제4차 산업혁명 시대

빅데이터 전문 기업

데이터인사이트

CONTENTS

I 회사 소개

– 데이터 인사이트

01 일반현황〉 개요

데이터인사이트는 2017년 설립이래 빅데이터 기반 기술 개발에 집중하여 Big Data 분석을 위한 No-SQL 기반 분석엔진 기술을 바탕으로 4차 산업 혁명에 발 맞추어 빅데이터 플랫폼 및 관련 솔루션을 개발, 보급하고 있습니다.

일반 현황 및 주요 연혁

회 사 명	(주)데이터인사이트	대 표 자	성 치 은
설 립 년 도	2017.12	자 본 금	
사 업 분 야	빅데이터 플랫폼 및 솔루션 개발 및 공급		
주 소	경기도 안양시 동안구 벌말로 66 하이필드 A동 F301, 302호		
해당부문 사업기간	2017.12~현재(2년 4개월)		

2017

- ㈜데이터인사이트 설립

2017

- 빅데이터 솔루션 개발

2017

- 통합 로그 분석 솔루션 출시
  : Log Insight

2019- 현재

- 한국정보보안기술원 CC 인증 획득
  - 로그인사이트
  - 인증번호 ISIS-0626-2015
- 한국정보통신 기술 협회 GS 인증
  - 인증번호 : ISIS-0626-2015
- 특허획득
  - 보안이벤트 분석 방법 및 분석 시스템 외 총 3건

02 일반현황〉 인증 내역

데이터인사이트는 빅데이터 기반 기술 핵심으로 Big Data 분석을 위한 No-SQL 기반 분석엔진 기술을 발전 시켜 나가고 있으며 이를 기반으로 보안적합성 인증(CC 인증), GS인증 및 각종 특허를 획득 하였습니다.

굿소프트 (GS) 인증서

획득시기 | 2015년 1월

인증기관 | 정보통신기술협회

기업 부설 연구소 인정서

획득시기 | 2017년 12월

인증기관 | 한국산업기술진흥협회

기술 특허증

획득시기 | 2016년 9월

인증기관 | 특허청

빅 데이터 분석 성능 인증을 통한 대용량 데이터 처리

한국정보통신기술협회

공인기관 기술 성능

TTA 성능검증 요약

- 데이터수집.인덱싱.분석 전체 성능: 200,000 EPS
- 원본데이터 검색 성능: 7TB 에 대해서 3초 이내 검색

– 국내 최고의 데이터처리 성능 및 검색 성능

04 데이터인사이트 빅 데이터 기술 확보

목표

- 데이터 실무인력 및 현안 해결 중심의 데이터 컨설턴트 양성
- 빅데이터 전문 기술력 확보를 위한 부설 연구소 운영

빅데이터 스터디

- 재직자 대상 데이터 인력 양성
- 실무인력 대상 빅데이터 교육 및 컨설팅 재 교육

빅데이터 기획/기술/분석 + 융합 전문가 육성

데이터 전문가 양성

- 데이터 전문가 및 데이터 컨설팅 교육 지속 실시
- 빅데이터 공인 자격증 취득 지원

빅데이터 분석/개발/설계

분석	ADP Advanced Data Analytics Professional 국·가·공·인	국가공인 데이터 분석 전문가 (공인자격 제2015-12호) ADP, Advanced Data Analytics Professional
개발	SQL Developer SQL 국·가·공·인	국가공인 SQL 전문가 (공인자격 제 2013-02호) SQLP, SQL Professional
설계	DAP Data Architecture Professional 국·가·공·인	국가공인 DA 전문가 (공인자격 제2015-11호) DAP, Data Architecture Professional

데이터분야 연구센터 운영

- 사내 데이터 분야 부설 연구소 전문 운영

빅 데이터 전문화를 위한 전문 부설 연구소 운영 중

AI기업 및 보안기업 협업으로 4차 산업 경쟁력확보

빅데이터 분석 수요가 있는 보안기업 대상 빅데이터 분석 솔루션 매칭 지원

·보안기업 빅데이터 활용 수요조사
·보안기업 전용 솔루션 기술 협업 지원
·빅데이터 분석 솔루션 매칭 협업 추진

아이디어, 협업 비즈모델 창출을 위한 협업 테스트 모델 제공

·타 솔루션 업체와 협업 모델 개발
·보안 솔루션 업체와 협업 신규 비즈 창출

데이터 컨설팅 및 신규아케택쳐 설계등 지속적인 기술 경쟁력 확보

·빅데이터 컨설팅 실시
·성능 향상 기술 개발
·빅데이터 분석 기법 지숫적인 연구개발 투자 및 인력 충원

아이디어 또는 웹(앱) 제품 및 서비스 개발 아이템을 발굴

II 로그관리 법률 규정

01 로그관리 주요 국가 법률 규정

계속되는 개인정보 유출.. 법조계 "법리적 처벌 강화 필요"

이유민 기자 yumin@ekn.kr 2017.10.10 15:19:20

트윗 페이스북

[에너지경제신문 이유민 기자] 최근 여기어때, 남양유업, 디비피아와 등에 이어 한국수력원자력 등 공공기관 직원들의 개인정보 유출 사고가 잇따르고 있는 가운데 법조계에서는 개인정보 유출에 관련된 법령정비의 필요성을 제기하고 있다.

10일 관련 업계에 따르면 지난 7월 유진그룹의 금융계열사 유진투자선물 회원 30만명의 개인 정보가 유출됐고, 같은 해커의 소행으로 남양유업의 홈페이지 내 회원 정보를 포함해 약 3000만건에 달하는 개인정보가 유출된 것으로 확인됐다.

또한 이찬열 국민의당 의원이 한수원으로부터 받은 자료에 따르면, 한수원 한울원자력

대기업 '중소기업 기술 유출'만 해도 처벌…공정위

김원진 기자 onejin@kyunghyang.com

9

입력 : 2017.09.08 13:2

공정거래위원회가 대기업의 중소기업 기술유용을 조사하는 조직을 신설해 내년 기계·자동차 분야를 시작으로 대기업의 기술유용을 집중 감시한다. 기술자료 유용 사실이 입증되지 않더라도 유출만으로 처벌할 수 있는 근거도 마련된다.

더불어민주당과 공정위는 8일 당정 협의를 열고 '대·중소기업 간 상생협력을 위한 기술 유용행위 근절 대책'을 추진하기로 합의했다. 당정은 전문적인 법 집행 체계를 구축하기 위해 올해 말 공정위에 기술유용 사건 전담 조직을 신설하고 기술심사자문위원회도 설치하기로 했다.

