

## (28) 소스코드 변경 영향도 평가를 이용한 불법 행위 감시시스템

### [ 기술개요 ]

- 내부 협력사/위탁직원에 의한 보안사고 위협이 증가하고 있으나 ‘권한’에 의한 접근 통제 방법으로는 유지보수 권한(소스코드 변경)을 가진 내부 협력/위탁 직원의 소스코드 조작 여부 탐지가 불가능(보안 사각지대)
- 본 발명은 위탁직원에 의해 시스템 소스코드가 수정될 때 해당 수정내역이 전체 시스템과 중요 비즈니스 로직에 얼마만큼 영향을 주는지 판단하는 기술임
- ※ 본 특허는 본사 안전보안처와 함께 입찰 시스템(SRMD) 침해 사고(15.2) 재발방지를 위해 연구한 결과물임

### 기술 특장점

- 핵심로직 및 프로세스상의 논리적 이상점을 검출할 수 있는 기술
- 본 특허는 아래 두 가지 기술(동적/정적)에 관한 것으로 상호 보완적 이상여부 판단 가능
  - ① SW수정영향도 분석기술(정적) : 수정코드를 운영시스템에 반영하기 전, 중요 로직에 어떤 영향을 주는지 평가하는 기술 (ex: 핵심 모듈 간 우회코드 삽입 기준에 없던 조건문 삽입 등)
  - ② 비즈니스 추적 기술(동적) : 프로세스 (시작→처리→종료)과정에서의 변이(Transition) 과정을 모니터링하여 이상점(Outlier) 검출

### 적용분야

- 기업의 중요 비즈니스 로직이 협력사/위탁직원에 노출 될 수 있는 공공기관의 정보IT 시스템
- 자체 개발된 시스템을 운영하거나 소프트웨어의 안전성을 중요시하는 기업

### 기술패키지 목록

구분	번호	명칭
특허	제10-20160133449호 (PCT/KR2016/013798)	소스코드 변경 영향도 평가를 이용한 불법 행위 감시시스템 (국내 특허등록/해외 특허출원)

① 원본소스에 보안 Annotation 삽입

```

Method()
- Method()
- Method()
Method call
- Method call
- Method call
                
```

② 감시 프로세스의 추적 범위 설정

[F(forward)/B(backward)]

- F=0/B=0 : 원시 프로세스(process)만 추적
- F=0/B=m : m번째 앞 프로세스까지 추적
- F=n/B=0 : n번째 뒤 프로세스까지 추적
- F=n/B=m : 앞/뒤, n/m번째 프로세스 추적

프로세스명	소스권	감시 대상	관심 영역
Process_3	A.java	알고리즘 조작	4~120
	B.jsp	프로세스 우회	4,26
	C.jsp	프로세스 우회	327

원본 소스 (컴파일언어) : Process\_3 Method() (라인번호 1, 2, 4, ..., 120, 121)

원본 소스 (인터프리언어) : Process P() call (라인번호 321), Process 3() call (라인번호 327), Process T() call (라인번호 378, 379, 380)

프로세스별 소스코드 Mapping 부 (번호 21)