# SMARTer

## 빅데이터 기반 실시간 자동분석솔루션

SMARTer V1.3

KiSTi www.kisti.re.kr
한국과학기술정보연구원
Korea Institute of Science and Technology Information
Seekers

# 배경 및 필요성

## IDS/IPS 보안관제 체계

**효용성**

### 알려진 공격, 실시간 탐지/대응에 효과적

▶해킹공격의 특징을 분석, 생성한 시그니처를 활용

### 여러 기관들의 정보보호에 활용

▶우리나라 공공분야 국가보안관제체계의 핵심 솔루션
※국가보안관제체계 : 공공분야 안전을 위해 구축된 국가사이버안전센터(NCSC) 중심의 중앙집중형 보안관제 체계

## 인력기반 보안관제 체계: 수동분석 중심

**문제점**

### 폭발적으로 증가하는 사이버위협 정보

▶일 평균 적게는 수천 건에서 많게는 수천만 건의 보안이벤트가 발생(국내 공공분야 사이버안전센터)
▶보안관제 요원이 전체 보안이벤트를 분석할 수 없어 보안 사각지대 발생(잠재적 해킹사고 위험 매우 높음)


### Human 기반 보안관제 체계

▶출현 빈도가 높고 분석 이력이 있는 보안이벤트에 편중되어 보안관제 업무 수행
▶보안관제 요원의 기술 및 경험 수준에 따라 보안관제 신속성 및 정확성에 영향을 미침
▶잦은 보안관제 요원의 교체로 인해 분석 기술 및 노하우 축적이 어렵고 서비스 수준이 낮아짐
▶Human error 발생 가능성이 상존(신체적 상태, 감정 상태 등에 따라 분석, 결정 등에 실수 유발)


### 텍스트 기반 보안관제 체계

▶텍스트 정보를 중심으로 보안관제 업무를 수행함에 따라 보안관제 요원의 업무 효율성이 매우 낮음
▶대량의 보안이벤트 더미에서 실제 공격과 연관된 보안이벤트를 직관적으로 발견하기 어려움

## 자동분석 기반의 보안관제체계 전환 필요성

지속적 · 폭발적으로 증가하는 사이버위협에 신속/정확하게 대응하기 위해서는 자동화된 보안관제체계 구축 필요

기존 Human 기반 보안관제체계에서 축적한 노하우 및 분석 기술을 활용하여 사이버공격 자동분석 기술 및 솔루션 개발 필요

# SMARTer 소개

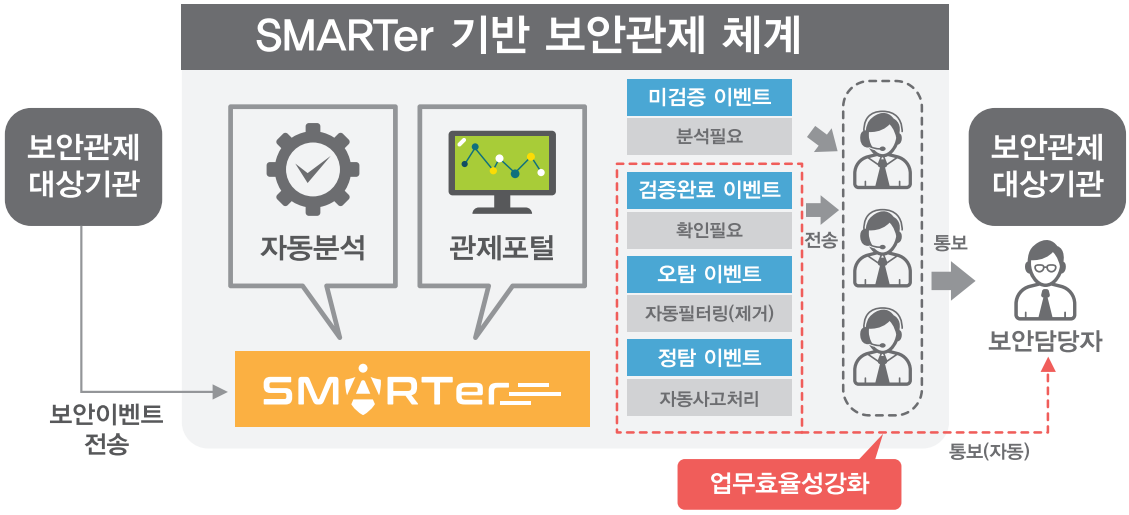
## SMARTer란?

