情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

개인정보 유출 방지를 위한 SRI(Security Risk Indicator) 기반 모니터링 시스템 개발

박 성 주,† 임 종 인‡
고려대학교 정보경영공학전문대학원

A study on the development of SRI(Security Risk Indicator)-based monitoring system to prevent the leakage of personally identifiable information

Sung-ju Park,† Jong-in Lim‡
Korea University, Graduate School of Information Management and Security

요 약

오늘날과 같은 정보화 사회에서는 정보가 기업의 핵심자산으로 인식되고 있으며, 특히 금융권에서는 고객의 개인정보 유출이 커다란 이슈로 대두되고 있다. 현재 상용화된 개인정보보호 기술은 전사적인 차원이 아닌 일부 기능으로 국한되거나 극히 일부분의 개인정보만 포함되는 경우가 많다. 따라서 전사적인 차원에서 개인정보 유출을 사전에 예방하기 위해서는 개인정보 유출의 징후를 지속적으로 모니터링 할 수 있는 체계에 대한 연구가 필요하다. 본 연구에서는 개인정보 접근에 대한 패턴분석 및 SRI(Security Risk Indicator)를 이용한 모니터링 체계 구축 방법론을 제안하였으며, 실제 금융권 기업에 적용하여 사례 연구를 수행하였다. 이를 통해 탐지된 개인정보 유출 시도는 탐지된 유형에 맞춰 체계화된 대응 방안을 수립할 수 있게 되었다.

ABSTRACT

In our current information focused society, information is regarded as a core asset and the leakage of customers' information has emerged as a critical issue, especially in financial companies. It is very likely that the technology that safeguards which is currently in commercial use is not focused at an enterprise level but is fragmented by function or by only guards portions of a customer's personal information. Therefore, It is necessary to study the systems which monitor the indicators of access at an enterprise level in order to preemptively prevent the compromise of such data. This study takes an enterprise perspective on such systems for a financial company. I will focus on examination of the methods of implementation of the monitoring system, the application of pattern analysis and examination of Security Risk Indicators (SRI). A trial of the monitoring system provided security managers and related departments with proper screening capabilities of information. Therefore, it is possible to establish a systemic counter-plans based on detectable patterns.

Keywords: monitoring system, Security Risk Indicators, SRI

접수일(2011년 11월 11일), 수정일(2012년 1월 30일), 게재확정일(2012년 2월 2일)

† 주저자, gialo@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

I. 서 론

정보기술(IT: Information Technology)이 확대보급 되고 정보화 사회가 점차 고도화됨에 따라 대부분의 기업에서는 정보를 핵심자산 중의 하나로 인식하기 시작하였으며, 기업의 경영 환경이 인터넷을 기반으로 한 e-Business 형태로 변화함에 따라 기업에서는 다양한 정보를 활용하여 고객들에게 제품 및 서비스를 신속하게 제공할 수 있게 되었다. 그러나 정보기술의 급격한 발달은 기업의 경영성과에 상당부분 기여하였지만 해킹, DDOS (Distributed Denial Of Service)등과 같은 정보화 역기능은 기업의 커다란 위협으로 대두되고 있다. 최근의 전자상거래 사이트에 대한 해킹사고를 보면, 개인정보의 유출이 기업에게 어떠한 피해를 입힐 수 있는지 여실히 보여준다. 기업은 이러한 정보 유출을 방지하기 위해 다양한 보안장치를 도입하고 있지만, 유출 사고는 끊임없이 일어나고 있으며 이에 따르는 기업의 소모비용은 적지 않다.

특히 금융권의 경우, 업무 시스템이 해킹 당하거나 고객의 개인정보가 유출되어 막대한 재무적 손실이 발생할 수 있으며, 기업의 대외 신뢰도 하락 등의 비재무적 손실을 야기할 수 있다. 고객으로부터 직접 수집하는 개인정보의 경우 수집되는 개인정보 항목으로 성명, 주민등록번호, 전화번호, 주소, 전자우편 주소 등 금융 분야가 평균 22개의 개인정보를 수집하는 것으로 조사되어 다른 분야(평균 11개)에 비하여 상대적으로 많은 항목을 수집하는 것으로 조사 되었다. 이는 다른 분야에 비하여 금융 분야는 서비스 개설 시에 고객의 신용도 판단 등을 위하여 보다 많은 정보가 필요하기 때문이다.