공정위는 전담 조직을 신설한 뒤 내년부터 매년 집중 감시 업종을 선정하고 실태조사를 벌인다. 내년 첫 번째 집중 감시 대상에는 직권조사 한시적 면제 기업이 많아 규제의 사각지대로 꼽히는 기계·자동차 분야가 선정됐다. 공정위는 이들 업종을 상대로 서면 실태조사를 벌인 뒤 혐의가 발견되는 기업은 직권조사를 하기로 했다.

공정위는 기술유용을 방지하기 위해 관련 제도도 대폭 손본다. 공정위는 기술자료의 제3자 유출만으로 처벌할 수 있는 근거를 마련할 예정이다. 지금까지 대기업의 기술 유출 행위가 확인돼도 기술유용을 한 증거가 나오지 않으면 처벌이 불가능했다.

기술유용에 무관용 원칙을 적용해 과징금 산정을 위한 매출액 산정이 어려워도 정액 과징금을 부과

주요 법규 및 지침	주요 내용
개인정보보호법 시행령 제 30조 1항 4호	개인정보 침해사고에 대응하기 위해 **접속 기록의 보관 및 위•변조 방지**
전자금융거래법 시행령	해당 전자금융거래와 관련 전자적 접속 기록에 대해 5년간 보존
금융회사의 정보통신수단 등 전산장비 이용관련 내부통제 모법규준 (금융감독원, 2011년 4월)	업무용 정보통신수단 **로그기록에 대해 3년 이상 보관**
개인정보의 기술적 관리적 보호조치 기준(방송통신위원회, 2001년 5월)	개인정보처리시스템 접속기록을 최소 **6개월 이상 보관, 관리, 위•변조 및 도난 분실 방지**
정보통신기반보호법 제 13조 1항	침해사고의 통지, **원본 로그에 대한 보관 및 사후 보고**
정보통신서비스 정보보호 지침 제 3조 5항	복구 대책, 정보보호 책임자는 **주기적으로 접속 기록을 분석해 침해사고 예방**
정보통신망 이용촉진 및 정보보호에 관한 법률 제 48조 4항	침해사고의 원인 분석 등 집적정보통신시설 사업자에게 **로그 관리 등 침해사고 관련자료 제출을 요구** 할 수 있도록 침해사고 원인 분석이 가능하도록 함

02 국가정보원 [정보보안 관리실태 점검] 내용

정보보안 관리실태 점검		정보보호대책			
점검 분야	점검 지표 항목	방향			점검 내용 및 항목
		관리	조직	기술	
정보시스템 보안	1. 정보보호시스템 보안관리	V			[관리1]정보보호정책/지침수립 - (지침) 제8장 IT 운영보안
				V	[기술1]개인정보 DB 암호화
				V	[기술11]정보보호/개인정보 관리시스템
	2. 무선랜 보안	V			[관리1]정보보호정책/지침수립 - (지침) 제8장 IT 운영보안 - (절차) 제2장 보안성검토 절차
	3. 네트워크 보안	V			[관리1]정보보호정책/지침수립- (지침) 제8장 IT 운영보안
				V	[기술3]접근통제 시스템 구축
				V	[기술6]네트워크 망 분리 솔루션 구축
				V	[기술7]네트워크 구간 암호화 구축
	4. 서버 보안관리	V			[관리1]정보보호정책/지침수립 - (지침) 제8장 IT 운영보안
				V	[기술3]접근통제 시스템 구축
	5. PC 보안관리				[관리1]정보보호정책/지침수립 - (지침) 제8장 IT 운영보안
				V	[기술5]통합계정관리 시스템 구축
	6. 로그 및 백업	V			[관리1]정보보호정책/지침수립 - (지침) 제37조 정보시스템 로그관리 - (지침) 제37조 정보시스템 백업관리
				V	[기술2] 통합로그관리 솔루션 구축

III 제품 소개

– Log Insight

빅 데이터 분석 을 위한 전문 분석 엔진 보유

제품 사진	제품명	주요 기능
	LOG INSIGHT	▫ 이 기종 장비의 다양한 대용량 로그를 일원화된 인터페이스를 통해 쉽게 관리 ▫ 간편한 설정 및 연동 방식 제공으로 구축 기간 단축 ▫ 장비연동현황, 경보현황, 시그니처현황, IP현황 , 커드현황 등 다양한 정보의 대시보드 제공 ▫ 데이터 필터링과 집계 및 임계 정책의 유연한 설정으로 동적 정책결과 자동 생성
	용도	대용량 데이터 분석 전문 엔징

1 Easy

- 다양한 IT자산에 대해서 간편하게 로그의 수집/연동이 가능함
- 손쉬운 시스템 관리 및 기능 설정이 간편하게 구성됨

2 Simple

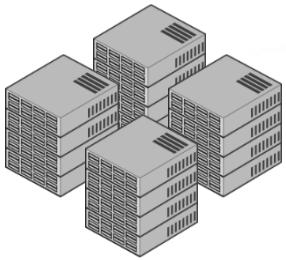
- 정책생성 시 조건 설정이 간단하게 구성되어 손쉽게 정책설정 가능
- 간편한 연동방식을 지원하여 구축 및 관리의 편리성 제공

3 Coast

- 다양한 로그포맷과 시그니처 관리로 로그의 수집과 관리의 시간 비용 절약
- 강력한 시나리오 설정을 통해 별도의 추가장비 없이 보안성 강화

Log Insight 만의 엔진 적용 기술

연동 장비



LOG

LOGInsight

- 대량의 데이터 처리
  - ❖ 데이터 수집, 정규화, 분석 저장의 일련의 단계에 최적화된 프로세스 간 내부 통신을 유기적으로 배치하는 기술 적용

- 프로세스 Scale – UP
  - ❖ 데이터 수집 시 데이터량의 비례하여 Log Insight 프로세스의 데이터 병렬 처리 및 부하분산

DATABASE

IN-Memory 프로세스

- ➢ Log Insight 분석 프로세스
- ➢ Log Insight 정규화 프로세스

대량의 로그 데이터

Log Insight 의 로그 수집 및 데이터 처리

네트워크 장비 로그
웹로그
SNMP
보안장비 로그
서버 로그

비정형, 반정형, 정형 등 모든 로그

■ 로그관리
- ✓ 90% 이상의 압축률 및 암호화하여 보관
- ✓ 매일 장비별 로그 자동 백업 진행
- ✓ 로그파일의 위·변조를 방지하기 위해 해시 값을 따로 저장하여 무결성 보장
- ✓ 고객이 원하는 보관 일자 설정을 통하여 보관주기가 지난 로그에 대해서는 자동 삭제

