KIPS Tr. Comp. and Comm. Sys.
Vol.4, No.2 pp.65~72 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2015.4.2.65

Log Analysis Method of Separate Security Solution using Single Data Leakage Scenario

Jang-Su Park† · Im-Yeong Lee††

ABSTRACT

According to recent statistics published by the National Industrial Security Center, former and current employees are responsible for 80.4% of companies' technology leakages, and employees of cooperative firms are responsible for another 9.6%. This means that 90% of technology leakages are intentionally or mistakenly caused by insiders. In a recent incident, a credit card company leaked private information, and the person responsible was an employee of a cooperative firm. These types of incidents have an adverse effect not only on a company's assets but also on its reputation. Therefore, most institutions implement various security solutions to prevent information from being leaked. However, security solutions are difficult to analyze and distinguish from one another because their logs are independently operated and managed. A large number of logs are created from various security solutions. This thesis investigates how to prevent internal data leakage by setting up individual scenarios for each security solution, analyzing each scenario's logs, and applying a monitoring system to each scenario.

Keywords : Data Loss/Leakage Prevention, Scenario of Internal Data Leakage

단일 정보유출 시나리오를 이용한 개별 보안솔루션 로그 분석 방법

박 장 수† · 이 임 영††

요 약

최근 산업기밀보호센터의 기밀 유출 통계에 따르면 기술유출 주체는 전·현직원이 80.4%이고, 협력업체 직원에 의한 유출은 9.6%로 내부자에 의한 고의 또는 실수로 발생하는 경우가 90%이다. 최근 발생한 카드사 개인정보유출 또한 내부시스템 컨설팅 프로젝트에 참여한 협력업체 직원이 정보유출을 감행한 것으로 밝혀져 사회적으로 큰 충격을 주었다. 이러한 내부정보유출 사고는 기관 및 기업의 이미지 손실뿐만 아니라 금전적인 손실을 발생시킬 수 있어, 다양한 보안솔루션을 도입하여 운영하고 있다. 하지만 보안솔루션들이 독립적으로 운영 및 관리되고, 보안솔루션에서 발생되는 대용량 로그와 다양한 형식의 이벤트를 보안 담당자가 식별하고 판단하기에는 어려움이 있다. 따라서 본 논문에서는 내부정보유출 방지를 위한 모니터링을 하기 위해 보안솔루션별로 정보유출 단일 시나리오를 도출하고, 솔루션별로 발생하는 로그 분석에 따라 이를 적용하기 위한 방안을 연구하고자 한다.

키워드 : 정보유출 방지, 내부정보유출 방지 시나리오

1. 서 론

기관 및 기업은 업무환경의 변화에 따라 주요 정보들이 온라인(E-mail, 메신저, 블로그 등) 및 오프라인(보조기억매체, 출력물, 스마트폰 등) 경로로 유출될 수 있다. 특히 최근에는 클라우드 및 BYOD(Bring Your Own Device)와 같은 환경의 변화로 이전보다 쉽고 빠르게 정보가 외부와 공유되어 유출될 수 있다. 이렇듯 업무환경의 변화는 업무의 효율성을 높여주지만 다른 이면에는 중요 정보들이 외부로 유출될 수 있는 위협이 존재한다.

산업기밀보호센터의 기밀 유출 통계에 따르면 전기전자, 기계, 정보통신, 화학, 생명공학 등 다양한 분야에서 정보유출이 발생되었고, 무단보관이나 개인의 영리를 위한 내부공모를 통해 문서 유출이 가장 많이 발생한 것으로 조사되었다[1]. 또한 최근 국내 대표적인 카드 3사에서 약 1억 4천만 건의 개인정보유출이 발생하는 대참사가 발생하기도 하였다. 이는 신용평가회사의 한 직원이 고객정보를 이동식 저장장치(USB : Universal Serial Bus)에 담아 유출을 한

† 준 회 원 : 순천향대학교 컴퓨터학과 박사과정
†† 종신회원 : 순천향대학교 컴퓨터소프트웨어공학과 교수
Manuscript Received : November 18, 2014
First Revision : December 29, 2014
Accepted : December 30, 2014
* Corresponding Author : Im-Yeong Lee(imylee@sch.ac.kr)

것으로 밝혀져 사회적으로도 큰 충격을 주었다.

