# 내부정보유출방지 모니터링을 위한 중점관리 대상(고위험군) 선정에 관한 연구+

박장수, 김수현, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[pjswise, kimsh, imylee]@sch.ac.kr

# A study on Priority Control Target(high-risk) Selection for Monitoring of Internal Data Leakage Prevention

Jang-Su Park, Su-Hyun Kim, Im-Yeong Lee
Dept of Computer Software Engineering, SoonChunHyang University

요 약

정보유출사고가 증가됨에 따라, 기업 및 기관 내 주요정보(개인정보 및 핵심기술)가 유출되어 큰 피해가 발생하고 있다. 이러한 정보유출 사고 중 대부분이 내부자에 의한 고의 또는 실수로 발생하는 경우가 대부분이다. 이를 방지하기 위해 다양한 보안 솔루션을 도입하여 운영하고 있지만 내부자에 의한 정보유출사고는 본인이 소유하고 있는 권한을 이용하여 불법적인 정보유출을 시도하는 것으로, 이러한 위험행동을 탐지하는 것은 쉽지 않다. 이를 해결하기 위해 기업 및 기관에서는 기 구축된 다양한 보안 솔루션을 통합하여 모니터링 할 수 있는 '내부정보유출방지 모니터링시스템'을 구축하고 있으며, 내부정보유출방지 모니터링을 위한 연구도 지속적으로 진행되고 있다. 따라서 본 논문에서는 중점관리 대상(고위험군) 선정을 통해 효율적인 내부정보유출방지 모니터링을 수행할 수 있도록 연구하고자 한다.

## 1. 서론

최근 연이어 발생하는 정보유출사고 사례를 살펴보면 금전적 이득과 직접적인 관계가 있거나, 내부직원에 의한 의도적인 유출사고가 대부분이다. 이러한 정보유출 사고가 증가됨에 따라, 기업 및 기관의 주요정보(개인정보 및 핵심기술 등)를 보호하기 위해 다양한 보안솔루션(PC보안, 매체제어, 문서보안, 프린터 보안, 데이터베이스 접근관리 등)을 구축하여 대응하고 있다. 하지만 나날이 발전하고, 지능화되고 있는 보안 위협을 차단하기 위해 새로운 보안 솔루션들을 지속적으로 도입한다고 문제가 해결되는 것은 아니다. 증가하는 보안솔루션에 따른 운영 및 관리 포인트 증대와 복잡성으로, 오히려 기업 및 기관의 보안조직에서 인지할 수 있는 범위를 초과하여 또 다른 보안 사고를 야기시킬 수 있다. 또한 내부자에 의한 정보유출은 자신의 역할과 직무에 따라 소유하고 있는 계정권한 또는 타인의 계정을 이용하여 정보시스템에 접근 후 보안솔루션을 우회하여, 다양한 경로로 데이터를 유출할 수 있기 때문에 사전 탐지가 점점 어려워지고 있다.

이러한 문제점을 해결하기 위해 최근 다양한 보안솔루션을 통합적으로 연계하여 내부정보유출방지를 위한 통합 보안 모니터링이 대두되고 있다. 내부정보유출방지 통합 모니터링은 개별 보안솔루션에서 발생하는 로그들을 수집하여, 이를 룰(위험행동 패턴, 정보유출 시나리오, 보안정책 등)에 기반하여 분석함으로써, 정보유출 및 시도에 대한 이상 징후를 탐지하고 모니터링 하는 것을 말한다. 여기서 중요한 것은 정보유출 분석 룰의 신뢰성으로 정보유출 분석 룰에 대한 다양한 방법론이 연구되고 있다[1-2]. 하지만 정보유출 분석 룰을 아무리 정확하고 신뢰성 있게 제시해도, 업무상 필요한 보안예외처리는 많은 위험행동의 이벤트를 발생시키고 이는 보안담당자가 인지할 수 있는 범위를 초과하기에 이를 해결할 수 있는 방안이 필요하다.