II. 관련연구

현재 개인정보와 관련된 기술 현황을 살펴보면, 시장에서 많이 언급되고 있지만 실질적으로 개발내용과 직접적으로 연관되어 상용화된 기술은 아직까지 구체적인 모습을 나타내고 있지 않다. 기업의 홈페이지에 악성코드가 삽입되어 사용자가 피해를 보는 경우 기업 이미지의 실추, 사용자들의 손해 배상 청구, 악성코드 감염으로 인한 사용자의 피해 등 많은 부작용이 발생하게 된다. 또한 이러한 악성코드로 인해서 개인정보 유출, 스팸 발송에 이용 등의 2차 피해가 발생하게 된다. 이와 같은 피해를 차단하기 위해서 웹 전용 보안장비를 도입하더라도 원천적인 해결책은 되지 않는다. 방화벽, 침입탐지시스템, 문서보안시스템, RFID 등 개인정보보호와 관련하여 언급되는 일반적인 보안 제품은 내부 인가자 PC에만 설치되어 개인정보 유출을 감지, 대응하는 것에 국한되고 있는 실정이다.

또한, 최근 출시되고 있는 네트워크 트래픽 기반의 모니터링 시스템은 기업의 내부 네트워크에서 외부 인터넷으로 전송되는 일반적인 콘텐츠 유형을 분석하여 패턴이 같을 경우 차단하는 것으로 웹 페이지의 게시물이나 문서 파일 형태의 개인정보 유출 탐지 시스템과 데이터베이스 유출 탐지 시스템으로 나눌 수 있다. 현재 시중에 나와 있는 문서 파일 및 텍스트 형태 개인정보 유출 방지시스템은 개인정보 유출 차단과 탐지 기능을 제공하고 있다. 구성은 단일조직의 망에서 개인정보의 유출을 탐지하는 구성을 가지고 개인정보가 포함된 파일의 업로드를 금지하거나 개인정보 유출 징후를 집중적으로 감시하는 것으로 네트워크 기반이라는 한계를 벗어나지 못하고 있다. 데이터베이스 정보 유출 방지시스템은 데이터베이스의 접근을 제어하는 방식과 데이터베이스 자체를 암호화 하는 방식으로 나눌 수 있다. 또한 최근에는 사용자의 데이터베이스 접근과 작업에 대한 로그 정보를 저장하고 저장된 로그를 분석 및 감사하는 기능도 제공하고 있다.

즉, 금융기관은 고객정보가 보관되어 있는 주전산기, 서버, DB, 금융관련 정보처리 시스템에 대한 보호를 위해 금융회사는 전산자료의 유출, 파괴 등을 방지하기 위하여 정보처리시스템 접근 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한해야 한다.(사용제한), 금융회사는 단말기(개인용 컴퓨터 포함)에 주요정보를 보관하지 않도록 하고, 단말기를 공유하지 아니하여야 한다.(주요정보 보관금지), 금융회사는 사용자가 전출, 퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제하여야 한다.(사용자 계정관리), 금융회사는 정보처리시스템에 대한 테스트를 할 때 실제 이용자 정보를 테스트 정보로 사용하지 아니하여야 한다.(테스트 정보관리), 금융회사는 단말기와 전산자료의 접근권한이 부여되는 관리자의 주요 업무 관련 행위는 소관 업무 책임자가 이중 확인 및 모니터링 등의 조치를 하여야 한다.(이중확인) 등의 금융위원회 규정을 지켜야 되고 금융감독원의 전자금융감독규정 시행세칙을 준수하기 위한 목적으로 주전산기 또는 서버에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록, 전산자료를

사용한 일시 사용자 및 자료의 내용 등을 확인할 수 있는 접근기록, 정보처리시스템 접근을 위한 사용자 로그인, 액세스 로그 등 자료처리 내용을 확인할 수 있는 접근기록을 저장하고 있지만 사용현황을 모니터링 하는 관점에서 개인정보 유출을 탐지 할 수 있는 기능과 규정은 부족하다.

따라서 본 논문에서는 다수의 개인정보를 취급하는 금융회사의 개인정보 유출 예방 및 방지를 위한 SRI(Security Risk Indicator) 도출 및 패턴분석을 통해 개인정보 유출 관점에서 상호 연관성을 도출하고 최근에 구축된 금융회사 시스템의 사례를 중심으로 대안을 제시하고자 한다.