이처럼 내부정보유출 사고가 연이어 발생하면서 기관 및 기업에서는 정보유출 방지 및 모니터링을 위하여 암호화, DRM(Digital Rights Management), 매체 제어, 유해 사이트 차단, 메일 및 메신저 모니터링 솔루션, 출입통제 시스템, DLP(Data Leakage/Loss Prevention) 등 다양한 보안솔루션을 도입하여 내부정보유출에 대응하고 있다.

하지만 지속적으로 보안사고가 발생하는 원인에 대해 살펴보면, 개별 보안솔루션 간 연동이 미비하고, 체계적인 내부정보유출 방지 보안프로세스가 적용되지 않아 보안사고가 발생한 것으로 생각된다. 또한 보안솔루션에서 생성되는 대용량 로그와 다양한 형식의 이벤트는 보안 담당자가 정확히 인지할 수 있는 범위를 초과하고, 분석시스템의 결과에 대한 판단은 기관 및 기업의 정보보호를 담당하고 있는 보안 담당자의 개인역량에 상당 부분 의존하고 있기 때문에, 효과적인 정보유출 방지 모니터링을 수행하기에는 어려움이 있다. 이에 내부정보유출 방지를 위한 근본적이고 효과적인 대책 마련이 필요하다. 따라서 본 논문에서는 효과적인 내부정보유출 모니터링을 위하여 보안솔루션별 정보유출 방지 단일 시나리오를 도출하고, 개별 솔루션에서 발생하는 로그를 분석하여 이를 적용하기 위한 방안을 제시하고자 한다.

본 논문의 구성으로, 2절에서는 최근 발생한 국내 내부정보유출 현황을 살펴보고, 3절에서는 정보유출 경로에 따른 장비유출 방지 방안에 대해 알아본다. 4절에서는 개별 보안솔루션에 따른 정보유출 단일 시나리오를 도출하고, 각 개별 보안솔루션에서 발생한 로그정보에 기반하여, 도출한 시나리오를 적용하고자 한다. 마지막으로 5절에서는 결론을 맺는다.

2. 국내 내부정보유출 현황

본 절에서는 정보유출 사고 중 내부자에 의한 정보유출 현황을 살펴본다. 본 논문에서는 내부유출범위를 전·현직 직원 이외에 해당 기관 및 기업의 협력업체 직원까지 포함한다.

Table 1. The case of industrial technology leakage in domestic

연도	유출 사례
2010	· 국내 3D 기술 중국 유출사건 · 반도체 핵심기술 해외 유출사건 · 양문형 냉장고 설계기술 중국 유출기도사건
2011	· 국내 첨단 디스플레이 기술 중국 유출사건 · 의약품 원료제조기술 중국 유출사건 · 중국인 연구원 가전기술 해외 유출기도사건
2012	· 첨단 에어컨 핵심기술 중국 유출기도사건 · 태양전지 생산 장비 제조기술 해외 유출사건 · 차세대 디스플레이 기술 해외 유출사건 · 선박부품 설계기술 중국 유출사건
2013	· 전략물자 기술 해외 불법유출사건 · AM-OLED 핵심기술 중국 유출기도사건

Table 2. The case of personal information leakage by insider

시기	유출대상	유출건수
2007	H 텔레콤	600만 건
2008	G 칼텍스	1,125만 건
2011	S 카드	47만 건
2012	K 통신	870만 건
2013	M 보험	16만 건
2013	S 은행	13만 건
2013	대리운전 운행정보업체	420만 건
2014	카드3사	1억 400만 건

2.1 산업 기술 유출 현황

국가정보원 산업기밀보호센터의 조사 결과 2005년부터 2013년까지 국내 기술유출 적발 건수를 살펴보면 Fig. 1에

Fig. 1. Exposure numbers of technology leakages

서 볼 수 있듯이 총 375건으로 지속적으로 기술 유출 사례가 발생하였다. 그리고 2009년부터 2013년까지 209건의 기술 유출 중, 중소기업의 정보유출이 73%로 가장 높았으며, 기술유출 분야는 전기전자 및 기계 분야에서 많이 발생하였다. 또한 기술유출 주체를 살펴보면 전직 직원 60.8%, 현직 직원 19.6%, 협력업체 직원 9.6%로 내부정보유출이 90%를 차지한다[1].

2.2 내부자에 의한 개인정보유출 현황

최근 국내 내부자에 의한 개인정보유출 현황을 살펴보면 Table 2와 같이 지속적으로 정보유출이 발생하고 있다[2].

