Logsaver®

내부통제 및 감사를 위한

통합로그관리시스템

JMTRUE

01. 제안 배경 및 목적

본 사업의 목적은 최근 해킹 및 개인정보 유출로 인한 감독기관의 의무 규정 및 향후 다양한 규정 대비와 보안사고 발생 시 사후 감사추적을 위한 정보시스템 및 개인정보 로그정보를 통합 저장 관리하여 신속한 원인 분석 및 대응 방안을 수립할 수 있는 통합로그관리 시스템을 구축하는 것입니다.

제안의 목적

법적/제도적 요구사항 증가	• 개인정보보호법, 정보통신망 법 등 법률 및 규정 제·개정에 따른 로그 기록 보전 의무화 • 해킹 및 내부정보 유출사고 발생 시 시스템 접속 기록 및 내부정보 이용에 대한 증거능력 확보 요구 • 각종 법률에서 접속기록의 보관 및 위 · 변조 방지에 대한 관리 요구
운영면에서의 로그관리 요구사항 증가	• 이기종 시스템 및 다양한 어플리케이션에서 발생하는 로그의 종류 및 양이 방대한 로그관리의 어려움 증가 • 고객의 주문/조회/이체 등 거래 현황 분석 • 장애발생시 장애 원인에 대한 정확한 분석 및 대책마련
감사/보안 측면에서의 요구사항 증가	• 내부인력 또는 외주인력에 의한 보안사고의 경우 기존의 정보보호시스템으로는 원인파악 및 분석의 한계가 있음 • 사용자 사용이력 로그를 통한 시스템 내부인력에 의한 사고 예방 및 탐지 필요성 증대 • 서버 감사 및 고객 거래로그 등 주요 원본로그의 위 · 변조 위험성 내재

02. 관련 법률 및 지침

개인정보보호법

- 개인정보 보호법(제 28조 개인정보의 보호조치)
  - 개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손 방지
- 개인정보보호법 시행령(제 30조 안정성 확보조치)
  - 접속기록의 보관 및 위·변조 방지를 위한 조치
- 보호조치 기준(제 5조 접속기록 위 · 변조방지)
  - 접속기록 위 · 변조방지 및 별도의 물리적 장치에 별도 보관

정보통신망법

- 정보통신망 관련 법률(제28조, 제 48조의 4)
  - 접속기록의 위 · 변조방지를 위한 조치
  - 침해사고 원인분석 을 위한 접속기록 보전
- 정보통신망 법률시행령(제58조)
  - 침해사고 관련 기록 훼손 · 변경 방지 조치
- 정보통신기반보호법(제 12~14조, 제21조)
  - 기록에 대한 접근권한, 사고 시 대응 및 복구 조치 침해사고통지내용, 조치 내용 등

전자금융거래 및 신용정보보호법

- 전자금융거래법(제22조)
  - 전자금융거래 내용 추정 · 검색 또는 오류 발생 시 확인 및 정정관련 기록 보전
- 신용정보 이용 및 보호에 관한 법률 시행령(제16조)
  - 다음사항의 기술 · 물리적 · 관리적 보안대책
    · 접속에 대한 접근, 차단 기록
    · 신용정보취급 · 조회 기록의 점검
    · 그 밖에 신용정보 안정성 확보

정보보호 관리체계(ISMS)

- 8.1.3 보안로그 기능
  - 보안사고 발생 시 책임추적을 위하여 감사증적(로그)를 확보하고, 보안로그의 비인가된 변조 및 삭제를 방지하여야한다.
- 11.6.2 로그기록 및 보존
  - 로그 기록 및 보존이 필요한 주요시스템 지정 하고 기록하여 할 로그 유형 및 보존기간을 정하여한다.
  - 비인가자에 의한 로그 기록 위변조 및 삭제 등이 방지하여야한다.

의료법 및 국방정보화 업무 훈령

- 의료법(제23조 전자의무기록)
  - 전자의무기록을 안정하게 관리 · 보존 필요한 시설이나 장비 구비 의무
  - 정당한 사유없이 전자의무기록 저장 정보 탐지 하거나 누출 · 변조 또는 훼손 금지
- 국방정보화업무훈령(제147조)
  - 감리주관부서는 감리 관련 문서를 5년간 보관 하여야 하며 전자적으로 관리

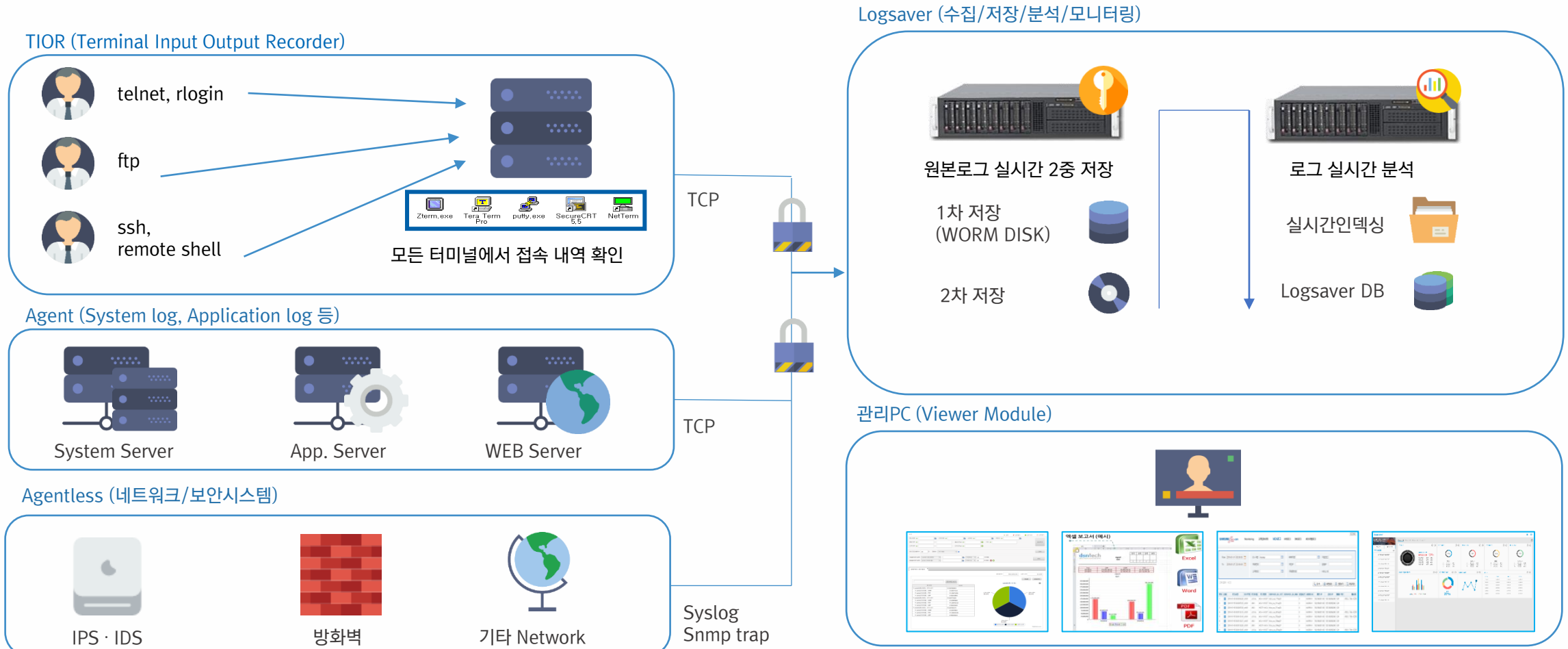
전자정부법

- 정보통신망 등의 보안대책 수립
  - 행정 업무의 전자적 처리를 위한 기본원칙, 절차 및 추진방법 등 규정
  - 전자적 대민 서비스 보안 대책, 정보통신망 등의 보안대책 수립 · 시행, 인증기록보관, 신원확인 및 접근권한 관리 체계의 구축관리