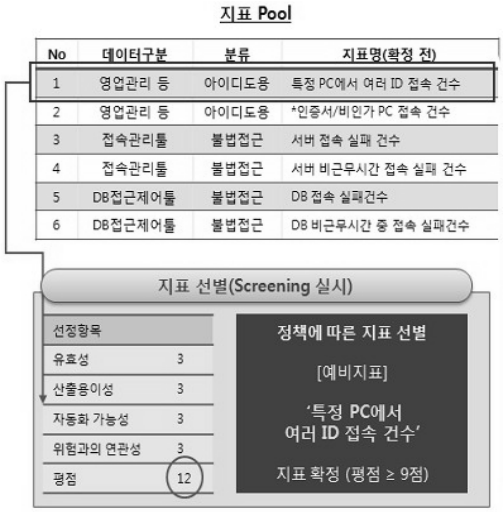
III. SRI기반 개인정보 유출방지 모니터링 방법론

개인정보 유출 모니터링의 체계를 구축하기 위해서는 현재 기업에서 사용하고 있는 업무 시스템 및 정보보안 솔루션의 로그 정보를 이용하여 개인정보 유출 징후의 패턴을 도출할 필요가 있다. 이러한 패턴 정보는 기업의 경영 목표 및 정보보안 목표를 저해하는 위험을 지표화 시킨 KRI(Key Risk Indicator)와 연계되어 임계값의 허용한도를 설정하여 개인정보 유출의 징후를 모니터링 할 수 있다. KRI(Key Risk Indicator)는 선행지표와 후행지표로 구분된다. 선행 지표는 위험 사건의 발생 가능성, 혹은 사전 예측 정보를 제공하며, 후행 지표는 리스크 발생 이후의 사후 결과를 보여준다. 이중 가장 핵심적인 부분은 KRI(Key Risk Indicator) 선행지표이다. 선행지표를 관리하면 위험의 사전 관리가 가능해진다.

본 장에서는 개인정보에 접근하는 패턴 분석 방법과 기존의 KRI 개념을 보안부문에 특화하여 적용할 수 있는 SRI(Security Risk Indicator)로 명명하여 이를 도출하는 방법론에 대한 연구를 수행하였다. SRI(Security Risk Indicator)는 보안부문에 대한 선행지표를 제공하며 이를 통해 사전에 고객정보 유출에 대한 위험의 사전관리가 가능해지고 사후지표를 이용해서 고객정보 유출에 대한 사고추적 및 증적을 남길 수 있는 기반을 제공한다.

3.1 개인정보 보안 SRI 도출

개인정보보안을 위한 SRI를 도출하기 위해서는 〔그림 1〕과 같이 먼저 기존 개인정보 접근 관련 데이터를 통해 개인정보 유출 위험을 초래하는 근본 원인



〔그림 1〕 SRI(Security Risk Indicator) 선정 절차

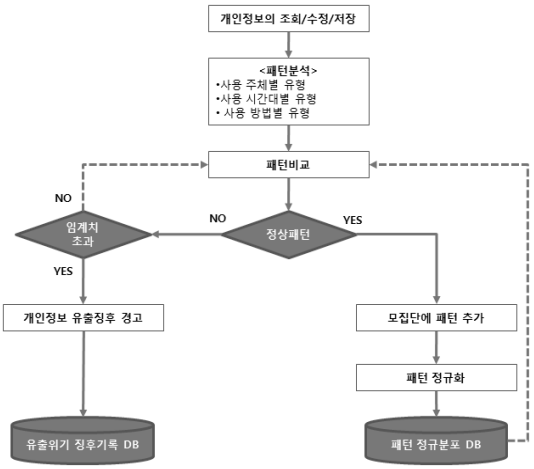
이 되는 요소를 추출하여 SRI 풀(pool)을 도출한다. SRI 풀에서 개인정보 유출을 식별할 수 있는 핵심지표인 SRI는 유효성, 산출 용이성, 자동화 가능성, 위험과의 연관성 항목에 대한 평점을 통해 선정된다. 각 항목에 대한 평가 점수의 범위는 0점 ~ 3점이며,

모든 항목에 대한 총합이 9점 이상인 경우 최종 SRI로 선정된다.

SRI 도출을 위한 지표의 근거는 KISA의 ISMS와 정보보호관리 체계에 대한 국제적인 표준인 ISO-27001을 참고로 하였다. KISA의 ISMS 인증은 정보통신부 산하 한국 정보보호 진흥원(KISA - Korea Information Security Agency)에서 ISMS에 대해 객관적이고 독립적으로 평가해 기준에 대한 적합여부를 보증해 주는 제도이며 정보보호 5단계 관리과정 요구사항 14개 필수항목, 문서화 요구사항 3개 필수항목, 정보보호대책 15개 분야 120개 세부항목의 총 137개 항목으로 구성되어 있다.

