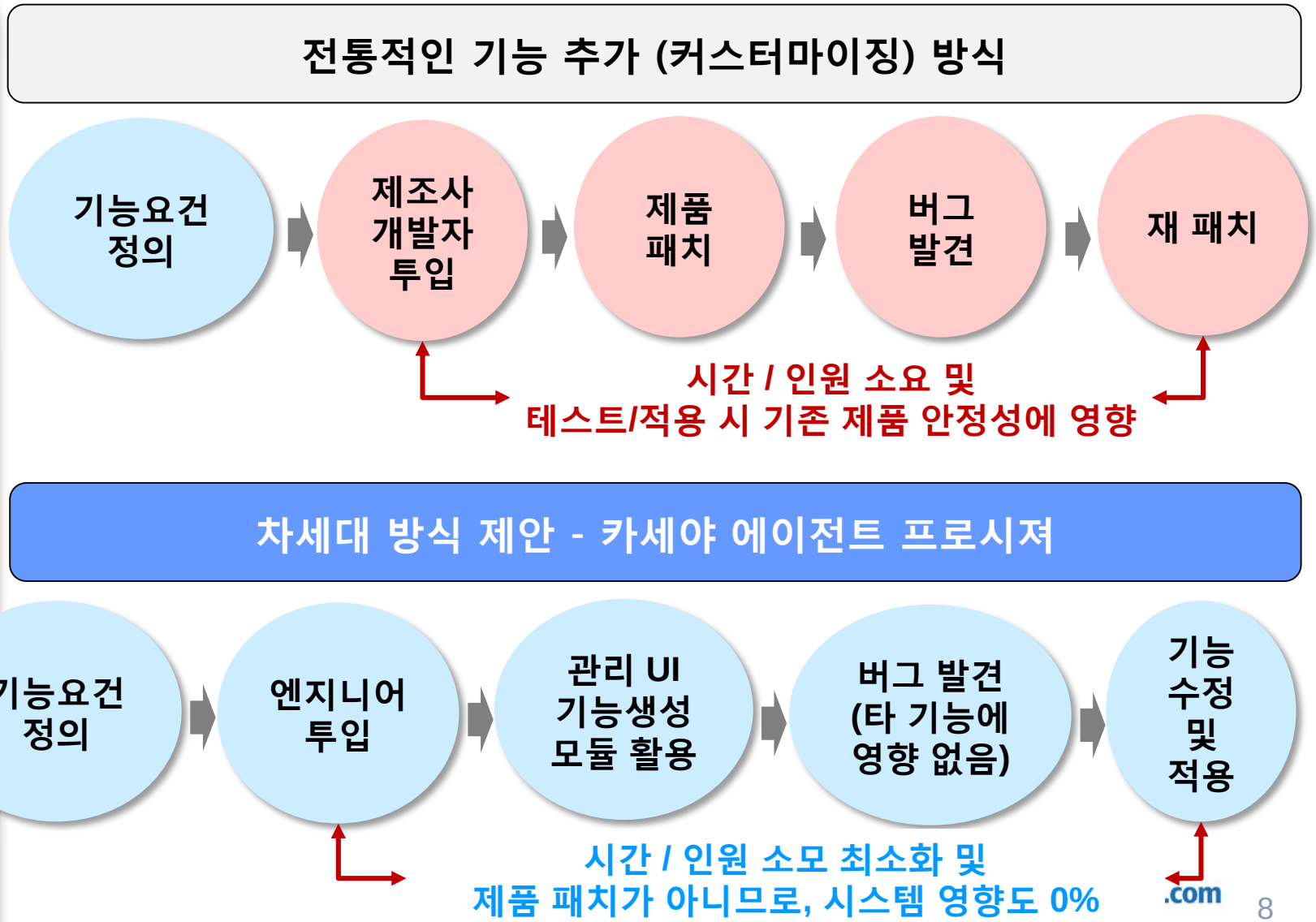
eWEEK a product to watch! · Gartner 2009 Emerging Vendor · Business Solutions BEST CHANNEL VENDOR 2009 · NETWORKWORLD BEST IN TESTS 2010 WINNER · VAR 500 09 AWARDS · CRNtech Rates Kaseya 4.5★

