

Log saver[®]




내부통제 및 감사를 위한
통합로그관리시스템



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

 <p>법적/제도적 요구사항 증가</p>	<ul style="list-style-type: none"> 개인정보보호법, 정보통신망 법 등 법률 및 규정 제·개정에 따른 로그 기록 보존 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
 <p>운영면에서의 로그관리 요구사항 증가</p>	<ul style="list-style-type: none"> 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
 <p>감사/보안 측면에서의 요구사항 증가</p>	<ul style="list-style-type: none"> 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



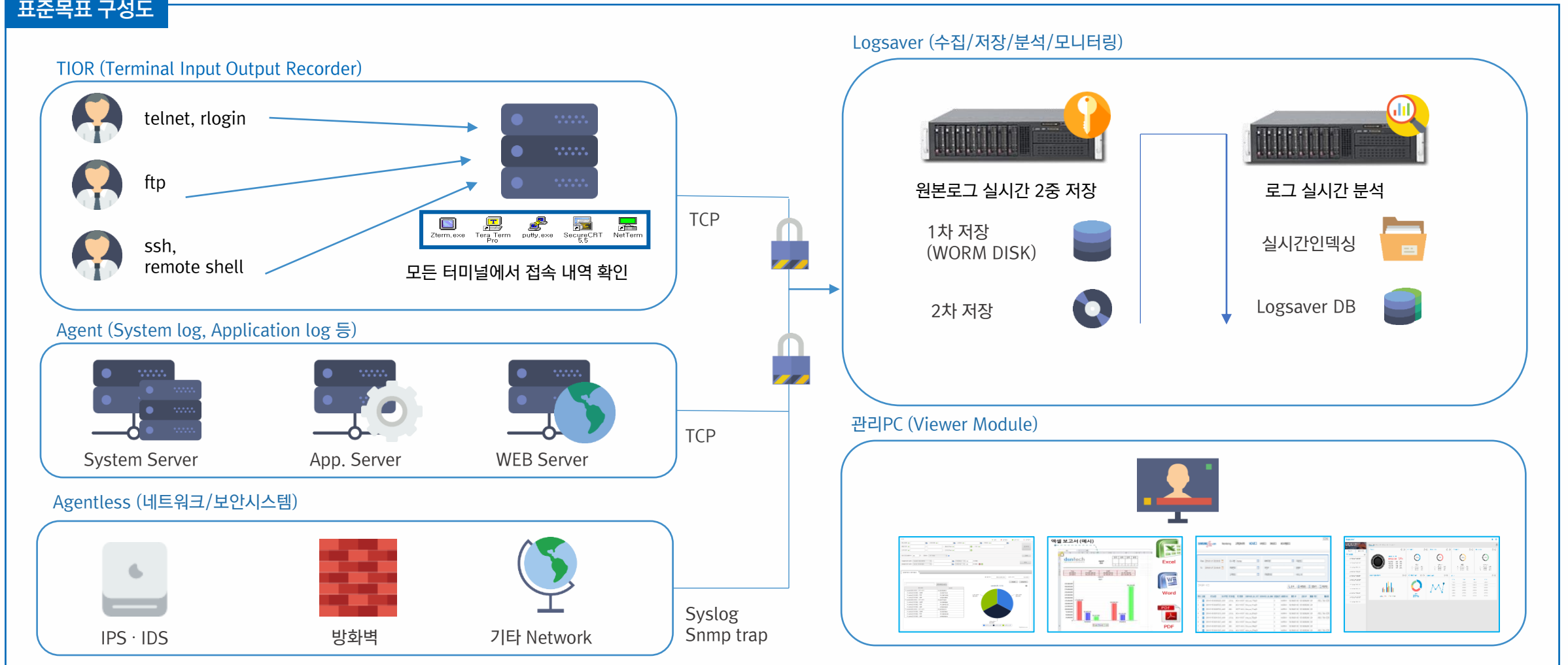
02. 관련 법률 및 지침

개인정보보호법	정보통신망법	전자금융거래 및 신용정보보호법
<ul style="list-style-type: none"> • 개인정보 보호법(제 28조 개인정보의 보호조치) <ul style="list-style-type: none"> - 개인정보의 분실, 도난, 유출, 위조, 변조 또는 훼손 방지 • 개인정보보호법 시행령(제 30조 안정성 확보조치) <ul style="list-style-type: none"> - 접속기록의 보관 및 위·변조 방지를 위한 조치 • 보호조치 기준(제 5조 접속기록 위·변조방지) <ul style="list-style-type: none"> - 접속기록 위·변조방지 및 별도의 물리적 장치에 별도 보관 	<ul style="list-style-type: none"> • 정보통신망 관련 법률(제28조, 제 48조의 4) <ul style="list-style-type: none"> - 접속기록의 위·변조방지를 위한 조치 - 침해사고 원인분석을 위한 접속기록 보존 • 정보통신망 법률시행령(제58조) <ul style="list-style-type: none"> - 침해사고 관련 기록 훼손·변경 방지 조치 • 정보통신기반보호법(제 12~14조, 제21조) <ul style="list-style-type: none"> - 기록에 대한 접근권한, 사고 시 대응 및 복구 조치 침해사고통지내용, 조치 내용 등 	<ul style="list-style-type: none"> • 전자금융거래법(제22조) <ul style="list-style-type: none"> - 전자금융거래 내용 추정·검색 또는 오류 발생 시 확인 및 정정관련 기록 보존 • 신용정보 이용 및 보호에 관한 법률 시행령(제16조) <ul style="list-style-type: none"> - 다음사항의 기술·물리적·관리적 보안대책 <ul style="list-style-type: none"> · 접속에 대한 접근, 차단 기록 · 신용정보취급·조회 기록의 점검 · 그 밖에 신용정보 안정성 확보
정보보호 관리체계(ISMS)	의료법 및 국방정보화 업무 훈령	전자정부법
<ul style="list-style-type: none"> • 8.1.3 보안로그 기능 <ul style="list-style-type: none"> - 보안사고 발생 시 책임추적을 위하여 감사증적(로그)을 확보하고, 보안로그의 비인가된 변조 및 삭제를 방지하여야한다. • 11.6.2 로그기록 및 보존 <ul style="list-style-type: none"> - 로그 기록 및 보존이 필요한 주요시스템 지정하고 기록하여 할 로그 유형 및 보존기간을 정하여야한다. - 비인가자에 의한 로그 기록 위변조 및 삭제 등이 방지하여야한다. 	<ul style="list-style-type: none"> • 의료법(제23조 전자의무기록) <ul style="list-style-type: none"> - 전자의무기록을 안정하게 관리·보존 필요한 시설이나 장비 구비 의무 - 정당한 사유없이 전자의무기록 저장 정보 탐지하거나 누출·변조 또는 훼손 금지 • 국방정보화업무훈령(제147조) <ul style="list-style-type: none"> - 감리주관부서는 감리 관련 문서를 5년간 보관하여야 하며 전자적으로 관리 	<ul style="list-style-type: none"> • 정보통신망 등의 보안대책 수립 <ul style="list-style-type: none"> - 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