가장 최근에 발생한 신용카드회사 개인정보유출은 역대 최대 규모로, 협력업체의 내부 직원이 카드부정사용시스템 개발 프로젝트를 담당하면서 카드 3사에 파견 다니며 고객정보에 접근해, 고객정보를 이동식저장장치(USB)에 몰래 담아 약 1억 4천만 건의 개인정보(이름, 주민번호, 주소, 휴대전화, 직장명, 카드이용실적금액, 카드결제계좌, 연소득, 카드신용등급, 신용카드 번호 및 유효기간 등)를 유출한 사례로 사회적으로 큰 파장을 주었다.

3. 내부정보유출 경로 및 정보유출 방지 방안

기업 및 기관의 정보유출 사고는 다양한 정보유출 경로로 발생하고 있으며, 각 경로별 취약점에 대해서 차단 가능한 단위 보안솔루션을 도입하여 정보유출을 방지하고 있다. 정보유출 경로를 살펴보면 Fig. 2에서와 같이 ① 인터넷, ② 저장장치, ③ 노트북 외부 반출, ④ 프린터 출력, ⑤ 스마트기기 등을 통한 유출로 구분할 수 있다[3-6].

3.1 인터넷을 통한 외부유출 대응

현재 사내 업무 망과 인터넷 망을 같이 사용함에 따라, 웹 메일, 블로그 게시판, 메신저 등을 이용하여 외부로의 정보 유출이 쉽게 발생할 수 있다. 이를 방지하기 위해 유해사이트 차단 솔루션, E-mail 및 메신저 모니터링 솔루션 등을 도입하여, 게시판, 블로그와 같은 웹 사이트 파일 업로드 정보, 통제된 웹 사이트 접근 시도 정보, 통제된 응용프로그램 사용 정보, 전송되는 첨부파일 정보, 대화 정보 등을 보안 관리자가 정기적인 점검을 통해 외부로 파일이 전송되는

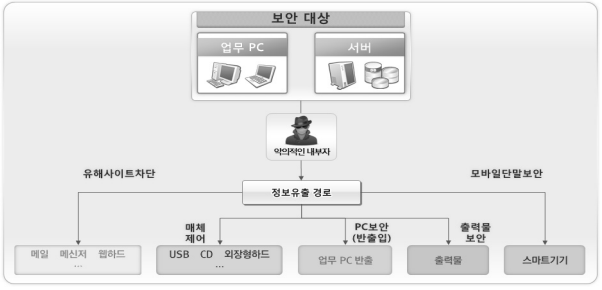

Fig. 2. The path of data leakage

것을 차단하거나 모니터링하고 있다.

3.2 저장장치를 통한 외부유출 대응

인터넷 망을 이용한 외부 전송 경로를 통해 파일이 유출되는 것 외에 주요한 유출 수단은 PC에 저장된 주요정보가 저장매체(USB, 외장형 하드, CD, 스마트폰 등)를 통해 유출되는 것이다. 이를 해결하기 위해서 매체 제어 솔루션을 통해 저장매체 사용 이력 정보, 통제된 매체 사용 시도 정보 등을 관리자 화면에서 확인함으로써, 유출되는 것을 모니터링하고 있다. 최근에는 이동식 저장장치 반입을 통제하는 기업 및 기관이 늘어나고 있다.

3.3 업무용PC 반출을 통한 외부유출 대응

최근 사무 공간 및 이동의 편의성을 고려하여 노트북 사용이 확산되었다. 이러한 업무용으로 사용된 노트북의 무단 외부 반출을 통제하기 위한 방안으로 PC 반출 시스템을 도입하여 대응하고 있다. PC를 반출하는 경우 Endpoint DLP 솔루션들은 외부, 즉 회사 밖으로 나가는 경우 다양한 매체 및 통신 방식을 차단하여 PC 내부에 있는 중요 정보가 외부로 나가지 못하게 한다. 만약 외부에서 사용이 필요한 경우 사전에 승인을 통해서 외부에서 사용할 권한을 획득한다. 단 외부에서 사용한 로그는 수집되어 내부에 들어오면 관리 서버에 전송되어 모니터링하게 된다.