03. 로그세이버 구성 개요

제안사는 다양한 통합로그서버 시스템 구축 프로젝트 수행에 의해 검증된 기술력과 인력 그리고, 풍부한 프로젝트 경험 등 구축 경력을 통해 축적된
노하우와 강력한 솔루션을 바탕으로 보다 효과적으로 구축, 적용함으로써 이를 기반으로 보다 효율적이며 안정적인 통합로그서버 시스템을 구축합니다

표준목표 구성도



04. 로그 수집 기술

제안 제품은 설치대상 서버의 다양한 OS를 지원하며 관리서버와 Agent간, 관리서버와 관리콘솔간 네트워크 전송 시에는 암호화 통신을 지원하며 로그수집 시 Agent의 성능은 대상 서버의 CPU 3% 미만의 자원을 활용하여 실시간 또는 비 실시간 로그수집을 지원합니다

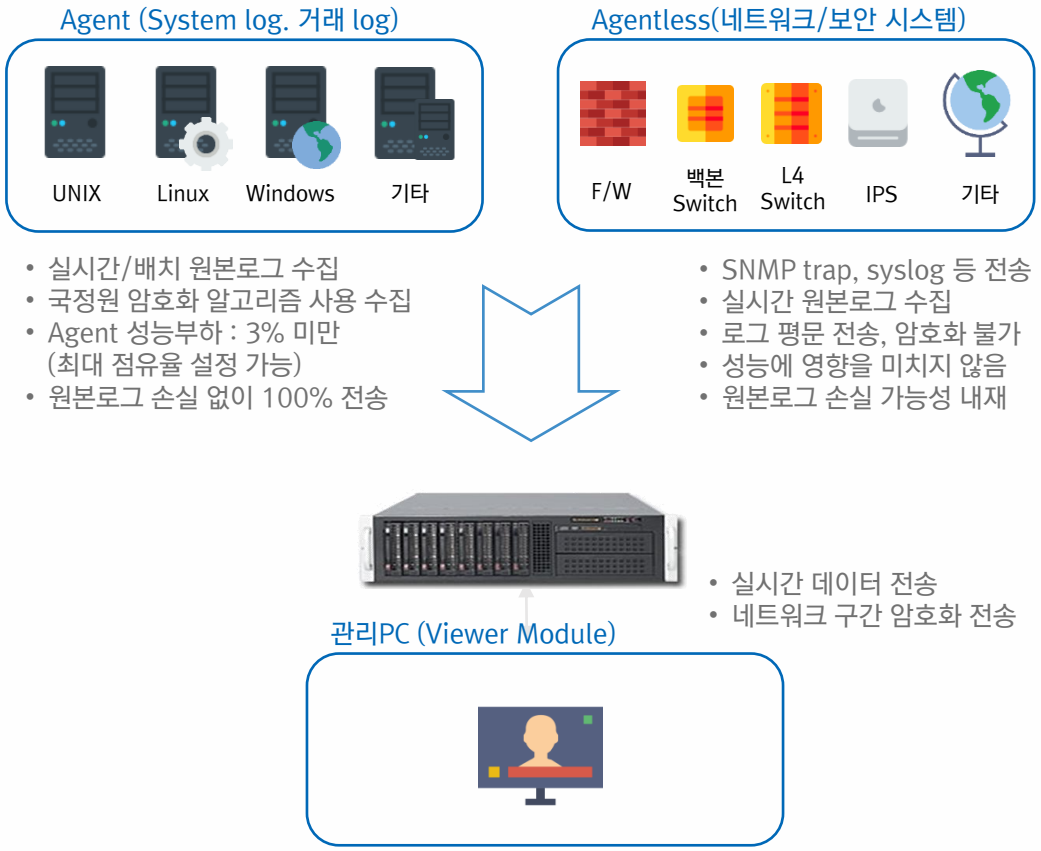
로그수집기술

서버 수집 대상 지원 OS

UNIX	IBM AIX	4.3 / 5.1 / 5.2 / 5.3 / 6.0 / 6.1 / 7.0
	HP-UX	10.20 / 11.00 / 11.11 / 11.23 / 11.31
	Solaris	6 / 7 / 8 / 9 / 10 / Sparc x86
Linux	Linux	2.2 / 2.4 / 2.6
	FreeBSD	
	Suelinux	10
Microsoft	Windows (32bit/64bit)	NT4.0 / 2000 / XP / 2003 / 2008 / 2012 /2016

* 지속적 버전 업데이트 진행 중

원본 로그 수집 – 실시간/비실시간. 암호화. 성능 보장



05. 로그 저장 기술

수집한 원본로그는 위 변조가 불가능한 매체에 보관하여 무결성을 보장하고, 정규화, 필터링, 축약 등의 절차를 통해 DB의 형태로 저장하여 실시간 분석 및 상호연관분석 등 을 지원합니다

로그 저장 기술

원본로그 수집대상

- 서버시스템 로그
- 보안시스템 로그
- 네트워크시스템 로그
- 기타 시스템 로그

원본 로그 실시간 수집

원본 로그 실시간 수집

압축

- 설정에 따른 주기적 압축
- 로그유형별/그룹별 압축 기능 제공
- 압축율 : 평균 90% 제공

암호화 SEED SEED SEED SEED

- 국정원 암호화 모듈 적용 (Option)

정규화

필터링

축약 2 2 3 3

원본 로그 저장

분석 로그 저장

- Logsaver 내장 스토리지
- WORM usable 10TB
- 원본로그 압축 저장

원본 로그 백업

Blu-Ray

- 원천적으로 위·변조가 불가능한 매체 사용
- 원본 로그의 장기 보존 지원
- 물리적 25GB 저장공간
  ➔ 압축된 로그 저장으로 실제 원본로그 200GB 이상 저장
- 매체 보관함 제공

