情 報 保 護 學 會 誌
第18卷 第3號, 2008. 6

민간 기업의 개인정보 유출 위험에 대한 측정 방법과 그 사례에 대한 연구

이 기 혁*, 윤 재 동**

요 약

본 논문은 개인정보를 취급하는 민간기업들이 개인정보유출을 사전에 방지하기 위한 일환으로 예방의 원칙에 기초를 두고 있는 개인정보영향평가를 수행할 수 있으며 이러한 일련의 프로세스를 이용한 개인정보 유출에 대한 차별화된 위험분석과 심각도 분석을 통해 민간기업에 실질적으로 영향을 줄 수 있는 위험과 위험평가 결과를 토대로 위험에 효율적으로 대응할 수 있는 방안을 제시한다.

Ⅰ. 서 론

급격한 IT기술의 발전에 따라 기업의 업무 환경이 e-Business 중심으로 변화하였으며 과거에는 문서 작성 등의 수작업 업무들이 대부분 시스템으로 자동화되어 신속, 편리하게 처리되고 있다. 이에, 고객에게 제품 및 서비스 공급하는 기업은 어플리케이션과 데이터베이스라는 형태로 고객들의 개인정보[1]를 대량으로 수집, 축적하고 이용하게 되었다.

그러나 IT의 발전은 또 다른 정보화 역기능으로 피싱, 악성코드 등 해킹 기술의 발전도 함께 이루었다. 이는 기업들이 내부통제가 미숙하거나, 해킹 등에 취약할 경우 대량의 개인정보를 무분별 수집, 방치, 유출, 판매할 위협에 직면하게 됨을 의미한다. 즉, 개인정보를 다량 보유/관리하는 정보시스템이 증가함에 따라 개인정보의 수집, 이용, 보관, 파기 과정상 유출 위험 및 내 부 직원에 대한 정보유출 위험요인이 급증하고 있는 것이다.

이런 개인정보 유출 위협이 현실화되어 위험으로 나타날 경우 유출된 개인정보가 2차적으로 악용될 수 있어 관련 기업들이 고객들과 법적인 분쟁이 발생하고, 금전적인 손해배상이 막대할 수 있다. 뿐만 아니라[2] 대외 신인도 하락으로 기업 가치 자체에 큰 타격을 입을 수 있다. 기업들은 기본적으로 그들이 보유하고 있는 고객의 개인정보 보호에 대해서 법적, 도의적인 책임을 져야 하며, 특히 통신 서비스 기업들은 정통망법[3]을 토대로 업계의 현실적인 수행 가능성에 맞게 세부 지침을 마련하여 자율적으로 적용하고 준수해가는 의지가 필요하다. 하지만 현재 많은 기업들이 개인정보 보호부문 에 관심을 가지고 있지만 자율적으로 개인정보 보호 체계를 수립하고 적극적으로 시행하는 기업은 극히 소수에 불과하다.

또한 기업들이 개인정보보호 만을 지나치게 강조하다 보면 정보산업을 위축시킬 수 있으므로 영업이익 추구와 개인정보보호 사이에서적정선을 찾는 것에도 관심이 필요하다.

본 연구는 개인정보를 취급하는 민간기업들 이 개인정보 유출을 사전에 방지할 수 있도록 하는 일환으로써

1) 개인정보란 개인의 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실, 판단, 평가를 나타내는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보를 말한다. (당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다.)

2) 사례1) 리니지 개인정보 유출 사건(2006, 1인당 50만원), 사례2) 일본 야후BB 개인정보 유출사건(2004, 1인당 6천엔) 등 다수의 사건이 발생했다

3) 민간분야의 종합적인 개인정보보호를 규정하고 있는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"(정통망법)은 국민의 프라이버시 보호를 위해 사업자의 개인정보 수집, 이용, 제공에 따른 제반 사항 등을 규정하고 있다.

* SK Telecom(주) 정보기술연구원 (kevin-lee@nate.com)
** 건국대학교 (phdyoon@paran.com)

개인정보영향평가를 수행할 수 있으며, 이러한 일련의 프로세스를 이용한 개인 정보 유출에 대한 위험 측정 방안과 위험평가 결과를 토대로 위험에 효율적으로 대응할 수 있는 방안을 제시한다. 또한 본 연구에서 제시하는 내용은 최근 구축된 'SK Telecom 개인정보 영향평가 체계 및 시스템'의 사례를 중심으로 서술한다.

Ⅱ. 본 론

2.1 개인정보 영향평가 모델

개인정보영향평가[4] 제도는 예방의 원칙에 기초를 두고 있다. 즉, 정보화 사업의 계획단계에서부터 개인정보의 보호를 위한 대책을 사전에 마련하게 되면 개인정보의 침해 가능성을 처음부터 최소화하여 정보화에 대한 불신감을 해소하고, 정보화 사업이 추진된 후에 개인정보 등의 침해를 이유로 사업이 도중에 중단되거나 변경됨으로써 발생하는 예산의 낭비를 미연에 방지할 수 있도록 하는데 취지가 있다.