LogInsight
로그 수집 방식
SYSLOG
FTP
DB2DB
AGENT

■ 로그수집
- ✓ 각 연동 장비의 정의된 로그포맷을 기준으로 정규화
- ✓ 수집된 원본로그 압축·암호화 저장
- ✓ 실시간 데이터 수신 상태 확인
- ✓ 다양한 조건 검색을 통한 로그 조회

LogInsight
통합로그관리시스템

■ 로그분석
- ✓ 기본, 상관, 종합 분석 정책을 통한 세밀한 데이터 분석 탐지
- ✓ 실시간 로그데이터 분석
- ✓ 자유로운 임계치, 집계 유형, 분석주기 설정
- ✓ 과거데이터 회귀, 추적 비교 분석

Log Insight 의 로그 수집 성능

Log Insight 엔진의 장비 로그데이터 수집 성능

- Log Insight 엔진 수집 성능은 2018.12.10 ~ 2018.12.14 기간동안 TTA(한국정보통신기술협회) 시험의뢰를 통해 엔진의 수집 성능을 검증함

TTA 시험의뢰 측정 범위

- 시험결과 1시간 약 7억3천 건의 로그데이터를 분당 평균 12,160,719건 수집->Parsing-DB적재 처리, 평균 202,679 EPS(Event Per Second) 의 성능 확인

ID	시험항목	시험목표	목표치	측정치
TC1	정책/수집 서버의 데이터 처리 성능	시험대상제품이 로그 정보를 처리하는 성능이 평균 200,000 EPS (Event Per Second) 이상인지 확인	평균 200,000 EPS 이상	평균 202,679 EPS

2018-12-11 15:50	12,254,394
2018-12-11 15:49	12,466,364
2018-12-11 15:48	13,095,362
2018-12-11 15:47	12,452,023
2018-12-11 15:46	11,701,821
2018-12-11 15:45	11,899,252

Log Insight 의 특장점

✓ 복잡한 로그의 이해를 위한 장비별 맞춤 로그필드 생성

연동 장비

보안 장비 | 네트워크 장비 | 서버 | 산업장비 | • • • • •

각 장비별 로그 필드

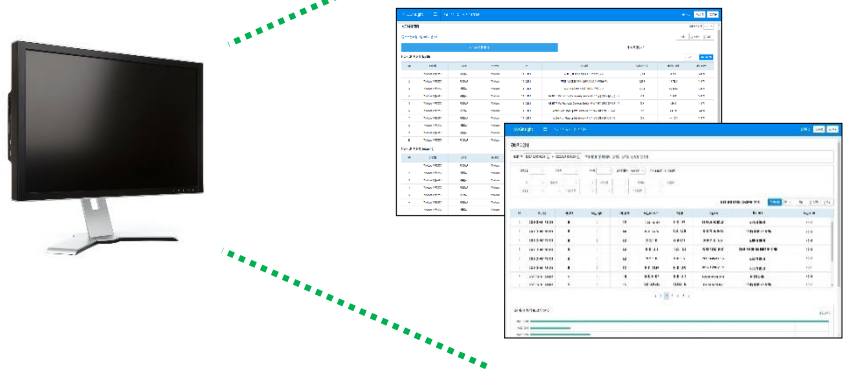
출발지IP | 목적지IP | Protocol | User | URL | • • • • •

Port | Message

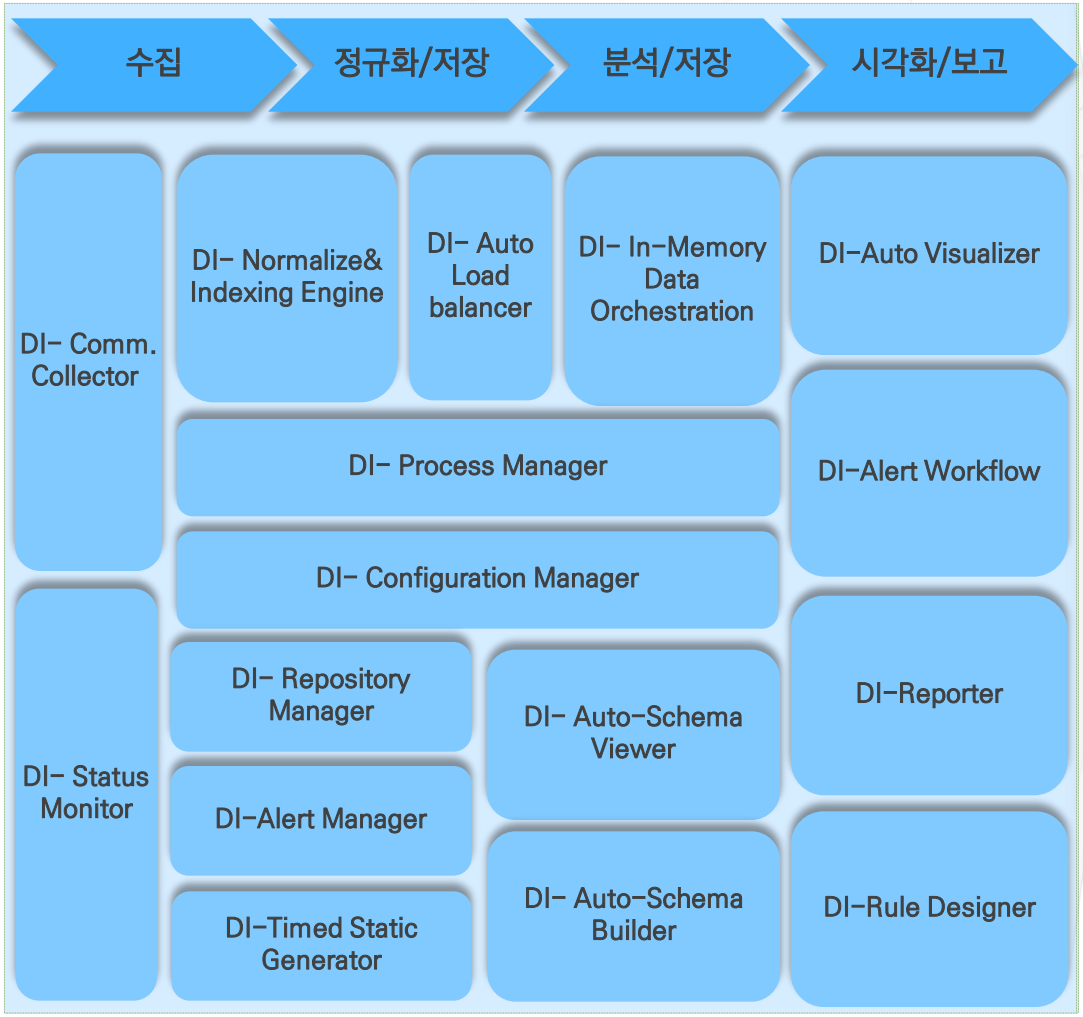
▪ 각 장비별 데이터가 저장될 DB 스키마가 고정되어 생성되지않고 장비별 로그 유형에 맞게 대응되는 스키마를 유동적으로 생성 가능