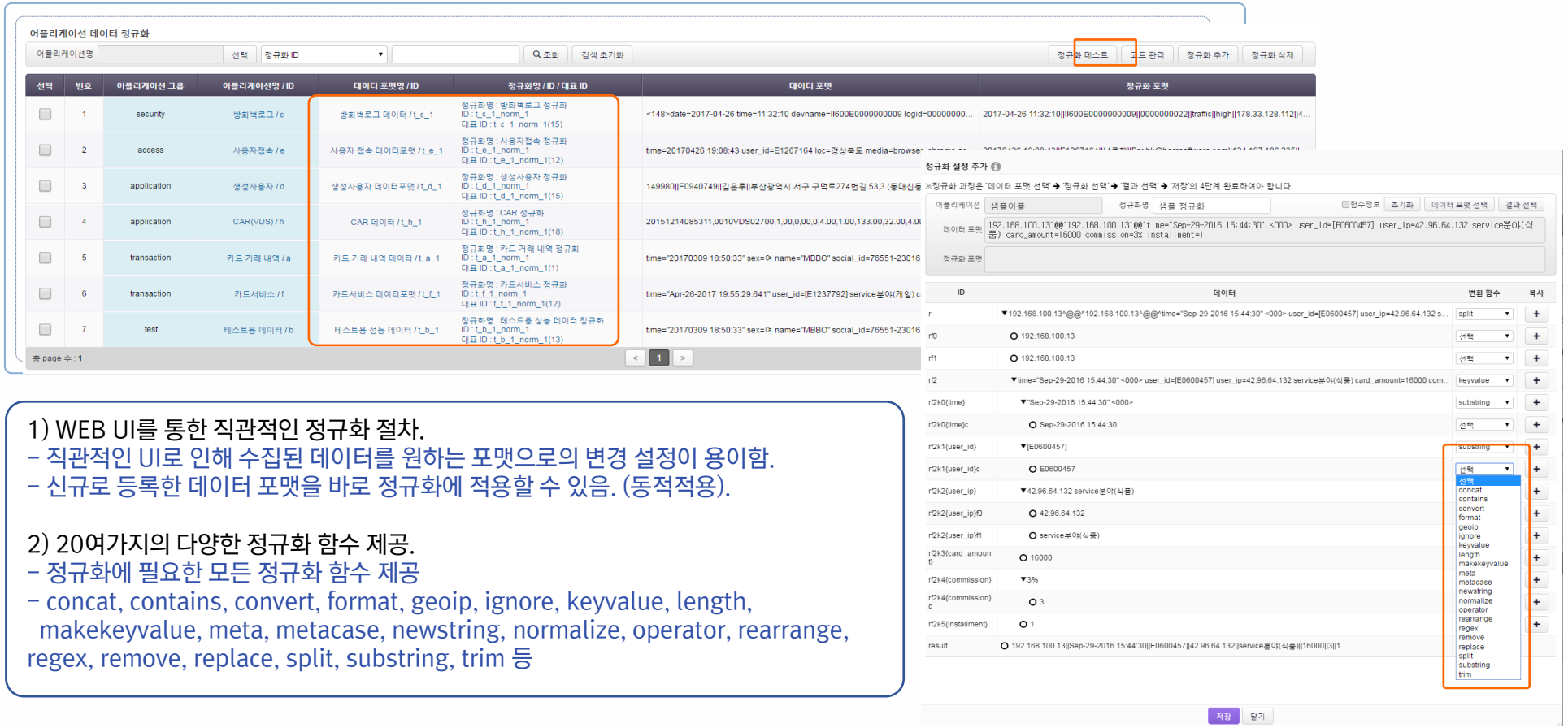
- Logsaver 분석 서버
- 고속 NoSQL 기반으로 고속 분석 지원
- 실시간 로그 조회/분석 지원

06. 로그 분석기술

로그의 분석은 정규화를 통하여 서로 다른 로그 포맷의 경우에도 공통의 필드 속성값을 부여할 수 있습니다. 모든 정규화 과정은 Web UI 컨피그레이션을 통하여 손쉬운 작성 환경을 제공합니다

로그 분석 기술(1/3)

비정형 로그 정규화



1) WEB UI를 통한 직관적인 정규화 절차.
- 직관적인 UI로 인해 수집된 데이터를 원하는 포맷으로의 변경 설정이 용이함.
- 신규로 등록한 데이터 포맷을 바로 정규화에 적용할 수 있음. (동적적용).

2) 20여가지의 다양한 정규화 함수 제공.
- 정규화에 필요한 모든 정규화 함수 제공
- concat, contains, convert, format, geoip, ignore, keyvalue, length, makekeyvalue, meta, metacase, newstring, normalize, operator, rearrange, regex, remove, replace, split, substring, trim 등

06. 로그 분석기술

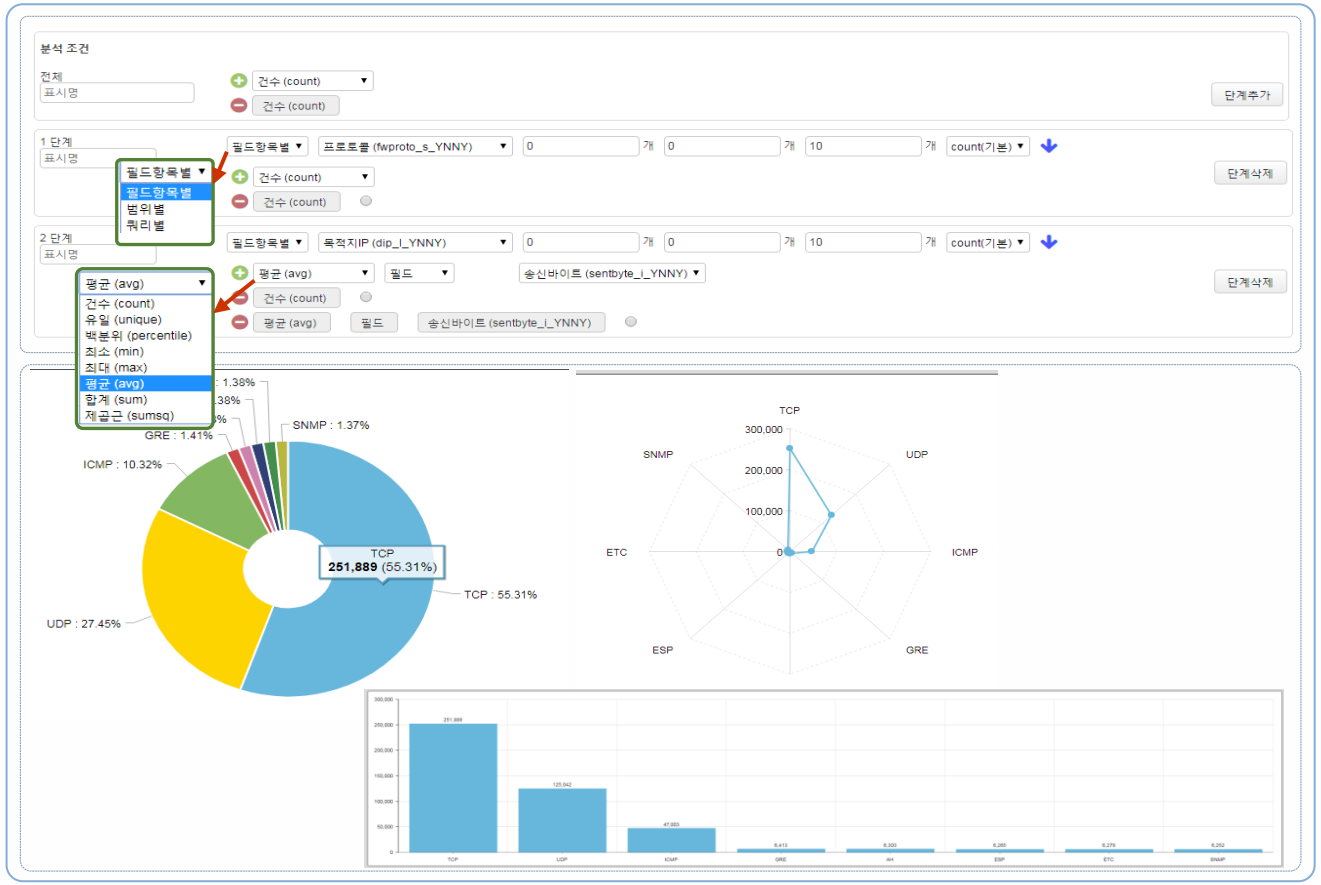
실시간으로 정규화 된 DB를 통하여 저장한 로그 데이터를 활용하여 사용자 조건 지정에 의한 실시간 조회 및 분석 뿐만 아니라, 이기종 시스템 로그간 연관 검색 및 상관분석 기능을 제공하여 효율적인 분석을 지원합니다