2.1.1 보호 대상 개인정보

개인정보 영향평가를 위해서는 가장 먼저 기업 내에서 취급하고, 보호해야 하는 개인정보는 무엇인지를 식별하고, 해당 개인정보가 가지는 조직 내 민감도를 확인하는 것이 중요하다. [표 1]은 보호대상이 되는 개인정보를 분류한 예이다.

[표 1]에서 민감도를 구분한 내용은 다음과 같다. 이때, 한 가지 이상의 민감도 S인 개인정보를 취급하는 경우는 일반적으로 개인정보영향평가를 수행하는 것이 바람직하다.[5]

〔표 1〕 보호대상 개인정보 식별(SK Telecom 사례)

대분류	소분류	개인정보	민감도	영향평가 여부
신상정보	고객기본정보	주민등록번호	SU	필수 조건
		사업자번호	SU	필수 조건
		성명	SG	필수 조건
		핸드폰번호	SN	필수 조건
		FAX번호	G	선택 조건
(중략)				
금융정보	신용정보	신용카드 사용여부	G	선택 조건
		카드번호	SU	필수 조건
		카드비밀번호	SG	필수 조건
		카드유효기간	G	선택 조건

G : 일반 정보

S : 민감 정보

(SU : 고유 식별정보, SN : 고유 식별정보는 아니나 핸드폰 번호와 같이 준고유 식별 정보, SG : 기타 비고유 정보)

산업군 별로 취급하는 개인정보의 종류, 중요도에 대한 인식도 차이가 있을 수 있다. 예를 들어 이동통신사업자의 경우에는 단말정보, 위치정보 등이 중요하며, 금융기관의 경우에는 신용, 계좌 정보 등이 가장 핵심 되는 개인정보가 될 수 있다.

2.1.2 평가의 주체

개인정보영향평가팀[6]의 구성은 조직에 따라 서 다를 수 있지만 사업주관부서의 PM(기획자), 영향평가자와

4) 개인정보영향평가(PIA: Privacy Impact Assessment)란 개인정보를 취급하는 정보화 사업을 추진하는 과정에서 신규로 도입 또는 개발할 경우, 중요한 변경이 발생할 경우에 정보시스템 등이 개인정보에 어떠한 영향을 미치는지를 사전에 파악하여 대책을 마련함으로써 개인정보의 침해 가능성을 최소화하는 일련의 절차를 말한다. (KISA, 기업의 개인정보 영향평가 수행을 위한 가이드, 2005)

5) ① 개인정보 영향평가의 대상이 되는 사업 범위는 다음과 같다.
- 개인정보를 다량 보유, 관리하는 정보시스템의 신규 구축 사업
- 신기술 또는 기존 기술의 통합으로 프라이버시 침해 가능성이 우려되는 기술을 사용하는 사업
- 개인정보를 보유.관리하는 기존 정보시스템을 변경하는 사업
- 개인정보의 수집.이용.보관.파기 등 일련의 단계에서 중대한 개인정보 침해 위험이 발생할 가능성이 있는 사업

② 다만, 개인정보의 수집.이용 등과 관련된 새로운 정보시스템의 구축이 기존 프로그램이나 시스템에 대한 경미한 변경인 경우에는 개인정보 영향평가를 수행하지 않을 수 있다.(KISA, 기업의 개인정보 영향평가 수행을 위한 가이드, 2005)

6) 개인정보 영향평가는 기업이 자율적으로 개인정보 침해 위험을 분석.평가하고 이에 따른 개선 방안을 도출하는 것이므로, 해당 기업 내 개인정보보호 전담조직 혹은 별도의 평가팀을 구성하여 수행한다. 그러나, 필요한 경우 관련 분야에 대한 외부 전문가의 도움을 받을 수도 있다. 개인정보 영향평가를 수행하는 자는 개인정보보호 관련 법령.지침, 시스템 개발.분석 등에 대한 전문지식을 갖추어야 하며, 개인정보관리책임자는 개인정보 영향평가 수행에 대한 총괄책임을 진다. (KISA, 기업의 개인정보 영향평가 수행을 위한 가이드, 2005)

보안관리자는 반드시 참여해야 한다. 이 때, 보안관리자가 영향평가자의 역할을 병행할 수도 있다.

