情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

개인정보보호를 위한 개인정보 유출 모니터링 시스템의 설계

조 성 규,† 전 문 석‡
숭실대학교

Privacy Leakage Monitoring System Design for Privacy Protection

Sung-kyu Cho,† Moon-seog Jun‡
Soongsil University

요 약

다수의 민간기업체 및 공공기관들은 영업, 홍보, 민원처리 등의 업무를 위하여 다양한 방법을 통해 개인정보를 수집하고, 조직의 이익 및 업무처리를 위해 개인정보를 활용하고 있다. 하지만 이렇게 수집된 개인정보에 대한 기술적, 관리적 조치 및 내부통제의 미숙으로 인해 개인정보의 오남용 및 유출이 사회적 문제로 크게 대두되고 있으며, 정부에서도 개인정보보호에 대한 중요성을 인식해 개인정보보호법의 시행을 추진하고 있는 실정이다. 본 연구에서는 조직에서 관리하고 있는 개인정보의 취급 패턴을 분석하여 이상징후를 탐지하고, 사전에 개인정보 유출 및 오남용에 대한 대처가 가능한 방안에 대해 기술하고 있다. 특히 개인정보 유출과 관련된 요소들을 객관적으로 측정이 가능한 핵심위험지표들로 수치화하여 관리할 수 있는 개인정보 유출 모니터링 시스템의 설계 방안에 대해 제시하고자 한다.

ABSTRACT

Numerous private corporations and public institutions are collecting personal information through the diverse methods for the purpose of sales, promotion and civil services, and using personal information for the profits of the organizations and services. However, due to immaturity of the technical, managerial measures and internal control for the collected personal information, the misuse, abuse and the leaks of personal information are emerged as major social issues, and the government also is promoting implementation of the act on the privacy protection by recognizing the importance of the personal information protection. This research describes on the measures to detect the anomaly by analyzing personal information treatment patterns managed by the organizations, and on the measures to coup with the leaks, misuse, and abuse of personal information. Particularly, this research is intended to suggest privacy leakage monitoring system design, which can be managed by making the elements related to personal information leaks to numeric core risk indexes to be measured objectively.

Keywords: Personal Information, Risk Management, KRI, PIA

I. 서 론

근래에 들어서도 개인정보의 유출 및 오남용 사건들이 계속하여 증가하고 있으며, 2010년에도 약 1억 건 이상의 개인정보 침해사고가 발생하였다. 이와 같은 개인정보 관련 사고로 인해 기업차원에서는 법정 분쟁 등에 따른 비용의 지출과 기업 신용의 하락 등을 경험하고 있으며, 개인차원에서도 본인의 정보가 무분별하게 사용됨에 따라 프라이버시 침해 및 보이스피싱 등의 피해 사례가 증가하고 있는 실정이다[1]. 정부에서도 이와 같은 부주의한 개인정보 취급상의 문제로 인한 피해를 줄이고자, 개인정보보호에 대한 인식 변

접수일(2011년 3월 29일), 수정일(2011년 6월 12일), 게재확정일(2011년 7월 23일)
† 주저자, flashbit@naver.com
‡ 교신저자, mjun@ssu.ac.kr

화를 위한 홍보를 지속적으로 강화하고 있으며, 개인정보보호법의 시행을 통해 공공기관에서 관리하고 있는 개인정보의 안전한 보호를 위한 노력을 기울이고 있다. 이처럼 개인정보보호는 더 이상 선택이 아닌 조직의 비즈니스를 지속시키기 위한 사활을 결정짓는 전략적 이슈로서 간주되어야 하며, 전사적 위험관리 차원에서 개인정보보호 체계가 구축되도록 해야할 것이다[2].

조직에서는 이전부터 정보보안의 중요성을 인식하고 지속적으로 전사적 위험관리(ERM : Enterprise Risk Management) 체계를 구축하여왔다. 위험관리는 정보보안관리의 초석으로서 조직의 자산을 보호하기 위해 자산에 대한 위험을 분석하고, 비용효과적인 측면에서 적절한 보호 대책을 선정하여 위험을 감수할 수 있는 수준으로 유지하는 일련의 과정으로 정의할 수 있다. 또한 위험분석은 위험관리의 주요 핵심 과정으로 위협을 분석하여 이들의 발생 가능성 및 위협이 미칠 수 있는 영향을 파악해서 보안 위험의 내용과 수준을 결정하는 과정이다[3]. 본 논문에서 제시하고 있는 개인정보 유출 모니터링 시스템은 이와같은 ERM의 개념을 개인정보보호 분야에 적용하여 사전에 위험징후를 포착하고 사고를 예방할 수 있는 방안을 연구한 것이다.

