http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.23, No.4, November 2018, pp.137-152
https://doi.org/10.7838/jsebs.2018.23.4.137

PC 이벤트 탐지 기능과 보안 통제 절차를 연계시킨 시나리오 기반 금융정보유출 위험 대응 모델에 관한 연구

A Study on a Scenario-based Information Leakage Risk Response Model Associated with the PC Event Detection Function and Security Control Procedures

이익준(Ig Jun Lee)*, 염흥열(Heung Youl Youm)**

초 록

기존 금융정보유출 행위를 탐지하기 위해 보안솔루션에서 생성한 행위 로그를 수집하여 패턴분석으로 정보유출 이상행위를 탐지하고 차단하는 활동에서 발생되는 한계점을 극복하고, 효과적으로 대응하기 위한 방안으로 첫 번째, PC에서 정보유출 경로(외부에서 읽기, 외부로 저장하기, 외부로 전송하기 등)로 이용되는 PC내 실행 프로그램들을 실시간으로 모니터링하고 두 번째, 해당 프로그램이 실행하는 시점에 연관된 보안 통제 프로세스와 상호 연동하여 정상・통제예외・통제우회 행위인지를 파악한 다음 마지막 단계인 시나리오 기반으로 생성한 처리 절차를 통해 금융정보유출 위험을 통제할 수 있는 위험 관리 모델을 제안함으로서 정보보호 측면의 보안성 강화 및 업무 효율성 향상의 기대효과를 창출하고자 한다.

ABSTRACT

It is a measure to overcome limitations that occur in the activity of detecting and blocking abnormal information leakage activity by collecting the activity log generated by the security solution to detect the leakage of existing financial information and analyzing it by pattern analysis. First, it monitors real-time execution programs in PC that are used as information leakage path (read from the outside, save to the outside, transfer to the outside, etc.) in the PC. Second, it determines whether it is a normal・controlled exception・control circumvention by interacting with the related security control process at the time the program is executed. Finally, we propose a risk management model that can control the risk of financial information leakage through the process procedure created on the basis of scenario.

키워드 : 정보유출시나리오, 위험분석, 엔드포인트 보안, EDR, DLP, 정보유출로그패턴분석, 위험관리
Information Disclosure Scenario, Risk Analysis, Endpoint Security, EDR, DLP, Information Leakage Log Pattern Analysis, Risk Management

* First Author, Department of Information Security, Graduate School, Soonchunhyang University (leemsjij@gmail.com)
** Corresponding Author, Department of Information Security, Graduate School, Soonchunhyang University (yyoum@sch.ac.kr)
Received: 2018-10-16, Review completed: 2018-11-26, Accepted: 2018-11-27

1. 서 론

금융회사의 망분리 환경에서 네트워크 구간의 데이타 이동 경로 변화와 암호화 전송 그리고 엔드포인트 영역에서 발생되는 신규 위협 등 금융정보유출 위협 경로에서 이상 행위 발생 시 연관된 통제 프로세스와 연관 정보들을 상호 연결시켜 보안 승인 통제 하에 실행되는 행위 인지 또는 보안 승인 통제의 예외 또는 우회 상황에서 발생된 행위인지를 파악한 다음 시나리오 기반으로 구성된 항목을 검증하여 금융정보유출 위험을 식별 및 차단함으로써 효과적인 보안통제와 업무 효율성 향상의 기대효과를 창출하고자 한다.

2. 관련 보안솔루션 연구

정보유출이란 개인의 경우 개인에 대한 신체적, 경제적, 사회적 사실・판단・평가 및 도용이 가능한 개인에 관한 고유 정보(성명, 주민등록번호 등), 기업의 경우 기업에 대한 경제적, 사회적 가치를 가지고 있는 물리적(핵심 장비, 결과물 등), 논리적(핵심 기술, 기업 기밀 등)정보를 다양한 이익을 위해 정보의 주체가 동의하지 않은 상태로 무단으로 가져가는 행위를 말한다[11].

전통적인 금융정보유출 보안 관리 방법은 개인 정보 또는 중요 정보를 암호화하고 개인 정보가 보관된 시스템에 대한 접근 통제 및 권한 관리를 통해 금융정보유출을 예방하고 있다. 그리고, 금융정보 내부 유출을 방지하고 관련 법률을 준수하고자 목적성에 맞는 다양한 보안 솔루션을 도입하여 운영하고 있다. 특히 주요 금융기관에서는 특정 보안 솔루션을 도입할 경우 타 금융기관은 이러한 사례를 바탕으로 비슷한 역할의 보안 솔루션을 사용하여 구축 운영하고 있다. 이로 인해 금융 업계는 일정 수준 이상의 보안 솔루션을 도입하여 운영하고 있다.

2.1 DLP(Data Loss Prevention) 보안 솔루션

DLP(Data Loss Prevention)시스템은 보호하고자 하는 영역을 기준으로 Endpoint DLP, Network DLP로 구분할 수 있으며 보호하는 영역이 구분되어있다. DLP 시스템은 3가지의 탐지 기술을 가지고 있다. 이는 이용자 정의 탐지 기술, 구조적 데이터 탐지 기술, 비정형적 데이터 탐지 기술로 나눌 수 있다[8].

첫째, 이용자 정의 탐지 기술(described content matching)정규 표현식, 키워드 데이터 식별자(주민등록번호, 신용카드 번호 등), 파일 속성(파일 크기, 파일 형식, 파일 이름 등), 시스템 이름, IP, URL 등 일반적인 Endpoint 시스템 내부에 있는 콘텐트를 탐지 및 차단할 수 있는 기술이다.

둘째, 구조적 데이터 탐지 기술(Exact Data Matching) 데이터베이스 테이블이나 개인 정보나 은행 계좌번호, 주소 등과 같은 구조적 형태를 가지고 있는 데이터를 기반으로 탐지하는 기술이다.

셋째, 비구조적 데이터 탐지 기술(Indexed Data Matching)은 워드문서, PDF, CAD 도면, 개발 소스 등과 같은 비구조적 형태를 가지고 있는 데이터 파일을 DLP 시스템에서 인덱싱(Indexing)하여 그 데이터를 기반으로 비교하여 탐지하는 기술이다.