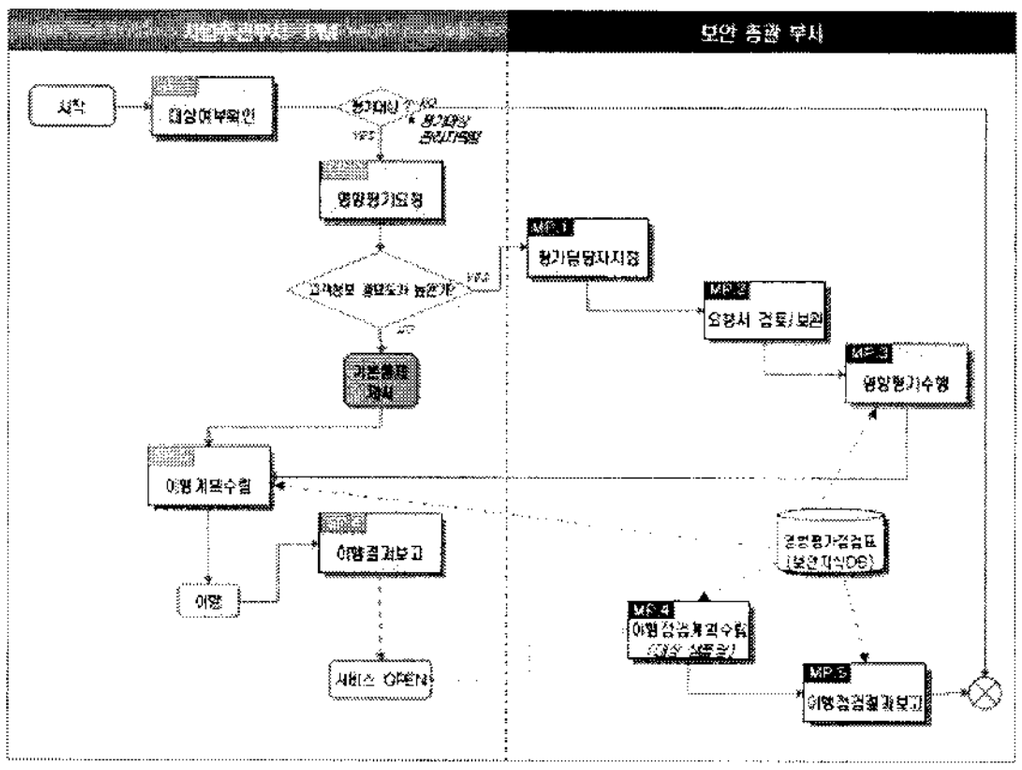
보안관리자는 위협으로 발생되는 위험결과에 대한 속성들을 식별 한 후에 각 속성에 대한가산성을 검토하고 최종적인 영향도를 산정할 수 있는 평가 속성의 가치를 도출하고 단일 속성함수를 정한다. 또한 개인정보가 유출될 위협을 정의 하고 이에 대한 표준 보안대책을 사전에 준비한다.

영향평가자는 사업주관부서 PM이 제공하는 사업 정보를 이해하고 보안 관리자가 제공하는 위협에 대한 정보를 모두 분석하여 정해진 단일 속성 함수를 사용하여 개인정보 보안 수준이 기업에 미칠 수 있는 영향도를 최종 평가하게 된다.

2.1.3 평가 프로세스

개인정보 영향평가는 새로운 시스템을 구축하거나, 기존 시스템을 변경하는 경우에 발생할 수 있는 개인정보 침해 요인을 사전에 분석하는 것이므로, 일반적으로 시스템(변경) 구축 전단계인 사업 방향 설정 및 업무 정의 단계, 시스템 제안단계, 시스템의 예비 설계 및 모형 설정 단계 등에서 수행된다. 그러나 기존 서비스 운영 중에라도 개인정보의 수집, 이용 및 관리상에 중대한 침해 위험이 발생할 가능성이 있다면 개인정보 영향평가를 수행한다.[7)]

[그림 1]은 개인정보영향평가 프로세스로 대상여부확인, 영향평가요청, 평가담당자지정, 영향평가수행, 이행계획수립, 이행결과보고, 이행점검계획수립, 이행점검결과보고로 구성되어 있다.



〔그림 1〕 개인정보영향평가 수행 프로세스(SK Telecom 사례)

대상여부확인 단계에서는 민감한 개인정보를 취급하는 사업을 선별함으로써 개인정보영향평가 대상여부를 확인한다.

영향평가 요청단계에서는 정보화사업의 유형 구분, 프로젝트 개요 정리, 조직 및 인프라정보 정리, 취급개인정보 확인, 데이터 흐름 및 업무분석, 점검표에 대한 보안대책 이행계획 작성 등을 수행한다.

평가담당자로 지정되면 평가담당자는 요청서를 검토/보완 후 영향평가를 수행하여 평가결과보고서를 전달한다.

평가결과 도출된 개선필요사항에 대해서 이행계획을 수립하고 이행 결과를 보고한다.

영향평가 종료 후 운영 중인 서비스에 대하여 점검대상을 선정하여 이행점검을 실시한다.

2.1.4 평가 내용

산업군 별로 사업 환경이 다를 수 있으며, 기업 내에서도 제공하는 서비스마다 고유 특성의 차이가 클 수 있는데 이러한 차이는 영향평가 시 집중해야 하는 보안위협이 서로 다를 수 있음을 시사한다. 일례로 웹서비스의 경우에는 악성코드를 이용한 웹 브라우저 해킹으로 개인정보가 유출될 위협이 중요한 이슈가 될 수 있지만 시스템 개발과 상관없이 개인정보를 이용하는 이벤트/프로모션의 경우에는 고려될 필요가 없다.