※SMARTer : Security Monitoring, Analysis and Response soluTion extended release

▶SMARTer 솔루션은 신속하고 정확한 사이버침해 탐지/대응을 목표로 자동화 방식을 채택해 개발되었습니다.

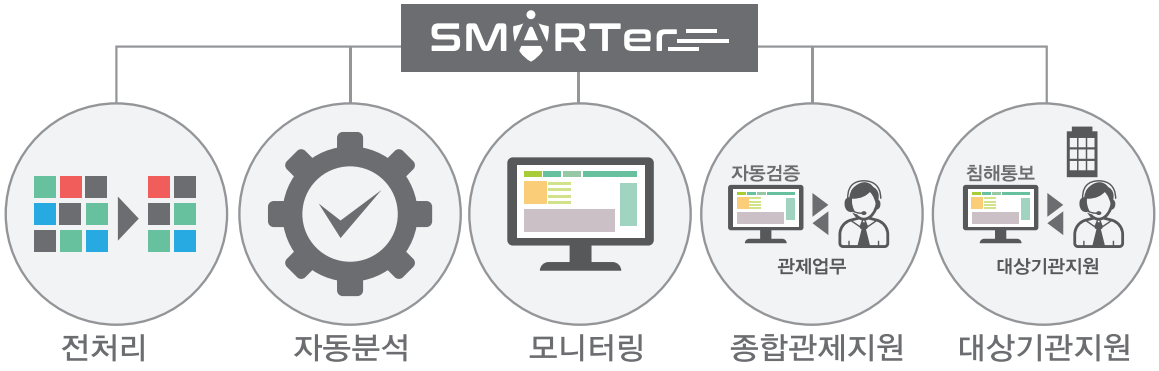
▶기존 휴리스틱 분석의 장점은 살리되 한계점은 극복하기 위해 분석 노하우를 정형화 해 탐지정보 분석에 활용하는 자동분석 방법론을 개발했습니다.

▶또한 2005년 부터 14년 이상 축적한 관제업무 노하우 및 분석기술을 반영하여 모든 관제업무를 SMARTer 솔루션에서 수행할 수 있도록 하였습니다.




## 솔루션의 구성

▶SMARTer솔루션은 총 5개의 모듈로 구성됩니다




## SMARTer 주요 특징

**20만건**
**보안이벤트 자동분석 가능**

2단계 자동분석과정을 통해
최대 20만건의 보안이벤트가
정탐, 오탐으로 신속하게 분석됩니다.

**99%**
**이상의 자동분석 정확도**

SMARTer솔루션을 통한
보안이벤트의 정오탐판별은
99%이상의 정확도로 이뤄집니다.