어떠한
복잡한 로그라도
사용자가 바로
이해 가능한
로그필드의 생성 가능

사용자의 로그 이해

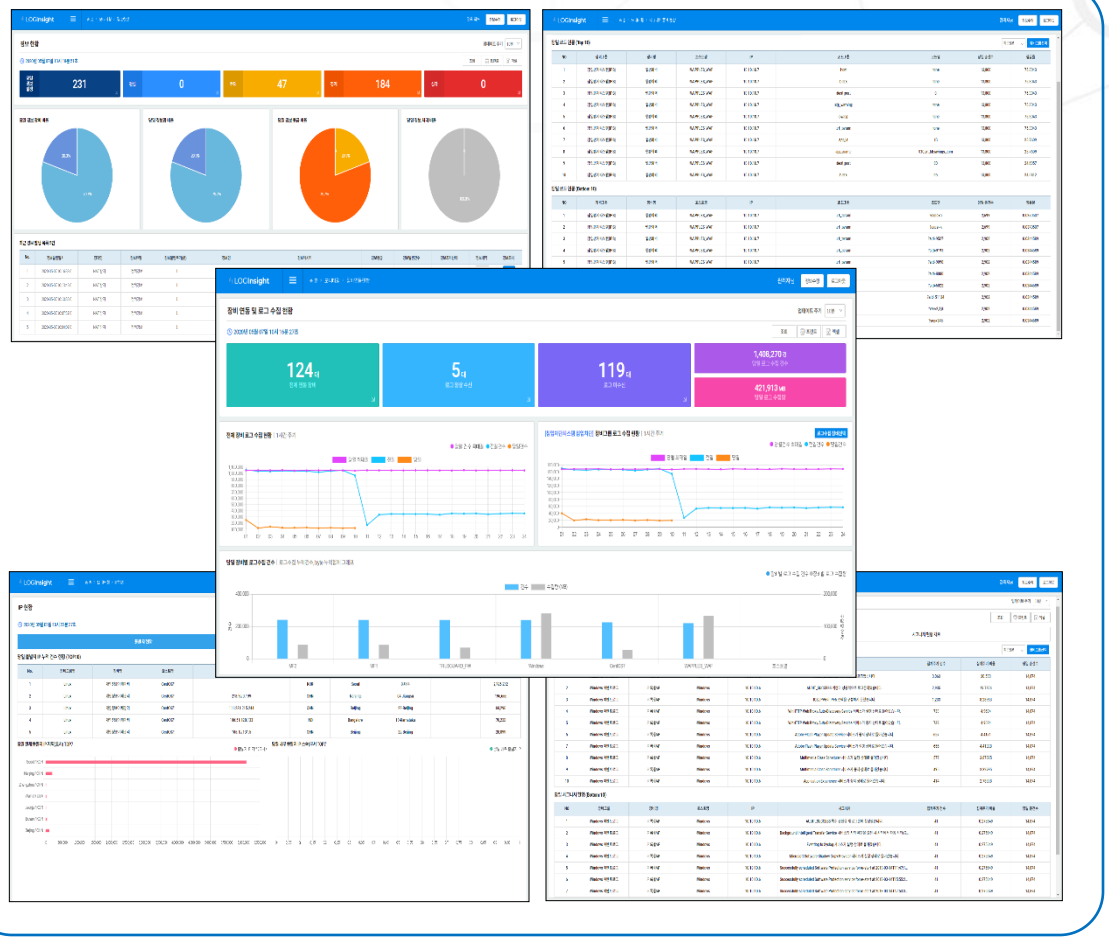


빅 데이터 활용을 위한 아키텍쳐 구성



- ✓ 데이터의 종류(질)와 생성(량)에 따른 동적 대응
- ✓ 각종 관심 데이터에 대한 동적 필터링 정책 설정
- ✓ 유동적인 스키마 생성 자동화로 RDBMS 한계를 극복
- ✓ 데이터 정규화 프로세스 자동 부하 분산 최적화
- ✓ 데이터 분석 프로세스 자동 부하 분산 최적화
- ✓ 관심 데이터 및 분석 데이터 조회 화면 자동 생성
- ✓ 각종 관심 데이터 항목에 대해 Top-N 그래프
- ✓ 특정 데이터 항목에 대한 집계 정보의 동적 생성
- ✓ 통계 정보에 대한 동적 임계치 설정 및 경보 정의
- ✓ 각종 집계 항목의 시간에 따른 변화 추이 그래프
- ✓ 특정 데이터 항목간 관계 그래프 동적 설정 및 조회
- ✓ 각종 분석 결과 내용 구성설정 및 자동 보고서 생성
- ✓ 각종 경보 이벤트 설정 및 대응에 대한 워크플로우
- ✓ 데이터 수집량의 증가에 따라 Scale-Up 자동화
- ✓ 데이터 종류나 수적 증가에 따른 Scale-Out 용이성