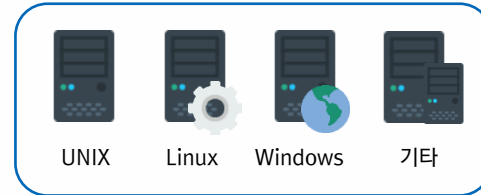
서버 수집 대상 지원 OS

	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	2.2 / 2.4 / 2.6
	FreeBSD	
	Suelinux	10
	Windows (32bit/64bit)	NT4.0 / 2000 / XP / 2003 / 2008 / 2012 / 2016

* 지속적 버전 업데이트 진행 중

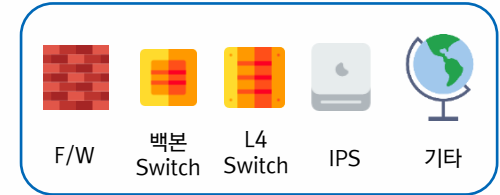
원본 로그 수집 - 실시간/비실시간. 암호화. 성능 보장

Agent (System log. 거래 log)



- 실시간/배치 원본로그 수집
- 국정원 암호화 알고리즘 사용 수집
- Agent 성능부하 : 3% 미만 (최대 점유율 설정 가능)
- 원본로그 손실 없이 100% 전송

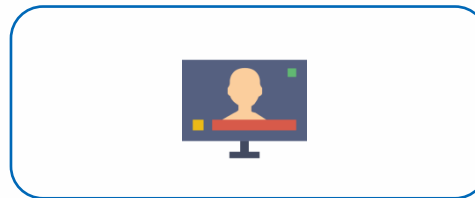
Agentless(네트워크/보안 시스템)



- SNMP trap, syslog 등 전송
- 실시간 원본로그 수집
- 로그 평문 전송, 암호화 불가
- 성능에 영향을 미치지 않음
- 원본로그 손실 가능성 내재



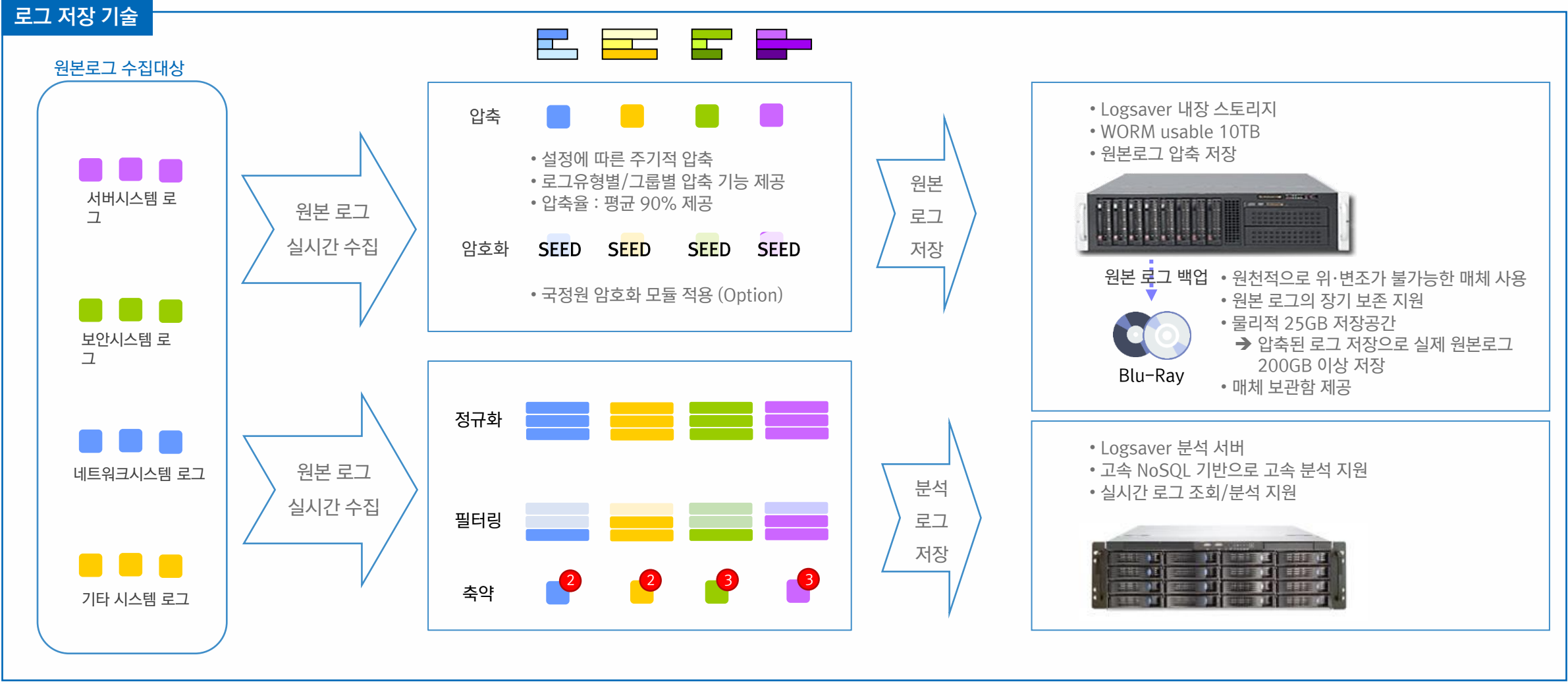
관리PC (Viewer Module)