보안관리자는 어떤 위협이 조직의 사업영역에 잠재적인 위험이 되는지를 결정하고 조직 내부의 서비스 유형을 정하여 유형별로 관심이 되는 위협을 순서대로 나열한 후 위협과 관련한 보안대책을 연관하여 검토한다.

[표 2]는 보안대책의 영역을 구분한 후 각 영역별로 점검 내용을 정리한 것이다.

2.2 개인정보 유출 위험의 측정 방안

위험이란 개인정보 자산에 대한 위협과 취약성으로 말미암아 발생할 수 있는 부정적 영향으로 보통은 사업 목적을 달성하는데 방해가 되는 현상을 의미한다. 개인정보 영향평가도 일련의 위험 평가 방법론으로써 개인정보가 유출될 경우 조직이 감당해야 하는 위험을 평가하는 작업으로 표현이 가능할 수 있다.

7) 참고자료 : 기업의 개인정보 영향평가 수행을 위한 가이드 (KISA, 2005)

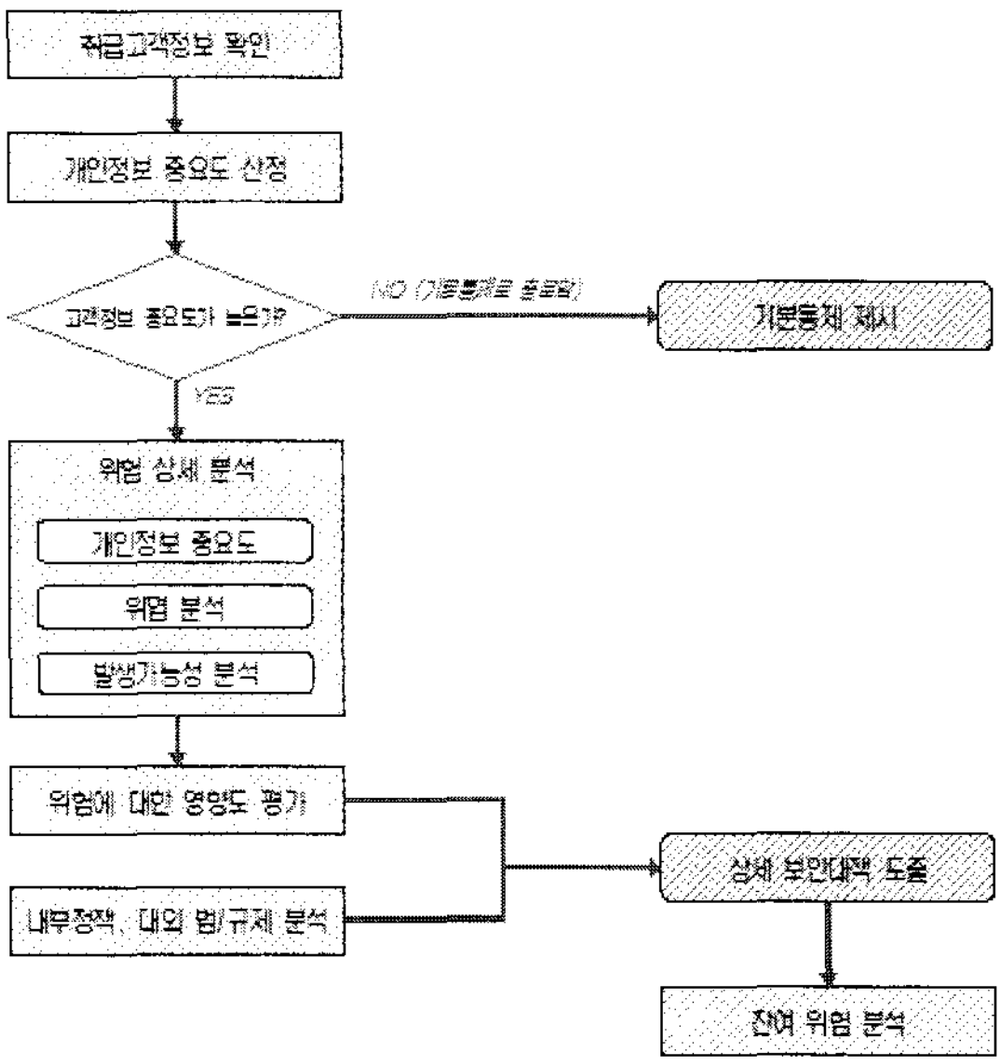
〔표 2〕 보안 대책 영역 (SK Telecom 사례)