로그 분석 기술(2/3)

실시간 분석

1) 분석 동작 방식.
- 어플리케이션별 다중 Depth별 분석
  분석 depth를 추가하면서 분석
- 필드항목별, 범위별, 쿼리별 분석
- 다양한 분석함수 제공
  건수(count), 유일(unique), 백분위, 최소(min), 최대(max), 평균(avg), 합계(sum), 제곱근(sumsq)

2) 다양한 분석 차트 제공.
- 파이(PIE)차트
- 바(BAR)차트
- 레이더(RADAR) 차트
- 스탭바(STACKBAR) 차트
- 시계열차트
- 실시간차트



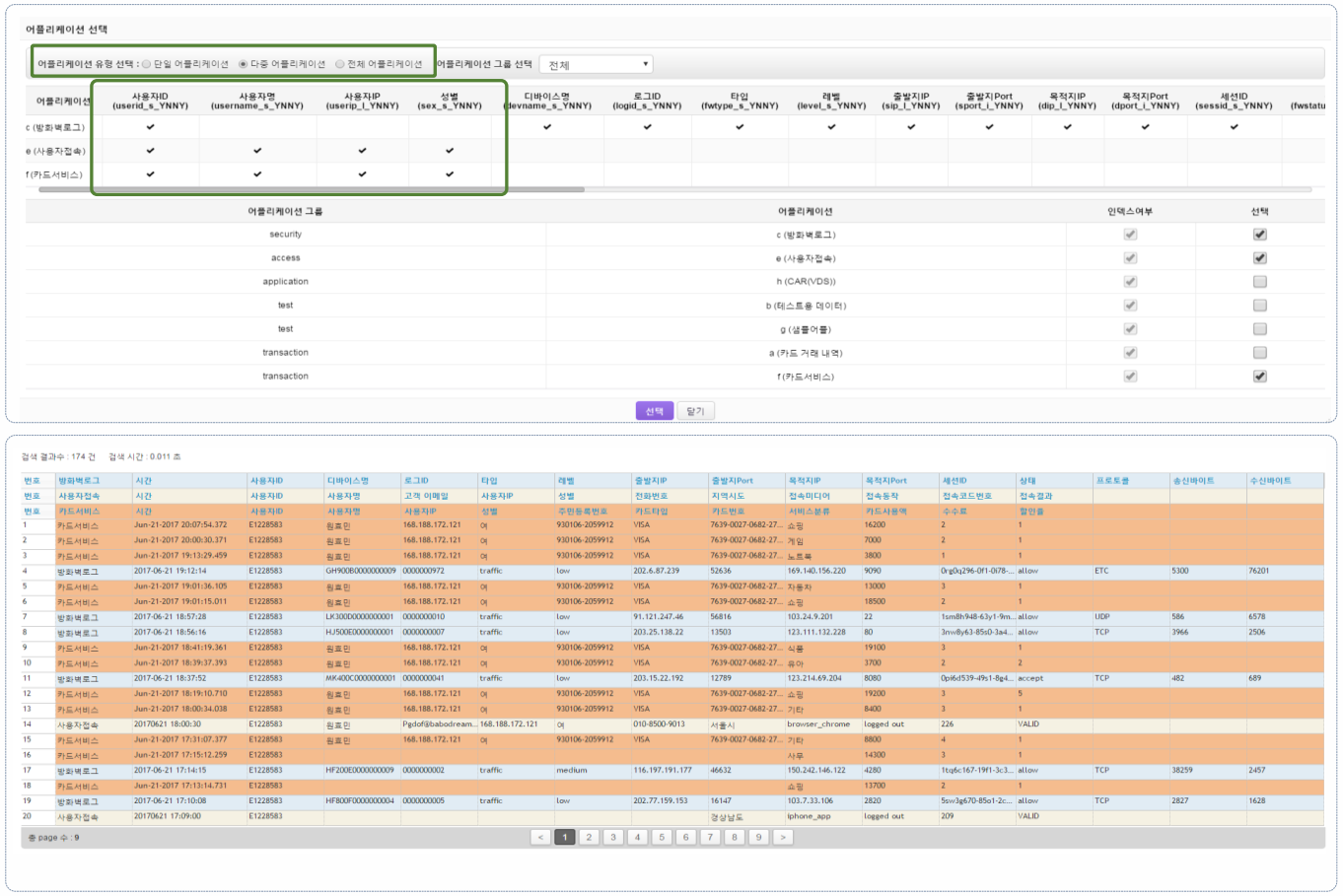
06. 로그 분석기술

로그 데이터를 활용하여 다양한 검색 조건을 지정하여 실시간 조회 및 분석 뿐만 아니라, 이기종 로그 간 공통된 연관 필드를 기준으로 연관 검색 및 분석을 제공하며, 시간 정렬을 통하여 검색대상 로그 간 추적 기능을 지원 합니다

로그 분석 기술(3/3)

연관 분석

- 하나 이상의 어플리케이션(들)의 교차 필드들로 연관 분석을 수행할 수 있다.
- 이를 시간순으로 정렬하면 어플리케이션 간 데이터 추적(track)에 유용하게 활용 가능함.



07. 리포팅 기능

사용자 정의 보고서를 포함한 다양한 포맷의 보고서 형태를 제공하며, 다양한 주기별(일간/주간/월간/분기 등) 보고서를 자동 생성하여 Word, PDF 등의 포맷으로 제공합니다

리포팅 기능

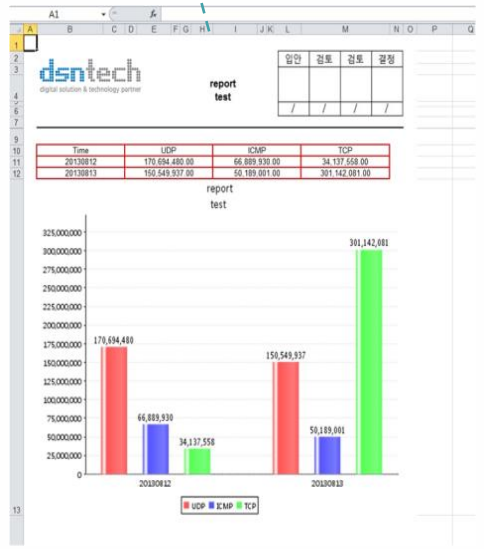
- 제공하는 프레임(표지요소, 데이터요소, 주석요소내의 모듈)으로 보고서를 설계
- 필요에 따라 프레임과 이미지, 표, 차트 등을 조정하여 사용자가 원하는 보고서를 구성

보고서 구성요소

- 표지요소
  - 회사 로고 / 서명란
  - 보고서제목 / 배경 이미지
- DATA요소
  - Table / 표
  - 각종 차트
- Comment요소
  - 각종 이슈 사항
  - 담당자 의견

- 3종의 파일 포맷(pdf, excel, word)을 지원.