- 실시간 데이터 전송
- 네트워크 구간 암호화 전송

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 등을 지원합니다



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

어플리케이션 데이터 정규화

어플리케이션명 | 선택 | 정규화 ID | 🔍 조회 | 검색 초기화 | 정규화 테스트 | 카드 관리 | 정규화 추가 | 정규화 삭제

선택	번호	어플리케이션 그룹	어플리케이션명 / ID	데이터 포맷명 / ID	정규화명 / ID / 대표 ID	데이터 포맷	정규화 포맷
<input type="checkbox"/>	1	security	방화벽로그 / c	방화벽로그 데이터 / L_c_1	정규화명: 방화벽로그 정규화 ID: L_c_1_norm_1(15) 대표 ID: L_c_1_norm_1(15)	<148>date=2017-04-26 time=11:32:10 devname=H600E000000009 logid=00000000... 2017-04-26 11:32:10 H600E0000000009 0000000022 traffic high 178.33.128.112 4...	
<input type="checkbox"/>	2	access	사용자접속 / e	사용자 접속 데이터포맷 / L_e_1	정규화명: 사용자접속 정규화 ID: L_e_1_norm_1(12) 대표 ID: L_e_1_norm_1(12)	time=20170426 19:08:43 user_id=E1267164 loc=경상북도 media=browser	
<input type="checkbox"/>	3	application	상성사용자 / d	상성사용자 데이터포맷 / L_d_1	정규화명: 상성사용자 정규화 ID: L_d_1_norm_1(15) 대표 ID: L_d_1_norm_1(15)	149980 E0940749 김은후 부산광역시 서구 구덕로274번길 53.3 (동대신동	
<input type="checkbox"/>	4	application	CAR(VDS) / h	CAR 데이터 / L_h_1	정규화명: CAR 정규화 ID: L_h_1_norm_1(18) 대표 ID: L_h_1_norm_1(18)	20151214085311.0010VDS02700.1.00.0.00.0.4.00.1.00.133.00.32.00.4.01	
<input type="checkbox"/>	5	transaction	카드 거래 내역 / a	카드 거래 내역 데이터 / L_a_1	정규화명: 카드 거래 내역 정규화 ID: L_a_1_norm_1(1) 대표 ID: L_a_1_norm_1(1)	time="20170309 18:50:33" sex=여 name="MBBO" social_id=76551-23016	
<input type="checkbox"/>	6	transaction	카드서비스 / f	카드서비스 데이터포맷 / L_f_1	정규화명: 카드서비스 정규화 ID: L_f_1_norm_1(12) 대표 ID: L_f_1_norm_1(12)	time="Apr-26-2017 19:55:29.641" user_id=[E1237792] service분야(게임) c	
<input type="checkbox"/>	7	test	테스트용 데이터 / b	테스트용 성능 데이터 / L_b_1	정규화명: 테스트용 성능 데이터 정규화 ID: L_b_1_norm_1(13) 대표 ID: L_b_1_norm_1(13)	time="20170309 18:50:33" sex=여 name="MBBO" social_id=76551-23016	

정규화 설정 추가

어플리케이션: 샘플어플 | 정규화명: 샘플정규화 | ▶ 함수정보 | 초기화 | 데이터 포맷 선택 | 결과 선택

데이터 포맷: 192.168.100.13@192.168.100.13@time="Sep-29-2016 15:44:30" <000> user_id=[E0600457] user_ip=42.96.64.132 service분야(식품) card_amount=16000 commission=3% installment=1

정규화 포맷:

ID	데이터	변환 함수	복사
r	▼ 192.168.100.13@192.168.100.13@time="Sep-29-2016 15:44:30" <000> user_id=[E0600457] user_ip=42.96.64.132 s...	split	+
r0	○ 192.168.100.13	선택	+
r1	○ 192.168.100.13	선택	+
r2	▼ time="Sep-29-2016 15:44:30" <000> user_id=[E0600457] user_ip=42.96.64.132 service분야(식품) card_amounts=16000 com...	keyvalue	+
r2k0[time]	▼ "Sep-29-2016 15:44:30" <000>	substring	+
r2k0[time]c	○ Sep-29-2016 15:44:30	선택	+
r2k1[user_id]	▼ [E0600457]	substring	+
r2k1[user_id]c	○ E0600457	선택	+
r2k2[user_ip]	▼ 42.96.64.132 service분야(식품)	concat	+
r2k2[user_ip]0	○ 42.96.64.132	contains	+
r2k2[user_ip]1	○ service분야(식품)	convert	+
r2k3[card_amount]	○ 16000	format	+
r2k4[commission]	▼ 3%	geoip	+
r2k4[commission]c	○ 3	ignore	+
r2k5[installment]	○ 1	keyvalue	+
result	○ 192.168.100.13 Sep-29-2016 15:44:30 [E0600457] 42.96.64.132 service분야(식품) 16000 3 1	length	+

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)