Log Insight의 다양한 Dashboard 제공



사용자 선택 모니터링

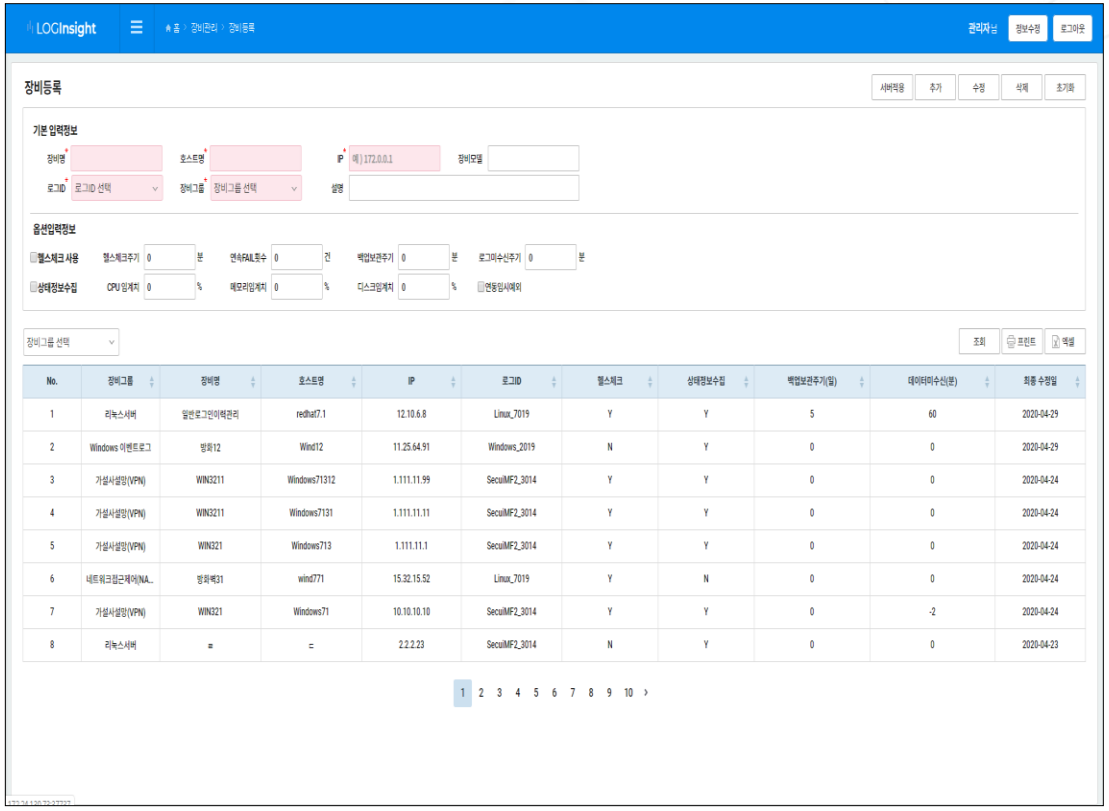
[장비연동 현황]
연동 장비의 실시간 데이터 수신 현황에 대한 정보 제공