3.4 출력물을 통한 외부유출 대응

일반적으로 업무 진행 시 무분별한 출력행위가 빈번히 일어나고 있다. 하지만 이미 출력된 주요정보는 복사되거나, 스캔과정을 통해 파일로 재저장되어 유통이 손쉽게 이루어진다. 이를 해결하기 위해 출력물 보안솔루션을 도입하여 업무PC에서 출력되는 이력을 관리하며 출력된 원본을 저장한다. 따라서 출력되는 문서에 대한 인쇄자, 출력 일시, 문서 제목 등을 모니터링할 수 있다. 또한 출력권한이 없는 사용자에 대해서는 출력을 차단하기도 한다. 일반적으로 출력된 문서가 외부로 유출되는 것을 방지하기 위해 보안게이트 검색대에서도 물리적인 검사를 병행하여 진행하기도 한다.

3.5 스마트 기기를 이용한 외부유출 대응

최근 IT의 발전으로 언제, 어디서나 시간과 장소에 구애받지 않고 업무를 처리함으로써 효율적인 업무환경을 구현할 수 있도록 스마트워크가 확대되고 있다. 이러한 형태의 업무환경에서는 대부분의 업무처리가 스마트 기기를 통해 이루어지므로 스마트 기기 내에 있는 사내 주요정보의 유출 가능성이 존재한다. 따라서 MDM(Mobile Device Management)과 같은 모바일 보안솔루션으로 단말 관리, 분실/도난 관리, 단말 제어, 애플리케이션을 관리함으로써 정보가 유출되는 것을 방지하고 있다.