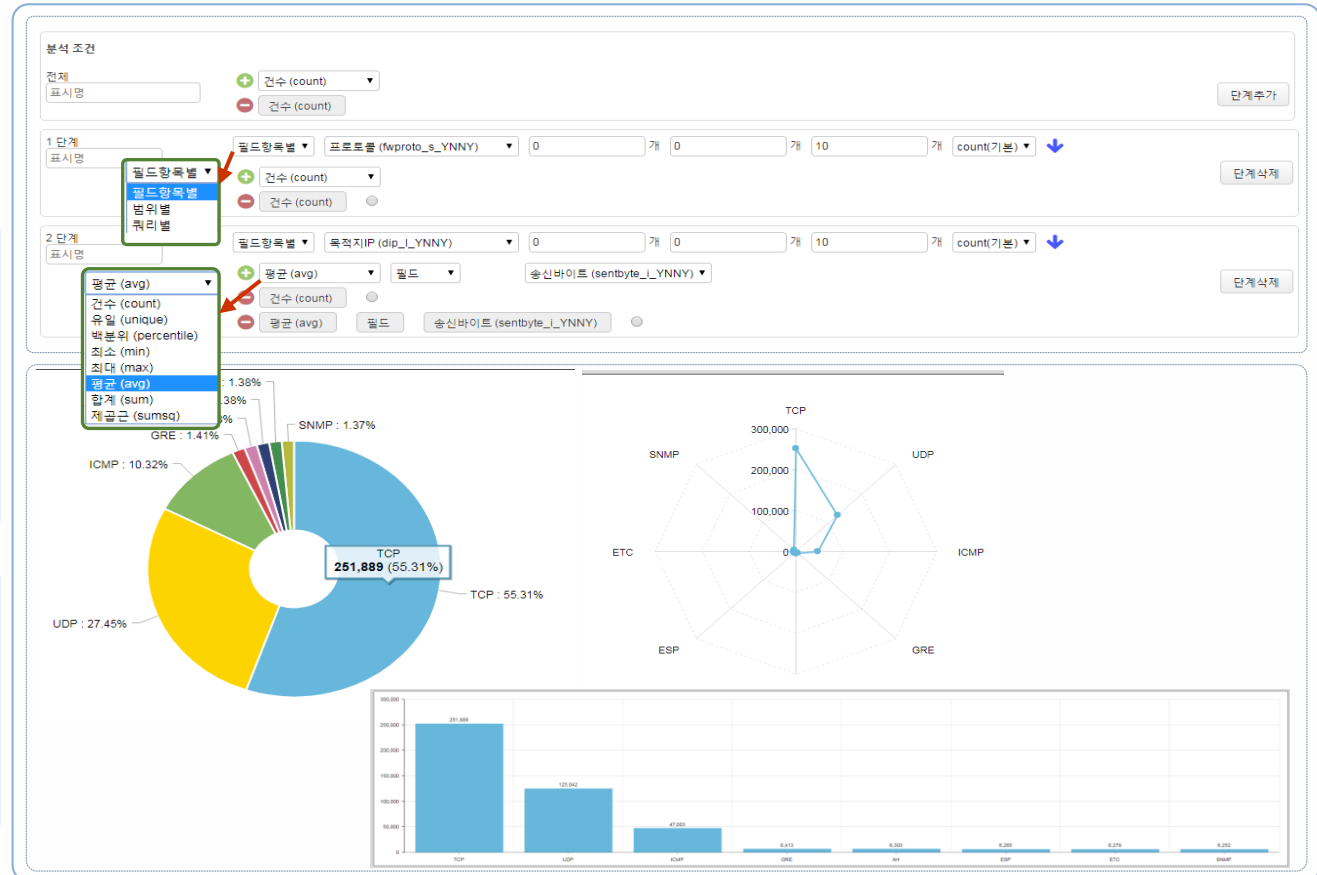
실시간 분석

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), 제공근(sumsq)

2) 다양한 분석 차트 제공.

- 파이(PIE)차트
- 바(BAR)차트
- 레이더(RADAR) 차트
- 스택바(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.

어플리케이션 선택

어플리케이션 유형 선택 : 단일 어플리케이션 다중 어플리케이션 전체 어플리케이션 어플리케이션 그룹 선택 : 전체

어플리케이션	사용자ID (userid_s_YYYY)	사용자명 (username_s_YYYY)	사용자IP (userid_ip_YYYY)	성별 (sex_s_YYYY)	디바이스명 (device_s_YYYY)	로그ID (logid_s_YYYY)	타입 (type_s_YYYY)	레벨 (level_s_YYYY)	출발지IP (src_ip_YYYY)	출발지Port (src_port_YYYY)	목적지IP (dst_ip_YYYY)	목적지Port (dst_port_YYYY)	세션ID (sessid_s_YYYY)	(teststatu)
c (방화벽로그)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
e (사용자접속)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
f (카드서비스)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

어플리케이션 그룹	어플리케이션	인덱스여부	선택
security	c (방화벽로그)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
access	e (사용자접속)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
application	h (CAR(VDB))	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
test	b (테스트용 데이터)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
test	g (샘플어플)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
transaction	a (카드 거래 내역)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
transaction	f (카드서비스)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

검색 결과수 : 174 건 검색 시간 : 0.011 초

번호	방화벽로그	시간	사용자ID	디바이스명	로그ID	타입	레벨	출발지IP	출발지Port	목적지IP	목적지Port	세션ID	상태	프로토콜	송신사이트	수신사이트
번호	사용자접속	시간	사용자ID	사용자명	고객 이력일	사용자IP	성별	진출번호	진출타입	지역사드	입속타입	접속코드번호	접속결과			
번호	카드서비스	시간	사용자ID	사용자명	사용자IP	성별	주요유용번호	카드타입	카드번호	카드종류	카드타입	승수	결판일			
1	카드서비스	Jun-21-2017 20:07:54.372	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	소필	14200	2	1			
2	카드서비스	Jun-21-2017 20:00:30.371	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	기타	7000	2	1			
3	카드서비스	Jun-21-2017 19:13:29.459	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	노스텍	3800	1	1			
4	방화벽로그	2017-06-21 19:12:14	E1228583	GH9080000000009	000000972	traffic	low	202.6.87.239	52636	169.140.156.220	9090	Org0u296-0f1-078...	allow	ETC	5300	76201
5	카드서비스	Jun-21-2017 19:01:36.105	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	자동차	13000	3	1			
6	카드서비스	Jun-21-2017 19:01:15.011	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	소필	18500	2	1			
7	방화벽로그	2017-06-21 18:57:28	E1228583	LR3000000000001	000000010	traffic	low	91.121.247.46	56816	103.24.9.201	22	Tsm8t948-63y1-9m...	allow	UDP	586	6578
8	방화벽로그	2017-06-21 18:56:16	E1228583	HJ5000000000001	000000007	traffic	low	203.25.138.22	13503	123.111.132.228	80	3rv8y63-85d0-3a4...	allow	TCP	3966	2506
9	카드서비스	Jun-21-2017 18:41:19.361	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	식물	19100	3	1			
10	카드서비스	Jun-21-2017 18:39:37.393	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	음악	3700	2	2			
11	방화벽로그	2017-06-21 18:37:52	E1228583	MK4000000000001	000000041	traffic	low	203.15.22.192	12789	123.214.69.204	8080	Op6id539-49s1-8q4...	accept	TCP	482	689
12	카드서비스	Jun-21-2017 18:19:10.710	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	소필	19200	3	5			
13	카드서비스	Jun-21-2017 18:00:34.038	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	기타	8400	3	1			
14	사용자접속	20170621 18:00:30	E1228583	원포민	Pedof@babodream...	168.188.172.121	여	010-8500-9013	서울시	browser_chrome	logged out	226	VALID			
15	카드서비스	Jun-21-2017 17:31:07.377	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	기타	8800	4	1			
16	카드서비스	Jun-21-2017 17:15:12.259	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	사무	14300	3	1			
17	방화벽로그	2017-06-21 17:14:15	E1228583	HF2000000000009	000000002	traffic	medium	116.197.191.177	46632	150.242.146.122	4280	1tqc6167-1911-3c3...	allow	TCP	38259	2457
18	카드서비스	Jun-21-2017 17:13:14.731	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	소필	13700	2	1			
19	방화벽로그	2017-06-21 17:10:08	E1228583	HF8000000000004	000000005	traffic	low	202.77.159.153	16147	103.7.33.106	2820	5sv3g67d-85o1-2c...	allow	TCP	2827	1628
20	사용자접속	20170621 17:09:00	E1228583	원포민	168.188.172.121	여	93106-2059912	VISA	7639-0027-0462-27...	iphone_app	logged out	209	VALID			