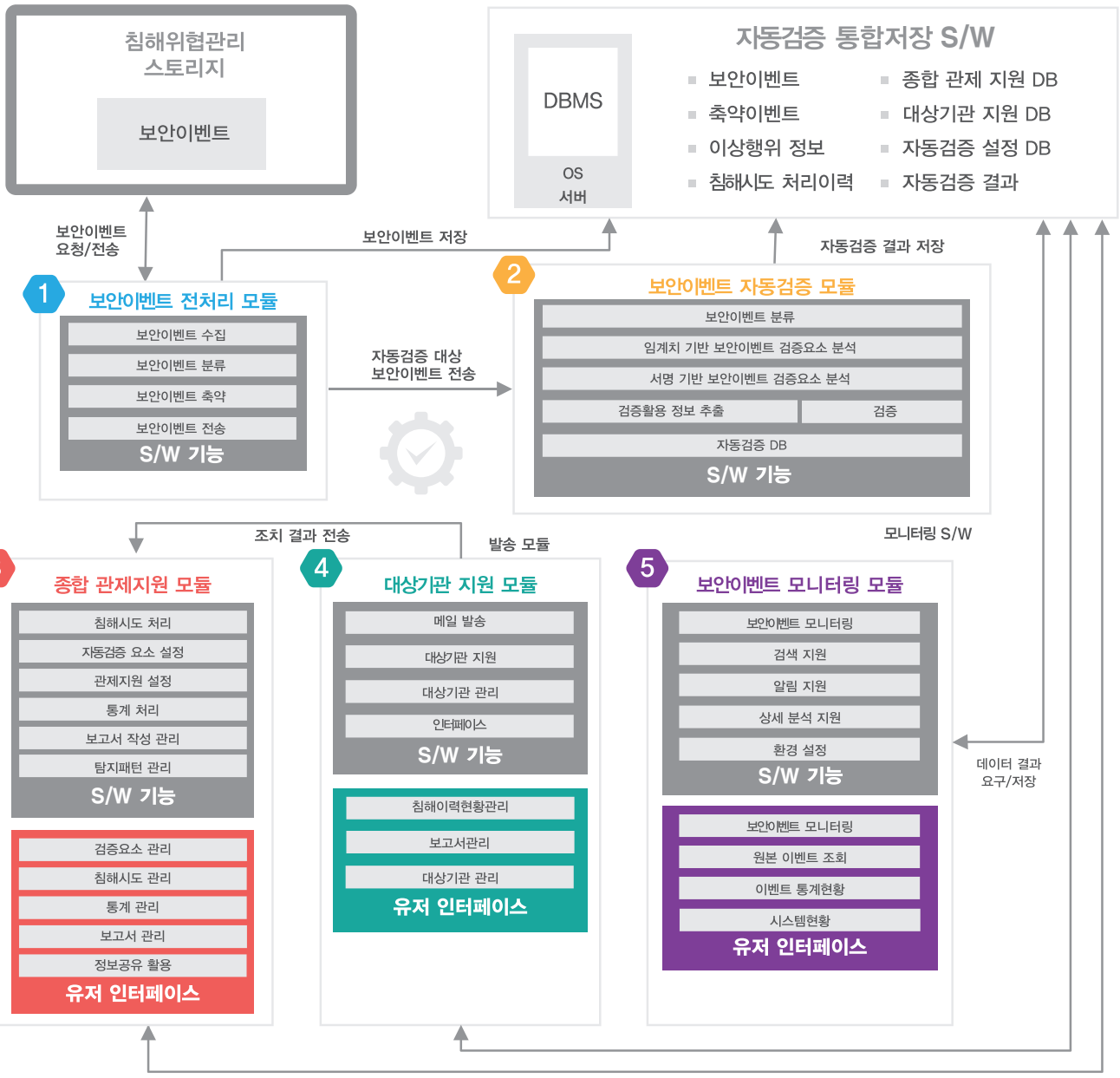
**14년**
**관제업무 노하우**

2005년부터 축적된 관제센터의
분석, 통보, 대응 등 관제업무 노하우가
고스란히 담겨있습니다.

**자동분석**
**보안관제 페러다임**

기존 체계의 문제점을 극복하고
대규모 공격에 대응 가능한
새로운 보안관제체계로 전환 합니다.

# SMARTer 전체 구조




## 클러스터링 적용이 가능한 원박스 설계

SMARTer

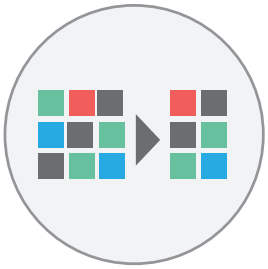
모든 기능이 1대의 하드웨어에서 운영 가능하도록설계(원박스) 되었습니다.

기관 규모 및 트래픽 양에 따라 클러스터링 구성(S/W 확장)이 가능합니다.