3.2 패턴 분석 및 임계값 설정

기업이 보유하고 있는 개인정보에 대한 접근은 접근주체에 따라 접근위치, 접근정보의 종류, 접근빈도, 접근방법 등에 대한 고유의 패턴을 가지게 된다. 이때 접근주체는 특정 시간에 개인정보가 저장된 데이터베이스로의 직접조회 또는 응용프로그램을 이용한 조회 등과 같은 방법으로 접근하게 된다. 접근하는 개인정보의 종류는 주민등록번호, 휴대폰번호, 주소, 아이



〔그림 2〕 패턴분석 및 임계값 설정에 따른 개인정보 유출징후 경고

디, 인증정보, 개인약력, 금융정보, 신체정보 등 접근주체의 업무 성격에 따라 제한된다. 이러한 내용을 포함한 정상적인 접근이력을 일정기간 데이터베이스화하면 패턴을 생성 할 수 있다.

정상적인 접근 패턴을 생성하여 데이터베이스화 한 후, 접근주체가 개인정보에 접근하는 경우 패턴을 이미 저장된 패턴과 비교분석하여 정상적인 접근시도인지를 판별할 수 있다. 반면 정상적인 접근 패턴을 벗어날 경우에는 개인정보 유출 징후로 인식하고 개인정보 관리자에게 실시간 경고함으로써 개인정보 유출을 예방할 수 있게 된다.

따라서 개인정보 접근 패턴을 분석하여 정상적인 접근 패턴과 비교하여 개인정보 유출 위기 징후를 판단, 경고하는 프로그램은 아래의 〔그림 2〕과 같이 도식화 할 수 있다.

〔그림 2〕과 같은 패턴 분석 및 임계값 설정을 위해서는 우선적으로 정당한 개인정보 접근의 속성을 정의내려야 하며, 접근 속성별 정상 패턴을 도출해야 한다. 또한 실제 개인정보 접근 시 패턴 매칭을 통해 개인정보의 유출 징후를 포착해야 하며, 사전에 개인정보 유출 징후에 대한 임계값을 설정하여 경고 메시지를 보낼 수 있어야 한다.

3.2.1 개인정보 접근 속성의 정의

기업의 성격에 따라 보유하게 되는 개인정보의 종류는 상이할 수 있지만, 일반적으로 금융회사가 보유하고 있는 개인정보에 대한 접근속성은 금융감독원의 전자금융감독규정 시행세칙을 준수하기 위한 목적으로 주전산기 또는 서버에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록, 전산자료를 사용한 일시 사용자 및 자료의 내용 등을 확인할 수 있는 접근기록, 정보처리시스템 접근을 위한 사용자 로그인, 액세스 로그 등 자료처리 내용을 확인할 수 있는 접근기록을 저장해야 하는 규정에 의해 다음과 같은 고유의 패턴을 가지게 된다.

- 접근위치:인터넷, 내부 네트워크 주소 등
- 접근빈도:1일 접근횟수, 접근횟수당 검색 수 등
- 접근방법:웹브라우저, C/S 프로그램, 원격콘솔 등
- 접근정보:신상정보, 금융정보, 의료정보 등
- 접근시간:공휴일, 업무시간 중, 업무시간 외 등

또한, 접근주체가 개인정보에 접근하는 속성을 수집하는 구체적인 기술에는 DBMS에서 직접 쿼리에 대한 메모리(예를 들면, Oracle의 SGA 등) 덤프 분석 기능 개발, 응용프로그램으로부터 조회 시 이를 기록하는 프로그램의 개발 등이 될 수 있다.

3.2.2 접근속성별 정상패턴 도출

상기에서 설명하였듯이, 정상적인 접근시도를 일정기간 수집하여 데이터베이스화하고 확률분석을 하면 패턴을 도출할 수 있다. 즉, 접근주체별로 접근위치, 접근시간대역, 접근빈도, 접근방법 등 수집된 접근시도를 모집단으로 하여 접근속성에 따라 적절한 방법으로 정상접근 여부를 판단하기 위한 패턴을 도출할 수 있다는 의미이다.

수집된 접근시도의 분석 결과 특정 사용자가 업무상 항상 내부에서만 접근한다면 접근위치의 경우 내부 네트워크는 True(1), 기타는 False(0)로 패턴을 생성할 수 있으며, 접근시간대역은 요일별, 업무시간대별로 업무상 접근이 가능한 시간을 True(1)로 하고 그 이외의 시간대의 접근은 False(0)로 하여 패턴을 생성할 수 있다. 한편, 접근빈도의 경우 접근횟수(시간당)로 산정하고 수집된 정보를 '평균(m)'과 '표준편차(α)'를 계산할 수 있다. 이 경우, 정상패턴의 범위는 확률이론에 따라 원하는 신뢰도 수준에 따라 'm + α', 'm+2α' 또는 'm+3α' 등으로 설정할 수 있다. 따라서 이와 같은 패턴은 접근주체(사용자)별로 분석되어 데이터베이스화하여 향후 비정상적인 접근시도를 탐지할 수 있다.