따라서, DLP 시스템에서는 위의 3가지 탐지 기술을 사용하여 정책을 생성하고 해당 정책의 목적에 맞는 대응을 설정할 수 있다. 차단과 이용자 취소, 그리고 알림, 원본 파일 저장 기능 등을 통하여 탐지에 대한 대응 설정이 가능하다. 차단 대응 규칙은 정책에서 설정한 탐지 기술에 매칭되는 행위가 있을 경우 그 행위의 모든 후속 작업을 중지시키는 동작을 하며, 이용자 취소 대응 규칙은 설정한 탐지 기술에 매칭되는 행위의 후속 작업을 대기 상태로 만들고 이용자 취소 대응 규칙에서 설정한 목적을 입력 후 후속 작업을 진행한다.

그리고 알림 대응 규칙은 정책에서 설정한 탐지 기술에 매칭되는 행위를 그대로 후속 작업을 진행하도록 하며 Endpoint 시스템에 알림 팝업을 통하여 안내 메시지를 띄운다.

2.1.1 망연계 보안 솔루션

정보통신 망 이용촉진 및 정보보호 등에 관한 법률에서의 '망분리 의무화' Compliance 준수를 위하여 망분리를 구축하고 업무망과 인터넷망 간의 파일전송을 위하여 망 자료 연계 솔루션을 도입하게 되는데, 주요 기능으로는 분리된 망 사이의 시스템 간 데이터를 연계 할 수 있는 송·수신 단방향 전송 기능과 파일 업로드·다운로드 허용 통제 권한에 대한 보안정책을 통해 파일을 내·외부 전송하고 전송 내역 및 사용 이력을 감사하는 기능이 있다.

2.1.2 DRM(Digital Right Management) 보안 솔루션

업무처리로 발생할 수 있는 문서 형태의 한글(.hwp), 워드(.word), 파워포인트(.pptx) 파일들을 암호화하여 허용된 권한 내에서만 사용하도록 제어하고자 DRM(Digital Right Manag ement)를 도입하는데, 주요기능으로는 문서 암호화, 문서 출력물 보안, 문서반출 제어 등이 있다. 그리고, DRM을 적용하면 문서를 열람만 해도 되는 사람에게는 열람 권한만 줄 수 있고,문서유통을 한시적으로 제한할 수도 있다. 기업 간의 문서유통에서 받는 사람, 혹은 특정 범위 내에서만 해당 문서를 볼 수 있도록 지정할 필요가 있다[11].

2.1.3 EDR 보안 솔루션

최근 보안 업계에서 떠오르는 용어가 EDR (Endpoint Detection & Response)이다. EDR이란 엔드포인트 레벨에서 지속적인 보안 위험 모니터링과 대응 기능을 제공 하는 보안 솔루션으로 정의하고 있다. 또한, 가트너[3]에서는 EDR 솔루션을 아래 4가지 기능으로 설명하고 있다.

첫째, 보안사고 탐지(Detect Security Incident) 영역에서 엔드포인트 행위(파일, 프로세스, 네트워크, 레지스트리)를 지속적으로 모니터링 함으로써 이상 행위를 탐지해야 하며, Known 및 Unknown 악성코드 탐지, Fileless 악성 코드 탐지 및 이동 매체 파일 실행, 공유 폴더 생성, 무선LAN 접근 등을 탐지하여야 한다.

둘째, 엔드포인트에서의 보안사고 통제(Contain the Incident at the Endpoint)영역에서는 악성코드 확산 범위 확인 및 횡방향 움직임(Lateral Movement)등의 모니터링을 통해 피해 확산을 방지한다.

셋째, 보안사고 조사(Investigate Security Incident)를 위해 타임라인 기반파일, 프로세스, 네트워크, 레지스트리 조사와 악성코드 유입 경로 조사 및 내부 확산 여부에 대한 조사를 한다.

넷째, 엔드포인트 치료(Remediate Endpoint to a Preinfection State)영역에서 네트워크 차단 기능 제공 및 파일 삭제 기능을 제공하도록 가이드하고 있다.

그리고, EDR 솔루션은 각 PC에 에이전트를 설치하도록 하는데 이 에이전트가 하는 역할은 엔드포인트 단에서 정보유출 관련 행위 기반의 위험을 탐지하고 대응하는 것이다.

즉 네트워크나 USB 등의 모든 경로를 통해 새로 유입되는 파일을 모두 탐지한다. 또한 어플리케이션을 통해 이용자가 취하는 모든 행동에 대해서도 감시하고 정리한다. 이 정리된 것을 바탕으로 자체적인 패턴 DB가 존재하면 그 패턴 DB에서 정리된 내용과 비교하여 문제가 되는 부분이 있다고 하면 막고, 혹은 격리하거나 제거한다.

그리고 패턴 DB에 존재하지 않으면 수집 및 분석 서버로 전송하고 수집 및 분석 서버는 각 PC에서 전송한 데이터(정리된 내용)를 빅데이터 시스템으로 모아서 분석하고 분석된 내용을 기반으로 기계학습을 진행하며 이렇게 진행된 내용을 기반으로 위험 여부를 기계학습을 통한 인공지능을 이용해 판별하게 되며 그 결과를 다시 해당 PC의 에이전트에 보내고 에이전트는 그 결과를 기반으로 막거나 격리, 혹은 제거를 한다[9].

대부분 금융회사에서 정보유출 예방을 위한 보안솔루션들을 사용하고 있으며, 중요정보가 포함된 문서파일을 보호하는 DRM 솔루션은 암호화된 파일에 대한 복호화 신청 및 승인을 위한 통제절차와 원활한 연계가 중요하지만 실제 승인한 내용(복호화문서 USB 복사)과 사용자의 행위(복호화문서 웹메일 발송)가 일치하지 않을 경우 검증이 명확하지 않다.