3.6 내부정보유출 방지 기술의 한계점

앞에서 언급한 각 정보유출 경로별 대응 이외에 기업 및

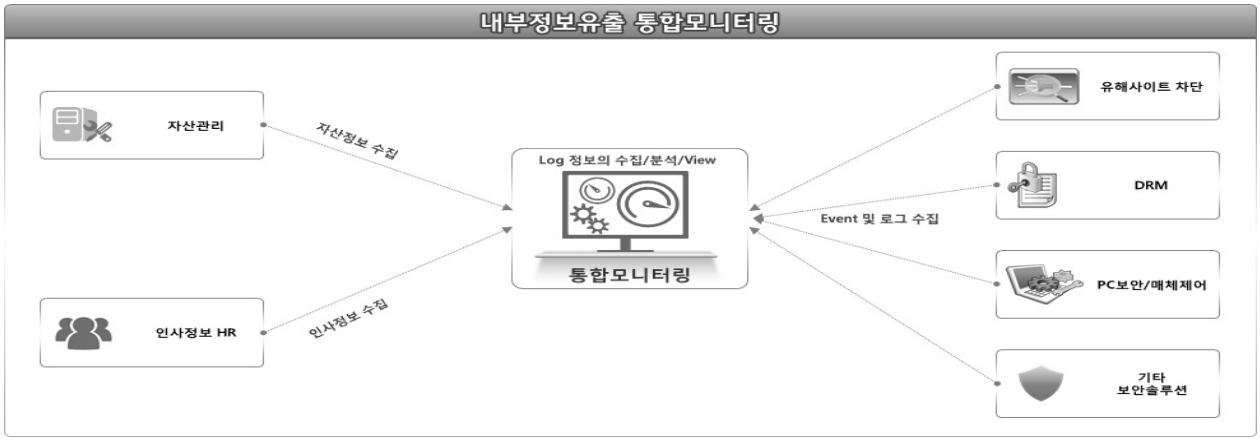

Fig. 3. Monitoring of internal data leakage

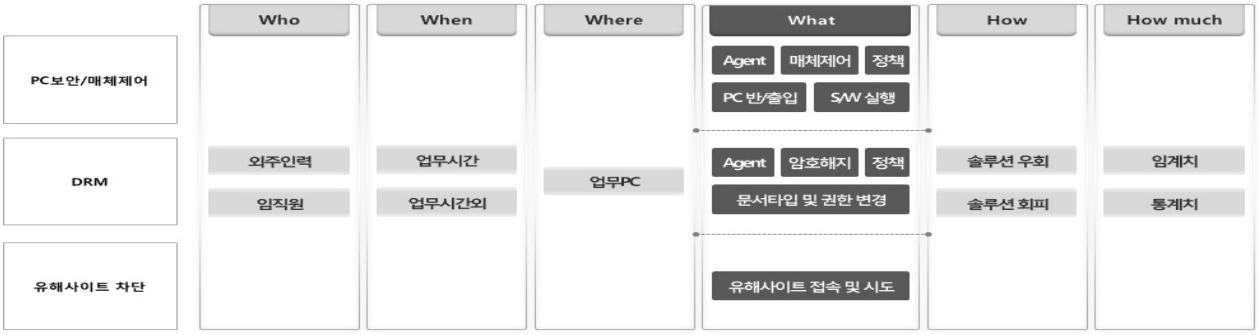

Fig. 4. 4W2H components of security solutions

기관에서는 Virtual Private Network, DB보안, 서버보안, 개인정보 검색, 출입통제 등 다양한 보안솔루션 및 시스템을 도입하여 정보유출 방지를 위한 대응을 하고 있다. 하지만 기업 및 기관에서 도입된 보안솔루션을 통합적으로 모니터링하는 것이 아니라, 개별적으로 모니터링을 수행하는 것이 일반적인 현황이다. 이처럼 정보유출 방지를 위한 보안솔루션들을 개별적으로 식별하고 판단하기에는 로그들의 양이 많아 제한된 인력을 보유한 기관 및 기업의 보안 담당자가 인지할 수 있는 범위를 초과한다. 또한 보안 담당자의 개인 역량에 상당 부분 의존하기 때문에 실시간으로 내부정보유출 위험행동에 대해 탐지하기에는 어려움이 있다. 따라서 Fig. 3과 같이 내부정보유출 통합보안모니터링을 위해서 기업 및 기관의 적용된 다양한 보안솔루션들의 로그를 수집하고 분석하여, 하나의 통합 화면에서 내부정보유출 위험행동을 실시간으로 탐지해야 한다. 이를 위해서는 각 기업 및 기관의 IT환경 및 체계적인 보안프로세스를 고려하여 보안솔루션 간 긴밀한 연동이 필요하다. 또한 각각의 보안솔루션에서 발생하는 보안 이벤트를 수집하여 정보유출시나리오에 근거한 이상 행위를 탐지함으로써 내부정보유출 모니터링을 실시간으로 수행해야 한다.

4. 정보유출 방지를 위한 시나리오 도출 및 적용

내부정보유출 방지를 위한 통합보안모니터링에서는 내부자의 이상행동에 대한 분석에 이용되는 정보유출 시나리오가 핵심이다. 하지만 기존 연구에서는 시나리오를 도출하는 방법이나 적용에 대해서는 제시를 하지 않았다.

따라서 본 논문에서는 내부정보유출 방지 모니터링을 수행하기 위해, 사용자 위험행위 모델링에 기반한 정보유출 단일 시나리오 도출방안과 도출된 정보유출 시나리오를 이용해 보안솔루션의 로그 테이블/필드 정보를 분석 후 “식별정보”, “정보유출 시나리오정보”, “분석정보” 필드로 구분하여 각 시나리오의 적용방안을 제시하고자 한다.

4.1 정보유출 단일 시나리오 설계방안

내부정보유출 시나리오 설계 작업은 보안위험행위에 대한 경험적 지식, 업무 연관성 등 핵심 프로세스에 대한 이해, 마지막으로 보안 규정에 대한 숙지가 필요한 전문성이 요구되는 작업이다. 따라서, 시나리오를 설계하는 단계에서 도움이 될 수 있도록 내부정보유출 방지를 위해서 최적화된 시나리오 설계 방안을 제시하여 기업 및 기관 내부정보의 보호를 위한 이상 행위에 대해 사전 탐지 및 대응, 정보유출 행위 추적 및 조치 등 효율적인 대응을 할 수 있도록 한다.

Fig. 5. Single scenario for data leakage

1) 4W2H에 의한 사용자 행위 Modeling

기업 및 기관에서 기 도입된 단위 보안솔루션에서 발생하는 이벤트가 단일 시나리오를 구성하는 중요 항목이 된다. 하지만 각 기업 및 기관에서 도입하는 보안솔루션의 종류는 이해관계로 인해 서로 상이할 수밖에 없다. 또한 동일한 기능의 보안솔루션일지라도, 제품마다 발생하는 로그는 서로 상이하다. 이러한 환경에서 유연한 시나리오 설계를 위해 본 논문에서는 4W2H에 의한 사용자 행위 모델링 기법을 이용한다.

4W2H는 Fig. 4에서와 같이 Who, When, Where, What, How, How much의 구성요소로 시나리오를 설계하는 것이다. 예를 들어, “퇴직예정자가 업무 외 시간에 외부에서 원격으로 사내 망에 접속하여 기술정보를 최근 3개월 이내 평균 발송량보다 3배 초과하여 이메일로 발송한 경우”를 살펴보면 아래와 같다.