3.2.3 개인정보 접근시 패턴매칭 통한 유출징후 포착

개인정보 접근 시 접근주체, 접근위치, 접근시간, 접근방법 별 개인정보 조회 회수를 탐지하여 관련 패턴과의 일치성을 검사한 후 개인정보에 대한 비정상 접근으로 유출 위기 징후가 있는 것으로 판단할 수 있다. 이를 위한 패턴 일치도는 금융감독원의 전자금융감독규정 시행세칙을 준수하기 위한 목적으로 주전산기 또는 서버에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록, 전산자료를 사용한 일시 사용자 및 자료의 내용 등을 확인할 수 있는 접근기록, 정보처리시스템 접근을 위한 사용자 로그인, 액세스 로그 등 자료처리 내용을 확인할 수 있는 접근기록을 저장해야 하는 규정에 의해 접근속성을 산출 할 수 있으며 이를 위한 패턴 일치도는 접근속성의 곱으로 정확성을 높인다.

패턴일치도 (0~1) = 접근위치 (0~1) x
접근시간대역 (0~1) x
접근방법 (0~1) x
접근빈도 (0~1)

패턴 일치도는 위에 언급한 것 이외에도 정확도를 높이기 위해 개인별 접근속성의 수를 늘려나갈 수 있다. 접근속성의 평점은 0~1사이 이며 1인 경우 패턴일치가 되어 안전한 경우이고 0인 경우 패턴일치가 되지 않아 유출징후가 보인다고 할 수 있다. 평점은 초기에는 경험치에 의해 주어지며 정상적인 패턴인 경우 모집단에 패턴이 추가되고 패턴정규화 DB에 업데이트 되어 정확도를 높여 나간다.

3.2.4 개인정보 유출 징후 임계값 설정 및 경고

개인정보 유출 징후에 따라 담당자에게 경고 메시지를 발송하기 위해서는 패턴 일치도에 대한 임계값을 개인정보의 민감도별로 산정할 필요가 있다. 예를 들어, 개인의 사생활에 미치는 영향이 큰 의료정보, 금융관련 정보 등에 대한 접근의 경우, 접근정보의 민감도를 높여서 적용하는 방법이 있을 수 있다. 이를 위해 개인정보별로 민감도를 0부터1까지 부여하고 (1-패턴일치도)와의 곱을 통해서 경보 임계값을 도출할 수 있다. 접근정보의 민감도가 0 인 경우 개인정보의 유출에 문제가 없는 정보가 되며 1에 가까울수록 민감한 개인정보에 해당되고 민감도 부여시 초기값은 경험치에 의해 부여하며 지속적인 경보 임계값 모니터링을 통해 최적의 민감도 부여를 하고 오탐을 줄일 수 있다.

경보 임계값 = 접근정보의 민감도 (0~1) x
(1- 패턴일치도)

위의 분석 및 비교 결과 개인정보 유출 경보 임계값을 초과하는 경우 이를 위기 징후로 판단, 개인정보 관리자에게 이메일, SMS 등을 활용하여 경보 발령함으로써 개인정보 유출의 징후를 사전에 파악할 수 있게 된다.

IV. 개인정보 유출 모니터링 금융회사 구축사례

4.1 개인정보 유출 모니터링 시스템

개인정보 유출 모니터링 체계는 〔표 1〕과 같이 현황분석 및 로그수집, 모니터링 방법 및 지표 선정, 모니터링 실시의 3 단계로 업무를 구분하여 수행하였다. 이 때, 회사 내의 주요 보안시스템, 기간계 업무시스템들과의 연계를 통한 자동화가 우선적으로 고려되었다.

〔표 1〕 개인정보 유출 모니터링 체계 수립을 위한 수행업무

수행 TASK		설 명	Output
현황분석 및 로그수집	대상분석	개인정보 유출 모니터링 대상 분석 및 선정, 관련 목표를 정의	모니터링 대상목록
	로그분석	대상 시스템의 샘플 로그를 수집하여 로그의 형식 및 필요 요건 분석	모니터링 대상별 로그분석 결과
	정규화 및 수집	대상으로 결정된 로그를 수집하고 일치하지 않는 로그 형식을 정규화 함	로그 정규화방안
모니터링방법 및 지표 선정	모니터링 방법 선정	최적의 개인정보 유출 모니터링 방법론을 수립	모니터링 방법론
	지표(SRI) 선정	개인정보 유출 위험을 조기에 포착 할 수 있는 핵심위험지표 선정	SRI 목록 SRI정의서
	임계값설정	지표별 임계값을 설정, 조정	SRI 정의서
모니터링 실시	정합성 검증	자동 수집을 위하여 레거시 시스템과 연계되는 지표 측정값의 정합성 검증	정합성 테스트 결과서
	임계값 재설정 및 조정	Alert 정보를 검증하여 지표별 임계값의 적정성 검토 및 재설정	SRI 정의서