Division	Search and investigate incident data	Triage warning or suspicious activity detection	Suspicious Activity Detection	hreat Hunting or Data Exploration	Stop malicious activity
Carbon Black	●	●	●	●	●
Cisco AMP	●	◑	◑	●	●
Confer	●	●	●	◑	●
CounterTack	●	●	●	●	●
CrowdStrike	●	●	●	●	●
Cybereason	●	●	●	●	●
FireEye	◑	◑	◑	●	◑
Guidance	●	●	◑	◑	●
RSA ECAT	●	●	◑	◑	●
Tanium	●	●	◑	●	●
○ 약함, ◑ 평균, ● 강함					

〈Figure 1〉 Comparison of Key Features of EDR Solution

또한, 네트워크와 엔드포인드로 나눠서 구분하는 정보유출방지 솔루션(Data Loss Prevention)은 PC, 메신저, 외부 저장 매체(USB, 외장하드 등) 등 엔드포인트 영역에서 일어날 수 있는 금융정보유출 사고를 예방할 수 있는데, 만약 엔드포인트(PC)에서 중요정보 포함여부를 탐지하는 패턴을 우회하거나, 탐지파일을 압축 후 비밀번호를 설정하는 경우와 암호화된 파일인 경우 데이터 유출을 차단하기 어렵다는 한계가 있다.

그리고, 네트워크 DLP는 네트워크 통신을 분석해 차단하기 때문에 암호화된 트래픽 또는 파일에 대해 탐지 할 수 없다는 문제점이 있다.

마지막으로, PC EDR 솔루션에서 탐지하는 행위 패턴은 금융회사 정보유출 관련 내부통제 절차와 연계하여 보안통제 활동을 수행 하는 것보다 악성 코드(멜웨어, APT 등)의 행위를 탐지하고 추적 및 대응하는 부분에 집중적으로 구성되어 있다.

3. 선행 연구와의 차이점

시나리오 기반 정보유출 관련 선행연구로는 개인정보유출 모니터링을 위해 분석되어야 할

로그를 정의하고 대상조직을 분류함으로써, 내부자에 의해 유출되는 상황을 대비하기 위하여 PIMS의 개인정보 생명주기와 은행부문에서 발생 가능한 상황들을 고려한 시나리오와 이를 기반으로 개인정보유출을 모니터링 방법이 있다[1].

그리고, 보안 대상 솔루션을 선정하고 해당 로그를 분석하여 정보접근 행위, 정보수집 행위, 정보가공 행위, 정보이용 행위에 따라 단일 행위 시나리오와 복합행위 시나리오를 구성함으로써 개인정보유출을 모니터링방법이 있다[10].

또 다른 연구로, 조직 내 다양한 시스템의 로그를 빅 데이터화 하고 이를 분석하여 예측 분석 가능한 프레임워크를 제시하였는데, 예를들면 DRM 복호화 건수를 여러가지 기법(회귀분석, ARIMA, Holt-Winters, 이동평균법)으로 통계화 하여 예측값을 산출함으로써 개인정보유출을 모니터링하는 방법이다[6].

그리고, 데이터베이스 접근제어 솔루션에서의 접근통제, 접속속기록, 감사기록(SQL, 데이터 추출 건수 등), 정책 위반 시 발생하는 이벤트 통제 기능 등을 활용하여 SQL문의 개인정보 위험도를 산정(개인정보 데이터의 조회 건수, 개인정보 임계치 설정 등)함으로써 개인정보유출 모니터링 방법이 있다[2].

상기 논문들에서 제시하는 정보유출방지 방법은 일관되게 정보보호 솔루션들 중 내부 통제 시스템, 서버 보안, 개인정보 암호화, 이동매체 사용 등의 정보유출 통제 활동에 필요한 보안 솔루션들의 모니터링 로그 또는 데이터베이스 접속로그를 수집하여 행위 기반의 위험을 식별하거나 모니터링하는 방법을 제시하고 있다.

이러한 방법은 금융회사에서 운영하는 다양한 보안 솔루션들 마다 로그 형식과 내용이 다르고 정보유출 가능 경로에 따라 독립적으로 운용되고 있는 환경에서 보안관리자가 모니터링하기 어려울 정도로 많은 비정형화된 로그들이 생성된다는 문제점이 있다. 따라서, 로그분석 시 특정한 정보유출 관련 이벤트가 발생할 경우 보안솔루션 및 내부통제 절차에서 제시한 정책 등과 연계를 통한 통합 관리를 위해 일부 금융회사에서는 '통합 보안 로그관리 솔루션'을 추가로 구입 하거나, 별도로 자체 구축하여 운용하고 있다.

이는 비용 투자, 신규 보안 솔루션 운용 방법을 익히기 위한 시간 투자, 운용을 위한 별도의 물리적 공간과 관리 조직 및 인력 확보가 필수로 요구 된다.

또한, 정보유출 행위란 목적과 동기를 가지고 의도적으로 하는 행동을 말하는데 누군가의 금융정보유출 행위를 예측 하기위해 이용자의 다양한 행동에서 정보유출 관련 행위를 패턴으로 정형화한 시나리오를 '통합 로그관리 시스템'에 등록하여 운영한다. 그러나, 금융정보유출 사고 발생이 가능한 행위에 대한 경우의 수를 모두 시나리오로 반영하기에는 한계가 있다.

따라서, 현재 금융회사의 보안 솔루션들이 생성한 로그를 활용하여 금융정보유출이 가능한 행위패턴을 탐지하는 기존 방식이 아닌 PC EDR 에이전트와 같은 PC 기반의 프로그램에서 탐지된 정보유출 관련 이벤트를 통해 PC 소유자의 행위가 금융회사 내부통제 프로세스에서 디바이스 또는 매체에 대한 사용 권한 및 정보제공 승인을 받은 행위인일 경우 정보제공 행위를 허용한다.

만약, PC 소유자의 행위가 승인 받지 않은 비정상 행위일 경우에 차단 후 정밀조사 등 시

나리오에 맞춰 효율적으로 금융정보유출에 대한 모니터링을 실행함으로써 보안관리자의 업무 부담을 줄이고 이상 징후 판단의 효율성을 높일 수 있는 금융정보유출 위험 대응 모델을 본 논문에서 제안하고자 한다.

4. 금융정보유출 위험 관리 모델

본 논문에서는 위험분석 방법론 중 비정형 접근법(Informal approach)을 적용한 위험파악과 위험평가로 구성한다[5].