엑셀 보고서 (예시)



Excel

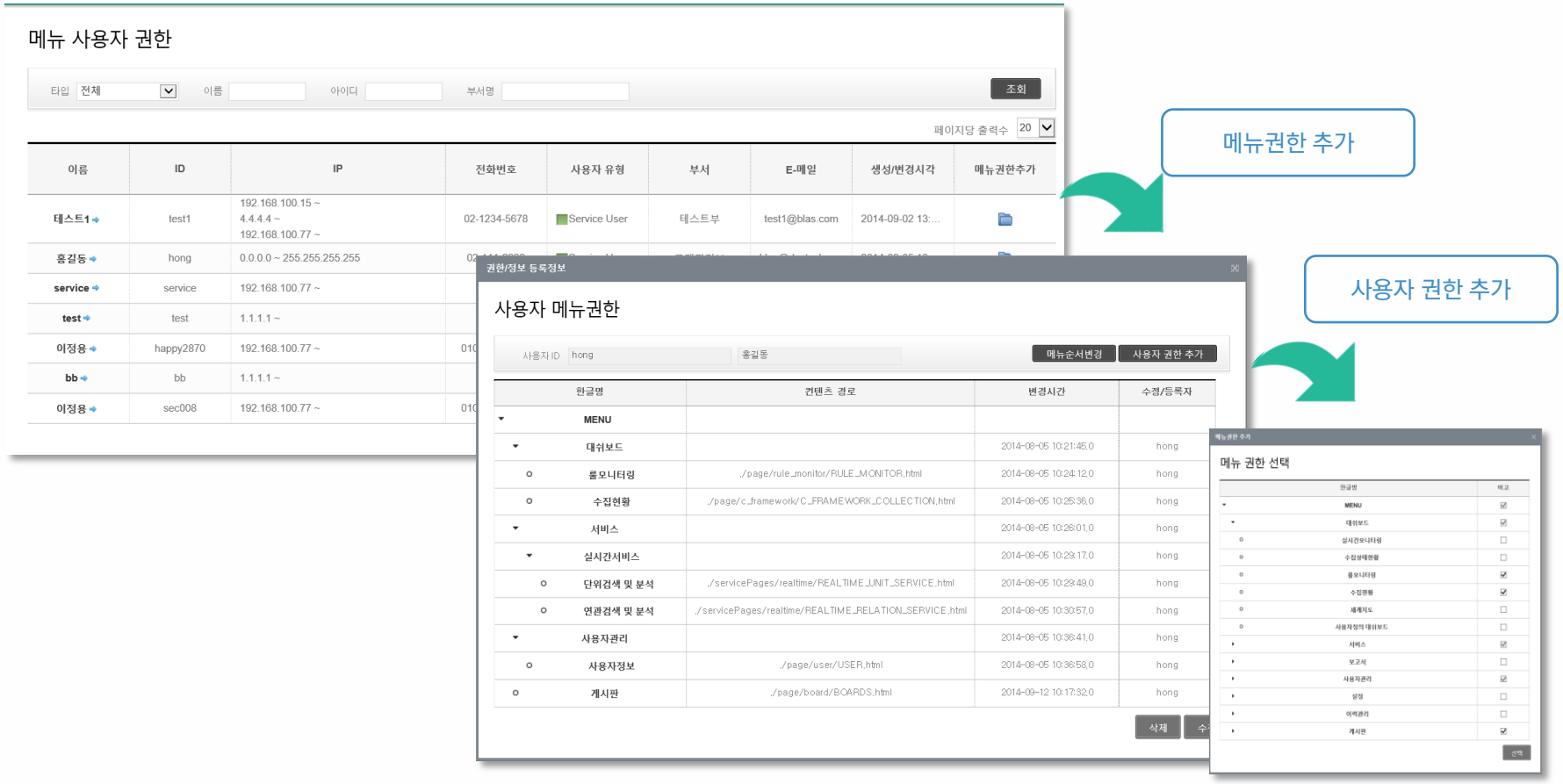
Word

PDF

08. 권한관리

통합로그시스템을 관리하는 관리자 및 일반사용자에 대한 권한이 분리되어 있으며, 관리자는 일반 사용자에 대한 권한을 차등 부여하여 관리할 수 있으며 이용 내역에 대한 내용을 감사할 수 있도록 제공합니다