본 연구에서는 조직에서 관리하고 있는 개인정보에 대한 취급패턴을 분석하여 이상 징후를 탐지하고, 사전에 개인정보의 유출 및 오남용을 모니터링 할 수 있는 개인정보 유출 모니터링 시스템의 설계 방안에 대해 제시하고자 한다. 이와 같은 개인정보 유출 모니터링 시스템을 설계하기 위해 먼저, 개인정보 유출과 관련해 발생 가능한 위험을 식별하고 위험을 발생하게 할 수 있는 근본 원인이 되는 핵심위험요인들을 정의하며, 핵심위험요인들을 수치화하여 관리할 수 있는 핵심위험지표들의 작성 방안에 대해 기술하고자 한다. 특히, 개인정보 유출과 관련된 핵심위험지표들의 예를 들고, 각 핵심위험지표들에 대한 지표 정의서 작성 방법 및 핵심위험지표들을 수치화하여 관리할 수 있는 산출식을 제시함으로써 개인정보보호를 위한 조직의 개념적 보호조치를 구체적인 시스템으로 구현할 수 있는 방안에 대해 제시한다.

II. 관련 개념

본 연구에서 제안하는 시스템을 설계하기 위해 필요한 관련분야의 개념에 대해 기술한다.

2.1 개인정보

공공기관의 개인정보보호에 관한 법률에 따르면 개인정보란 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다[4].

2.2 개인정보보호법

그동안 개인정보와 관련된 법률로는 공공기관 개인정보보호법(공공기관), 정보통신망법(정보통신사업자, 준용사업자) 등의 개별법 체계로 헌법기관, 오프라인 사업자, 비영리기관 등은 관련법이 부재한 실정이었다. 이러한 개별법 체계에서는 법 적용의 사각지대가 발생하여, 개별법간 보호원칙, 처리기준 및 추진체계가 상이함에 따른 국민적 혼란을 겪게 되었고, 일관된 정책 추진에 한계를 나타내고 있었다[5]. 이와 같은 법적용의 사각지대를 해소하고자 정부에서는 개인정보보호에 대한 일반법으로써 개인정보보호법 제정을 추진하게 되었으며, 2011년 3월 법률 제정으로 인해 시행을 앞두게 되어 향후 국민들의 개인정보보호 및 피해 구제 절차 등이 강화될 전망이다.

2.3 개인정보영향평가(PIA)

개인정보영향평가(Privacy Impact Assessment)란 개인정보를 활용하는 새로운 정보시스템의 도입 및 기존 정보시스템의 중요한 변경 시, 시스템의 구축・운영이 기업의 고객은 물론 국민의 프라이버시에 미칠 영향에 대하여 미리 조사・분석・평가하는 체계적인 절차를 말한다[6]. 개인정보영향평가를 수행함으로 인해 개인정보 라이프 사이클인 수집・저장・이용・제공・파기의 각 단계에서 발생할 수 있는 위협 요소들을

〔표 1〕 개인정보의 유형

구분	내용
일반정보	이름, 주민등록번호, 주소, 전화번호 등
신체정보	얼굴, 지문, 음성, 홍채, 키, 몸무게 등
의료정보	건강상태, 진료기록, 신체장애, 장애등급 등
금융정보	신용평가정보, 통장계좌번호, 대출정보 등
법적정보	전과, 범죄기록, 과태료 납부내역 등

사전에 발견하고 대처하는 것이 가능하여 진다[7].

2.4 핵심위험지표(KRI)

근래에 기업들 가운데 전사적 위험 관리(ERM)를 도입하는 경우가 많아 졌으며, 미국의 주요 회계, 감사 위원회 조직인 COSO의 보고서에서는 구체적인 리스크 관리 방안으로 KRI(Key Risk Indicator) 관리, 내부 프로세스 개선, 적절한 보고 시스템, 사전 대비가 불가능한 경우의 시나리오 플랜 등의 대안들을 제시하였다. ERM의 다양한 산출물 가운데서도 가장 핵심적인 부분은 KRI 선행 지표이며, KRI 선행지표는 위험 사건의 발생 가능성, 혹은 사전 예측 정보를 제공하여 준다[8].