- Who : 퇴직예정일이 일주일 이내의 직원
- When : 업무시간 외
- Where : 외부 네트워크에서 원격으로 접속
- What : 기술정보
- How : 메일로 발송
- How much : 최근 3개월 평균 발송량보다 3배 초과

2) 보안솔루션별 정보유출 단일 시나리오 도출

정보유출 시나리오는 각 보안솔루션을 우회 또는 회피하여 정보유출 가능성이 있는 시나리오를 말한다. 정보유출 시나리오는 단일과 연계 시나리오로 분류할 수 있으며, 단일 시나리오는 수집되는 정보로부터 각 단위 보안솔루션의 이벤트, 보안정책 위반, 프로파일의 패턴 정보가 될 수 있으며, 연계 시나리오는 2개 이상의 단일 시나리오 조합으로 구성된다[6]. 본 논문에서는 보안솔루션의 개별적 분석을 통해 적용하는 방안의 연구로써 단일 시나리오만 언급한다.

PC보안/매체 제어, DRM, 유해사이트 차단 솔루션의 정보유출 시나리오를 도출하기 위해 각 솔루션별 기능 분석 후 사용자 행위 Modeling을 이용하여 4W2H의 구성요소를 살펴보면 Fig. 4와 같으며, 이를 각 솔루션별 정보유출 단일 시나리오를 도출하면 Fig. 5와 같다.

4.2 보안솔루션별 정보유출 시나리오 적용 방안

보안솔루션에서 발생하는 로그 테이블 및 필드정보에 대해 “식별정보”, “정보유출 시나리오정보”, “분석정보” 필드로 구분 후, 정보유출 시나리오정보 필드를 이용하여 앞에서 도출한 내부정보유출 시나리오를 적용한다. 각 보안솔루션에서 발생하는 로그정보에 따라 도출된 내부정보유출 단일 시나리오의 적용 가능 여부를 판단하기에 정확한 분석을 필요로 한다.

PC보안/매체제어

식별 정보	정보유출 시나리오 정보	분석 정보		
로그 순번	로그생성시간	사용자 ID	사용자 IP	사용자 부서
사용자 이름	사용자 직위	Agent MAC	Agent 고유정보	사용자 연락처
사용자 Mail 주소	승인상태	Agent 설치일시	프로세스 명	매체구분
접근유형	파일명	파일크기	Agent 로그인 정보	차단 S/W 목록
반출입 예정일자	승인 일시	접근프로세스 경로	S/W 실행 구분	매체사용 예정일자
매체사용 종료일자	승인자	매체 한글명	매체 영문명	...

Fig. 6. A classification of log filed in pc security and media control solution

PC보안/매체제어

정보유출 단일 시나리오	정보유출 시나리오 탐지 항목			
임직원 및 외주인력의 업무 PC에 PC보안 Agent를 설치를 하지 않은 경우	Agent 설치일시	...	....	...
임직원 및 외주인력의 업무 PC에서 PC보안 Agent를 로그인하지 않은 경우	Agent 설치일시	Agent 로그인정보	...	...
임직원 및 외주인력의 업무 PC에서 미승인 매체제어(USB, DVD/CD-RW 등) 사용을 시도하는 경우	승인상태	매체구분	...	...
임직원 및 외주인력의 업무 PC에서 미승인 공유폴더 사용을 시도하는 경우	승인상태	매체구분	...	...
읽기만 승인된 임직원 및 외주인력이 이동매체에 파일쓰기를 시도하는 경우	승인상태	매체구분	...	...
승인된 임직원 및 외주인력이 특정(보안) 확장자 또는 파일명에 대해 복사한 이력이 있는 경우	승인상태	매체구분	파일명	..
임직원 및 외주인력의 업무 PC를 외부로 미승인 반출 시도를 하는 경우	승인상태	...	...	...
반출승인을 받은 임직원 및 외주인력의 업무 PC가 반출기간을 어긴 경우	승인상태	반출입예정일자	..	...
임직원 및 외주인력의 업무 PC에서 차단된 S/W실행을 시도하는 경우	차단 S/W 목록	S/W 실행구분	프로세스명	...
임직원 및 외주인력의 업무 PC 패스워드가 주기적으로 변경되지 않은 경우	이전 패스워드 변경일	최종 패스워드 변경일	...	...
임직원 및 외주인력의 업무 PC에서 공유폴더 사용을 하는 경우	매체구분	...	...	...