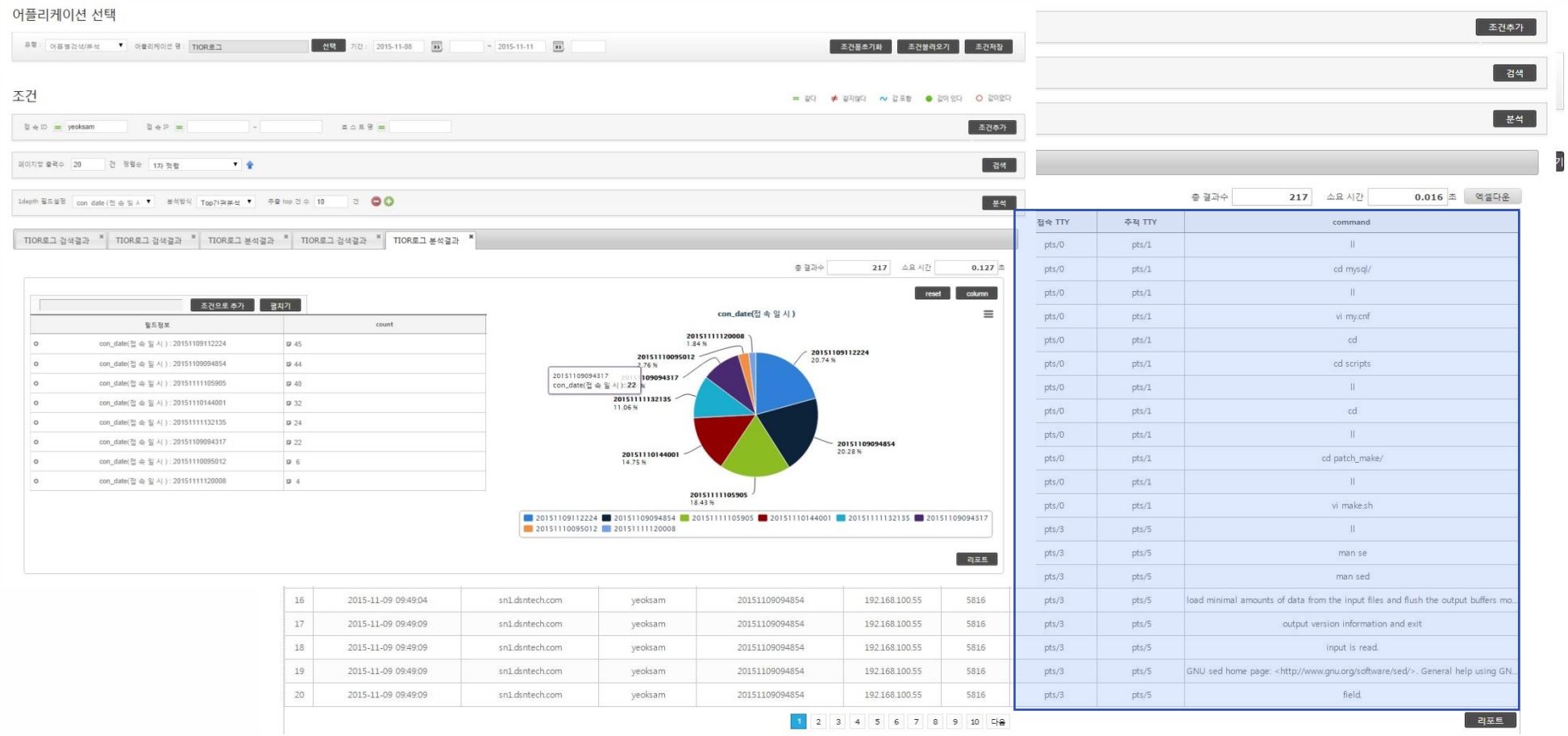
권한관리 기능



09. TIOR – 서버 추적 감사 S/W

서버 감사 추적 소프트웨어 TIOR 는 (Terminal Input Output Recorder)의 약자로 터미널 접속 사용자의 모든 Keystroke 정보를 활용하여 해킹 및 내부자 작업 실수로 인한 정보 유출이나 장애발생시 감사 추적 기능을 제공하여 시스템 오남용 방지 및 사후 책임성을 확보합니다.

감사 추적 기술 – Unix, Linux



09. TIOR – 서버 추적 감사 S/W

WindowsTIOR 는 윈도우 기반의 개인 PC 및 서버의 감사소프트웨어로 화면, 마우스, 키보드, 이벤트 등 Windows OS 특성인 GUI 기반에서 이루어지는 모든 사용자 행위에 대한 실시간 감사 추적 기능을 제공합니다

감사 추적 기술 – Windows

➔ Windows GUI 사용자행위 재생 감사추적도구

감사(수집) 대상 PC

- 키보드 정보 로그
- 화면 이미지 및 동작 정보 로그
- 마우스 정보 로그
- 프로세스 정보 로그
- 터미널 접속 정보
- 파일 변경 정보

감사(수집) 대상 서버

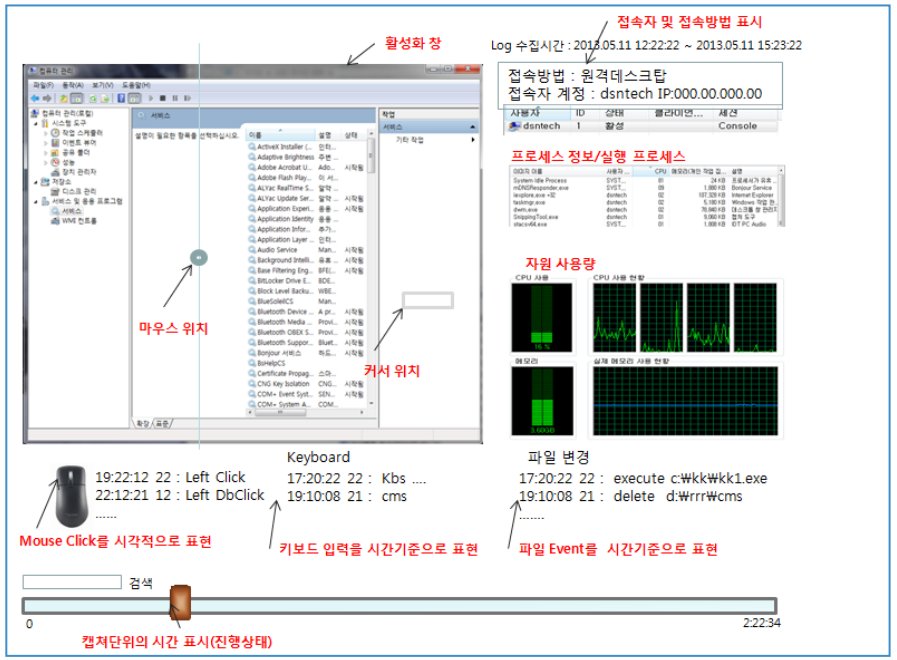
- 키보드 정보 로그
- 화면 이미지 및 동작 정보 로그
- 마우스 정보 로그
- 프로세스 정보 로그
- 터미널 접속 정보
- 파일 변경 정보

실시간
로그 수집

수집 서버 (Logsaver)

- 로그 파일 수집
- 로그 파일 파싱 및 DB화
- 로그 정보 조회/검색
- 감사 레포터
- 통합 재생(영상 포함)