Windows IT Pro 2010 Editors' Best AWARDS · Best of SaaS Showplace BoSS AWARDS · EDITORS' CHOICE Awards · tucows

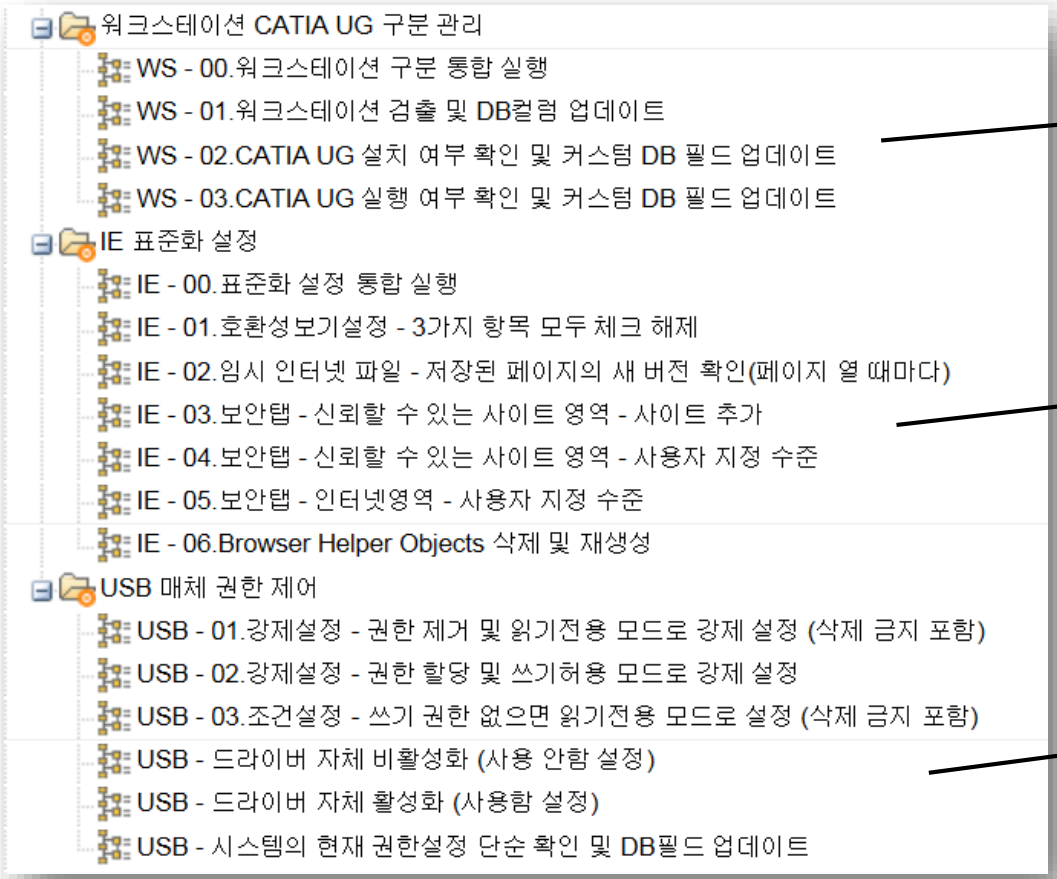




유연한 기능 추가 프레임워크



추가(생성)된 기능 샘플 - 1