조직에서 발생할 수 있는 위험을 관리하기 위해서는 먼저 위험을 사전정의하고 이를 수치화해 표현할 수 있어야 한다. 위험은 추상적인 개념이므로 측정하기가 어려운 성질을 지니고 있다. 하지만 이런 위험을 대변하는 핵심위험지표를 정의하고, 이를 주기적으로 측정할 때 비로서 조직이 갖고 있는 위험의 정도에 대한 정확한 측정이 가능하여 진다. 핵심위험지표(KRI : Key Risk Indicator)란 바로 위험을 측정해 모니터링 하기 위한 수단으로써 수치화가 가능한 지표를 의미한다. 또한 측정된 KRI 별 한도값을 정확히 설정하여 운영함으로써 조직에서 발생할 수 있는 침해사고에 대한 경고 및 조기대응이 가능해질 수 있다.

2.5 정보보호관리, 위험관리 및 위험분석의 개념

정보보호관리는 위험관리의 상위개념이며 위험관리는 위험 분석의 상위개념이다. 각 개념들의 정의는 다음과 같다[9].

2.5.1 정보보호관리

조직의 정보시스템에 대한 전반적인 사항을 다루며 정보보호에 관련된 업무를 몇 개의 통제분야로 나누고 각 통제분야 별로 다수의 통제대책으로 구성된다. 통제항목은 보안관리의 수준을 상위 수준 또는 관리적, 비기술적 수준에서 평가하는데 활용될 수 있다.

2.5.2 위험관리

정보보호관리에 대해 최적의 비용으로 최고의 효과를 거두기 위해 통제분야의 우선순위를 결정하고 실제의 통제를 수행하는 방법중의 하나이다. 일반적으로 위험관리는 위험분석과 보안대책의 선택을 포함한다.

2.5.3 위험분석

위험분석은 보안관련 항목들에 대한 위험파악과 위험평가로 구성된다. 위험파악은 정보시스템 내에 각 항목의 세부사항을 발견 및 식별하는 것이며, 위험평가는 파악된 항목에 대해 그의 발생가능성과 피해가능성 등을 수치적 또는 등급적으로 부여하는 것이다.

III. 제안하는 시스템

여기에서는 본 연구에서 제안하는 개인정보와 관련된 위험 식별, 핵심위험요인 정의, 핵심위험지표의 작성 방안에 대해 살펴본다.

〔표 2〕 위험측정을 위한 구성요소

구성요소	설명
위험	조직의 목표달성을 방해하는 사건
핵심위험 요인	위험을 발생하게 할 수 있는 근본 원인이 되는 요소
핵심위험 지표	위험을 수치화하여 측정할 수 있는 대표성이 있는 지표

위의 표에서 위험이란 조직의 업무 목표 달성을 방해하는 사건이나 잠재가능성을 의미하며, 핵심위험요인은 위험을 발생하게 할 수 있는 근본 원인이 되는 요소들을 의미한다. 또한 핵심위험지표는 핵심위험요인을 수치화하여 측정할 수 있는 대표성이 있는 지표들을 의미한다. 이와 같은 피라미드 구조를 통해, 여러 가지 핵심위험지표들을 측정하여 핵심위험요인의 위험수준을 판단하여 결과적으로 조직의 목표 달성을 방해할 가능성이 있는 위험의 발생가능성 및 정도에 대한 객관적 판단 자료를 얻게 되는 것이다.

3.1 개인정보관련 위험 식별

위험이란 개인정보 자산에 대한 위협과 취약성으로 말미암아 발생할 수 있는 부정적 영향으로 보통은 사업목적을 달성하는데 방해가 되는 현상을 의미한다. 일반적으로 개인정보와 관련된 조직의 위험을 식별하기 위해서는 보편적으로 “2.3 개인정보영향평가”에서

기술된 개인정보의 수집・저장・이용・제공・파기의 각 단계에 속하는 내용들 중 조직의 개인정보처리 업무와 관련된 항목들 가운데 취약한 부분을 도출하여 작성할 수 있다[10]. 예를 들어, 개인정보와 관련된 위험으로 개인정보 처리시스템의 운영미흡, 개인정보 유출, 불법아이디도용 등 여러 가지 위험을 식별할 수 있을 것이다. 본 연구에서는 개인정보와 관련된 위험들 중 조직에 가장 심각한 피해를 유발할 수 있으며, 본 논문에서 중심 과제로 다루고 있는 개인정보유출을 위험으로 식별하여 연구를 진행하도록 한다.