[경보발생 현황]
경보 발생내역에 대한 현황 및 경보 발생 비율을 그래프로 제공

[IP현황]
IP데이터를 집계 후 출발지, 목적지 IP에 대해 통계하여 Top10 정보 제공

[시그니처 현황]
각 장비의 주요필드에 대한 로그를 집계하여 로그 종류별로 통계하여 Top 10 정보 제공

Log Insight의 간단한 장비 등록 제공



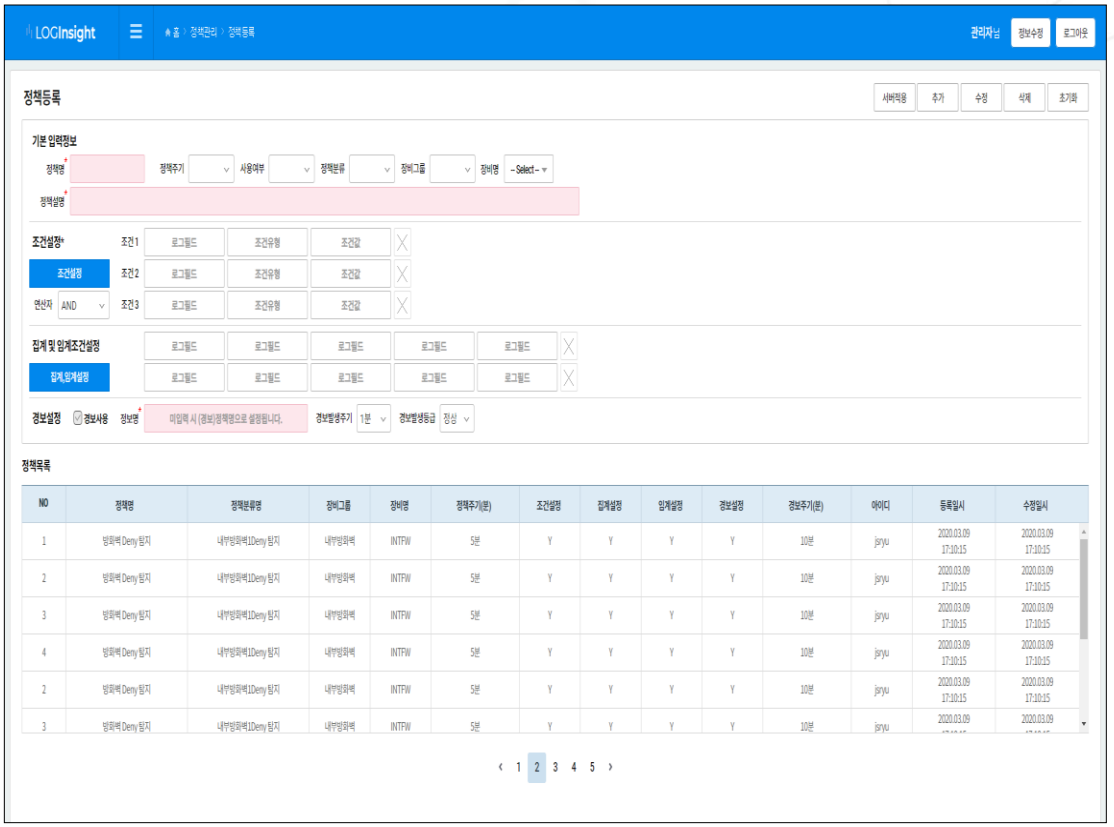
장비등록 및 장비현황 파악

[장비 등록]
필수 입력 항목만 기입하여 간단한 장비 등록부터 특정 장비의 특이사항이나 필요내용을 입력하여 구분할 수 있도록 기능 제공

[추가 옵션 설정]
헬스 체크, 상태정보수집 기능을 세분화하여 사용자가 세세한 설정이 가능하도록 제공

[등록 장비 현황]
전체 장비 및 장비 그룹별(장비군) 분류 선택으로 장비 현황을 한눈에 파악 가능토록 기능 제공

Log Insight의 간편한 정책 설정 기능 제공



간편한 정책 다중 조건 설정

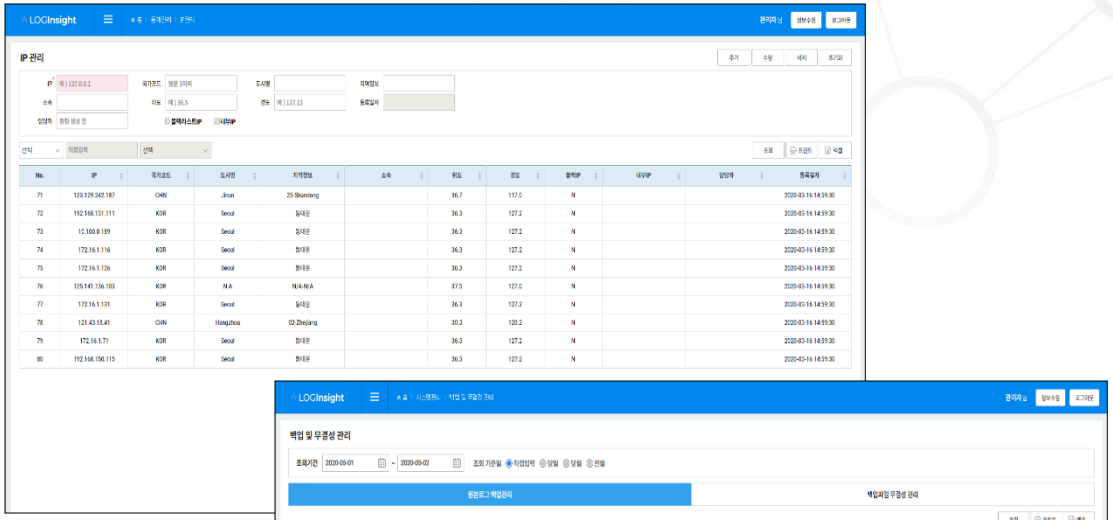
[조건설정]
단일 또는 동일 기종의 장비별 각필드에 대해 조건을 설정하여 해당 조건설정대로 데이터의 필터링을 할 수 있으며, 여러 개의 조건 설정을 통한 필터링의 최소화 가능

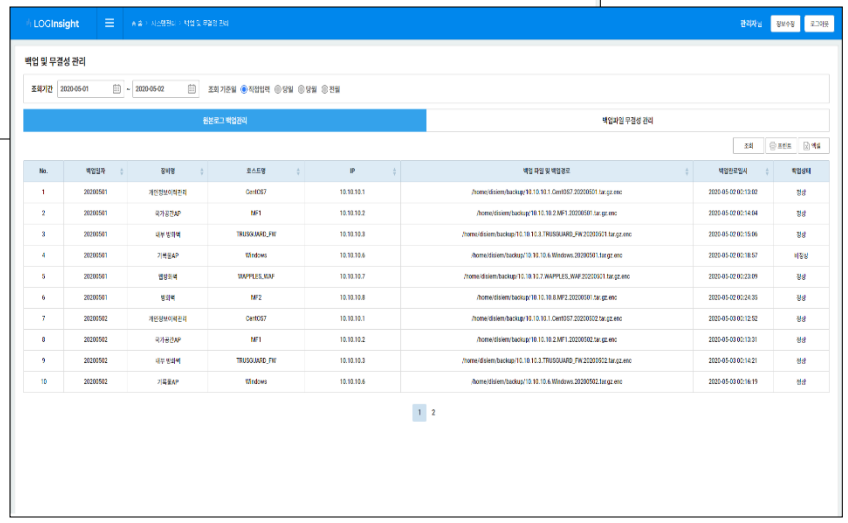
[집계 및 임계치 설정]
조건 설정 후 해당 조건 필드에 대해 임계치를 설정하여 데이터의 집계 및 발생 현황을 파악할 수 있도록 기능 제공

[경보설정]
등록된 정책에 대해 경보발생주기 및 등급을 설정하여 해당 정책 탐지 시 경보를 발생토록 기능 제공

[등록 정책 현황]
등록된 정책의 정보 및 현황을 파악 가능

Log Insight의 IP관리 및 백업 무결성 관리



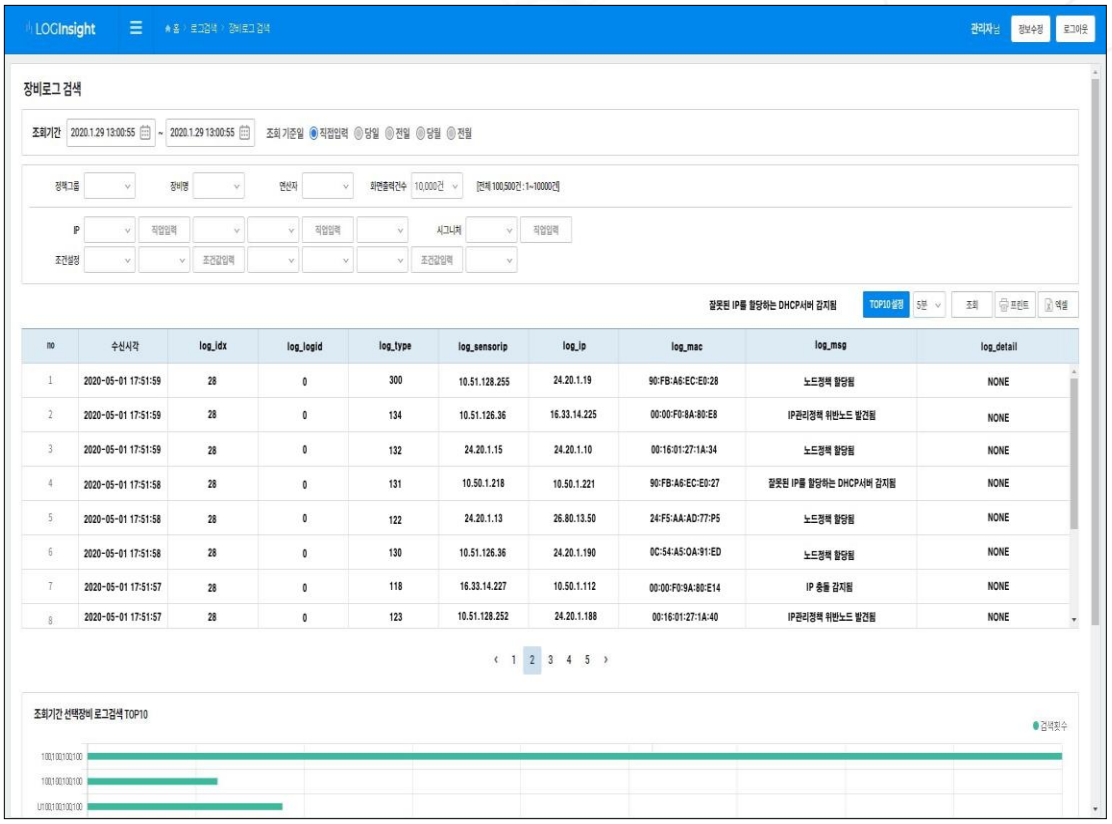


IP관리 및
원본로그 백업&무결성 관리

[IP관리]
장비에 들어오는 IP데이터를 GeoIP를 통해 매칭하여 IP의 위치를 파악 가능하며 내부, 블랙리스트IP 설정 및 직접 IP 등록하여 관리할 수 있도록 기능 제공

