소명을 이용한 내부정보유출 방지 관리 방안에 대한 연구+

박장수*, 강용석**, 이임영*
*순천향대학교 컴퓨터소프트웨어공학과
**인포섹(주)
e-mail:[pjswise, imylee]@sch.ac.kr, yskang@skinfosec.co.kr

A Study on The Management Plan for Prevention of Information Leak by Using Call-out

Jang-Su Park*, Yong-Suk Kang**, Im-Yeong Lee*
*Dept of Computer Software Engineering, SoonChunHyang University
**Infosec

요 약

최근 정보유출 피해사례가 빈번히 발생하고 있으며, 발생 건수 중 대부분이 내부자에 의한 고의 또는 실수로 발생하는 경우가 대부분이다. 이를 방지하기 위해 기관 및 기업에서는 다양한 보안 솔루션을 도입하여 구축해서 운영하고 있다. 그러나 독립적으로 보안솔루션이 운영 및 관리되기 때문에 상관분석의 어려움으로 통합적인 내부정보유출 모니터링이 불가능하다. 또한 제한된 리소스로 과도하게 발생하는 보안 이벤트를 모니터링하여 내부정보유출을 탐지하고 관리하기에는 어려움이 있다. 따라서 본 논문에서는 사용자 본인이 보안 정책에 위반되는 행위를 했을 시 “어떠한 목적으로 보안위반 행위를 하였는지” 파악하기 위해 소명절차를 이용한 내부정보유출 방지 관리 방안에 대해 연구하고자 한다.

1. 서론

최근 정보유출 사고가 연이어 발생하면서 사회적 이슈가 되고 있다. 산업기밀보호센터의 기밀 유출 통계에 따르면 전기전자, 기계, 정보통신, 화학, 생명공학 등 다양한 분야에서 정보유출이 발생되었고, 무단보관이나 개인의 영리를 위한 내부 공모를 통해 문서 유출이 가장 많이 발생한 것으로 조사되었다[1]. 또한 1월 국내 대표적인 카드회사 중 국민카드, 롯데카드, 농협카드에서 약 1억 4천만건의 개인정보 유출이 발생하는 대참사가 발생하기도 하였다. 이는 신용평가회사의 한 직원이 고객정보를 이동식 저장장치(USB: Universal Serial Bus)에 담아 유출을 한 것으로 밝혀져 사회적으로도 큰 충격을 주었다.

이처럼 내부에서 외부로 내부정보가 유출되는 것을 해결하기 위해 기관 및 기업에서는 문서 암호화, DRM(Digital Rights Management), 매체제어, DLP(Data Leakage/Loss Prevention), 유해 사이트 차단, 메일 및 메신저 모니터링 솔루션, 출입통제 시스템 등 다양한 보안 솔루션을 도입하여 이를 관리하고 있다. 하지만 이러한 보안 솔루션들은 기업 내에서 각각 별도로 관리 및 운영되기 때문에 상호 연계가 되지 않고 과도하게 발생하는 보안 이벤트로 보안담당자가 이를 통합하여 정보유출을 탐지하고 관리하기에는 어려움이 따른다. 이에 내부정보유출 방지를 위한 근본적이고 효율적인 대책 마련이 필요하다[2].

따라서 본 논문에서는 보안 정책에 위배되는 행동을 시도하였거나 위반 시 발생한 이벤트에 대해 사용자가 소명을 하고 이를 상위결재권자의 결재를 통해 내부정보유출 방지 방안을 제시하고자 한다. 본 논문의 구성으로, 2장에서는 최근 발생한 내부정보유출 사례에 대해 알아본다. 3장에서는 내부정보유출 경로 및 유출 경로에 따른 보안기술들을 정의하고, 4장에서는 위협 이벤트에 따른 소명 및 결재를 이용하여 내부정보유출 방지 관리 방안을 제시한다. 마지막으로 5장에서는 결론을 맺는다.