보안대책 영역	점검 내용
정보화 사업 기획의 검토	- 기획 시 법률 검토 및 인허가 - 개인정보 취급 계획의 명시 등
개인정보보호 체계 수립	- 개인정보 보호 조직 및 개인정보 보호 정책 등
개인정보 주체의 권리 보장	- 고객의 고충처리 - 고객의 개인정보 처리 요구에 대한 대응 등
개인정보 수집 시 보호	- 개인정보 수집관련 방침 고지 - 수집 시 본인확인, 동의, 제한 절차 등
개인정보 이용 시 보호	- 이용약관 고지 - 이용 시 동의/승인, 제한, 통제 등
개인정보 저장 시 보호	- 저장기간의 제한, 저장매체의 백업 - 저장 시 통제방안 마련 등
개인정보 제공 시 보호	- 제공 시 신원확인, 동의/승인, 제한, 통제 등
개인정보 파기 시 보호	- 장비 및 데이터의 안전한 파기 - 파기 시 통제방안 마련 등
개인정보 기입서류 등의 처리 및 파기	- 구비서류의 수집/보관/관리/파기 시 통제 등
개인정보 처리의 위탁 시 통제	- 위탁계약 및 범위, 수탁업체 감사, 통제 등
개인정보보호를 위한 인적통제	- 개인정보 취급자, 수탁업체, 외주인력 관리 등
개인정보보호를 위한 관리적 조치	- 개인정보 현황 파악, 최신성 유지 - 교육 및 훈련 - 백업시스템, 보안시스템 구축/유지보수 - 운영 환경의 분리 및 모니터링 접근통제 등
개인정보보호를 위한 기술적 조치	- 인증, 암호화, 접근통제, 로깅, 안티 바이러스, 소스코드보안 - 신상정보 마스킹 등 기술적 보안통제 등
침해사고 발생 시 사후 구제체계	침해사고 대응 등

개인정보 영향평가 시, 최종적인 위험 수준 산정을 위해서는 평가 대상 서비스가 취급하는 개인정보 중요도와 개인정보 유출시 위험의 심각도, 발생가능성을 고려해야 한다.

2.2.1 개인정보 중요도 분석

일반적인 위험분석을 효과적으로 수행하기 위해서는 우선 서비스의 중요도를 파악하여 영향도 평가의 범위 및 깊이를 결정해야 한다. 개인정보 영향평가의 경우에는 서비스가 취급하는 개인정보의 중요도가 서비스 자체의 중요도를 대변할 수 있다.



〔그림 2〕 위험 분석 프로세스의 차별화

영향도 분석은 수준에 따라서 수행 절차가 복잡하고, 시간과 인력 소모가 크므로, 시스템 환경에 맞는 분석 수준을 선택하는 것은 중요하다.

[그림 2]는 개인정보 중요도에 따라서 위험분석 프로세스가 차별화 되는 것을 보여준다.

일반적으로 개인정보 중요도가 높아서, 개인정보가 유출될 경우 조직에 미칠 영향이 크다고 판단되면 상세 영향도 분석을 수행하는 것이 바람직하며, 그 외의 경우는 기본 통제 제시만으로도 충분할 수 있다.

기본 통제 방식으로 구분을 하는 목적은 보안 대책을 실시하는데 드는 비용과 시간을 최소화할 수 있다는 장점 때문이다. 하지만 기본통제의 수준이 지나치게 높을 경우에는 불필요한 고정비용이 들 수 있고 너무 낮을 경우에는 필수 통제가 간과되어 해당 서비스들이 공통된 취약성을 그대로 노출 시킬 수 있는 단점도 가진다.

따라서 보안 관리자는 기본통제 방식을 대내외 규제 수준에 따라서 적절한 수준으로 조정하는 것이 중요하다.

[표 3]은 개인정보를 보유한 서비스의 개인정보 중요도를 평가하는 방법으로써 단일 개인정보가 아니더라도 조합했을 때 수준이 높은 경우에는 중요도가 높아질 수 있음을 보여준다.

개인정보 중요도 산정 결과는 유효성을 확보하기 위하여 현실과의 일치성을 검토한 후 조정하는 것이 바람직하다.

〔표 3〕 서비스별 취급 개인정보의 중요도 산정 기준

개인정보조합	개인정보조합 설명	중요도	설명	영향평가 필요여부
G	민감하지 않은 일반정보	N/A	아무런 영향을 미치지 않는 수준	선택조건
G + G	민감하지 않은 일반정보가 두 개 이상 조합이 되는 경우	Level 1	정확한 개인정보에 대해서는 알 수 없지만 대외 이미지 저하가 생길 수 있는 수준	필수조건
SN	핸드폰번호	Level 2	개인의 신분에 대한 추정이 가능하여 소액의 피해보상을 요구 받을 수 있는 수준	필수조건
SG	일반적인 민감정보			
SG + G	일반적인 민감정보와 민감하지 않은 일반정보의 조합			
SN + G	핸드폰번호와 민감하지 않은 일반정보가 조합되는 경우	Level 3	개인의 신분과 신상정보에 대한 추정이 가능하여 다소 큰 금액의 피해보상을 요구 받을 수 있는 수준	필수조건
SU	개인 및 회사 고유 식별 정보	Level 4	개인의 신분을 알 수 있으며 회사에 지대한 피해를 미칠 수 있는 수준	필수조건
SU + G	개인 및 회사 고유 식별 정보와 민감하지 않은 일반정보가 조합되는 경우	Level 5	개인의 신분 및 신상정보에 대해 알 수 있으며 회사의 경영 상태에 영향을 미칠 수 있는 수준	필수조건

2.2.2 위험 심각도 분석

위험의 심각도는 서비스 환경이 잠재적으로 가지고 있는 속성인 취약성이 위협에 의하여 현실화 되었을 때, 나타날 수 있는 잠재 위험의 정도를 말한다.