따라서 본 논문에서는 효율적인 정보유출방지 모니터링을 하기 위해 기업 및 기관에서는 어떠한 대상을 중점관리 대상으로 선정하고, 선정된 중점관리 대상을 어떻게 모니터링 해야 하는지 알아보고자 한다.

## 2. 관련연구

### 2.1 내부정보유출방지 기술과 모니터링 방식의 변화

기업 및 기관에서의 내부정보유출 방지를 위하여 물리적/기술적/관리적 보안으로 수행하고 있다(그림 1). 기술적 보안으로 PC보안, 매체제어, 문서보안, 프린터 보안 유해사이트 차단 등 다양한 어플리케이션 보안솔루션을 구축하여 개별솔루션의 콘솔화면에서 위험행동에 대해 모니

+ 본 논문은 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0221609)의 연구수행으로 인한 결과물임을 밝힙니다.


(그림 1) 내부정보유출방지 보안

터링하여 정보유출 이상 징후를 탐지하고 있다. 또한 물리적 보안으로 출입통제, 보안스티커, 보안검색대 등 업무 PC/스마트 기기 불법반출, 외장형 저장장치/출력물 유무 검색을 통해 정보유출 및 시도를 차단하고 있다. 관리적 보안으로는 보안운영관리 정책 설정, 사내보안 규정, 외부 아웃소싱 협력업체 인력에 대한 보안서약서, 구성원에 대한 보안 교육 등 다양한 관리적 관점에서 정보유출방지를 위해 노력하고 있다.

하지만 다양한 보안솔루션에서 발생하는 수많은 이벤트에 대한 개별 모니터링은 사람이 인식할 수 있는 범위를 초과하게 된다. 따라서 이기종의 개별 보안솔루션에서 발생하는 로그들을 수집하고 분석할 수 있는 내부정보유출방지 통합모니터링 시스템이 필요하게 되었으며 현재 기업 및 기관에서 빅 데이터 기반의 내부정보유출통합 모니터링시스템을 구축하고 있는 추세이다[2].

2.2 분석단계별 모델 기반 정보유출 모니터링

분석단계별 모델 기반 정보유출 모니터링은 경험기반의 사이버공격 분석방법에 대한 개념을 응용하여 정보유출 방지 모델을 제시하였다. 이 방식은 경험 중심 시나리오 기반으로 정보유출 위험행동을 분석하고 이를 5가지 모델로 구분하여 판단하는 방법이다. 크게 수집계층과 분석계층으로 구분되어진다. 수집계층은 보안솔루션에서 발생하는 로그들과 인사정보에 대한 배치 및 실시간 수집부분으로 이루어져있다. 분석계층은 사용자 경험지식이 적용된 경험저장소, 분석을 여러 관점에서 평가하는 모델저장소 그리고 경험저장소와 모델저장소를 관리하는 경험조정자로 구성되어 있다(그림2)[3].

이 방식은 한 사람이 일일 분석할 수 있는 분석량을 고려하여 이벤트량을 기존 방식들 보다는 감소시켰지만, 정보유출방지 모니터링에서 가장 중요한 분석 룰인 경험 DB의 설정방법이나 초기 경험 DB 설정에 대해서는 미흡하며, 사용자의 분석결과를 보안 분석가가 경험 조정자를 이용하여 수동으로 반영되기 때문에 보안 분석가에 의존도가 매우 크다. 또한 모델기반 5가지 분석방법은 정규화 분류, 위치정보, 사용자, 출발/목적지 IP 및 Port, 로그간 시간순서로 단계별 분석을 진행하는데 분석정보 요소가


(그림 2) 분석단계별 모델 기반 내부정보유출 모니터링

정보유출방지의 관점보다는 외부침해대응 관점에 해당되므로, 정보유출방지 모니터링의 분석정보 요소로는 적합하지 않다. 마지막으로 발생한 이벤트 중 정보유출의 위험행동에 소명절차 및 결재시스템을 적용하거나, 중점관리 대상을 선정하여 정보유출방지 모니터링을 수행한다면 보안분석가가 분석해야하는 이벤트량을 기존보다 더 감소시킬 수 있다.