3.2 핵심위험요인 정의

핵심위험요인이란 식별된 위험을 발생하게 할 수 있는 근본 원인이 되는 요소들을 말한다. 개인정보처리 단계에 속하는 핵심위험요인들의 예는 다음과 같이 열거할 수 있다. 표의 예들은 타 논문 및 세미나 자료, 보안컨설팅 업체에서 컨설팅 진행 시 작성한 산출물들에서 개인정보 유출과 관련하여 발생할 수 있는 요소들을 핵심위험요인으로 열거한 것이며, 조직의 업무 운영 환경에 따라 좀 더 구체적이고 다양한 핵심위험요인들을 도출할 수 있을 것이다[10].

근래에는 개인정보 유출 사고의 증가 및 개인정보 보호 인식의 확산에 따라 개인정보와 관련된 다양한 위협 징후들을 탐지할 수 있는 보안솔루션들이 많이 개발되어 사용되어지고 있다. 예를 들어, 모기업에서 개발된 개인정보 검색 솔루션의 경우 사용자의 PC 안에 저장된 파일 가운데 개인을 식별할 수 있는 주민등록번호, 신용카드번호, 계좌번호, 핸드폰 번호 등의 개인정보가 포함된 파일 및 메일을 검출하고 건수도 측정할 수 있는 기능을 지원하고 있다. 또한 식별된 개인정보 파일을 완전 파기하거나, 암호화 정책 적용, 특정 폴더로의 격리 기능 등을 지원하고 있다. 본 연구에서는 개인정보 취급 단계별 핵심위험요인들 가운데, 3.1에서 정의한 개인정보유출 위험에 해당하는 핵심위험요인으로써 "개인정보 조회 오남용", "개인정보 과다 보유"를 선정하여 사용하도록 한다. 선정한 핵심위험요인들은 개인정보 유출과 관련해 직접적으로 관련된 요인들이며, 수치화 하거나, 자동화하기에 적합한 특성을 보유하고 있는 핵심위험요인들이다.

〔표 3〕 개인정보 취급 단계별 핵심위험요인 예

단계	핵심위험요인
수집	・개인정보 수집시 동의절차 미흡 ・최소한의 개인정보 수집 절차 미흡
저장	・데이터베이스 접근통제 미흡 ・개인정보 보유 시 고지 의무 불이행
이용	・개인정보 조회 오남용 ・민감정보 평문노출 방지 미준수
제공	・개인정보 제공 시 법규 미준수 ・위탁 및 제3자 제공 계약 미흡
파기	・개인정보 파기 시 법규 미준수 ・개인정보 파기 시 통제절차 미흡

3.3 핵심위험지표 작성

핵심위험지표란 핵심위험요인을 수치화하여 측정할 수 있는 대표성을 갖는 지표들을 말한다.

3.1.1 핵심위험지표의 정의

본 연구에서는 3.2에서 정의한 핵심위험요인들에 해당하는 핵심위험지표를 2가지씩 선정하도록 한다. 핵심위험지표들은 조직의 상황에 맞게 핵심위험요인을 발생하게 할 가능성이 있는 항목들을 도출하여 열거한 후, 실제 위협이 될만한 가능성이 있는 지표들을 정해진 산출식을 이용하여 선정한 후 사용하도록 한다. "〔표 3〕"에서 예로 든 핵심위험지표들의 경우는 보안컨설팅 업체들에서 작성한 세미나 자료 및 개인정보처리 관련 보안솔루션을 개발하는 회사들의 개인정보 종합관리시스템 및 개인정보 검색 솔루션에서 지원하는 기능들로부터 지표를 유추하여 작성하였으며, 수치화의 용이성 및 자동화 가능성 등을 고려하여 작성한 것이다[11][12].

또한, 조직에서 개인정보에 대한 유출을 모니터링하기 위해 여러 가지 KRI들을 선정한 후, 개인정보 유출 모니터링 시스템에 적용하기 위해서는 실제 해당 KRI들이 유효하며, 활용 가치가 있는지에 대한 선별 작업이 선행되어야 한다. 이와같은 선별을 하기 위해서는 다음과 같은 지표선정 방법을 활용하여 일정 수준 이상인 지표들에 대해서만 지표로써 적용하도록 선정을 할 수 있다.