[백업 무결성 관리]
장비별 원본로그의 백업여부의 확인을 할 수 있으며, 해당 백업 내용에 대해 변조가 있는지 무결성 검사를 진행한 검사의 내역 확인 가능

빅데이터 활용 사용자 편의 로그 검색 기능 제공



다양한 조건 검색

[조건 검색]
IP 및 각필드에 대해 다양한 조건유형을 주어 간단한 검색부터 상세한 조건부여로 정밀한 검색 필터링이 가능하며 저장된 시그니처를 선택하여 바로 조회할 수 있도록 빠른 검색 기능 제공

[컬럼명 변경]
사용자 편의의 필드명 설정 가능
Ex)src_ip 〉 공격자IP

[로그검색 Top10]
조회할 장비의 필드를 선택하여 조회 기간 동안 해당 장비에서 발생된 로그의 Top10을 표출

항목	기능 규격
일반사항	- 한국정보통신기술협회(TTA)에서 GS 1등급 인증을 획득한 제품 - 시스템 자체보안 강화를 위해 Linux기반 OS를 사용
로그수집	- 다양한 방식의 로그수집 기능 제공 (Syslog, SNMP, FTP, SFTP, DB to DB, WMI 등) - 필요 시 Agent 방식의 로그수집 기능 제공 - 공인 시험기관에서 평가된 초당 200,000EPS 이상의 로그 처리 성능 제공 - 로그 수집 지연, 불가 시 경보 알림 기능 기본 제공 - 멀티라인 로그 수집 기능 제공
로그저장	- 수집된 원본로그의 로그 생명주기 완벽지원 - 수집된 원본로그를 매일 압축, 암호화 하여 별도 디렉토리에 백업 보관 기능 제공 (원본로그 압축률 90% 이상) -백업된 원본로그의 해쉬값을 기록하여 무결성을 검증하고, 무결설 위배 시 경보 발생 기능 제공 - 불필요한 로그는 파싱에서 제외하여 필요한 원본로그만 보관가능한 기능 지원
로그 검색	- 수집 로그의 모든 필드에 대한 조건검색, 키워드 검색 기능 제공 - 출발지IP, 목적지IP, 국가, 도시, 블랙리스트IP 등 IP 조건 구분 검색 기능 제공 -Sql 함수를 사용한 논리적 검색 기능(Equal, Not, Like, Greater, Less, IN, Except)과 Regex, 키워드 문자열 검색 등 유연한 검색 방식 제공 - 모든 이벤트의 조건검색 결과에 대해서 로그필드별로 Top-10 차트 생성 기능 제공

항목	기능 규격
로그분석	- 수집 로그의 분석을 위한 정책등록 및 정책로그검색 기능 제공 - 로그 분석은 Sql 함수를 사용한 조건설정(Equal, Not, Like, Greater, Less, IN, Except) 분석을 기본으로 분석 결과에 대해 집계설정(Sum, Count, Maximun, Minimun) 및 임계설정(No-limit, Greater, Less, Between)을 선택적 추가하여 보다 세밀한 로그분석 정책 수립 - 분 단위의 로그분석 결과 집계 기능 지원으로, 지속적인 추이 분석 가능 - 수집 로그데이터 속성별 변동량 자동분석 기법으로 이상 탐지 기능 제공 - 정책명 기반 로그 분석 결과 저장 동적 테이블 자동 생성 기능 지원 - 동일 기종의 장비를 하나의 분석 정책으로 설정하는 기능 제공
대시보드	- 당일 로그연동 현황 대시보드 제공 - 당일 경보발생 현황 대시보드 제공 - 당일 출발지IP, 목적지IP, 국가, 도시, 지역 현황 대시보드 제공 - 당일 시그니처 포함 로그필드 TOP10, Bottom 10 현황 제공 - 당일 코드 포함 로그필드 TOP10, Bottom 10 현황 제공
보고서	- 일별, 기간별 연동 장비 연동통계보고서 제공 - 일별, 주별, 월별, 기간별 경보발생보고서 제공 - 일별, 주별, 월별, 기간별 경보대응보고서 제공 - 시간별, 주별, 월별, 기간별 출발지TOP10, 목적지TOP10 보고서 제공

Ⅳ LogInsight를 활용한 데이터인사이트 사업 소개

01 SCADA망 사업〉 발전 제어망 빅데이터 사업 참여

발전제어 보안 모니터링 데이터 수집, 분석, 연계 참여

1 사업 개요

- 사업명 : 발전제어 보안 모니터링 개발
- 사업 기간 : 2019.11 부터 24개월
- 발주처 : 한전 KDN

발전본부 데이터 취득 네트워크 구성
제어시스템 데이터 취득 연계

▪이상행위탐지시스템 모델
(이상행위탐지기능 + 연계·변환 기능 개발)
▪로그수집/분석시스템 모델
(로그수집/분석기능 + 연계·변환 기능 개발)
▪단위·부문 위협관리시스템 모델
(위협관리기능 + 연계·변환 기능 개발)