위험파악은 PC EDR과 같은 AGENT에서 탐지되는 정보유출 관련 이벤트 항목의 세부사항을 발견 및 식별하는 단계이다.

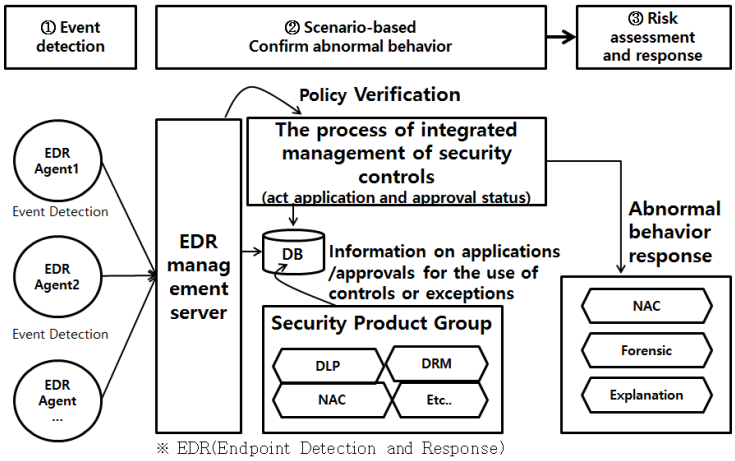
그리고, 위험평가는 위험이 파악된 이벤트 항목과 관련된 보안통제 프로세스를 연계하여 위험 등급을 부여하고 대응하는 시나리오 기반 금융정보유출 위험 관리 모델링을 <Figure 2>와 같이 3단계 절차를 통해 수행한다.

첫 번째, PC내 정보유출 관련 이벤트 탐지영역으로, PC 외부와 연계(외부에서 읽기, 외부로 저장하기, 외부로 전송하기 등)가 가능한 기능을 가진 PC내 실행 프로그램들을 실시간으로 모니터링 한다.

두 번째, 보안정책과 연계한 시나리오기반 비정상행위 확인 및 분석 영역은 PC 내에서 탐지된 행위와 '보안통제 프로세스'가 연계하여 보안 승인 통제 하에 실행되는 행위 인지 보안 승인 통제 예외 또는 우회 상황에서 발생된 행위인지를 파악한 다음 <Table 3>에서 제시한 '위험 시나리오'의 '금융정보유출 위험검증 항목'을 통해 위험을 분석한다.

그리고, 상기한 보안정책 연계 방법은 PC내 EDR Agent에서 제공하는 이벤트 정보와 보안제품별 통제 기능에서 제공하는 정책 허용·예외관련 정보를 매칭해서 보관된 데이터베이스(DB) 정보를 '보안통제 통합관리 프로세스'가 참조하는 방법으로 구성된다.

세 번째, 상기 분석결과에 따라 관리되는 위



〈Figure 2〉 Scenario-based Information Leakage Threat Detection and Response Model

험과 관리되지 않는 위험 그리고 잠재위험으로 분류한 위험등급을 기준으로 위험을 자동 또는 수동으로 평가하고 보안통제 우회 행위 파악 시 시나리오에서 제시한 대응 절차(포렌직, 소명 등)를 수행 한다.

4.1 시나리오 기반 금융정보유출 위험 대응 3단계 모델을 적용하기 위한 방법

본 절은 시나리오 기반 금융정보유출 위험 대응 3단계 절차를 단계별로 적용하기 위한 구체적인 방법을 제시한다.

4.1.1 금융정보유출 경로 분석 식별(1 단계)

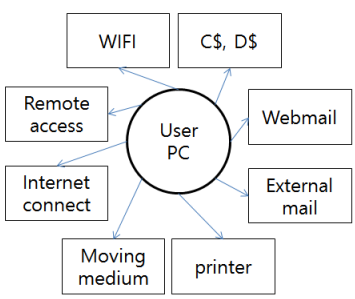
첫째, PC 중심으로 금융정보가 이동할 수 있는 경로를 <Figure 3>과 같이 확인하고, 각 경로에 대한 보안 환경을 파악한다.

여기서 보안환경이란 파일반출신청, USB 사용신청 등 보안통제 현황과 금융회사에서 사용하는 보안제품(NAC, DRM, 매체제어 등)의 현황을 말한다.

즉, PC내 정보유출 경로를 사용하는 행위와 보안제품별 통제(신청・승인 절차)현황은 다음과 같이 매칭이 가능하다.

- ○ 인터넷 사용 행위(보안제품; 망연계)
  - 통제: 인터넷망을 통한 파일 반입 및 반출 신청 및 승인
- ○ 특정 APP 사용 행위(보안제품: 방화벽, NAC, 불법프로그램 탐지솔루션)
  - 통제: 원격접속 사용 신청 및 승인
  - 통제: P2P 프로그램 사용 신청 및 승인
  - 통제: 비인가 프로그램 예외사용 신청 및 승인
- ○ 특정 중요파일 사용 행위(보안제품: DRM)
  - 통제: 보안문서 암호화 해제 신청 및 승인 (예: 상세절차 <Figure 3>, <Figure 4> 참조)
  - 통제: 대량 압축파일 사용 신청 및 승인
- ○ 특정 외부 URL 접근행위(보안제품: 웹키퍼)
  - 통제: 웹하드・웹메일 사용 신청 및 승인
- ○ 무선환경 접근행위(NAC, WIPS)
  - 통제: WIFI 등 사용 신청 및 승인
- ○ 공유폴드 접근행위(NAC)
  - 통제: C$, D$사용 신청 및 승인

그리고 이용자의 특정 행위에 대한 정상행위 여부를 판단하기 위한 금융회사 내부에서 외부 또는 내부에서 내부로 정보 이동에 대한 승인 프로세스는 ○○증권회사의 내부통제 절차[12]를 사례로 하여 <Figure 4>와 <Figure 5>에서 소개한다.