〔표 4〕 핵심위험지표의 정의

핵심위험요인	핵심위험지표
개인정보 조회 오남용	휴일 부서평균 대비 개인정보 조회 건수
	하나의 ID로 여러PC에서 접속 건수
개인정보 과다 보유	개인PC 내 개인정보 보유 건수
	메일 전송 시 개인정보 전송 건수

〔표 5〕 지표선정 방법의 예

선정항목	점수	설명
지표가치	H: 3 M: 2 L: 1	어느정도 지표로써 활용할 수 있는지에 대한 가치를 나타낸다.
측정가능성	H: 3 M: 2 L: 1	측정한 값들은 수치화가 가능하여야 한다.
자동화정도	H: 3 M: 2 L: 1	지표들을 자동으로 측정할 수 있어야 한다.
발생빈도	H: 3 M: 2 L: 1	선정한 지표의 발생가능 정도를 나타낸다.
위험수준	H: 3 M: 2 L: 1	개인정보와 관련해 위험의 정도를 나타낸다.
* 산출식 · 평점 = 지표가치 + 측정가능성 + 자동화정도 + 발생빈도 + 위험수준 · 지표 선정 : 평점 〉= 10		

3.3.2 핵심위험지표 산출식의 작성

핵심위험지표를 선정하였다면, 핵심위험지표를 수치화할 수 있는 산출식을 작성하여야 한다. 조직의 보안관리자는 각각의 핵심위험지표별 임계치를 설정한 후, 산출식에서 구한 값이 임계치를 초과할 경우 경보를 알리고, 조치를 취할 수 있는 보안대책을 강구하여야 한다. 임계치 측정에 사용되어지는 항목(주민번호, 이메일주소, 핸드폰번호 등)들은 각각의 항목이 갖는 정보 민감도나 중요도에 따라 조직의 보안관리 방침에 맞게 임계치에 차이를 두어 설정할 수 있으며, 조직에서 일정 기간 동안 모니터링을 실시한 후 적절한 측정치를 임계값으로 설정하여 사용하도록 한다.

3.3.3 지표정의서

여러 가지 핵심위험지표들을 선정한 후, 실제 조직에서 채택하고자 하는 지표들을 선별하여 지표정의서를 작성한다. 시스템을 운영하면서 업무상 필요한 추가 지표들이 발생할 경우 신규로 지표정의서를 작성하여 추가하도록 한다.

이와 같은 개인정보유출과 관련된 핵심위험지표들을 상세하고 다양하게 만들어 관리하면 개인정보가 유출될 가능성이 있는 위험요인들을 사전에 탐지하여 대비하는 것이 가능해지므로, 조직의 보안담당자는 지속

〔표 6〕 핵심위험지표 산출식 예

핵심위험지표	산출식
휴일 부서평균 대비 개인정보 조회 건수	count { (개인정보조회건수 〉 부서평균조회건수) and date = 휴일 in 개인정보저장시스템 } 〉= 1;
하나의 ID로 여러PC에서 접속 건수	count { 동일 로그인 id and (1차 접속PC MAC 주소 ≠ 2차 접속PC MAC 주소) } 〉= 2;
개인PC 내 개인정보 보유 건수	count { 개인정보 보유 건수 in 사용자PC } 〉= 임계치; * 임계치 - 주민번호 〉= 50 건 - 이메일주소 〉= 100 건 - 핸드폰번호 〉= 100 건
메일 전송 시 개인정보 전송 건수	count { 개인정보 포함 메일 전송건수 in 메일전송 내역 } 〉= 임계치;

〔표 7〕 지표정의서 양식

No	구분	내용
1	지표명	하나의 ID로 여러PC에서 접속 건수
2	위험명	개인정보유출
3	위험요인	개인정보 조회 오남용
4	지표설명	개인정보에 해당하는 정보를 과다 조회하는 사용자를 검출
5	산출식	count { 동일 로그인 id and (1차 접속PC MAC 주소 ≠ 2차 접속PC MAC 주소) } 〉= 2;

〔표 8〕 위험, 핵심위험요인, 핵심위험지표의 예

위험	핵심위험요인	핵심위험지표
내부 임직원의 개인정보 유출	개인정보 조회 오남용	비근무시간 중 고객정보 조회 건수
인터넷 서비스 상의 개인정보 유출	웹 서비스 해킹 방지 대책 미준수	SQL Injection 관련 대책 미조치 여부
데이터베이스 상의 개인정보 유출	DB 조회 오남용	SELECT를 이용한 DB 쿼리 건수