## 3. 중점관리 대상(고위험군) 선정을 통한 모니터링

정보유출방지 체계는 물리적 보안, 관리적 보안 그리고 기술적 보안의 세 가지 구성요소를 가지고 있다. 이 세 가지가 정보유출 사고에 대해 예방, 탐지, 대응행위의 상호작용을 하게 된다.

본 장에서는 기업 및 기관에서 내부정보유출방지 모니터링을 효율적으로 수행하기 위하여 어떠한 대상을 중점관리 대상(고위험군)으로 선정하고, 선정된 중점관리 대상들의 모니터링 방법에 대해 알아보고자 한다.

3.1 중점관리 대상(고위험군) 선정과 관리 방법

기업 및 기관의 환경 마다 조금씩 상이하겠지만, 다음과 같이 중점관리 대상을 선정할 수 있으며, 대상에 따라 적합한 모니터링을 수행해야 한다.

① 사내보안 규정 및 정책에 대해 지속적으로 위배를 하는 임직원 및 협력업체 직원

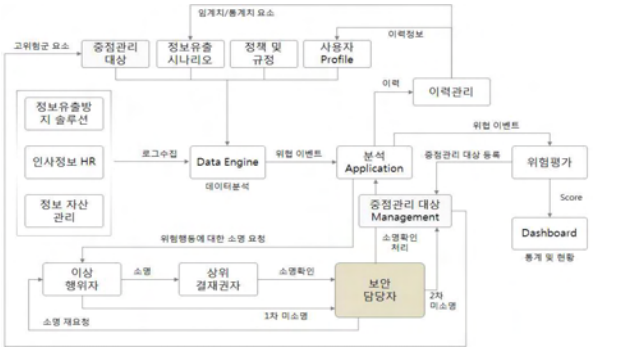
② 중요(가중치 높은) 정보유출 시나리오에 탐지된 임직원 및 협력업체 직원

③ 중요정보(개인정보, 핵심기술정보 등)에 접근할 수 있거나 취급하는 임직원 및 협력업체 직원

④ 각종 보안통제에 대해 예외대상인 임직원 및 협력업체 직원

⑤ 높은 보안 등급을 가지고 있는 임직원

⑥ 퇴직예정자 또는 퇴직자




(그림 3) 중점관리 대상(고위험군)에 따른 모니터링

⑦ 사업종료 또는 사업중간에 철수하는 협력업체 직원

⑧ 진급이 누락되거나, 처벌 받은 임직원

①번의 경우는 보안 규정 및 정책 위배 건수의 임계치 이상 지속되면 의무적인 사내보안교육을 실시하거나 인사고과에 반영하여 규제를 강화할 필요가 있다. ②번의 경우는 과거의 정보유출 시나리오에 탐지된 이력에 대해 고의 또는 실수였는지 소명을 통해 확인하고, 이후에 동일한 위험행동으로 정보유출이 발생하지 않도록 가중치를 부여한 모니터링을 수행해야 한다. ③번의 경우는 데이터 유출 경로(전송, 출력, 매체저장 등)에 따라 모니터링을 수행해야 한다. ④번, ⑤번의 경우는 자신의 소유하고 있는 정당한 권한 및 예외절차를 이용하여 보안기술을 우회할 수 있기 때문에 모든 이력에 대해 Top-Down Analysis 방법으로 모니터링을 수행해야 한다. ⑥번, ⑦번의 경우는 퇴직 시점 또는 철수 시점 기준으로 3~6개월 전의 이력에 대해 이상행위가 없었는지, 중요정보에 접근이 없었는지 모니터링을 수행해야 한다. ⑧번의 경우는 고의적으로 악의를 품고 위험행동을 할 수 있기에, 모든 이상행위에 대해 모니터링을 수행해야 한다.