## 솔루션 개발 환경

| 이벤트 수집 | 이벤트 분류 및 축약 | Web GUI |
|---|---|---|
| syslog-ng Open Source Edition, Flume | STORM, elasticsearch, kafka | eGovFrame, spring |

# SMARTer 주요기능 및 기대효과



전처리

## 보안이벤트를 분류, 압축 합니다.

| 분류 | 압축 |
|---|---|
| Flooding | 이벤트명, 소스IP, 목적지IP, 소스포트, 목적지포트 = 동일 |
| Scanning | 이벤트명, 소스IP, 목적지IP = 동일 |
| Signature | 이벤트명, 소스IP, 목적지IP, 목적지포트, 페이로드 = 동일 |

※ 분류 및 압축 결과 : 원본데이터 대비 10% 수준으로 보안이벤트 감소

자동분석

## 2단계 분석을 통해 정오탐을 판별합니다.

| | |
|---|---|
| 자동검증 요소 추출 | 필수정보 3종을 추출 합니다. |
| 공격유형 분류 | 공격유형 6종을 분류 합니다. |
| 공격유형 기반 자동검증 | 유형별 알고리즘을 활용, 1차 검증을 합니다. |
| 보안이벤트 기반 자동검증 | 이벤트별 공격특성을 활용, 2차 검증을 합니다. |

관제업무포털

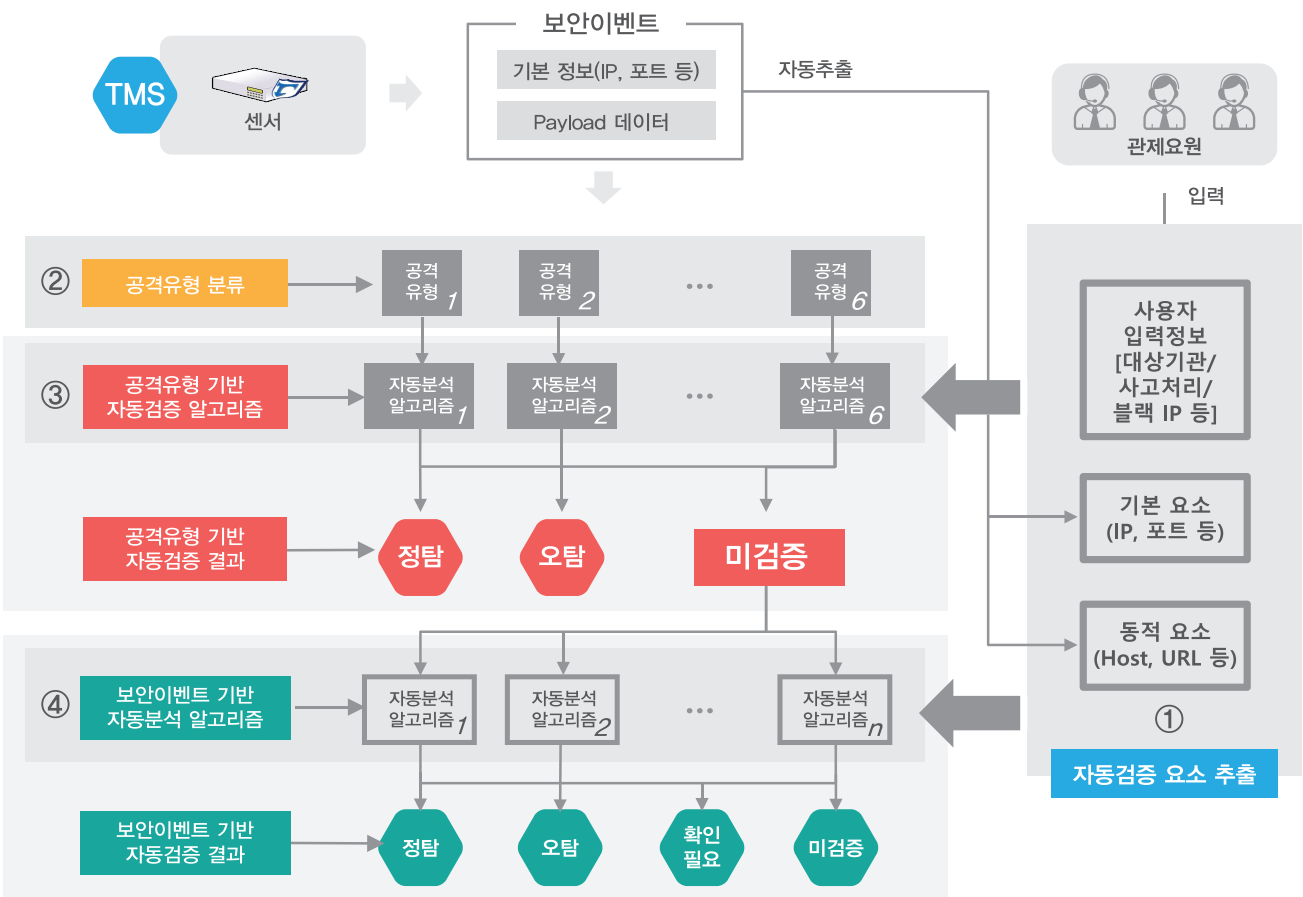
## 보안관제 관련 모든 업무를 지원합니다.