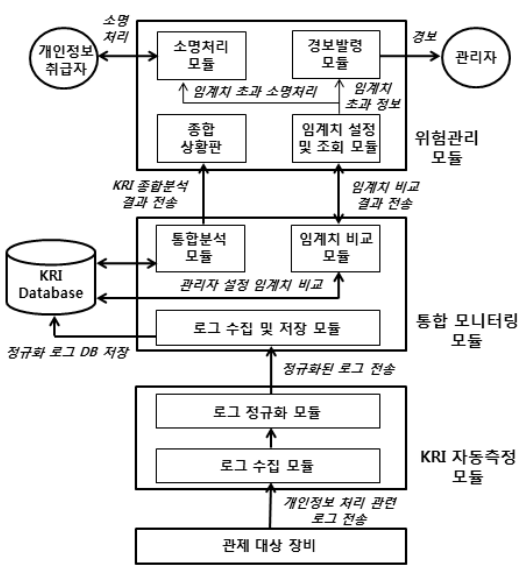
적인 연구를 통하여 핵심위험지표들을 추가적으로 발견하고 개선하는 노력을 기울여야 할 것이다. 다음의 표는 위험, 핵심위험요인, 핵심위험지표들의 몇 가지 예를 제시한 것이다.

IV. 개인정보 유출 모니터링 시스템 설계

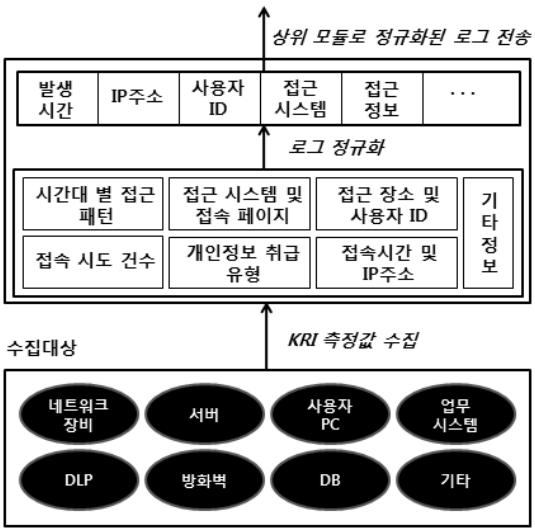
앞장에서 기술한 내용들을 바탕으로 위험과 핵심위험요인, 핵심위험지표들을 기반으로한 개인정보 유출 모니터링 시스템을 설계하도록 한다. 개인정보 유출 모니터링 시스템은 크게 KRI 자동측정 모듈, 통합 모니터링 모듈, 위험관리 모듈의 서브 시스템들로 구성되어지며, 관리대상 시스템들로부터 로그를 수집하는 에이전트, 관리자에게 경보를 알리는 모듈, 개인정보 취급자에 대한 소명처리 등의 세부 기능들을 포함한다.

4.1 KRI 자동측정 모듈

개인정보를 취급하는 다양한 IT자산들(Network, System, Database, Application 등)에서 발생하는 개인정보와 관련된 KRI들을 자동으로 수집하여 측정하는 모듈이다. 개인정보유출과 관련된 정보를 수집하기 위해, 측정하고자 하는 개인정보의 용도에 알맞은 보안솔루션을 선택하여 조직에 적용하도록 한다. 이러한 개인정보와 관련된 보안솔루션들로는 개인PC 내 보유하고 있는 개인정보의 검출, E-mail이나 첨



〔그림 1〕 개인정보 유출 모니터링 시스템

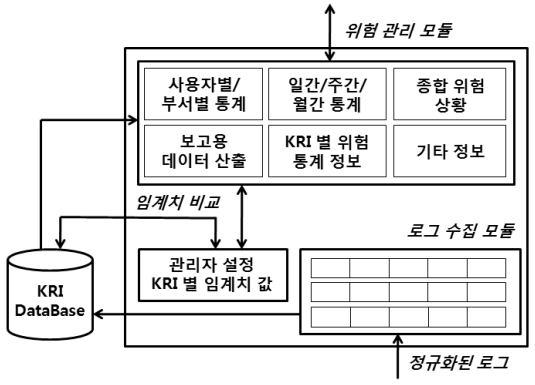


〔그림 2〕 KRI 자동측정 모듈

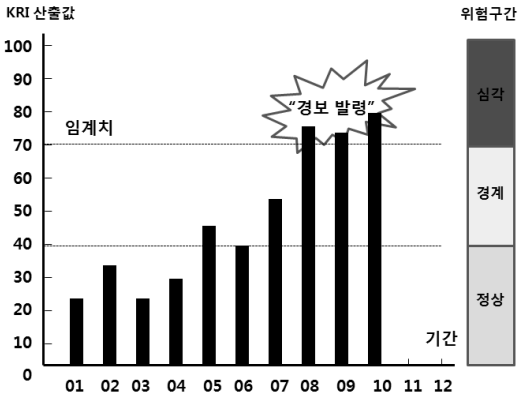
부파일에 포함되어 있는 개인정보 검출 등의 기능을 제공하는 보안솔루션 등이 현재 개발되어 사용되어지고 있다〔11〕〔12〕〔13〕. 각각의 측정 대상 장비들로 부터의 개인정보는 특정 프로토콜(Syslog, SNMP 등)을 이용하여 전송을 받을 수도 있고, 이와 같은 프로토콜이 지원되지 않을 경우는 직접 대상 장비에 Agent를 설치하여 정보를 수집하도록 한다.