〈Figure 3〉 Financial Information Leakage Threat Route (Example)

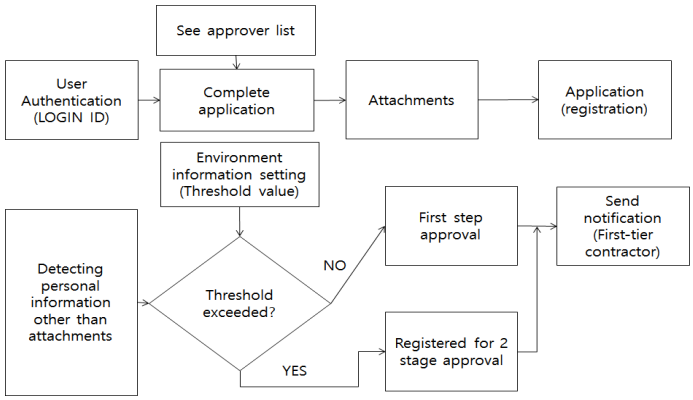
둘째, 금융정보유출 위험 예상 경로와 보안 현황 정보를 참조하여 PC에 센서 즉, EDR(Endpoint Detection & Response)과 같은 기능의 에이전트를 설치하여 금융정보유출 경로로 악용할 목적으로 특정 프로그램의 실행을 시도하는 행위를 탐지할 수 있는 항목을 정의한다.

〈Table 1〉 Status of Security Activities and Security Solutions

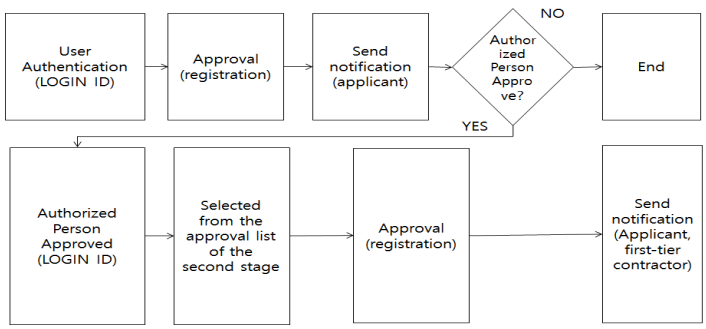
Division	Security Activity Status Information	Security Solution Status
Security Environment Information	Internet use behavior, Use of specific APP, Use of certain critical files, External URL access behavior, Wireless environment accessing behavior, Shared Fold Access behavior	NAC, DRM, Media Control ・DLP, Webkeeper, Firewall, Illegal SW Detection, Export Approval SYS, WIPS, Network Connection System

탐지 이벤트는 유저 행위 기반의 이벤트와 데이터 기반 그리고 시스템 기반의 이벤트로 구분할 수 있다[7]. 유저 이벤트는 P2P, 원격프로그램 등 비인가 프로그램의 실행을 탐지하고 데이터 이벤트는 파일을 복사하고 이동하거나 파일 압축 시 비밀번호를 설정하는 파일에 대한 특정 행위를 탐지하고 USB, 프린트 등 디바이스 사용 시 이벤트가 발생 한다.

그리고, 시스템 이벤트는 PC의 유저 영역에서 실행되는 프로그램을 우회하는 정보유출 관련 행위를 커널 영역에서 해당 프로세스를 모니터링 하고, 네트워크를 통한 외부 송수신 행위를 감시하는 기능을 제공한다.



〈Figure 4〉 Application Phase for Document Decryption



〈Figure 5〉 Authorization Steps for Decrypting Documents

〈Table 2〉 Detecting Events Related to PC Financial Information Leakage Risk〔12〕

Division	Event name	EDR detection method
USER Event	Internet access	Realtime (log)
	Remote access	Realtime (behavior)
	P2P program	Realtime (behavior)
	Unauthorized program	Policy Allowed/Exceptions/Blocked List
DATA Event	ZIP file	Realtime (behavior)
	Bulk archive	
	Copy/Move files	
	Attach webmail	
	Clipboard Copy	
	Download file	
	Using USB	
	Device Usage	
	Using print	
SYSTEM Event	Process exe	
	DLL image Load	
	Network events	
	Creating a binary file	
	Registry change	

4.1.2 금융정보유출 이상 행위 시나리오 도출 (2단계)

금융정보유출 경로에서 발생 가능한 이상 행위 식별은 PC내 특정 이벤트의 행위가 금융정보유출로 악용되는 시점에 신뢰 경계(권한 및 승인)를 넘으면 금융정보유출을 위한 이상 행위로 식별하도록 시나리오를 작성한다.

예를 들면, 내부통제 프로세스에서 이동매체 사용 권한 승인 여부와 DRM 암호화 해제 신청 및 결재 여부 등 파일 반출 시 승인 프로세스(<Figure 4>, <Figure 5> 참조)를 정상적으로 수행하였는지 여부가 정상행위와 비정상 행위를 판단하는 기준이 된다.

<Table 3>에서는 PC내에서 발생되는 정보유출 관련 이벤트와 내부 보안통제 프로세스가 연계한 금융정보유출 '위험 시나리오'를 기반으로 비정상 행위를 식별하는 방법을 제시하였다.

4.1.3 시나리오 위험 평가(3단계)

상기 '위험시나리오' 검증 단계에서 파악된 정보유출 위험 항목에 대한 위험 평가는 PC내 발생된 이용자의 정보유출 관련 행위가 내부통제 프로세스를 통한 권한 및 승인을 획득한 행위인지에 대한 여부가 위험평가의 가장 중요한 기준이 된다.

즉, 내부통제 프로세스로 정상적인 권한 및 승인을 받은 행위에 대해 이벤트가 발생한 상황은 관리되는 위험 이므로 대응이 용이하며, 관리되지 않는 위험 중 파악된 위험은 내부통제 프로세스를 통해 권한 및 승인 절차에서 예외가 허용된 이용자의 행위이지만 파일 변조, 압출파일 사용 여부 등 비인가행위 여부를 검증할 필요는 있다.

그리고, 관리되지 않는 위험 중 파악 안된 위험은 보안통제 정책 우회 또는 정보유출 활동 행위가 사전에 파악이 되지 않은 경우이므로 정보유출의 가능성이 있어 위험도를 높음으로 설정하였다,

또한, PC내 정보유출 접근경로에 대한 사용권한과 정보유출 관련 행위에 대한 승인도 받지 않은 이용자의 행위에 대해서는 잠재 위험으로 분류하고 위험도는 높음으로 설정하였다. 상기 한 위험 유형별로 특징을 고려하여 분류한 위험등급과 조치방법(포렌직 등)에 대해 <Table 5>에 제시하였다.