이 때, 취약성이란 위협이 개인정보 자산에 기밀성, 무결성, 가용성의 상실을 가져올 수 있게 하는 상황으로 정의되며, 일반적으로 대상 시스템의 취약성은 반드시 내재되어 있다. 취약성은 위협 요소와 연계되어 현실화 되었을 때 위험으로써의 시나리오를 이루기 때문에 보안관리자는 이러한 시나리오가 현실에서 가능한 것인지를 반드시 검토해서 영향도 반영 여부를 결정해야 한다.

[표 4]는 위험 별로 심각도에 대한 산정 방법으로 영향평가 시 사용되는 점검표의 개별 점검항목 별로 보안관리자가 조직의 특성을 고려하여 책정한다.[표 4]에서는 위험의 심각도 산정 시, 가산속성으로써 사법처리, 재무손실, 기업이미지, 업무연속성이 사용되었다. 이러한 가산속성은 조직에 따라서 달라질 수 있다. 즉, 영리를 추구하는 기업의 경우에는 재무손실 등이 중요한 속성이 될 수 있지만, 공공성이 강한 조직의 경우에는 재무손실 보다는 공신력 등이 더 중요한 속성으로 활용될 수도 있으므로 보안관리자는 조직의 비전 및 특성을 정확히 이해하여 가산속성을 정해야 한다.

2.2.3 위험 발생가능성 분석

위협이란 개인정보 자산의 기밀성, 무결성, 가용성을

〔표 4〕 위험별 심각도 산정 방법 (SK Telecom 사례)

구분		가산 속성				심각도
분류	관련 위험	사법처리	재무손실	기업이미지	업무연속성	
유출	내부 직원에 의한 개인정보 유출	1	1	1	0	0.75
	내부에서 협력직원에 의한 개인정보 유출	2	2	3	1	2.00
	외부의 개인정보취급자에 의한 개인정보 유출	-				
	외부에서 비인가자의 시스템 침입에 의한 개인정보 유출					
위변조	개인정보 무단 위변조					
대응	보안사고 발생 시 적절한 대응 부재					
	보안사고 발생 시 추적이 불가능함					
법률	관련 법률 위반					
관리	안전한 개인정보 처리 불가능함					

〔표 5〕 점검표 중 이행수준 확인 부분 (SK Telecom 사례)
(※ 이행수준: Y는 적용, N은 미적용, P는 부분적용, N/A는 해당없음)

구분		점검 항목	심각도	이행수준
정보화 사업 기획의 검토	법률 검토	신규사업이나 서비스 기획 시, 관련 법률이나 정부의 인허가를 필요로 하는지 검토하였습니까? ※ 이벤트 및 프로모션도 포함함	1.0	Y
	개인정보 취급계획 명시	사업기획서 혹은 시스템 개발 계획서에 사용할 개인정보의 수집 목적 및 최소 범위가 명시되어 있습니까? 예) 수집목적 사용자인증, 수집범위 성명, 주민등록번호, MIN, ESN	0.5	N
	개인정보 취급계획 명시	개발하고자 하는 시스템의 명칭 및 목적, 이용범위, 개발/운영조직, 시스템 운영자의 역할 등이 정의되어 있습니까?	0.5	Y
	개인정보 취급계획 명시	제3자에 대한 개인정보 제공이 시스템 구축 시부터 계획된 사항입니까? ※ 제3자란 고객과 내부직원(내부조직)을 제외한 외부자를 총칭함	0.8	P
개인정보 보호 체계 수립	개인정보 보호 직	개인정보 보호 활동을 수행하는 조직 체계가 구축되어 있습니까? ※ 일반 현업부서에서 수행해야 하는 개인정보보호 활동이란 개인정보의 식별, 흐름파악, 개인정보의 수집/저장/이용/제공/파기 단계에서의 보호대책 수립 등을 포함함	0.8	N/A

위태롭게 할 수 있는 상황으로 즉, 서비스가 근원적으로 가지고 있는 취약점이 현실화 될 수 있는 가능성을 의미하며 발생가능성은 이러한 위협의 정도에 따라 결정되는 수준이다. 또한 발생가능성의 정도는 보안대책의 적용 수준에 따라서 정해진다.

[표 5]는 영향평가 시 점검항목(위협요인)에 대한 보안대책 이행수준을 확인하는 점검표의 예시로써, 점검항목별로 평가하게 된다.

2.2.4 서비스별 위험수준 산출

서비스별 영향도(개인정보 유출 위험)는 다음과 같은 공식으로 산출된다.[8)]

$$\text{서비스별개인정보영향도} = A\frac{1}{n}\left(\sum_{i=1}^{n} Bi(1-Ci)\right)$$

- A : 서비스별 개인정보 중요도
- B : 점검항목별 위험 심각도
- C : 점검항목별 보호대책 이행 수준
- n : 서비스별 총 점검항목 수

이때, 수치가 클수록 위험이 심각하다는 것을 의미하며 반대로 수치가 작을수록 보안수준은 높아진다.