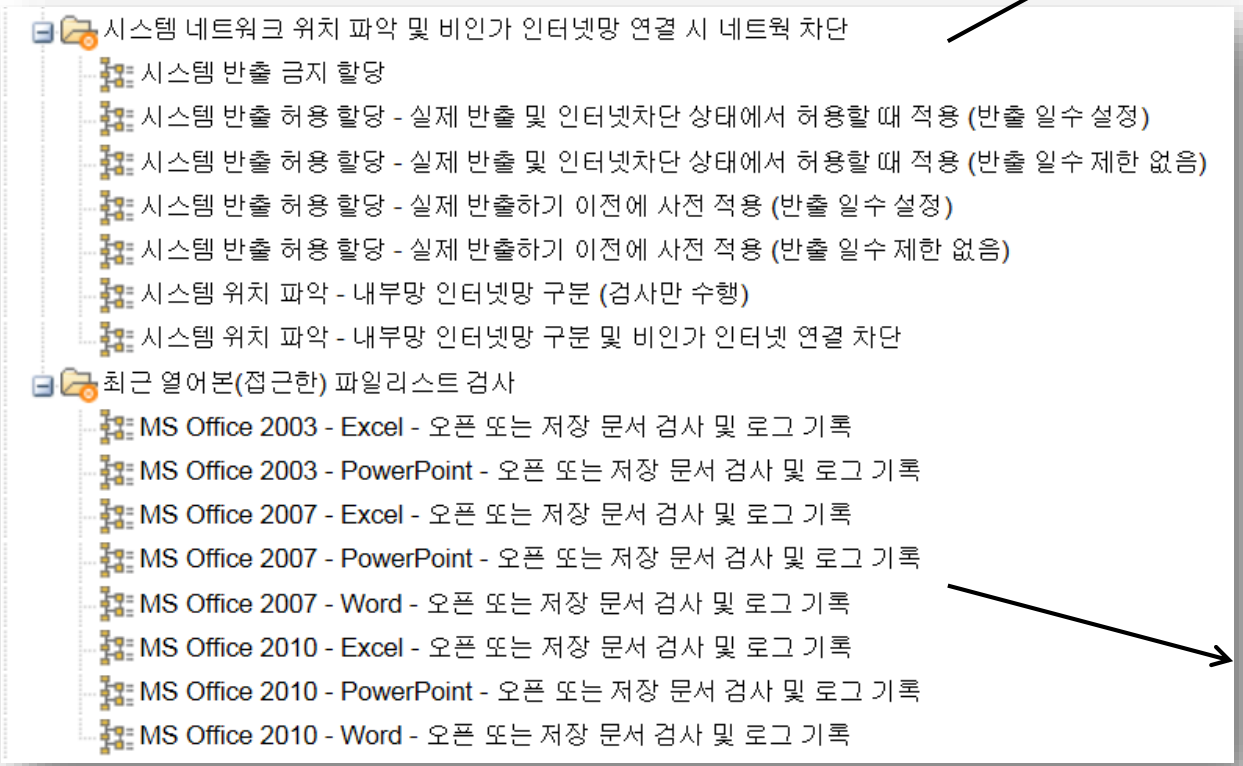
특정 HW/SW 상태 보고 기능

IE 설정 표준화 기능 추가

조건에 따른 USB 매체제어 기능 추가

추가(생성)된 기능 샘플 - 2

노트북 시스템 반출 제어 기능 추가



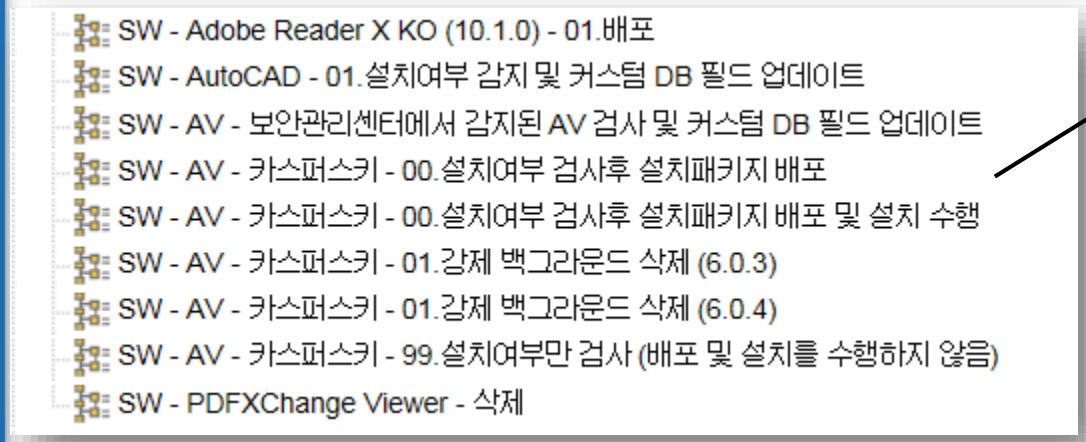
MS Office 문서열람기록 로그생성기능 추가 (향후 감사용도)