Fig. 7. Matching of each data leakage scenario information for pc security and media control solution

1) 식별정보

보안 위반행위자로 판단된 사용자를 식별하기 위한 정보로 개별 단위 보안솔루션의 로그정보에는 기본으로 식별할 수 있는 고유한 정보가 한 개 이상 존재한다. 하지만 보안솔루션마다 로그 필드 항목이 서로 상이하기 때문에, 인사정보 및 PC 자산관리를 이용하여 보안 위반행위자를 식별할 수 있는 공통된 식별정보와 추가로 식별할 수 있는 추가 식별정보로 분류하여 식별정보로 사용한다.

2) 정보유출 시나리오정보

각각의 단일 시나리오를 적용하고자 사용되는 정보로, 개별 단위 보안솔루션에 따라 여러 개의 로그 테이블 및 수십여 개의 로그 필드가 존재한다. 따라서 도출한 정보유출 단일 시나리오에 대해 사용되는 정보유출 시나리오 정보필드를 매칭시켜 개별 시나리오가 적용 가능한지 확인해야 한다. 하나의 정보유출 방지 단일 시나리오에 한 개의 필드 또는, 한 개 이상의 필드가 존재한다.

3) 분석정보

보안 위반행위로 탐지된 정보가 정탐인지 오탐인지 판단하기 위한 정보로 개별 단위 보안솔루션에서 발생한 모든 로그 필드가 여기에 해당되며 정보유출 시나리오에 따라 식별정보, 정보유출 시나리오정보가 포함될 수도 있다.

4) 정보유출 단일시나리오 적용

내부정보유출 방지 모니터링을 위해서 각 개별 보안솔루션에 대한 정보유출 시나리오 적용방안은 다음과 같다. 본 논문에서는 앞서 시나리오에서 도출한 PC보안/매체 제어 솔루션을 기준으로 설명한다.

① 해당 솔루션의 로그 필드정보를 확인하여 정리한다. 보안솔루션마다 로그 테이블 및 필드정보는 상이하기 때문에 개별적으로 분석이 필요하다. 또한 단일 보안솔루션도 여러 개의 테이블과 필드로 구성되어있기 때문에 각각의 로그정보를 “식별정보”, “정보유출 시나리오정보”, “분석정보” 필드로 Fig. 6과 같이 구분한다.

② 정보유출 시나리오별로 탐지항목을 정리하면 Fig. 7과 같이 표현 가능하다. 앞서 도출된 시나리오가 모두 적용될 수 있는 것이 아니라, 솔루션에서 발생한 로그정보 중 정보유출 시나리오정보로 사용되는 항목이 존재해야 적용 가능하므로, 솔루션별 로그 분석이 중요하다.

Fig. 8. Single scenario based data leakage detection

4.3 보안솔루션별 정보유출 시나리오 도출 및 적용 결과

본 논문에서는 효율적인 내부정보유출 방지 통합 모니터링을 위한 방안으로 단위 보안솔루션의 기능을 우회하거나 회피하여 발생할 수 있는 정보유출 단일 시나리오를 사용자 행위 모델링을 이용하여 PC보안/매체 제어 솔루션 13개, DRM 솔루션 14개, 유해사이트 차단 솔루션 7개를 도출하였다. 그리고 도출한 정보유출 단일 시나리오를 각 보안솔루션에서 발생한 로그정보의 정보유출 시나리오정보를 이용하여 PC보안/매체 제어 솔루션 11개, DRM 솔루션 12개, 유해사이트 차단 솔루션 5개를 적용하였다. 이처럼 도출한 정보유출 단일 시나리오가 모두 적용 가능한 것은 아니다.

이는 보안솔루션에서 발생하는 로그정보가 존재하지 않으면 적용하기가 어렵기 때문이다. 하지만 적용하지 못한 시나리오는 모두 건수, 용량, 임계치/통계치 관련된 시나리오로 보안솔루션에서 개별 적용이 어려워도, 추후 통합 모니터링 시스템의 뷰어화면에서는 이를 적용할 수 있다. PC보안/매체 제어, DRM, 유해사이트 차단 솔루션의 기반으로 단일시나리오를 적용하였을 때의 탐지 화면은 Fig. 8과 같다.