2.2.5 보안대책 도출

영향평가의 가장 큰 목적은 영향도를 측정하는 것이지만 이에 못지않게 비용효과적인 보안대책을 제시하는 것이 중요하다. 비용효과적인 보안대책을 제시하기 위해서는 제한된 비용을 조직에 가장 필요하고, 시급한 보안대책에 우선적으로 투자해야 한다.

보안관리자는 기본적인 보안대책 목록을 사전에 준비하겠지만, 상세한 서비스 유형 및 관련 조직의 환경에 따라서 항상 새로운 보안 대책을 모색하는 노력이 필요하다. 뿐만 아니라 보안대책의 수준을 어느 정도로 할 것인지를 결정하는 것도 중요하다. 보안 대책의 수준이 너무 높은 경우에는 보안성은 높으나 사업성과 측면에서 부담이 될 수도 있기 때문이다.

2.3 개인정보 흐름도를 이용한 위험 통합 모니터링 체계

2.3.1 서비스별 개인정보 흐름 분석

다양한 배경 지식을 가진 담당 실무자들이 당해 사업과 개인정보의 흐름에 대한 이해를 쉽게 하고, 상호간의 의사소통을 원활하게 하기 위하여 계획된 사업의 주요 업무절차와 그에 따라 조직 내에서 개인정보가 어떻게 흘러가는지를 대략적으로 보여주는 것이 중요하다.[9)]

개인정보의 흐름 분석을 위해서는 개인정보 라이프

8) 참고 : KISA에서 제시하는 영향도 산정 공식
개인정보 자산의 민감도 평가 결과와 위협/취약성 평가 결과를 종합하여 기밀성, 무결성, 가용성 측면의 위험도를 산출한다
* 위험도 산출(Risk Value) = 개인정보 자산의 민감도(Asset Value) + 위협의 정도(Threats Value) + 취약성의 정도(Vulnerability Value)
(KISA, 기업의 개인정보 영향평가 수행을 위한 가이드, 2005)

9) 참고자료 : 기업의 개인정보 영향평가 수행을 위한 가이드 (KISA, 2005)

〔표 6〕 개인정보 라이프 사이클별 흐름분석을 위한 검토항목 (SK Telecom 사례)

단계	구분	검토 항목
수집	수집하는 사람 혹은 시스템	서비스 기획자, 개발자, 운영자, 현업부서 담당자, 외부협력업체 직원, 대리점/위탁업체 그리고 시스템 등
	수집 방법	WEB(WAP)을 통한 고객의 직접 입력, 종이신청서 혹은 FAX, 개인정보 기보유 시스템(혹은 DB)와의 연동, 고객센터/대리점 등에서의 담당자 입력, Air 구간 등 타시스템(혹은 DB)와의 연동 시에는 연동과 관련된 상세 정보 필요
저장	저장장소(매체)	PC, 파일서버, DBMS, 서버의 로그파일 등
	저장 형태	암호화, *로 마스킹처리 등
이용	이용하는 사람 혹은 시스템	서비스 기획자, 개발자, 운영자, 현업부서 담당자, 외부협력업체 직원, 대리점/위탁업체 그리고 시스템 등
	이용 방법	화면 조회, 출력, 파일저장 등
제공	제공하는 사람 혹은 시스템	서비스 기획자, 개발자, 운영자, 현업부서 담당자, 외부협력업체 직원, 대리점/위탁업체 그리고 시스템 등
	제공받는 사람 혹은 시스템	서비스 기획자, 개발자, 운영자, 현업부서 담당자, 외부협력업체 직원, 대리점/위탁업체 그리고 시스템 등
	제공 방법	시스템과 네트워크를 이용한 연계, 대량의 개인정보 파일을 송신 등
파기	파기하는 사람 혹은 시스템	서비스 기획자, 개발자, 운영자, 현업부서 담당자, 외부협력업체 직원, 대리점/위탁업체 그리고 시스템 등
	파기 방법	주기적 DB 삭제(Delete, Drop포함), HDD포맷, 전송후 파기, 서류 파쇄 등

사이클을 수집, 저장, 이용, 제공, 폐기 등과 같이 구분하여 각 단계의 수행 업무를 명확히 하는 것이 바람직하다. 또한 보안관리자는 각 단계별로 검토되어야 하는 항목을 정해야 한다.

[표 6]은 개인정보 라이프 사이클 단계별 흐름분석을 위한 검토 필요 항목이다.