〈Table 3〉 Risk Scenario

Financial information leak event detection	Scenarios that identify risk of financial information leakage				
	NO	Access permission	Authorization of behavior	risk-job (high)	Verification item of financial information leakage risk[12]
Detecting the threat of financial information leakage on PC	1	With permission	Acknowledgment	Y/N	<Abnormal behavior of licensor: misuse and abuse> - Approve DRM release with non-approvers IP - If the file name contains special characters or characters such as 'Book' in the default title - Document content and file title are inconsistent. - Moving document with external export disapproval - If you are applying for a revocation of DRM, the source or application is unclear
	2	With permission	Un_approved		<Authorized person's abnormal behavior: Information leakage risk-TYPE I> -DRM release large file(20M ↑) -DRM release multiple files(50 cases) - Overdue application within a certain period <Behavior of unauthorized person: Risk such as hacker-TYPE II> - Malicious code infected - Whether to use the Internet for a certain period - Whether remote access program is executed - Does my personal information file on the PC exist? - Is the password set in ZIP file?
	3	No permission	Acknowledgment		<Unauthorized person's behavior: risk of information leakage by policy exception handler> - Approve DRM release with non-approvers IP - If the file name contains special characters or characters such as 'Book' in the default title - Document content and file title are inconsistent. - Moving document with external export disapproval - If you are applying for a revocation of DRM, the source or application is unclear - DRM release large file(20M ↑) - DRM release multiple files(50 cases) - Overdue application within a certain period - Excessive self-certification approval?
	4	No permission	Unapproved		<Behavior of unauthorized persons: hackers, etc.> - DRM release large file(20M ↑) - DRM release multiple files(50 cases) - Overdue application within a certain period - Excessive self-certification approval? - Malicious code infected - Whether to use the Internet at a certain time - Whether remote access program is executed - Does my personal information file on the PC exist? - Is the password set in the ZIP file?

그리고, 보안정책에 대해 허용 또는 차단 권한을 가진 정보보호 담당자와 보안정책 예외행위를 허용하는 승인권자(매체 사용, DRM 해제, 반출 승인 등) 그리고, IT 시스템에 대한 막강한 권한을 가지고 있는 시스템 관리자, 서버 담당자, 네트워크 담당자와 금융정보에 접근할 수 있는 DB담당자 그리고, 일반 직원으로 자신의 업무 수행을 위해 금융정보를 처리하는 개인정보처리자와 중요 단말 이용자를 금융 회사의 정보유출 고위험 직무로 구분하여 위험평가 시 특별 관리하여야 한다.

다만, 본 논문에서 위험분석 및 평가 방법으로 적용한 비정형 접근법(Informal approach)의 단점인 보안관리자의 경험을 중심으로 위험을 분석하고 평가할 경우 신규 위험과 같은 경험하지 못한 위험에 대해 대응이 미흡한 문제점은 <Table 4> PC내 주요행위 이벤트[12]의 예와 같이 최근 PC내 주요 행위를 탐지하는 기술이 계속 발전하고 있고 탐지항목 또한 다양해지고 있어 이러한 정보를 주기적으로 수집하여 '위험 시나리오'의 금융정보유출 이상행위 탐지항목에 신속하게 반영함으로써 보완이 가능하다.

〈Table 4〉 Major Action-Related Events on PC

Division	Detailed event item
File	Create/Move/Rename/Save as/Network File Download/ Network File Upload/ Print Screen/File Restore/ Screen Capture
Mail	Send MAIL/Attach Mail
Print	Print/Print Process
Device	Device Missing/Added

〈Table 5〉 Risk Estimation and Measures for Each Type of Risk

Risk Type		Contents		Rating
Potential Risk		If there is no access to the means of use and the financial information providing behavior is not approved		high
		Countermeasures	It is recommended to perform forensics immediately by using End Point Detection On Response(EDR) solution on PC, when detecting unusual behavior (hacker, etc.) as scenario verification.	
Unmanaged Risk	Unidentified risk	If you have access to the means of use but are not authorized to provide financial information		high
		Countermeasures	TYPE I) Recommendation to immediately execute the calling procedure TYPE II) It is recommended to perform forensics immediately by using End Point Detection Response (EDR) solution in PC.	
	Identified risk	If there is no access right to the means of use, and the financial information providing activity is approved(policy exception permitted)		Medium
		Countermeasures	It is advisable to carry out the calling procedure	
Managed risk		If you have access to the means of use and you are authorized to provide financial information		Low
		Countermeasures	If abuse by the licensor is detected, it is recommended to carry out the calling procedure	
			It is advisable to carry out the calling procedure	

또한, 내부통제 프로세스 수립 과정에서 개인적 경험에 지나치게 의존 할 우려가 있는 비정형접근법의 위험에 대해서 금융회사가 년 1회 정보보호 전문업체의 전문 컨설턴트를 통해 수행하는 컨설팅 수행 시 주기적으로 시나리오를 검증 받는 방법으로 객관화 할 수 있다.

5. 금융정보유출 위험관리 모델을 적용한 위험평가 사례

(주)ㅇㅇ캐피탈을 대상으로 시나리오 기반 금융정보유출 위험관리 3단계 방법론을 다음과 같이 적용하였다.

위험관리 1단계는 금융정보유출 위험 관리 모델의 공통 단계로 금융정보유출 경로를 확인(<Figure 2> 참조)하고, 금융정보유출 행위와 관련된 PC 내 특정 프로그램에 대한 항목 정의(<Table 2> 참조) 및 보안활동 현황(<Table 1> 참조)을 파악한다.

그리고, 2단계는 금융정보유출 이상행위가 정상적인 승인 절차에 의한 행위인지 여부 확인과 시나리오 상황별 대응 절차를 수행하는 단계로 개발 직원 PC내 비인가 프로그램이 실행되는 행위가 탐지(<Table 2> 참조)되어 다음과 같이 대응절차를 수행 하였다.