| | |
|---|---|
| 모니터링 | 자동분석 결과를 보안관제 요원이 확인 합니다. |
| 종합관제지원 | 침해시도 통보, 등록된 조치결과 확인 및 처리에 활용 됩니다. |
| 대상기관지원 | 통보된 침해시도를 확인 · 접수 및 조치결과 등록에 활용 됩니다. |

## SMARTer 적용 시 보안관제 기대효과

| AS-IS | TO-BE |
|---|---|
| 100% 수동분석 | 90% 이상 자동분석 |
| 평균 14분 소요 | 최대 2분이내 자동분석 |
| 미탐지 발생 (휴먼 에러) | 미탐지 Zero(0) |

# SMARTer 자동분석 기술




## SMARTer 자동분석 기술 상세

**자동검증 요소 추출**

필수정보 3종을 추출합니다.
- 사용자입력 정보 : 보안관제 요원이 직접 입력
- 기본 요소 : 보안이벤트 내 정보와 직접 비교 가능한 정보
- 동적 요소 : 외부시스템 확인이 필요한 정보

**공격 유형 분류**

공격유형 6종을 분류합니다.

악성 URL | 악성파일 다운로드 | 악성파일 감염 | 정보전송 | 웹쉘 업로드 | 임계치 기반 공격

**공격유형 기반 자동검증**

유형별 알고리즘을 활용, 1차 검증을 수행합니다.
- 검증이 완료된 보안이벤트는 정탐,오탐,미검증으로 분류
- 미검증 보안이벤트는 보안이벤트 기반 자동검증 수행

**보안이벤트 기반 자동검증**

보안이벤트별 공격특성을 활용, 2차 검증을 수행합니다.
- 관제요원의 전문기술 및 노하우를 활용한 검증방식
- 보안이벤트는 정탐 ,오탐, 확인필요, 미검증으로 분류

## 특허등록 현황

### 국내 특허 등록 5건

"보안이벤트 자동 검증 방법 및 장치"

| | 등록번호 |
|---|---|
| (악성 URL 공격 유형) | 10-1689295 |
| (악성코드 다운로드 공격 유형) | 10-1689296 |
| (정보 전송 공격 유형) | 10-1689297 |
| (파일 업로드 공격 유형) | 10-1689298 |
| (임계치 공격 유형) | 10-1689299 |

등록일 : 2016.12.19

### 국내 특허 출원 1건

"보안이벤트 자동 검증 방법 및 장치 (악성코드 감염 공격 유형)"

출원번호: 10-2016-001725 출원일 : 2016.02.15

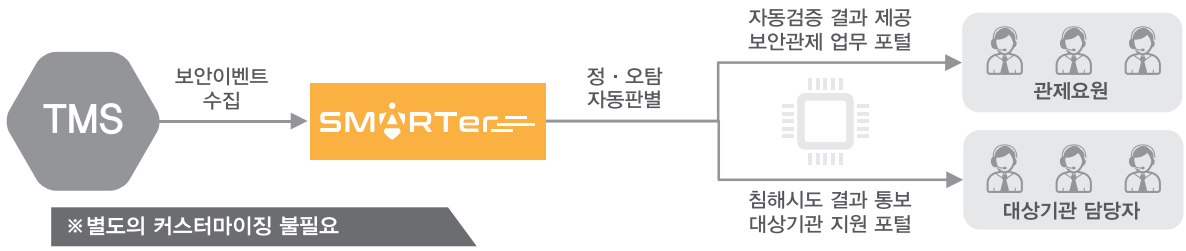
### 국제 특허 출원 1건

"METHOD AND DEVICE FOR AUTOMATICALLY VERIFYING SECURITY EVENT"