4.2 통합모니터링 모듈

자동으로 측정된 KRI 정보들을 분석 알고리즘을 이용하여 분석을 수행하고 다양한 통계치를 산출한다. 또한 관리자가 사전에 설정해 놓은 KRI들의 임계치와 비교하여 위험의 정도(심각, 경계, 정상 등)를 분



〔그림 3〕 통합 모니터링 모듈



〔그림 4〕 임계치 초과에 따른 경보발령

〔그림 6〕 화면 설계 예

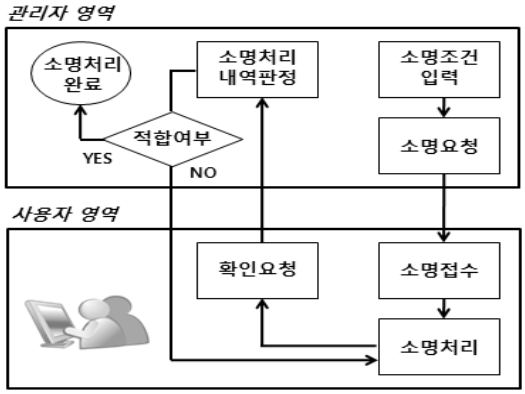
류하며, 개인정보유출과 관련된 다양한 지표들에 대한 정보를 관리자에게 제공하여 준다.

4.3 위험관리 모듈

일정 임계치 이상의 이상징후에 대해서는 관리자에게 Mail, SMS, PopUp 등의 방법을 이용하여 경보를 발령할 수 있도록 하여, 개인정보유출에 대한 위험을 사전에 탐지하고 대처할 수 있도록 한다. 또한 일정 임계치 이상의 개인정보와 관련된 위험 징후를 나타낸 사용자에게는 소명 기회를 부여하며, 소명 처리 결과에 따라 경보에 대한 대응방안을 마련하도록 한다.

4.4 프로토타이핑

개인정보 유출을 모니터링 하기 위한 모듈의 기능 및 알고리즘, 업무처리 상세 절차 등에 대한 설계를



〔그림 5〕 소명처리 절차

바탕으로 프로그램의 화면을 설계할 수 있을 것이다. 화면에서는 정의된 위험의 현재 정도 및 관련 핵심위험요인, 핵심위험지표 들의 현재 현황을 파악할 수 있는 기능을 제공하여 주며, 관리자가 설정한 임계치 이상의 비정상 사용자들에 대해서는 소명처리 절차를 갖도록 구현할 수 있다. 다음은 프로그램의 주요 위험정보들을 조회할 수 있는 화면 설계 예시이다.

V. 결 론

본 연구에서는 조직에서 발생할 수 있는 개인정보의 유출로 인한 피해를 사전에 탐지하여 예방할 수 있는 개인정보유출 모니터링 시스템의 설계 방안에 대해 제시하였다. 개인정보보호법이 제정되고 이제 시행을 얼마 남겨놓지 않은 상황에서 개인정보를 취급하는 조직에서는 법률 시행에 대비하기 위해서 어떤 보안대책을 마련해야 할지 구체적인 대안을 갖고 있지 않은 조직이 많을 것이다. 위험을 관리하기 위해서는 위험의 발생 가능성을 판단할 수 있어야 하며, 각각의 위험요소에 대해 세부적으로 측정할 수 있는 지표들을 선정해야만 효율적인 보안대처 방안들을 마련할 수 있을 것이다. 본 연구에서는 조직의 업무 연속성을 저해할 수 있는 개인정보유출이라는 위험을 정의하고, 개인정보유출이 발생할 수 있는 근본 요소들인 핵심위험요인을 정의하였다. 또한 핵심위험요인들을 수치적으로 정량화하여 관리할 수 있는 핵심위험지표를 활용함으로써, 실제 조직에서 개인정보유출과 관련된 위험요소들은 무엇이 있으며, 어느 정도인지 직관적으로 파악할 수 있는 방안에 대해 제시하였다.