첫 번째, 비인가 프로그램의 사용에 대한 권한 및 승인 내역을 '외부 파일 반출 승인 시스템'을 통해 확인한 결과 승인 내역은 없는 것으로 확인이 되었으며, 두 번째, 본 행위가 금융정보유출 위험 시나리오 NO(4)인 비인가자(해커 등)행위에 해당되어 시나리오(<Table 3> 참조)에 정의한 위험을 검증한 결과문서암호화가 해제된 대용량(20M 이상)파일은 존재 하지 않았으며, 문서암호화 해제된 다수(5건 이상) 파일과 일정기간 내 문서암호화 해제 이력 및 과도한 문서암호화 자가 승인 이력 그리고, 악성 코드 감염 이력 및 일정시간 망연계 사용 이력과 원격 접속 프로그램 실행 이력 마지막으로 PC내 개인 정보 포함된 파일을 보유 이력이 없었다.

따라서, 시나리오 기반 금융정보유출 위험관리 3단계에서 본 행위에 대한 위험평가(<Table 5> 참조)는 고위험군 이용자가 아닌 행위자의 PC에서 상기 이벤트 발생 원인이 외부에서 반입된 PC가 당시 악성코드 감염 여부 미확인 상태에서 내부 네트워크에 연결 시 탐지된 것으로 추정되어 재발 방지를 위해 외부 PC 반입 시 악성코드 유입 방지 절차를 철저히 이행 할 필요가 있는 것으로 판단되며, 이러한 행위는 잠재위험(위험도: 높음)으로 즉시 PC내 EDR 솔루션 등을 이용한 포렌직 수행을 권고 하였다.

그리고, 또 다른 위험평가 사례로 특정 URL인 웹메일을 통해 인터넷을 사용하는 행위가 PC 이벤트에 탐지(<Table 2> 참조)되어 금융정보유출 이상행위가 정상적인 승인 절차에 의한 행위인지 여부 확인과 시나리오 상황별 대응 절차를 다음과 같이 수행 하였다.

첫 번째, 특정 URL 사용에 대한 권한 내역을 '망연계 시스템'을 통해 확인한 결과 승인 내역이 있는 것으로 확인이 되었으며, '외부파일 반출승인 시스템' 또한 파일 사용 승인 내역이 존재 하였다.

두 번째, 본 행위가 금융정보유출 위험 시나리오 NO(1)인 인가자 이상 행위(오남용)에 해당되어 시나리오(<Table 3> 참조)에 정의한 위험을 검증한 결과 비승인권자 IP로 문서파일의 암호가 해제된 사실은 없었으며, 파일 명칭에 특수문자 또는 기본 제목에 'Book'과 같은 문자

가 포함되지 않았고, 문서의 내용과 파일 제목이 불일치한 내역도 없었음. 그리고, 외부반출이 불승인된 문서 파일(예: Z IP파일)의 이동 및 인가 용도 외 파일 이동도 없는 것으로 '외부파일 반출 승인 시스템'을 통해 확인 하였다.

그러나, DRM 해제 신청 시 반출처 또는 신청 용도가 불분명한 경우로 반출처 입력항목에 "1", "aa", ".." 등으로 입력 후 반출 승인한 사례가 10여 건 존재하며, 개인정보가 포함된 출력 요청・승인 건수 또한 사유가 불분명한 항목이 32건 존재하였다.

따라서, 시나리오 기반 금융정보유출 위험관리 3단계에서 본 행위에 대한 위험평가(<Table 5> 참조)는 고위험군 이용자가 아닌 행위자의 PC에서 발생한 상기 이벤트가 관리되는 위험(위험도: 낮음)으로 '외부 파일 반출승인 시스템'을 통해 내부 보안통제 승인 단계에서 기 인지된 상태로 정상 행위이며, PC내 이용자가 사용한 웹메일은 신청 단계에서 제시한 것과 동일하므로 이용자의 행위를 정상행위로 특정 URL 사용을 허용(자동 또는 수동)하였다.

그러나, 문서암호화 해제 신청 시 신청 사유 및 반출처를 명확하게 명시하지 않아 사후 이슈 발생 시 책임 소재 및 추적에 어려움이 예상되므로 이에 대한 이에 대한 예방 절차를 마련할 필요가 있다.

6. 제안 모델의 특징 및 기능 비교분석

금융회사는 정보유출 행위를 차단하기 위해 다양한 보안솔루션들이 생성하는 보안 로그를 수집하여 패턴 중심의 분석을 수행하는 방법을 선호한다.

그러나, 이러한 방법은 패턴에 미리 지정되지 않은 비정형 데이터나 암호화된 데이터 등은 패턴 탐지가 어려워 정보유출 행위를 차단하는데 한계가 있으며 다양한 보안솔루션에서 생성되는 로그정보를 표준화하여 분석하는데 별도 비용이 수반된다.

또한, 보안로그 수집 및 분석 기능을 가진 일부 보안솔루션만 반출승인 시스템 등 보안통제 절차와 연계하여 정보유출에 대응하고 있다.

그리고, 과거 엔드포인트 PC에서 발생하는 이상행위를 탐지한 후 포렌직을 통한 사고대응을 하는 방법은 소요시간과 분석인력 부족 등의 이유로 일회성 수동적인 사고 대응이 주류였다.

그러나, 최근에 보안사고 탐지, 엔드포인트의 보안사고 통제, 보안사고 조사 및 엔드포인트 치료의 기능을 제공하는 EDR 기능을 통해 엔드포인트 레벨에서 지속적 모니터링과 대응을 요구하고 있으나, 대부분 악성 프로그램에 의한 행위에 중점을 두고 있다.

따라서, 본 논문에서 제안한 금융정보유출 위험대응 3단계 방법론은 타 논문에서 시도하지 않은 PC내 정보유출 행위를 유발할 가능성이 있는 프로그램이 실행되는 시점에 생성된 이벤트에 대해 보안 통제 절차에서 승인 및 권한 여부를 확인하여 이용자가 목적과 동기를 가지고 의도적으로 하는 행동인지 여부를 판단하고 대응함으로써 금융정보유출 행위를 효과적으로 예방 할 수 있다.