출원번호: 15/768,002 출원일 : 2018.04.12

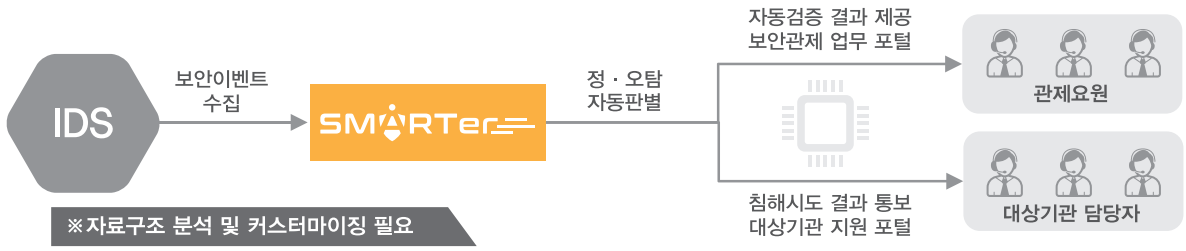
# SMARTer 적용 시나리오

## 1.TMS 기반 보안관제체계




※별도의 커스터마이징 불필요

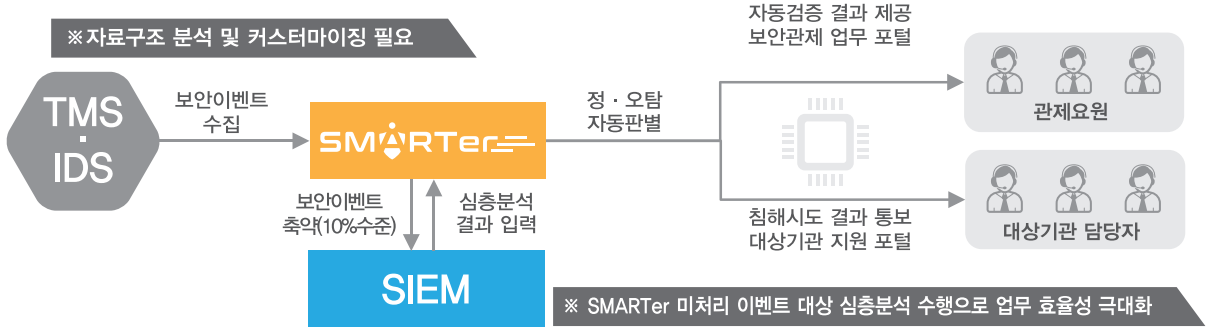
## 2.기타 IDS 기반 보안관제체계




※자료구조 분석 및 커스터마이징 필요

## 3.TMS · IDS 기반 보안관제체계

※자료구조 분석 및 커스터마이징 필요




※ SMARTer 미처리 이벤트 대상 심층분석 수행으로 업무 효율성 극대화

# SMARTer 도입 시 보안관제 기대효과

### 사이버침해위협 탐지 대응 신속도 향상

반복적으로 수행하던 분석업무를 자동화 함으로써 보안관제 탐지/대응시간을 획기적으로 단축할 수 있습니다.

### 보안관제요원 분석수준 향상

보안관제요원들은 반복적 분석업무를 수행할 필요가 없어, 전문가의 분석이 요구되는 고도화된 해킹공격 분석에 집중할 수 있습니다.

### 분석기술 및 노하우 등 기술 축적

갑작스런 보안관제요원의 이직과 같은 상황에도 분석수준이 저하되는 위험이 없고, 오히려 분석 노하우가 지속적으로 축적됩니다.

### 관제업무 프로세스 속도향상 및 간소화

관제업무포털의 지원으로 관제업무 처리속도가 향상되고 프로세스가 줄어듭니다.

KiSTi
www.kisti.re.kr
한국과학기술정보연구원
Korea Institute of Science and Technology Information

한국과학기술정보연구원
주소 : 대전광역시 유성구 대학로 245
문의전화 : 042-869-0729 / 팩스 : 042-869-1119

Seekers

(주)씨커스
주소 : 서울시 구로구 디지털로 32길 30, 코오롱디지털타워빌란트 815호
대표전화 : 02-2039-8160 / 팩스 : 02-2039-8161