한국전력공사 사업화 유망기술

(25) 체인룰 기반 내부자 불법 행위 탐지장치 및 방법

[기술개요]

○ 내부 협력사/위탁직원에 위한 보안사고 증가 추세
  · 공공기관 협력사 침해사고('15), KB·NH/카드협력사 고객정보 2500만건 유출('14)등

○ 기존의 '권한에 의한 접근통제' 방법으로는 유지보수 권한을 부여받은 내부 위탁직원의 불법행위를 탐지해내기란 사실상 불가능에 가까움(보안 사각지대)

○ 본 특허는 권한을 가진 이들을 대상으로, [정상적 소스코드 수정 행위]와 [소스코드 불법 조작 행위]간의 모호함을 해결하기 위한 SW보안 기술 특허임

※ 본 특허는 본사 안전보안처와 함께 입찰 시스템(SRM) 침해 사고('15.2) 재발방지를 위해 연구한 결과물임

기술 특장점

○ 행동 체인룰(chain rule method) 기반의 내부자 행동 추적 기술
  · 3W1F(who/what/when/frequency)특징을 기본룰로 하여 내부자 단위행동들을 체인화하고 연쇄행동 패턴구성(체인룰 생성)후 이진(binary) 평가 수행으로 '정상' 및 '이상'을 판정

○ [특정시간에 짧게] 벌어지는, [드물게] 발생하는, [기존 패턴과 다른] 행동의 검출 가능

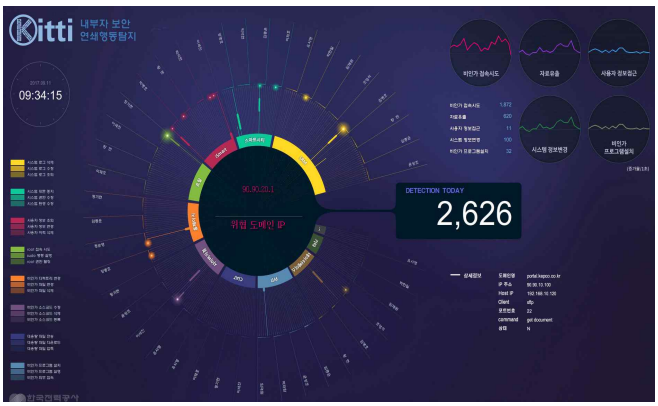
적용분야

○ 기업의 중요 비즈니스 로직이 협력사/위탁직원에 노출 될 수 있는 공공기관의 정보IT 시스템

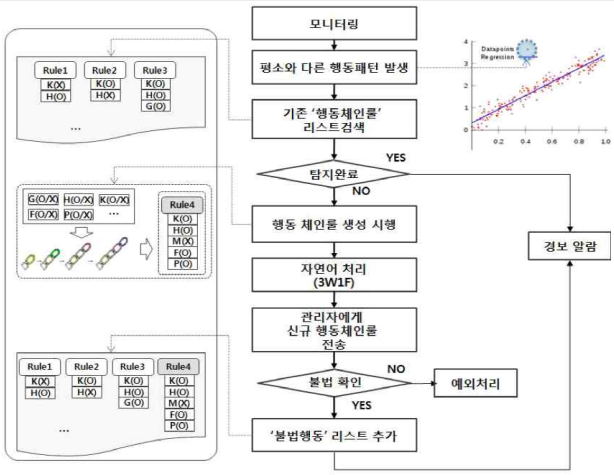
○ 불법탐지 이외에 시스템 운전 실수 조기 검출, 시스템 이상동작 감지 기술로 적용 가능

기술패키지 목록

구 분	번 호	명 칭
특허	제10-16601810000호 (PCT/KR2016/008858)	체인룰 기반 내부자 불법 행위 탐지 장치 및 방법 (국내 특허등록/해외 특허출원)
SW	-	내부자 연쇄행동탐지 시스템



내부자 연쇄행동탐지 시스템 화면



불법행위 검출 프로세스

연락처 : (성명) 김영준 (전화) 0461-5706 (이메일) juny.kim@kepco.co.kr