2. 국내 내부정보유출

2.1 산업 기술 유출 사례

국내 전자업체 기술마케팅부 부장과 팀장이 기술개발을 담당하며 연구비 공금횡령 사실이 자체 감사에서 적발되자 회사 PC에 접속하여 최대용량 빌딩용 첨단 에어컨 연구결과물을 노트북에 전량 복사한 후 연구 자료가 담긴 파일박스와 함께 불법 반출한데 이어 중국으로 유출을 시도하다 적발된 사례로 임직원의 출입통제 및 기밀정보에 대한 접근제어와 집중관리대상자의 필요성을 입증해주는 사건이다[3].

국내 디스플레이업체에서 근무하던 연구원이 퇴사전 비인가 USB를 이용하여 첨단 디스플레이 기술 자료를 무단 유출 후 중국 회사로 전직하여 기술자료 유출한 사례

+ 본 논문은 중소기업청에서 지원하는 2014년도 산학연협력 기술개발사업(No. C0119289)의 연구수행으로 인한 결과물임을 밝힙니다.

로 내부직원대상 기술 유출 경각심 제고 및 보안 시스템 강화가 지속적으로 필요함을 입증해주는 사건이다[3].

국내 반도체 제조회사에 반도체 장비를 납품하는 협력업체 직원이 A/S 등을 빙자해 영업비밀 서류를 절취하거나 친분을 이용해 영업 기밀을 빼내는 수법으로 국가 핵심기술로 지정된 반도체 핵심기술을 해외로 유출하다 적발된 사례로 협력업체 직원에 의해 이루어졌다는 점에서 협력업체에 대한 보안관리 강화의 필요성을 입증해주는 사건이다[3].

2.2 개인정보 유출 사례

카드회사 개인정보 유출은 역대 최대 규모로 KCB(KOREA CREDIT BUREAU)의 내부 직원이 카드부정사용시스템 개발 프로젝트를 담당하면서 각 카드사(국민카드, 롯데카드, 농협카드)에 파견 다니며 고객정보에 접근할 수 있었고, 고객정보를 이동식저장장치(UBS)에 몰래 담아 약 1억 4천만건의 개인 정보(이름, 주민번호, 주소, 휴대전화, 직장명, 카드이용실적금액, 카드결제계좌, 연소득, 카드신용등급, 신용카드 번호 및 유효기간 등)를 유출한 사례로 사회적으로 큰 파장을 주었다. 이는 과도한 고객정보 공유와 허술한 보안 의식 및 시스템 접속 및 활용에 대한 접근 통제 및 계정관리 시스템 부재로 초래한 결과이다[4-6].

KT통신사 개인정보 유출은 정상적인 영업대리점이 고객정보시스템을 조회하는 것처럼 가장해 5개월간 약 870만건의 개인정보(이름, 휴대전화, 주민등록번호, 기기명, 요금제, 요금액, 기기변경일 등)를 유출하여 텔레마케팅에 사용되었다. 이는 대리점 관리 시스템의 부재뿐만 아니라 사용자 인증뿐만 아니라 Device 인증과 이상행위에 대한 검증이 미비하여 초래한 결과이다.

GS칼텍스 고객정보 유출은 자회사에서 근무하는 직원이 고객들의 개인정보 DB에 접근할 수 있는 권한을 이용하여 1125만건의 개인정보를 자신의 업무용 컴퓨터로 빼돌려 금품을 노리고, 언론에 제보 했다가 GS칼텍스 수사의뢰로 검거되었다. 이는 내부직원들의 보안의식 부족과 윤리교육의 부재, DB 접근통제 및 감사 시스템 미비로 초래한 결과이다.

<표 1> 국내 산업 기술 유출 사례

년도	유출 사례
2010	· 국내 3D 기술 중국 유출사건 · 반도체 핵심기술 해외 유출사건 · 양문형 냉장고 설계기술 중국 유출기
2011	· 국내 첨단 디스플레이 기술 중국 유출사건 · 의약품 원료제조기술 중국 유출사건 · 중국인 연구원 가전기술 해외유출 기도 사건
2012	· 첨단 에어컨 핵심기술 중국 유출 기도사건 · 태양전지 생산 장비 제조기술 해외유출사건 · 차세대 디스플레이 기술 해외유출 사건 · 선박부품 설계기술 중국 유출 사건