5. 결 론

최근 지속적으로 발생하는 기업 및 기관의 내부정보유출 사고에 대응하기 위해서는 기 구축된 보안솔루션을 통합적으로 모니터링할 수 있는 체계가 구축되어야 한다. 따라서 기업 및 기관에서는 정보유출 방지의 필요성을 인식하고 다양한 보안솔루션을 도입하여 관리하고 있다. 그러나 내부정보유출 방지 통합 모니터링 체계가 아닌, 특정 시스템의 단발성 도입과 이를 개별 관리 및 모니터링하면서 한정된 자원과 인력으로 다양한 보안솔루션에 대한 모니터링을 수행하기에는 어려움이 있다.

따라서 본 논문에서는 효과적인 내부정보유출 방지 통합 모니터링 체계를 위해 보안솔루션별 정보유출 단일 시나리오를 도출하고 적용하는 연구를 진행하였다. 하지만 신뢰성을 보장받기 위해서는 다양한 보안솔루션에 따른 정보유출 시나리오의 정규화 작업과 지속적인 개선 및 관리가 반드시 수반되어야 한다. 또한 내부정보유출 방지를 위해서 기술적 관점의 연구방안도 중요하지만 무엇보다도 모든 기업 및 기관 구성원이 중요 정보는 스스로 지키고자 하는 보안 의식 강화와 기업 및 기관의 환경에 맞추어진 정책 및 보안 프로세스가 필히 상반되어야 한다.

향후 연구로는 단일 시나리오 이외에 연계 시나리오까지 고려한 내부정보유출 방지 통합 모니터링 및 내부정보유출 방지 모니터링의 프레임워크에 대한 연구가 필요하다.

References

[1] National Industrial Security Center, http://service12.nis.go.kr
[2] Privacy Information Protection Portal, http://www.privacy.go.kr
[3] Jung-Ho Eom, Seon-Ho Park, and Tai M. Chung, “An Architecture of Access Control Model for Preventing Illegal Information Leakage by Insider,” *Journal of The Korea Institute of Information Security and Cryptology*, Vol.20, No.1, pp.59, 67, 2010.
[4] Dae-Sung Lee, Jason Kim, and Kui-Nam Kim, “Research and Technology Trends for Prevention of Data Leakage,” *Review of The Korea Institute of Information Security and Cryptology*, Vol.20, No.1, pp.56-65, 2010.
[5] Hang-Bae Chang, “The Design of Information Security Management System for SMEs Industry Technique Leakage Prevention,” *Journal of Korea Multimedia Society*, Vol.13, No.1, pp.111-121, 2010.
[6] Ji-Hoon Song, Si-Jin Lee, “A Study of Information Security Measures Requirements Analysis Considering Insider Threats,” *Proceedings of the conference on Korean Society for Internet Information*, pp.399-404, 2010.
[7] Song-Young Kim, Joseph Kim, Jong-In Lim, and Kyung-Ho

Lee, “A study on the security policy improvement using the big data,” *Journal of The Korea Institute of Information Security and Cryptology*, Vol.23, No.5, pp.969-976, 2013.

[8] Jang-Su Park, Jung-Hyun Park, Yong-Suk Kang, and Im-Yeong Lee, “A study on Scenario Design Methodology for Prevention of Information Leak by Using Modeling of User Behavior,” *Proceedings of the conference on Korea Information Processing Society*, Vol.20, No.1, 2013.

[9] Jang-Su Park, Yong-Suk Kang, and Im-Yeong Lee, “A Study on The Management Plan for Prevention of Information Leak by Using Call-out,” *Proceedings of the conference on Korea Information Processing Society*, Vol.21, No.1, 2014.

[10] Jang-Su Park, Im-Yeong Lee, “A Study on Log Analysis Plan for Prevention of Information Leak Security Solution - focusing at a Single Scenario for Information Leak,” *Proceedings of the Korea Institute of Information Security and Cryptology Chungnam Conference*, 2014.

박 장 수

e-mail : pjswise@sch.ac.kr

2004년 순천향대학교 정보기술공학부(학사)

2006년 순천향대학교 컴퓨터학과(석사)

2006년~현 재 순천향대학교 컴퓨터학과 박사과정

관심분야 : 인증, 전자서명, 내부정보유출 방지

이 임 영

e-mail : imylee@sch.ac.kr

1981년 홍익대학교 전자공학과(학사)

1986년 오사카대학 통신공학전공(석사)

1989년 오사카대학 통신공학전공(박사)

1985년~1994년 한국전자통신연구원 선임연구원

1994년~현 재 순천향대학교 컴퓨터소프트웨어공학과 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안