총 page 9

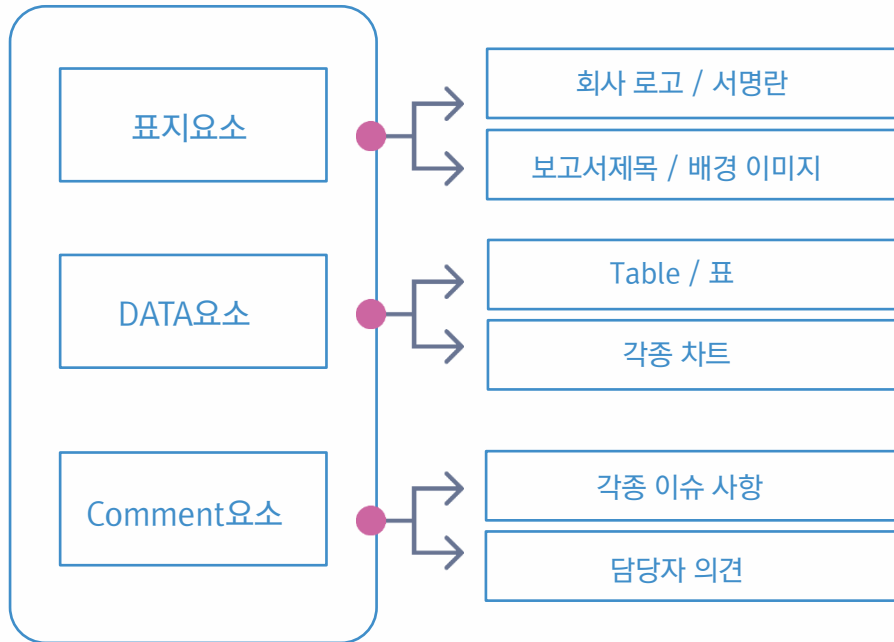
07. 리포팅 기능

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



- 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 사용자에게 대한 권한을 차등 부여하여 관리할 수 있으며 이용 내역에 대한 내용을 감사할 수 있도록 제공합니다

권한관리 기능

메뉴 사용자 권한

타입 전체 이름 아이디 부서명 조회

이름	ID	IP	전화번호	사용자 유형	부서	E-메일	생성/변경시간	메뉴권한추가
테스트1	test1	192.168.100.15 ~ 4.4.4.4 ~ 192.168.100.77 ~	02-1234-5678	Service User	테스트부	test1@blas.com	2014-09-02 13:...	
홍길동	hong	0.0.0.0 ~ 255.255.255.255	02-111-2222	관리자	홍길동	hong@blas.com	2014-08-05 10:21:45.0	
service	service	192.168.100.77 ~						
test	test	1.1.1.1 ~						
이정용	happy2870	192.168.100.77 ~	010-111-2222	일반사용자	이정용	happy2870@blas.com	2014-08-05 10:23:49.0	
bb	bb	1.1.1.1 ~						
이정용	sec008	192.168.100.77 ~	010-111-2222	관리자	이정용	sec008@blas.com	2014-08-05 10:36:58.0	

권한/정보 등록정보

사용자 메뉴권한

메뉴권한 추가

사용자 ID : hong 홍길동 메뉴순서변경 사용자 권한 추가

한글명	컨텐츠 경로	변경시간	수정/등록자
MENU			
대위보드		2014-08-05 10:21:45.0	hong
○ 모니터링	./page/rule_monitor/RULE_MONITOR.html	2014-08-05 10:24:12.0	hong
○ 수집현황	./page/c_framework/C_FRAMEWORK_COLLECTION.html	2014-08-05 10:25:36.0	hong
서비스		2014-08-05 10:28:01.0	hong
실시간서비스		2014-08-05 10:28:17.0	hong
○ 단위검색 및 분석	./servicePages/realtime/REALTIME_UNIT_SERVICE.html	2014-08-05 10:23:49.0	hong
○ 연관검색 및 분석	./servicePages/realtime/REALTIME_RELATION_SERVICE.html	2014-08-05 10:30:57.0	hong
사용자관리		2014-08-05 10:36:41.0	hong
○ 사용자정보	./page/user/USER.html	2014-08-05 10:36:58.0	hong
○ 게시판	./page/board/BOARDS.html	2014-09-12 10:17:32.0	hong

메뉴권한 추가

메뉴 권한 선택

한글명	비고
MENU	전
대위보드	전
○ 실시간위탁현황	<input type="checkbox"/>
○ 수집상태현황	<input type="checkbox"/>
○ 모니터링	<input checked="" type="checkbox"/>
○ 수집현황	<input checked="" type="checkbox"/>
○ 통계지도	<input type="checkbox"/>
○ 사용자정의 대위보드	<input type="checkbox"/>
서비스	전
보고서	<input type="checkbox"/>
사용자관리	전
설정	<input type="checkbox"/>
액세스관리	<input type="checkbox"/>
게시판	전