추가(생성)된 기능 샘플 - 2

SW 삭제 기능 추가

SW 설치 기능 추가

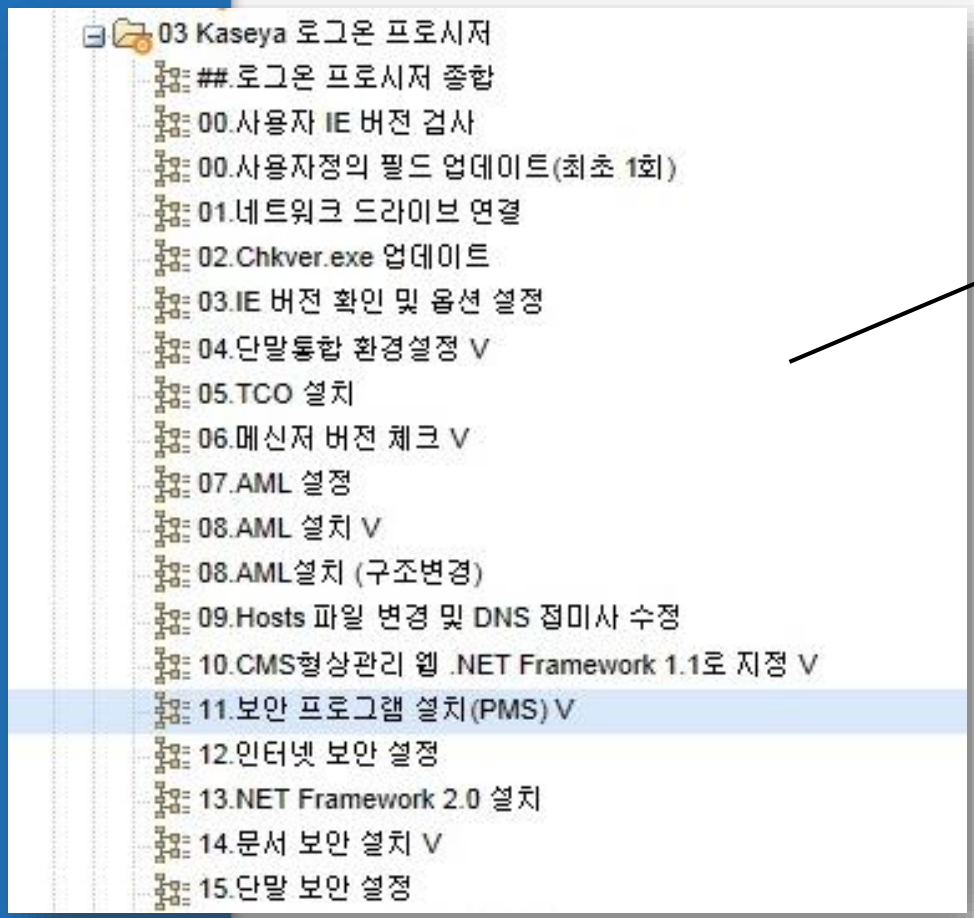
추가(생성)된 기능 샘플 - 2



백신 SW에 대한 조건별 기능 추가

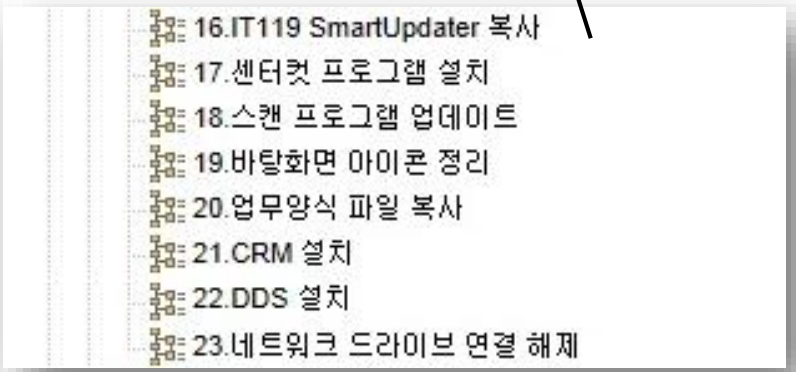
시스템 설정 표준화 기능 추가

추가(생성)된 기능 샘플 - 2



B 은행에서 요청 및 구현한 기능 전체 리스트

(개발자가 아닌, 엔지니어에 의한 직접 구현 및 적용)



Kaseya

Thank you