<표 2> 국내 주요 개인정보 유출 사례

시기	유출대상	유출건수	유출경로
2008.02	옥션	1800만건	외부해킹
2008.09	GS칼텍스	1125만건	내부직원
2011.04	현대캐피칼	175만건	외부해킹
2011.07	네이트	3500만건	외부해킹
2012.05	KT	870만건	외부해킹
2014.01	카드3사	1억400만건	외주업체
2014.03	KT	1200만건	외부해킹

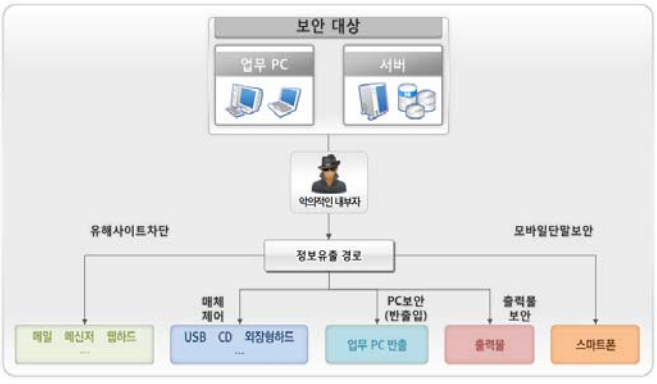
3. 내부정보유출 경로 및 정보유출방지기술

3.1 내부자 정보유출 경로

기업/기관 내 정보인프라 구축이 활발히 이루어짐에 따라 디지털화된 내부 주요 정보가 외부로 유출할 수 있는 형태는 ① 인터넷을 통한 유출 ② 저장장치를 통한 유출 ③ 프린터 출력에 의한 유출 ④ 노트북, 태블릿 PC 외부 반출을 통한 유출 ⑤ 스마트폰을 통한 유출로 구분할 수 있다.

3.2 인터넷을 통한 외부 유출 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 유해한 사이트에 대해 웹사이트 차단 솔루션, E-mail 모니터링 솔루션, 메신저 모니터링 솔루션 등이 존재하며, 해당 솔루션으로 게시판, 블로그 등 웹사이트 파일 업로드 정보, 통제된 웹 사이트 접근 시도 정보, 웹사이트 접근 정보, 전송되는 첨부파일 정보, 대화 정보 등을 보안 관리자가 정기적인 점검을 통해, 외부로의 파일 전송되는 것을 차단하거나 모니터링하고 있다.



(그림 1) 정보유출 경로별 대응방안

3.3 휴대용 저장장치를 통한 외부 유출 대응

인터넷 망을 이용한 외부 전송 경로를 통해 파일이 유출 되는 것 외에 주요한 유출 수단은 PC에 저장된 주요 정보가 저장 매체(USB, 외장형하드, CD, 스마트폰 등)를 통해 유출되는 것이다. 이를 해결하기 위해서 매체 제어 솔루션을 통해 저장 매체 사용 이력 정보, 통제된 매체 사용 시도 정보 등을 관리자 화면에서 확인함으로써, 유출되는 것을 모니터링하고 있다.

3.4 출력물을 통한 외부 유출 대응

일반적으로 업무 진행시 무분별한 출력행위가 빈번히 일어나고 있다. 하지만 이미 출력된 주요정보는 복사되거나, 스캔과정을 통해 파일로 재 저장되어 유통이 손쉽게 이루어진다. 이에 많은 기업 및 기관에서는 출력물관리 시스템을 도입하여 출력물에 대한 모니터링을 진행하고 있다. 또한 출력물에, 인쇄자, 출력 일시, 문서 제목, 회사 로고 등 출력물에 워터마킹 기술을 적용하여 출력물이 외부로 유출되는 것에 대해 대응하고 있다.