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

어플리케이션 선택

유형: 어플리케이션명: 선택 기간: 2015-11-08 ~ 2015-11-11
 조건등록하기 조건불러오기 조건저장

조건

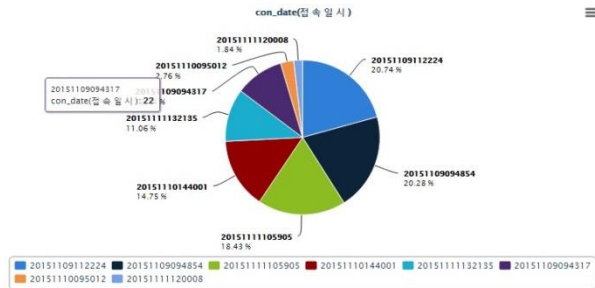
접속 ID: 접속 IP: 접속 포트: 프로세스명:
 조건등록하기

페이지당 출력수: 20 건 정렬순: 1차 정렬
 검색

idpath 필드설정: con_date (전 순 역) 분석방식: Top기과분석 주위 top 건 수: 10
 분석

TIOR로그 검색결과 * TIOR로그 검색결과 * TIOR로그 분석결과 * TIOR로그 검색결과 * TIOR로그 분석결과 *
 총 결과수: 217 소요 시간: 0.127 초
 reset column

필드정보	count
con_date(접속 일시) : 20151109112224	45
con_date(접속 일시) : 20151109094854	44
con_date(접속 일시) : 20151111105905	40
con_date(접속 일시) : 20151110144001	32
con_date(접속 일시) : 20151111132135	24
con_date(접속 일시) : 20151109094317	22
con_date(접속 일시) : 20151110095012	6
con_date(접속 일시) : 2015111120008	4



16	2015-11-09 09:49:04	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
17	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
18	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
19	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
20	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816

조건등록하기
 검색
 분석
 총 결과수: 217 소요 시간: 0.016 초 역설다운

접속 TTY	주위 TTY	command
pts/0	pts/1	ll
pts/0	pts/1	cd mysql/
pts/0	pts/1	ll
pts/0	pts/1	vi my.cnf
pts/0	pts/1	cd
pts/0	pts/1	cd scripts
pts/0	pts/1	ll
pts/0	pts/1	cd
pts/0	pts/1	ll
pts/0	pts/1	cd patch_make/
pts/0	pts/1	ll
pts/0	pts/1	vi makesh
pts/3	pts/5	ll
pts/3	pts/5	man se
pts/3	pts/5	man sed
pts/3	pts/5	load minimal amounts of data from the input files and flush the output buffers mo...
pts/3	pts/5	output version information and exit
pts/3	pts/5	input is read.
pts/3	pts/5	GNU sed home page: <http://www.gnu.org/software/sed/>. General help using GN...
pts/3	pts/5	field

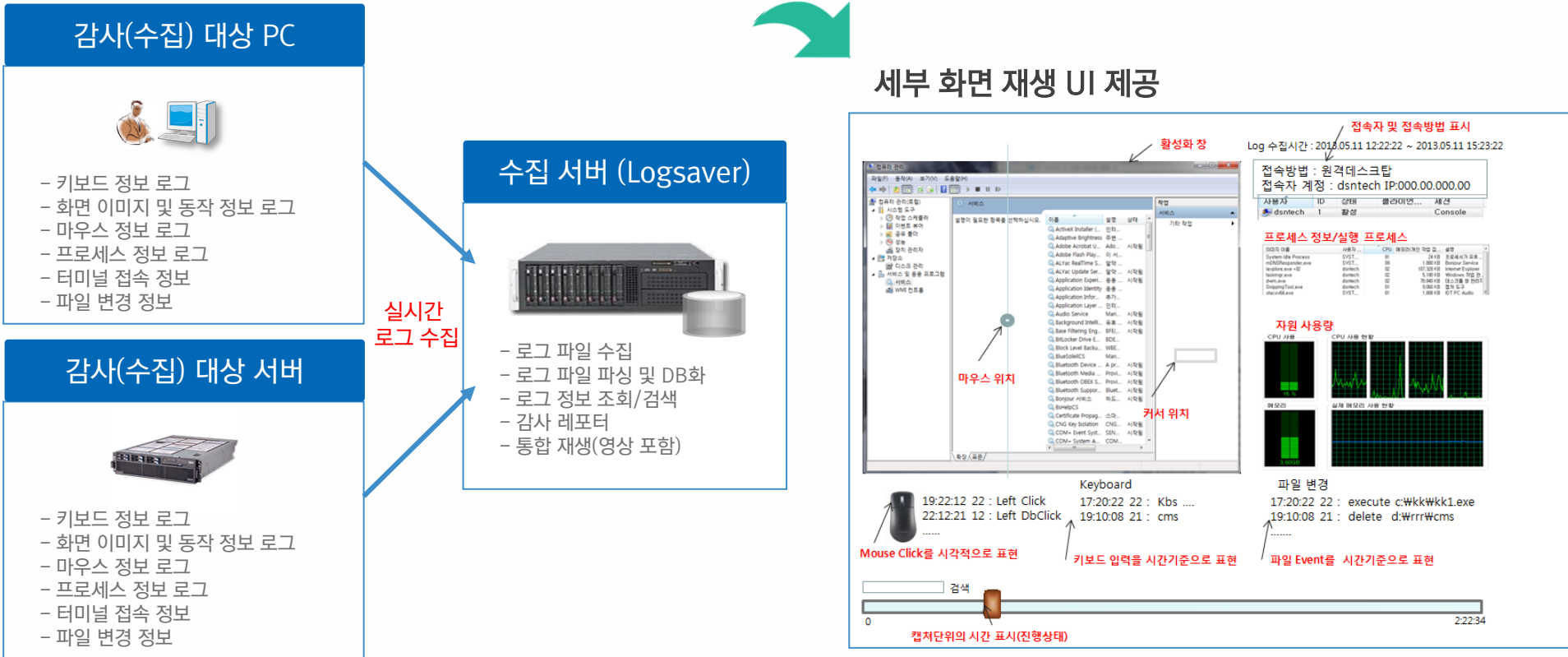
리포트

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



10. 사용자 정의 대시보드

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

사용자 정의 대시보드

The dashboard displays a top navigation bar with categories: 노드 현황, 데이터베이스, 분산 코디네이터, NoSQL, 수집 컨트롤러(FAC), 웹 서버, 코어 프레임워크, 검색 엔진, and 관리 프로세스. Below this, there are circular status indicators for each category, with 'LOAD NoSQL 서버' highlighted in orange. A detailed view of the 'freeasia.bossoftware.com 리소스 상세' (Resource Details) is shown, including sections for '프로세스 상세' (Process Details) and '리소스 상세' (Resource Details) with various charts and data points.