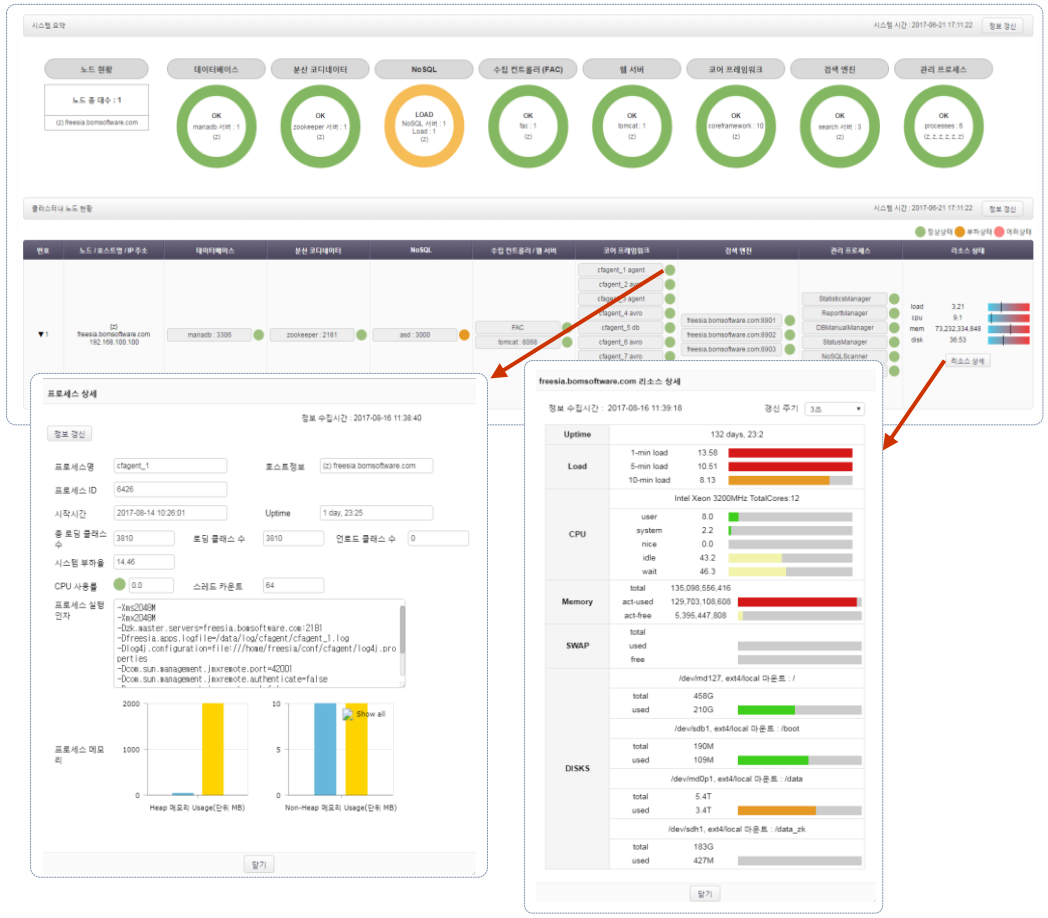
세부 화면 재생 UI 제공

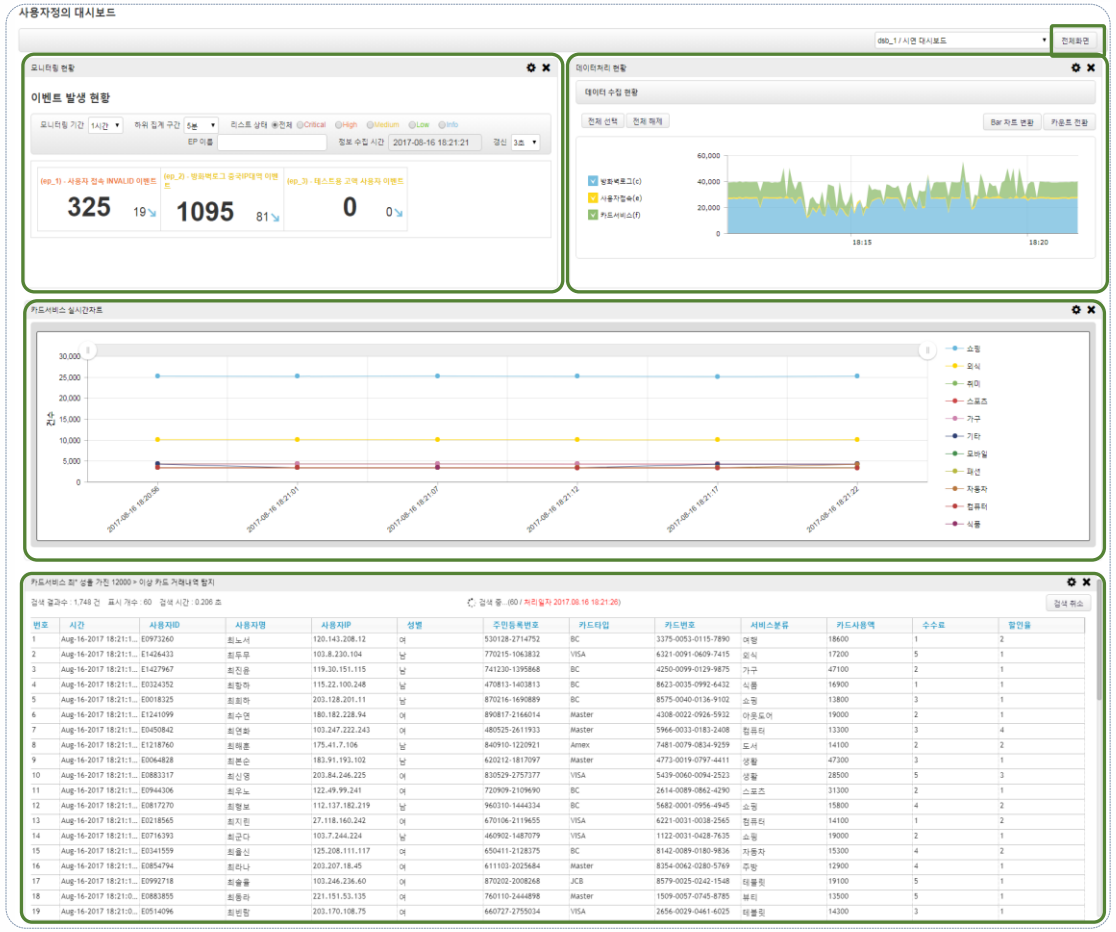


10. 사용자 정의 대시보드

통합로그시스템을 관리하는 담당자 및 업무 별 목적에 맞게 사용자 정의 대시보드를 제공합니다.

사용자 정의 대시보드





01. 전체 구축 실적

제안사가 제안하는 제품은 은행, 증권, 카드, 보험 등의 금융권을 비롯하여, 공공기관, 일반기업체 등 다양한 분야에서 고객을 확보하고 있는 우수한 제품으로서, 국내 시장 점유율 1위 제품입니다.

레퍼런스(요약)

공공

- 대통령비서실
- 대법원(호적망, 등기망, 가족망)
- 기획경제부(NAFIS), 해양수산부
- 기획예산처(디지털회계예산)
- 안전행정부, 산업통상자원부
- 고용노동부, 한국산업기술시험원
- 경찰청(사이버테러대응센터)
- 조달청, 국세청, 서울지방경찰청
- 식품의약품안전처, 철도청
- 충청남도교육청, 한국토지주택공사
- 한국인터넷진흥원(KISA)
- 국가정보원, 한국정보화진흥원
- 한국가스공사, 인천공항공사
- 국민연금공단, 국민체육진흥공단
- 인사혁신처, 한국정보인증
- 한국원자력연구소, 한국마사회
- 부산항만공사, 광물자원공사
- 건강보험심사평가원, 김해경전철
- 한국도로공사, 한국전력공사
- 수원시청, 한국석유공사
- 교육부, 국회사무처, 제주시청
- 한국산업단지공단, 한국환경공단
- 국가정보자원관리원
- 경남도청, 성남시청
- 전국 16개 시도 교육청
  (서울, 경기, 인천, 강원, 충북, 충남, 대전, 경북, 경남, 대구, 울산, 부산, 전북, 전남, 광주, 제주) 외 다수

은행/금융

- 금융감독원
- 금융정보분석원
- 한국자산관리공사
- 한국예탁결제원
- 한국신용정보원
- 한국금융연수원
- 저축은행중앙회
- 농협중앙회, 농협생명
- 농협NH카드
- 수출입은행
- 산업은행
- 신한은행, 신한금융지주
- 신한생명, 신한카드
- 신한금융투자
- 삼성생명, 삼성화재
- 삼성증권
- 한화생명, 한화손해보험
- 하나카드, 하나멤버스
- SC은행, SC증권
- KTB투자증권
- 미래에셋생명, 미래에셋대우
- SK증권
- KB증권, KB손해보험
- 롯데손해보험, 롯데멤버스
- 메리츠화재
- ING생명보험
- 흥국생명, 흥국화재
- EB카드 외 다수

일반 기업체

- KT본부
- KT IT 본부(목동)
- KTNET(전자문서보관소)
- KT(정보보호본부)
- 삼성전자(15곳)
- 삼성종합기술원
- SK OCMP
- SK C&C
- 나눔로또위원회
- 메가스터디
- 노틸러스효성
- 롯데면세점
- NC소프트
- 쇼핑엔티 외 다수

대학교 및 병원

- 건국대학교
- 중앙대학교
- 한성대학교
- 서울교육대학교
- 서울여자대학교
- 삼육대학교
- 동남권 원자력 의학원
- 대구 파티마 병원
- 구미 차 병원
- 강동경희대학교 병원 외
- 다수