4.1.1 개인정보 유출 모니터링 방법 및 SRI 선정

모니터링 방법 및 지표 선정 단계에서는 금융회사의 개인정보보호 목표 달성을 위한 기준을 선정하고 목표달성을 방해하는 위험과 SRI(Security Risk Indicator)를 선정한다. 이 때, SRI는 다양한 지표 pool을 정의한 후 임계값을 설정하여 측정 및 모니터링 함으로써 임직원 별 개인정보 보유현황 및 이용현황, 외부 전송현황을 자동분석하고 이상 징후를 탐지하여 유출사고에 대한 조기징후를 포착하는 기능을 제공할 수 있도록 설계된다. 또한, 정보보안 기준을 저해하는 위험 중 개인정보 유출 위험을 발생하게 할 수 있는 근본 원인이 되는 요소를 식별하여 SRI로 수치화하여 대표성이 있는 지표 정의서를 작성하게 된다. 이때, 지표 정의서에는 지표명, 지표에 대한 설명, 산식, 데이터의 원천, 위험도 등을 작성하고, 각 지표 별로 유효성, 조기경보 가능성, 통합 가능성, 추적가능성, 추출가능성, 이용가능성, 실행가능성 등을 평가함으로써 관리가 필요한 보안위험지표(SRI)를 선정하게 된다.

지표 정의서에서 가장 중요한 항목은 임계값으로 개인정보 유출 징후의 모니터링을 위한 관리한도 값을 지정하는 것으로 비즈니스 부서별 또는 개인별 개인정보 보호 수준을 평가하는 기준이 될 수 있다. 금융회사에서 보유하고 있는 보안 솔루션 기반으로 개발/유지보수(Application), 접근통제(System, Database), 통신/운영보안(Network, PC) 에 해당하는 3개 부문에 SRI를 선정한다. 네트워크 보안솔루션 및 네트워크 장비에 대하여 위험에 대한 원천정보를 수집한다. 네트워크 장비는 별도 Agent 등의 설치가 불가능한 경우가 많으므로 SNMP(Simple Network Management Protocol) 기반의 검색을 주기적으로 수행함으로써 수집할 수 있고 VPN, 메일보안등의 경우에는 솔루션에 저장되어 있는 로그를 이용해 수집할 수 있다.

〔표 2〕 Network 부문 선정 SRI

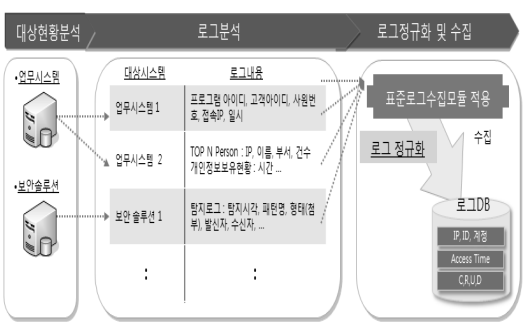
솔루션	수집 정보	선정된 SRI	SRI 조치
방화벽	방화벽 정책	특정 공격에 대한 시간당 차단건수	임계치 초과시 포트차단
IPS	침입탐지로그	특정 공격 및 IP에 대한 시간당 탐지건수	임계치 초과시 공격포트 및 IP 차단
네트워크 통제	IP 차단 로그	비정상적 접근 IP 차단건수	임계치 초과시 IP 사용자 조사
DLP	메일 차단 로그	고객정보 포함된 메일 차단 건수	고객정보 발신인 추가조사
VPN 보안	VPN 로그	업무시간외 VPN을 통한 접속건수	VPN 사용자 사용여부 확인

4.1.2 분석 및 로그 수집

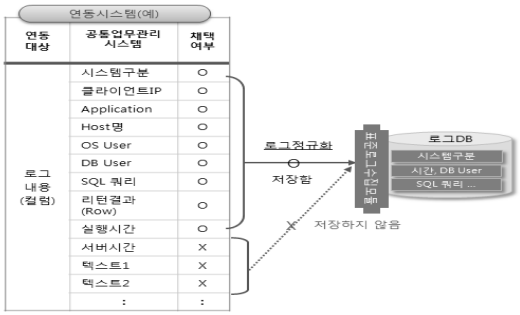
분석 및 로그수집 단계는 아래의 〔그림 3〕과 같이 대상 현황분석, 로그분석, 로그 정규화 및 수집으로 구성되며, 현황분석을 통해 내부 시스템과의 연계를 위한 대상 시스템을 파악하고, 연계 대상 시스템으로부터 샘플로그를 취합하여 분석한 후, 수집 대상으로 선정된 로그들을 표준로그 수집모듈을 이용해 정규화하여 수집하게 된다.