This section shows a '사용자정의 대시보드' (Custom Dashboard) with several components:

- 이벤트 발생 현황** (Event Occurrence Status): A summary of event counts (325, 1095, 0) with filters for severity and time range.
- 서비스별 실시간 그래프** (Real-time Graph by Service): A line chart showing the number of requests per second for various services like '소셜', '교육', '회원', etc., over time.
- 서비스별 상세 로그** (Detailed Log by Service): A table listing service details such as ID, time, user, status, and IP address.

번호	시간	사용자ID	사용자명	사용자IP	성별	주민등록번호	카드타입	카드번호	서비스분류	카드사용액	수수료	할인율
1	Aug-16-2017 18:21:11	E097260	최노서	120.143.208.12	여	530128-2714752	BC	3375-0053-0115-7890	여행	18600	1	2
2	Aug-16-2017 18:21:11	E142643	최두우	103.8.230.104	남	770215-1063832	VISA	6321-0091-0609-7415	교육	17200	5	1
3	Aug-16-2017 18:21:11	E142797	최진윤	119.30.151.115	남	741230-1395868	BC	4250-0099-0129-9875	가구	47100	2	1
4	Aug-16-2017 18:21:11	E0324352	최정하	115.32.100.248	남	470813-1403813	BC	8623-0035-0992-6432	식물	16900	1	1
5	Aug-16-2017 18:21:11	E018325	최희라	203.128.201.11	남	870216-1469889	BC	8575-0040-0136-9102	소금	13800	3	1
6	Aug-16-2017 18:21:11	E1341099	최수연	180.182.228.94	여	890817-2166014	Master	4208-0022-0026-5932	아파트oyer	19600	2	1
7	Aug-16-2017 18:21:11	E0505842	최정우	103.247.222.243	여	480525-2611953	Master	5966-0033-0183-2408	한글타	13300	3	4
8	Aug-16-2017 18:21:11	E1218760	최복순	175.41.3.106	남	840910-1229911	Amex	7481-0079-0834-9259	도서	14100	2	2
9	Aug-16-2017 18:21:11	E0964828	최보은	183.91.193.102	남	620212-1817097	Master	4773-0019-0797-4411	생활	47300	3	1
10	Aug-16-2017 18:21:11	E0983317	최신영	203.84.246.225	여	830529-2757377	VISA	5439-0040-0094-2523	생활	28500	5	3
11	Aug-16-2017 18:21:11	E0944306	최은호	122.49.99.241	여	72909-2019690	BC	2614-0089-0862-4290	스포츠	31300	2	1
12	Aug-16-2017 18:21:11	E0817270	최정호	112.137.182.219	남	960310-1444334	BC	5682-0001-0956-4945	소금	15800	4	2
13	Aug-16-2017 18:21:11	E0218565	최지현	27.118.160.242	여	670106-2119655	VISA	6221-0031-0038-2565	한글타	14100	1	2
14	Aug-16-2017 18:21:11	E0716393	최근다	103.7.244.224	남	469092-1487079	VISA	1122-0031-0428-7635	소금	19000	2	1
15	Aug-16-2017 18:21:11	E0341559	최은진	125.208.111.117	여	650411-2128375	BC	8142-0089-0180-9836	자동차	15300	4	2
16	Aug-16-2017 18:21:11	E0854794	최하나	203.207.18.45	여	611103-2025684	Master	8354-0062-0280-5749	주방	12900	4	1
17	Aug-16-2017 18:21:11	E0992718	최승용	103.246.236.60	여	870202-2008268	JCB	8579-0025-0242-1548	타물장	19100	5	1
18	Aug-16-2017 18:21:10	E0683855	최용라	221.151.53.135	여	760110-2444898	Master	1509-0057-0745-8785	뷰티	13500	5	1
19	Aug-16-2017 18:21:10	E0514096	최병환	203.170.108.75	여	660727-2755034	VISA	2656-0029-0461-6025	타물장	14300	3	1

01. 전체 구축 실적

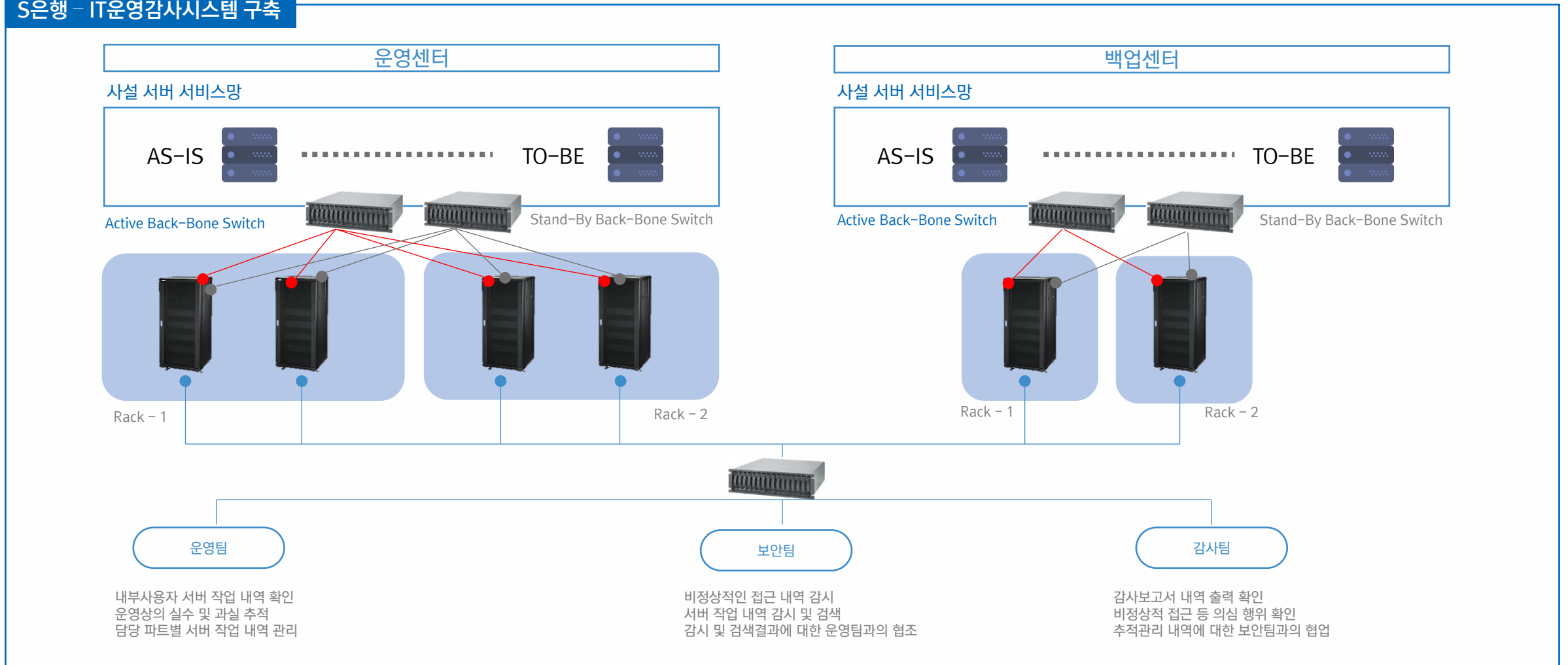
제안사가 제안하는 제품은 은행, 증권, 카드, 보험 등의 금융권을 비롯하여, 공공기관, 일반기업체 등 다양한 분야에서 고객을 확보하고 있는 우수한 제품으로서, 국내 시장 점유율 1위 제품입니다.