<Table 6>에서 패턴 중심의 로그분석 솔루션과 악성코드 중심의 EDR 솔루션 그리고 본 논문에서 제안한 금융정보유출 위험대응 3단계 모델에서 제공하는 기능에 대해 비교하여 보았다.

〈Table 6〉 Compared with Risk Modeling

Division	Detailed features	Feature availability		
		Log Analysis Solution	EDR	Suggested model
Agent behavior information collection	Collecting execution process information(file information, network traffic information, Windows registry access information, driver level information, etc.)	Partial	Provide	Scenario Risk Response Steps 1-2 (Provide)
Abnormal behavior detection and analysis	Malware detection	Not provide	Provide	
	Ability to associate with security control procedures such as granting and approving access to actions	Partial	Not provide	Scenario Risk Response Steps 2 (Provide)
	Correspond to security policy exception or violation item to counter information leakage risk	Partial	Not provide	
Tracking and Investigation Capabilities	Track malware funnels	Not provide	Provide	Scenario Risk Response Steps 3 (Provide)
	Provides visibility into file execution through the process tree			
	Event Correlation Analysis			
	Event Details			
Suspicious PC support	Suspicious PC management (Process and file deletion)			
	Suspicious PC network blocking			

첫 번째, 다양한 보안로그를 수집하여 정보유출 위험을 패턴으로 분석하는 로그분석 시스템에서 제공하는 기능들은 PC내 정보유출 의심행위를 탐지하는 기능 중 이동매체 통제 등 일부기능과 반출승인 등 보안정책과 연계한 통제 절차와 일부 연동하는 기능을 제공하고 있으며, 두 번째, 악성코드 탐지 및 추적에 강점이 있는 PC EDR은 PC내 정보유출 의심 행위를 탐지하고 추적하는 기능을 제공하나 악성코드 행위 분석 중심으로 운영되고 있어 보안통제 절차와 연계는 미흡한 수준이다[9].

그러나, 금융정보유출 위험대응 3단계 모델은 PC내에서 정보유출 의심행위가 탐지되면 보안통제 절차와 자동 또는 수동으로 연동하여 의심행위를 식별하고 필요 시 추적기능을 이용해 효과적인 금융정보유출 위험에 대응하고 있다.

7. 결론 및 향후연구

금융회사 정보 중 개인정보는 금융거래의 성립조건이며 금융회사의 핵심자산이다. 그러나 정보사회의 부작용으로써 나타난 개인정보 침해사고는 중대한 사회적 위험이 되고 있으며, 이러한 위험은 개인과 회사의 실제적 피해로써 현실화되고 있다[4].

따라서, 금융권이 정보유출을 사전에 예방하고자 구축 운영 중인 역할별 보안솔루션의 기능과 금융회사에서 수행하는 내부통제 프로세스의 보안환경 정보를 최근 이슈가 되고 있는 PC EDR 솔루션의 탐지 기능과 상호 연계하여 시나리오 기반 금융정보유출 위험 대응 3단계 모델을 정의 하여 보았다.

그러나, 금융정보유출 위험을 식별하고 위험

평가 및 대응 조치를 수행하는 절차가 일부 수동으로 이루어져 담당자 실수 및 수행을 위해 소요 시간에 대한 문제점이 남아 있다.

따라서, 향후 RPA(Robotic Process Automation)를 이용하여 '금융정보유출 위험 관리 3단계 방법론'에 따른 조치 작업을 자동화 처리로 해결할 수 있는 연구가 필요하다. 예를 들어 특정 데이터에 추가 맥락 및 상황 정보를 덧입히는 작업, 사건 대응 시 해야 할 일을 여러 부서에 지정하는 일 등은 자동화로 해결이 가능하다.

또한, 금융정보유출 시나리오 상황별로 발생하는 이상 징후의 범위나 규모를 파악해 자동으로 위험 등급을 부여하고 필요 시 격리시키는 일은 의외로 해결하기가 어려운 부분이므로 기계학습을 활용하는 방안도 추가 연구가 필요할 것이다.

References

[1] Chae, E. J., "A study on the PIMS based methodology for monitoring to prevent leakage of personal information in the banking industry," Master Thesis, The Graduate School Dongguk University, 2014. 2.

[2] Choi, J. W., "Detection of personal information leakage using database access control system," 2015. 2.

[3] http://www.gartner.com/newsroom/id/3143521, gartner, 2016.

[4] Kim, J. H. and Lim, J. I., "Composition and Policy Direction of Compensation Insurance Against Customer Information Infringements in Financial Transactions," The Journal of Society for e-Business Studies, Vol. 19, No. 3, pp. 1-21, 2014.

[5] Kisa, "guideline for risk management," 2004. 12. 14.

[6] Lee, S. J., "Real time predictive analytic system design and implementation using Bigdata-log," Master Thesis, He Graduate School Korea University, 2016. 2.

[7] Newgen CNI, "Introduction of export approval system," 2017. 9.

[8] Oh, Y. S., "A Study on the utilization of digital forensic evidence using the DLP (DataLoss Prevention)system," Master Thesis, The Gra duate School Dongguk University, 2013.

[9] Redston, "guideline for edr solution iron," 2018.

[10] Ryu, S. T., "A study of detection measures about the personal information leakage through scenario-bas ed integrated security log analysis," Master Thesis, The Graduate School Korea University, 2016. 2.

[11] Song, J. H., "Evaluation Security of Inside Information Leakage Prevention Solution," Master Thesis, The Graduate School Daejin University, 2009.

[12] Tocsg, "guideline for Digital Guardi an Platform," 2018.

저 자 소 개

이익준 (E-mail: leemsjij@gmail.com)
2014년 동국대학교 국제정보대학원 (석사)
2016년~2018년 순천향대학교 정보보호대학원 박사과정 수료
2018년~현재 (주)삼위
관심분야 위험관리, 정보보호관리체계, 보안아키텍쳐

염흥열 (E-mail: yyoum@sch.ac.kr)
1990년~현재 순천향대학교 정보보호학과 교수
2011년 제16대 한국정보보호학회 회장
2017년 ITU-T SG17 의장