3.5 업무용PC 반출을 통한 외부 유출 대응

최근 사무 공간 및 이동의 편의성을 고려하여 노트북 사용이 확산되었다. 이러한 업무용으로 사용된 노트북의 무단 외부 반출을 통제하기 위한 방안으로 PC반출 시스템을 구축하여, 보안 담당자로부터 승인 절차를 통해서만 외부로 반출되도록 하고, 승인되지 않은 외부 반출 시에는 노트북 화면이 잠겨 사용할 수 없도록 하여 정보 유출 되는 것을 대응하고 있다.

3.6 스마트폰을 이용한 외부 유출 대응

최근 IT의 발전으로 언제 어디서나 시간과 장소에 구애 없이 업무를 처리함으로써 효율적인 업무환경을 구현할 수 있도록 스마트워크가 확대되고 있다. 이에 따라 스마트모바일 기기를 통해 정보유출이 가능하다. 따라서 모바일 보안 솔루션으로 단말관리, 분실/도난관리, 단말제어, 어플리케이션 관리 기능으로 정보 유출 되는 것을 대응하고 있다.

4. 소명 및 결재를 이용한 내부정보유출 방지

위와 같이 내부정보유출 경로를 보호하기 위해서 기업/기관에서는 각 경로별 또는 복수의 경로에 다양한 보안 솔루션을 도입하여 정보유출 방지 체계를 구축하고 운영하고 있다. 정보유출 방지 체계는 물리적 보안, 관리적 보안 그리고 기술적 보안의 세 가지 구성요소를 가지고 있다. 이 세 가지가 정보유출 사고에 대해 예방, 탐지. 대응 행위의 상호작용을 하게 된다.

본 연구에서는 내부정보유출 방지를 위한 보안솔루션들의 구축을 가정 하에, 사용자가 실수 또는 고의로 보안정책에 위배되는 행위를 함으로써 각 보안솔루션으로부터 이벤트가 발생하면, 일정기간 내에 사용자가 어떠한 업무 또는 목적을 가지고 보안행동에 위배하였는지 명확하게 소명을 하고, 상위 결재권자에게 결재요청 함으로써 정보의 접근 사실과 위험행동에 대한 근거를 마련하고자 한다.

또한, 정보보안 담당자의 업무를 줄여줌으로써 정보유출 행위 추적 및 조치에 대해 효율적인 대응을 할 수 있도록 한다.

4.1 소명 및 결재를 이용한 정보유출방지 관리프로세스

① IT Infra : 정보유출 방지를 위해 로그 수집할 대상(정보자산 및 보안솔루션)을 선정한다. 선정된 대상에서 발생하는 로그명세를 명확하게 분석 후, 추가할 수 있는 정보유출 방지 시나리오를 도출한다.

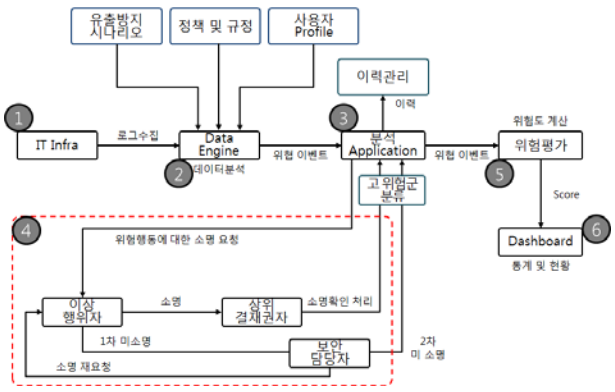
② Data Engine : 정보유출방지 시나리오, 정책 및 규정, 사용자 Profile 정보를 이용하여 수집된 로그에서 위험행동 여부를 판단한다.

③ 분석 Application : 위험행동을 한 사용자에게 소명을 요청하며, 소명 여부 및 내용에 따라 고 위험군을 분류한다. 마지막으로 위험행동이 발생 시 이력 관리를 한다. 이력관리를 통해 집중관리 대상자를 선정한다.

④ 소명 후 결재 : 위험행동을 한 사용자는 일정기간 내에 소명을 하고 상위결재권자에게 결재 요청을 한다. 일정기간 설정은 기업 및 기관의 법규 및 규정에 맞추어 설정한다.