레퍼런스(요약)	공공	은행/금융	일반 기업체	국방	해외
	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • KT본부 • KT IT 본부(목동) • KNET(전자문서보관소) • KT(정보보호본부) • 삼성전자(15곳) • 삼성종합기술원 • SK OCMP • SK C&C • 나눔로또위원회 • 메가스터디 • 노틸러스효성 • 롯데면세점 • NC소프트 • 쇼피엔티 외 다수 <div data-bbox="1174 872 1538 932" style="background-color: #0056b3; color: white; text-align: center; padding: 5px;">대학교 및 병원</div> <ul style="list-style-type: none"> • 건국대학교 • 중앙대학교 • 한성대학교 • 서울교육대학교 • 서울여자대학교 • 삼육대학교 • 동남권 원자력 의학원 • 대구 파티마 병원 • 구미 차 병원 • 강동경희대학교 병원 외 • 다수 	<ul style="list-style-type: none"> • 국방재정 • 국방인사 • 국방인증 • 국군수송사령부 • 합동참모본부 • 방위사업청 • 육군본부 • 해군본부 • 공군본부 • 국방 CPAS • 합참KJCCS(지휘통제체계) • 국방동원 • 국방과학연구소 • 국방기술품질원 • 국군통신사령부 • 국군기무사령부 • 각급 부대 별 납품 외 다수 	<ul style="list-style-type: none"> • 미국 : Princeton University • 일본 : 일본과학기술청, NHK, 삼성JAPAN, 일본 Dreamware, Mitsubishi Research Institute • 독일 : BW Bank, Bohn University • 말레이시아 : Alliance System • 싱가포르 : 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



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 활용 하기 위한 데이터 제공 및 타 업무를 지원합니다

S증권 - 통합로그관리시스템 구축

번호	유형	로그번호	로그내용	로그일시	로그대상	SERVER_IP	USER_ID	SERVER_IP	USER_ID	접속시간	접속유형	종료시간	종료유형	종료유형	종료유형
1		2019-01-24 09:00:00	로그	2019-01-24 09:00:00	로그	192.168.1.100	admin	192.168.1.100	admin	2019-01-24 09:00:00	로그	2019-01-24 09:00:00	로그	로그	로그
2		2019-01-24 09:00:00	로그	2019-01-24 09:00:00	로그	192.168.1.100	admin	192.168.1.100	admin	2019-01-24 09:00:00	로그	2019-01-24 09:00:00	로그	로그	로그

〈MCA 거래로그 검색〉

날짜	구분	구분명	구분코드	구분내용	구분수	구분비율	구분비율	구분비율	구분비율	구분비율	구분비율	구분비율	구분비율	구분비율	구분비율	구분비율
2019-01-24	로그	로그	로그	로그	100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

〈서버별 로그 처리 일별 통계〉

번호	유형	로그번호	로그내용	로그일시	로그대상	SERVER_IP	USER_ID	SERVER_IP	USER_ID	접속시간	접속유형	종료시간	종료유형	종료유형	종료유형
1		2019-01-24 09:00:00	로그	2019-01-24 09:00:00	로그	192.168.1.100	admin	192.168.1.100	admin	2019-01-24 09:00:00	로그	2019-01-24 09:00:00	로그	로그	로그

〈MCA 개발로그 조회 화면 - 개발자 전용〉

시간	수행 시간 범위	처리 건수	평균 수행 시간	최대 수행 시간	수행시간 분포	평균분포	최대분포
2019-01-24 09:00	0.0000	1	0.0000	0.0000	0.0000	0.0000	0.0000
2019-01-24 09:05	0.0000	1	0.0000	0.0000	0.0000	0.0000	0.0000

〈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



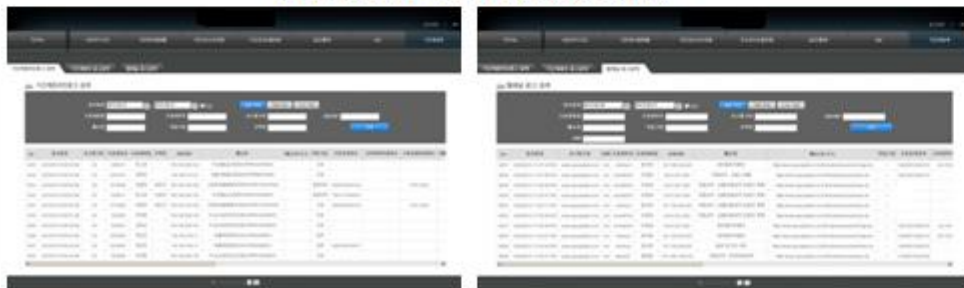
02. 주요사업 실적

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 통합대시보드 화면〉



Log saver[®]



감사합니다



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