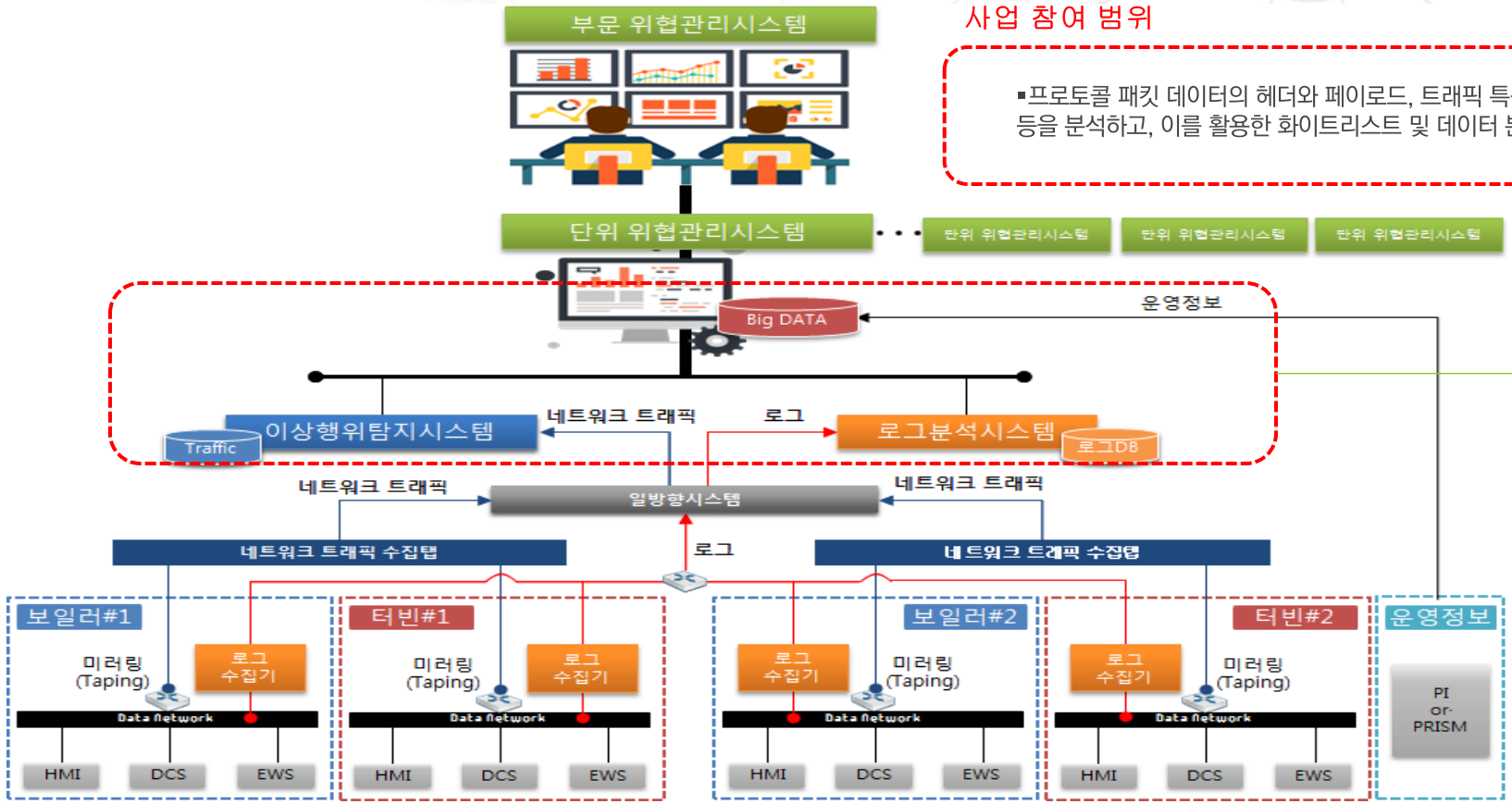
2 참여 부문

- 로우 데이터 수집 , 분석, 위협 관리 기능 제공
- 데이터 수집 , 분석을 위한 빅데이터 기반 엔진 공급 , 참여

제어시스템 분석 및 이상행위 탐지 알고리즘 개발

▪ 제어시스템 제작사(4개社)별 프로토콜 패킷 데이터의 헤더와 페이로드, 트래픽 특성 등을 분석하고, 이를 활용한 화이트리스트 및 프로토콜 분석 보고서를 제출

발전제어시스템 운영에 대한 안정성 및 보안성 확보



발전제어시스템 시범 후 전체 발전 제어망 확대 예정

사이버 보안위협으로부터 중요 국가기반시설인 발전설비를 효율적으로 보호하고 파급효과가 큰 표준분석모델 정립·확산

- 발전소 제어망의 보안침해 공격에 대한 실시간 탐지 및 방어기능 제공으로 발전소의 안전운전 도모

산업통상자원부 http://www.motie.go.kr

보도참고자료

정부혁신 보다나은 정부

배포 즉시 보도하여 주시기 바랍니다.

배포일시	2019. 5. 3.(금)	담당부서	정보보호담당관실
담당과장	여영섭 과장(044-203-5590)	담 당 자	양희준 사무관(044-203-5597)

사이버위협으로부터 발전제어망 보호를 위한 공동연구 착수
- 산업부, 국가정보원 · 발전사 공동으로 발전시스템 사이버보안 강화키로 -

□ 산업통상자원부(장관 성윤모)는 5. 3.(금) 국가정보원, 발전사 등 9개 기관과 함께 발전제어시스템 보안관제 체계구축을 위한 연구개발을 공동으로 추진하기로 하고 필요한 업무협약을 체결했다.

* 산업통상자원부, 국가정보원, 한국수력원자력(주), 한국남동발전(주), 한국중부발전(주), 한국서부발전(주), 한국남부발전(주), 한국동서발전(주), 한국지역난방공사, 한전KDN

○ 동 사업은 발전소운전 제어시스템에 대한 내외부에서의 사이버 공격을 모니터링하고 보안위협을 사전에 차단함으로써 발전시설의 안정적인 운영을 확보할 수 있도록 하는 사업이다.

○ 최근, 해외 에너지 제어시스템에 대한 사이버위협이 지속적으로 보고되고 있어, 이에 대한 선제적 대응 및 기술개발의 필요성이 제기되고 있다.

* 2015년의 우크라이나 발전소에 대한 악성소프트웨어 공격으로 발전소

국내 발전소 제어시스템의 사이버보안 강화

- 산업통상자원부(장관 성윤모)는 3일, 9개기관(산업통상자원부, 국가정보원, 한국수력원자력(주), 한국남동발전(주), 한국중부발전(주), 한국서부발전(주), 한국남부발전(주), 한국동서발전(주), 한국지역난방공사, 한전KDN)과 함께 발전제어시스템 보안관제 체계구축 예정

데이터인사이트 레퍼런스 소개

공공

서울특별시 SEOUL METROPOLITAN GOVERNMENT
평택시
안동시
Marine Pia 친환경 울진
철원군 Cheorwon
삼국유사의 고장 군위
Seoul Design 서울디자인재단
춘천교육대학교 CHUNCHEON NATIONAL UNIVERSITY OF EDUCATION
역동적인 민생청도 청도군
군포문화재단

국방 / 공사 / 협회

대한민국 해병대 REPUBLIC OF KOREA MARINE CORPS
한국가스공사 삼척기지본부
서울교통공사 Seoul Metro
한국대학교육협의회 Korean Council for University Education

발전제어 보안모니터링 개발 시범사업

산업통상자원부
HUNESION DIGITAL CULTURAL PROMOTION

금융 / 클라우드 / 기업

참! 좋은 은행 IBK기업은행
제노솔루션(주) XENO SOLUTION
multicampus

감사합니다