현황분석 및 로그수집 단계를 세부적으로 살펴보면, 우선 대상 현황분석 단계에서는 개인정보 유출 모니터링의 대상인 업무 시스템 및 정보보안 시스템을 파악하여 샘플로그 제공 여부 및 로그의 형태(DB, CVS, MDB, TXT 등), 로그제공 가능 시간 등을 정의한다. 다음으로 로그분석 단계에서는 프로그램 ID, 접속 IP 및 일시 등 샘플 로그 수집을 통해 개인정보 유출 모니터링에서 보이는 데이터의 형태를 가늠해보며 해당 시스템의 로그를 사용 할지 여부를 결정한다. 이 때 로그의 내용이 데이터로서 활용가치가 떨어지거나 형태가 불규칙적일 때는 사용할 수 없게 된다.

마지막으로 로그 정규화 및 수집 단계에서는 수집된 샘플 로그를 표준로그 수집모듈을 통해 로그 DB에 수집하고, 불규칙한 형태의 로그들은 모니터링 수행



〔그림 3〕 현황분석 및 로그수집 절차



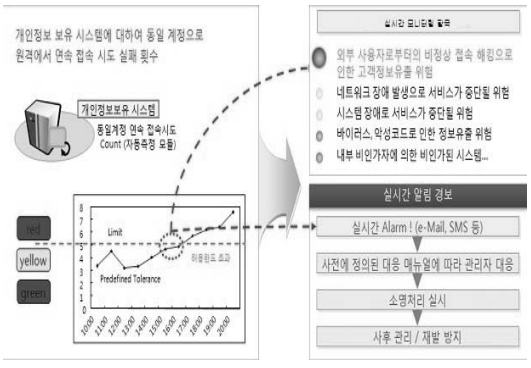
〔그림 4〕 로그 정규화 및 수집

시에 최적화될 수 있도록 정규화 되어 로그 DB에 저장하게 된다. 이 때 정규화 여부에 따라 지표 측정 시 성능에 부화를 최소화할 수 있다. 위의 〔그림 4〕는 로그 정규화에 대한 예시를 보여준다.

4.1.3 개인정보 유출 탐지

개인정보 유출 모니터링의 마지막 단계에서는 지표 및 연동대상 시스템 등을 토대로 연동 정의서를 작성하고, 모니터링을 수행하게 되는데, 이 때 임계값 초과 시 자동으로 이메일, SMS 등을 이용해 실시간 알림 경보를 발생하여 관리자로 하여금 사전에 정의된 대응 매뉴얼에 따라 대응할 수 있도록 지원한다. 〔그림 5〕는 SRI를 통한 실시간 모니터링의 예로, 개인정보 보유 시스템에 대하여 동일 계정으로 원격에서 연속 접속 시도 실패 횟수라는 SRI에 패턴 분석 후 임계값 허용한도 초과 시 실시간 알림 경보를 통해 사후 관리 및 재발방지까지의 과정을 보여준다.

마지막으로 이러한 모니터링 활동은 데이터 자체에 대한 신뢰성이 기반이 될 때, 가능하므로 적합성 검증 활동이 중요하다. 적합성 검증 활동은 연동 시스템의



〔그림 5〕 실시간 모니터링

데이터가 일관되고 약속한 형태로 반환되는지 지속적으로 테스트 하여 개인정보 유출 모니터링의 신뢰도를 높이기 위한 필수적인 단계이다. 이러한 적합성 검증은 연동 초기단계에서는 수작업으로 진행되지만 연동 확정 후에는 시스템으로 자동화가 가능하다.

V. 결 론

민감한 고객정보를 대량으로 취급하는 금융기관의 고객정보에 대한 위협은 날로 커지고 있으며, 이러한 금융기관의 개인정보가 대량으로 유출될 경우에 사회에 미칠 수 있는 피해는 추정하기조차 어렵다. 이에 개인정보의 취급현황을 실시간으로 파악하고 내/외부 사용자에 의한 유출을 사전에 예방할 수 있어야 한다. 뿐만 아니라 관련 위험 징후를 조기에 발견하여 대응할 수 있도록 체계와 개인정보 유출 사고가 발생했을 경우 사후에 감사할 수 있는 체계의 구축도 반드시 필요하다. 따라서 본 연구는 금융권에서 수행할 수 있는 개인정보보호 노력의 일환으로 개인정보 유출 위험을 사전에 파악하고 자동으로 측정하여 사고 징후를 조기에 포착, 대응하여 사고를 사전에 예방하며 사후 감사가 가능할 수 있도록 하는 방안을 제시하고 있다. 금융기관들의 이러한 노력이 있을 때, 사고에 대한 사후처리 비용 및 정량적으로 환산하기 어려운 사회적 파장을 미연에 방지할 수 있을 것이다.