3.2 중점관리 대상을 통한 모니터링 프로세스

중점관리 대상이 선정되면 정보유출 시나리오와 연계하여 집중관리 대상이 위험행동이 탐지되었을 때는, 즉각적인 경고를 확인 해줘야 한다.

① 정보유출방지를 위한 로그 수집 대상(보안솔루션, 인사정보, 정보자산 등)을 선정하고 이를 통합 연계할 수 있도록 한다.

② 중점관리 대상, 정보유출 시나리오, 정책 및 규정, 사용자 Profile 정보를 이용하여 수집된 로그에서 위험 행동 여부를 판단한다.

③ 위험행동에 대해 이상 행위자에게 소명 요청과, 위험행동에 대한 이력관리를 한다.

④ 위험행동을 한 사용자는 일정기간 내에 소명을 해야 하며, 상위결재권자에게 결재를 받는다.

⑤ 상위결재권자는 위험행위자의 소명을 확인 후 결재 승인를 해주고, 이를 보안담당 부서의 협조를 받는다.

⑥ 위험행동을 한 사용자는 일정기간 내에 소명을 해야 하며, 상위결재권자에게 결재를 받는다.

⑦ 보안담당자는 위험행동자의 소명 결과 및 내용에 따라 중점관리 대상 선정을 확인 하고, 기업 및 기관의 인사정보 시스템, 외주인력 관리시스템 등에서 제공하는 정보에 따라 해당 정보를 수집하여 추가 중점관리 대상 발생 시 수동 또는 자동으로 등록한다. 단 중점관리 대상자를 등록 시에는 보안담당자만이 처리하는 것보다는 보안담당부서의 결재를 통해 이루어져야 한다.

⑧ 소명 여부 및 발생 이벤트의 위험도 Level, 중점관리 대상여부, 과거 이력 및 임계치 정보 등을 고려하여 정보유출 위험 Score를 계산한다.

⑨ 내부정보유출 방지 모니터링을 위한 통합 View로 내부정보유출 위험도 현황, 중요정보 접근 현황, 시나리오별 발생 추이 현황, 부서별 이상행위 누적건수 등 각 기관 및 기업에 적합한 정보를 보여준다.

## 4. 결론

정보유출방지를 위하여 기업 및 기관에서는 다양한 보안솔루션을 도입하여 운영중에 있다. 이러한 보안솔루션에서 발생하는 개별 로그량만 보아도 사람이 인지하여 분석할 수 있는 범위를 초과하기 때문에, 내부정보유출 모니터링에서는 이를 효과적으로 감소시키는 것도 매우 중요하다. 따라서 본 연구에서는 중점관리 대상을 선정하고 이에 따라 효율적인 모니터링방안을 연구하였다.

## 참고문헌

[1] 박장수, 박정현, 강용석, 이임영, “사용자 행위 Modeling을 이용한 내부정보유출 방지 시나리오 설계방안에 관한 연구,” 한국정보처리학회 추계학술발표대회 논문집, 제 20권, 제 1호, 2013

[2] 김송영, 김요셉, 임종인, 이경호, “빅데이터를 이용한 보안정책 개선에 관한 연구,” 한국정보보호학 논문지, 제 23권, 제 5호, 2013

[3] 김두상, 김성락, “어플리케이션 로그를 활용한 정보유출 징하 모니터링 연구”, 한국정보기술학회 학회지 제 11권, 제 8호, 2013

[4] 박장수, 강용석, 이임영, “소명을 이용한 내부정보유출 방지 관리 방안에 대한 연구,” 한국정보처리학회 춘계학술발표대회 논문집, 제 21권, 제 1호, 2014