국방

- 국방재정
- 국방인사
- 국방인증
- 국군수송사령부
- 합동참모본부
- 방위사업청
- 육군본부
- 해군본부
- 공군본부
- 국방 CPAS
- 합참KJCCS(지휘통제체계)
- 국방동원
- 국방과학연구소
- 국방기술품질원
- 국군통신사령부
- 국군기무사령부
- 각급 부대 별 납품 외 다수

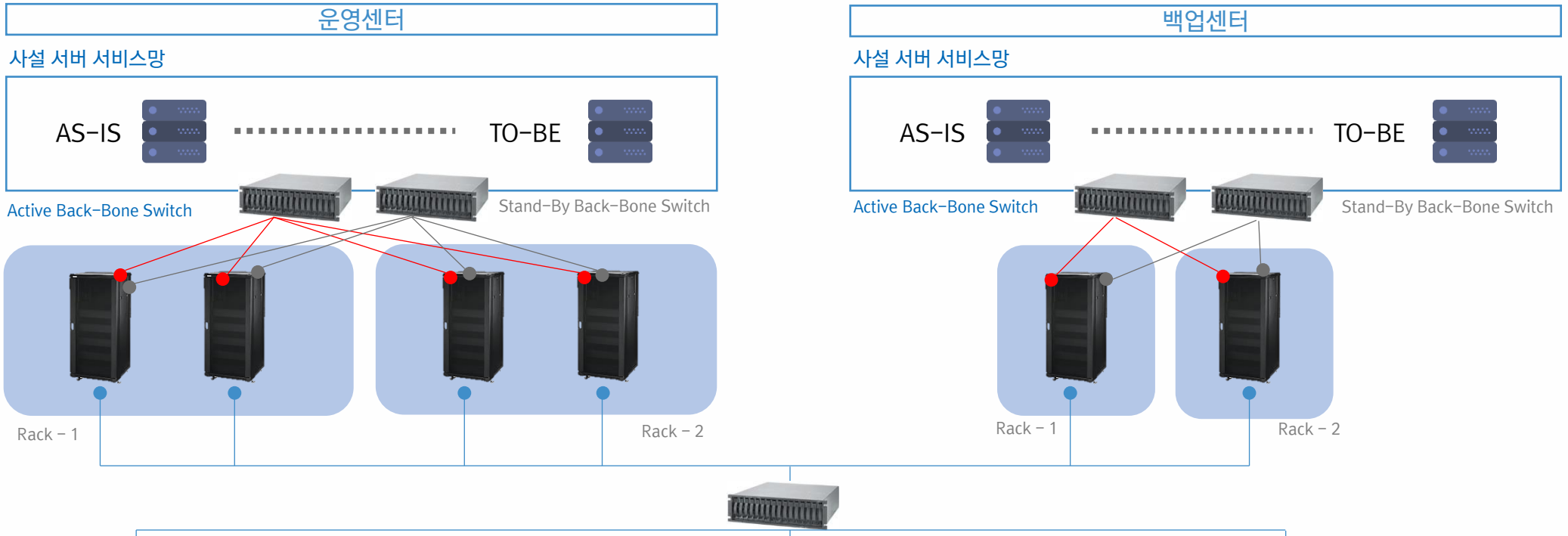
해외

- 미국 : Princeton University
- 일본 : 일본과학기술청, NHK, 삼성JAPAN, 일본 Dreamware, Mitsubishi Research Institute
- 독일 : BW Bank, Bohn University
- 말레이시아 : Alliance System
- 싱가폴 : snttec
- 신한은행 해외 지점
  (독일, 캐나다, 일본, 베트남)

02. 주요사업 실적

내부 운영자에 의한 실수 또는 과오로 인한 운영시스템의 서비스 장애 발생 시 신속히 원인을 찾아내기 위해 주요 운영 서버에 설치하여 인증된 경로를 통하지 않고 비정상적으로 접속하는 사용자의 행위를 감시하기 위한 감사시스템 구축 프로젝트입니다

S은행 – IT운영감사시스템 구축



내부사용자 서버 작업 내역 확인
운영상의 실수 및 과실 추적
담당 파트별 서버 작업 내역 관리

비정상적인 접근 내역 감시
서버 작업 내역 감시 및 검색
감시 및 검색결과에 대한 운영팀과의 협조

감사보고서 내역 출력 확인
비정상적 접근 등 의심 행위 확인
추적관리 내역에 대한 보안팀과의 협업

02. 주요사업 실적

HTS 주식 거래관련 민원 발생에 따른 거래로그 검색이 인력 및 시간 소모가 많아 통합로그 시스템 구축을 통하여 민원 관련 업무를 자동화 하고, 마케팅 자료로 활용하기 위한 데이터 제공 및 타 업무를 지원합니다

S증권 – 통합로그관리시스템 구축

〈MCA 거래로그 검색〉

〈서버별 로그 처리 일별 통계〉

〈MCA 개발로그 조회 화면 – 개발자 전용〉

〈서버간 Response time 분석〉

02. 주요사업 실적

중요 정보시스템에 대한 사용자의 행위 감시 내역을 수집하여 내부 정보에 대한 감사 및 보안관리 업무를 수행하고 인터넷뱅킹과 같은 거래로그 관련 정보를 수집/저장/분석/조회를 통하여 각종 법적 규제 및 지침을 만족하기 위한 프로젝트 입니다

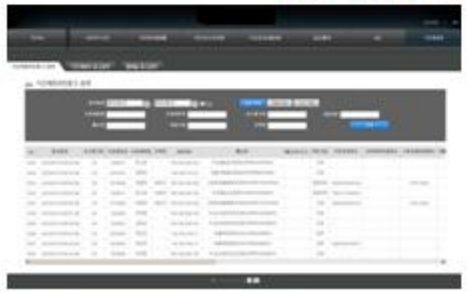
H카드 – 거래로그관리시스템 구축

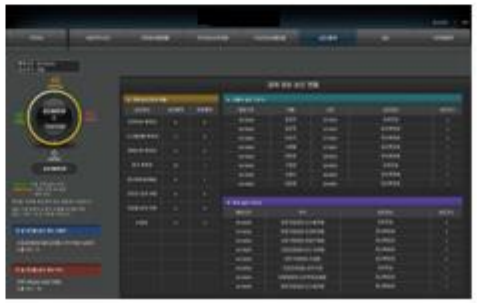
02. 주요사업 실적

신용정보법 개정에 따른 고객 신용업무 처리 현황 관리 및 법률/지침을 만족을 목적으로 고객 신용정보의 유통에 대한 전사적 차원의 감사 모니터링 체계를 구축함으로써 회사 내부의 고객 신용정보의 유출을 사전에 방지하고 글로벌 경영시스템의 안정성 확보를 목적으로 프로젝트를 수행하였습니다

A캐피탈 – 개인정보감사시스템 구축

〈개인정보 감사 통합 대시보드 화면〉





Logsaver®

감사합니다

JMTRUE
(주)제이엠트루
주소 : 서울시 금천구 가산디지털1로 5, 2026-2호(가산동, 대륭테크노타운 20차)
Tel : 02-2224-0925, Fax : 02-2224-0935
http://www.jmtrue.co.kr