본 논문에서 제안한 개인정보유출 모니터링 시스템은 국내 법규 등의 컴플라이언스에서 요구하는 사항을 만족하도록 내부 임직원들의 개인정보 취급현황을 추적할 수 있는 감사(Audit) 기능으로 효과가 높으나, 실질적으로 실시간 탐지 및 차단활동을 돕는 데는 아직은 한계가 있다고 볼 수 있다. 이는 위험 발생 이전에 징후를 예측할 수 있는 선행성 지표를 개발하고 이를 실시간 분석하는 것에 대한 보다 더 큰 노력이 필요함을 시사한다. 개인정보 유출 사고는 하나의 현상만으로 예측하기는 불가능하다. 다양한 이벤트의 전후관계를 복합하여 유기적으로 분석할 수 있을 때, 정확한 판단이 가능할 수 있다. 이를 위해서는 개인정보 유출과 관련한 실제 사고사례의 발생 패턴을 분석할 수 있는 방법론을 지속적으로 발전시켜야 한다. 예를 들어 특정 임직원의 개인정보 조회 건수의 증가, PC 내 개인정보 보유 건수의 증가, mail 등을 이용한 개인정보 외부전송 건수의 증가를 개별적으로 분석하는 것이 아니라 전후관계를 유기적으로 분석할 수 있다면 보다 정확한 상황판단이 가능할 것이다. 보편적으로

개인정보 유출사고가 발생할 경우, 관련 법류에 대한 과징금, 과태료 등의 금전적 책임과 유출된 개인정보의 양과 비례하여 개인들의 소송에 대한 대응 비용 등이 정해질 수 있다. 이와 관련하여 본 논문에서 제시한 개인정보 유출 모니터링 시스템을 활용하여 특정 유출 위험 징후가 포착될 경우, 예상되는 회사의 기대손실액을 제시할 수 있다면 개인정보보호에 대한 경영진의 정보보호 예산집행에 대한 의사결정을 돕는데 효과적으로 활용될 수 있도록 정량적 기대손실의 측정에 대한 연구가 필요할 것이다.

참고문헌

〔1〕 진승헌, "u-IT 환경에서의 개인화서비스를 위한 개인정보 보호방안 연구," 전자통신동향 분석, 25(2), pp. 3, 2010년 4월.

〔2〕 김성언, "개인정보 침해에 관한 조사 연구," 한국형사정책연구원, pp. 36, 2001년.

〔3〕 정연수, "민간분야 개인정보관리 현황조사 연구," 한국전산원, pp. 70, 2004년 8월.

〔4〕 노민선, "기업연구소 산업기밀 관리실태 및 개선방안," 한국산업기술진흥협회, pp. 23, 2006년 8월.

〔5〕 정연수, "개인정보 영향평가 최근 동향 및 활성화 방안," 한국정보보호진흥원, pp. 42-43, 2006년 12월.

〔6〕 이명수, "2009 정보시스템 해킹, 바이러스 현황 및 대응," 한국인터넷진흥원, pp. 37, 2009년 12월.

〔7〕 한승원, "개인정보 저장 형태에 따른 유출 탐지 방안," 정보과학회지, pp. 43, 2009년 12월.

〔8〕 금융위원회, "금융회사 정보기술(IT)부문 보호업무 모범규준," pp. 10-18, 2011년 10월.

〔9〕 이상진, "개인정보 유출 공격 탐지 방안에 관한 연구," 한국인터넷진흥원, pp. 201-202, 2009년 06월.

〔10〕 이형효, "개인정보보호를 위한 DB 보안감사로그 표준화 연구," 한국정보보호진흥원, pp. 5, 2008년 10월.

〔11〕 Jonathan Davies, "Key Risk Indicators - Their Role in Operational Risk Management and Measurement," RiskBusiness International Limited, pp. 2-4, June. 2006.

〈著者紹介〉

박 성 주 (Sung-ju Park) 정회원
1998년 2월: 동국대학교 산업공학과 졸업
2012년 2월: 고려대학교 정보경영공학전문대학원 석사
2000년 2월~현재: (주)삼성SDS 금융CERT
〈관심분야〉 개인정보보호, 금융보안

임 종 인 (Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
1986년 3월~2001년 1월: 고려대학교 자연과학대학 정교수
2001년 2월~현재: 고려대학교 정보보호대학원 원장, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 방송통신 위원회 인터넷협의회 운영위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등