위험은 측정할 수 있을 때, 비로소 관리가 가능하여진다. 막연히 정보보안을 어디에서부터 시작하여야 할

지 방향을 잡지 못하는 조직들도 많을 것이다. 본 연구에서 기술한 것처럼 조직의 업무를 지속시키기 위해 가장 큰 위험이 무엇인지 가장 먼저 인지를 한 후, 위험을 발생시킬 수 있는 요소들을 하나씩 정량화하다 보면 조직에서 발생할 수 있는 위험요소들의 파악이 전체적으로 그려질 것이다.

개인정보보호법의 시행을 앞두고, 각 공공기관 및 민간기업체들에서 근래에 개인정보영향평가나 PIMS 인증의 추진 등 개인정보유출에 대한 대비를 하기 위해 여러 방향으로 노력을 기울이고 있다. 이와같은 법제정과 인증 등을 통해 어느정도 조직의 개인정보유출 피해를 예방할 수는 있을 것이다. 하지만 개인정보보호와 관련된 근본적인 해결책은 우리 모두가 개인정보의 중요성에 대해 다시한번 생각하고, 개인정보를 처리함에 있어 개인 사생활 침해와 관련된 사회적 문제의 심각성에 대해 중요하게 여기는 인식의 변화가 무엇보다 필요할 것이다.

참고문헌

〔1〕 유진호, 지상호, 임종인, "개인정보 유노출 사고로 인한 기업의 손실비용 추정," 한국정보보호학회논문지, 19(4), pp. 63-75, 2009년 8월.

〔2〕 김정덕, "개인정보보호를 위한 관리체계와 거버넌스," 정보보호학회지, 18(6) pp. 1-5, 2008년 12월.

〔3〕 김정덕, 이성일, "정보기술 위험관리 과정과 기법," 정보보호학회지, 11(3), pp. 16-23, 2001년 6월.

〔4〕 이강신, 이기혁, 반진식, 최일훈, "개인정보보호 기초와 활용." 인포더북스, vol. 1, pp.12-15, 2010년 10월.

〔5〕 "개인정보보호법 워크숍," 한국정보보호학회 세미나 자료, vol. 1, pp. 6-13, 2011년 2월.

〔6〕 "개인정보 영향평가 수행을 위한 교육교재," 한국인터넷진흥원, vol. 2, pp. 141-148, 2010년 11월.

〔7〕 남기효, 박상중, 강형석, 남기환, 김성인, "개인정보보호기술의 최신 동향과 향후 전망," 정보보호학회지, 18(6), pp. 11-19, 2008년 12월.

〔8〕 김상일, "KRI 선행 지표의 유용성," LG주간경제 818, vol. 9, pp. 16, 2005년 2월.

〔9〕 최상수, 방영환, 최성자, 이강수, "보안관리 및 위험분석을 위한 분류체계, 평가기준 및 평가스케일의 조사연구," 정보보호학회지, 13(3), pp. 38-49, 2003년 6월.

〔10〕 이기혁, 윤재동, "민간 기업의 개인정보 유출 위험에 대한 측정 방법과 그 사례에 대한 연구," 정보보호학회지, 18(3), pp. 92-100, 2008년 6월.

〔11〕 (주)인포섹 홈페이지, http://www.skinfosec.com

〔12〕 (주)이지서티 홈페이지, http://www.easycerti.com

〔13〕 박중환, 조남욱, 이기혁, 최일훈, "기업내부 개인정보 보호 시스템 개발," 정보보호학회지, 18(6), pp. 28-34, 2008년 12월.

〈著者紹介〉

조 성 규 (Sung-kyu Cho) 정회원
1998년 2월: 성결대학교 컴퓨터공학과 졸업
2002년 2월: 숭실대학교 컴퓨터학과 석사
2005년 8월~현재: 숭실대학교 컴퓨터학과 박사과정
〈관심분야〉 네트워크보안, 개인정보보호, 암호학, 인증

전 문 석 (Moon-seog Jun) 종신회원
1981년 2월: 숭실대학교 전자계산학과 졸업
1986년 2월: University of Maryland Computer Science 석사
1989년 2월: University of Maryland Computer Science 박사
1989년 3월~7월: Morgan State University 조교수
1991년 3월~현재: 숭실대학교 컴퓨터학과 정교수
〈관심분야〉 정보보호, 전자여권, 전자상거래, 암호학