⑤ 위험 평가 : 소명 여부 및 발생 이벤트의 위험도 Level, 집중관리 대상자 여부, 과거 이력 및 임계치 정보 등을 고려하여 정보유출 위험 Score를 계산한다.

⑥ Dashboard : 내부정보유출 방지 모니터링을 위한 통합 Dashboard로 내부정보유출 위험도 현황, 중요 및 기밀정보 접근 현황, 시나리오별 발생 추이 현황, 부서별 이상행위 누적건수 등 각 기관 및 기업에 적합한 정보를 보여준다.



(그림 2) 소명 및 결재를 이용한 유출방지 흐름도

(그림 3) 소명 및 결재 상세 화면 Sample

4.2 소명 및 결재 상세 화면

(그림 3)에서와 같이 크게 결재정보와 소명정보로 나눠진다. 소명정보에는 위협이벤트에 따라 위험행동 구분, 시나리오명, 사번, 시나리오 코드, 위험행동 발생시간 등 정보가 보여 진다. 위험행동을 한 사용자는 소명요청을 받았다면, 해당 내용 확인 후, 일정기간 내에 소명내용을 입력 후 상위결재권자에게 결재승인 요청을 해야 한다. 소명내용은 구체적으로 명확하게 어떠한 업무목적으로 보안에 위배되는 행동을 하였는지 입력해야 한다.

결재정보에는 위반행위 사용자가 결재승인요청, 상위결재권자(위반행위 사용자의 팀장, 관리부서의 담당자 및 팀장)의 결재 및 반려기능이 있다.

5. 결론

IT 기술의 발달에 따라 기업의 구성원은 언제 어디서나 편리하게 사내정보에 접근할 수 있게 되었으나, 내부정보유출 방지는 더욱 힘들어져 기업 및 기관의 중요 정보 유출시 막대한 손실을 주고 있다. 그동안 기업 및 기관에서 정보유출 방지를 위해 법, 규정, 제도 마련에 많은 노력을 기울였으나 정보유출 사건 사고는 지속적으로 발생하고 있다.

본 연구에서는 정보유출 방지를 위한 보안 솔루션들을 통합하여 내부자에 의한 정보유출을 탐지하고 관리할 수 있는 통합 보안 모니터링 체계에서 위협 이벤트 발생 시 소명 및 결재를 이용하여 어떠한 목적으로 위험행동을 한 것인지 판단할 수 있고, 사용자로 하여금 보안위반행동을 했다는 것에 대해 경각심을 줄 수 있다 또한 위협 이벤트 발생시 마다 보안담당자가 확인해야 하는데, 소명 및 결재를 이용하여 명확한 업무로 인해 발생할 수 있는 이벤트에 대한 것들은 집중적으로 살펴보지 않아도 되기 때문에 업무의 효율성을 가져올 것으로 기대된다.

하지만 무엇보다도 모든 기업 및 기관 구성원이 중요정보는 스스로 지키고자 하는 보안 의식 강화가 필요하다. 또한 내부정보유출 모니터링은 보안솔루션에서 발생한 이벤트를 이용하여 시나리오 및 Rule을 적용하고 이상행위를 탐지하기 때문에, 정보유출 방지 시나리오 설계가 중요한 부분 중 하나로 지속적인 개선 및 관리가 반드시 수반되어야 한다.

참고문헌

[1] 산업기밀보호센터, “기술유출 통계” http://service12.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00

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

[3] 산업기밀보호센터, “기술유출 사례” http://service12.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_2&menu=AAB00

[4] 금융위원회, http://www.fsc.go.kr

[5] 금융감독원, http://www.fss.or.kr

[6] 금융결제원, http://www.kftc.or.kr/

[7] 개인정보보호 종합지원 포털, “개인정보 침해사례”, http://www.privacy.go.kr/nns/ntc/pex/personalExam.do

[8] 윤인수, “내부자에 의한 정보유출 방지를 위한 보안시스템 구축에 관한 연구,” 학위논문, 2007.

[9] 엄정호, 박선호, 정태명, “내부자의 불법적 정보 유출 차단을 위한 접근통제 모델 설계,” 한국정보보호학회 논문지, 제 20권, 5호, 2010.