보안담당자는 단계별로 발생할 수 있는 위험의 유형을 숙지하고 이를 판별할 수 있는 근거자료로써 활용될 수 있는 검토항목을 정할 수 있어야 한다. 이 때, 각 단계별로 조직 내에서 개인정보가 가지는 위협을 먼저 이해하는 것이 필요한데, [표 7]은 개인정보 라이프사이클 단계별로 고려될 수 있는 위험의 유형을 정리한 것이다.[10)]

이 때, 타시스템(혹은 DB)와의 연동을 통한 개인정보 수집 혹은 제공 시에는 연동과 관련한 직접적인 개인정보 흐름도 상세 구성 정보가 추가적으로 필요하다. 상세 구성정보는 연동 개인정보, 연동 상대 시스템(혹은 DB), 연동 업무 목적, 연동 프로토콜(예 : FTP, DB Link 등)이 포함된다.

〔표 7〕 개인정보 라이프사이클 단계별 위험 유형

발생 단계	침해유형	설명
수집	불법 수집	정보주체의 동의 없는 개인정보 수집 개인의 사생활이나 권리를 침해할 수 있는 정보 수집 등
	수집시 해킹으로 인한 유출, 위변조, 손실	- 암호화, 마스킹처리 미흡으로 인한 유출 - 접근통제, 인증 등의 취약으로 인한 해킹수집 시 악성코드, 바이러스 등으로 인한 유출 등
저장	불법 저장	- 허용되지 않은 형태로의 보관 ex. 개인 PC상의 파일 형태로 보관 등
	저장 시 해킹으로 인한 유출, 위변조, 손실	접근통제, 인증, 암호화 등의 취약으로 인한 해킹 등 - 백업 체계의 부재로 데이터 복구 불가능
이용	불법 이용	- 수집 목적 이외의 용도로 정보를 활용하는 행위 - 정보 주체의 동의를 구하지 않은 채, 제3자에게 정보를 제공하거나 판매하는 행위 - 동의가 철회되거나 수집 목적이 달성된 자료의 불법 보유부당하게 취득한 개인정보를 2차적으로 악용
	수집 시 해킹으로 인한 유출, 위변조, 손실	- 암호화, 마스킹처리 미흡으로 인한 유출 - 접근통제, 인증 등의 취약으로 인한 해킹 - 이용시 악성코드, 바이러스 등으로 인한 유출 등
제공	불법 제공	정보주체 동의 없이 제 3자에 제공 등
	제공 시 해킹으로 인한 유출, 위변조, 손실	- 암호화, 마스킹처리 미흡으로 인한 유출 - 접근통제, 인증 등의 취약으로 인한 해킹 등
파기	파기된 데이터가 유출	- 파기 시 통제 부재로 파기자에 의한 악용 - 기술적으로 불완전한 파기로 인한 유출

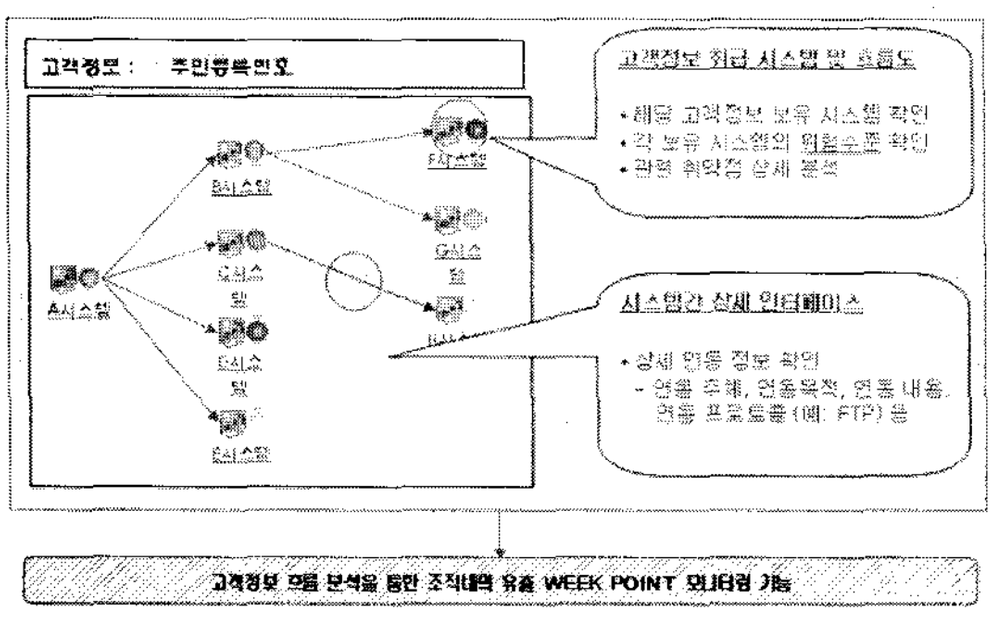
10) 참고자료 : 개인정보 수명주기에 따른 개인정보관리모델에 관한 연구 (김현철, 고재우, 최명길)

2.3.2 전사적 개인정보 흐름 분석 및 통합 모니터링

개별 서비스에 대한 영향도 평가 후 위험수준이 결정되고, 개인정보 흐름도 분석이 완료되면 다음 단계로써 조직 전체적으로 개인정보가 유출될 수 있는 가능성을 통합하여 모티터링 하는 것이 가능해진다.

[그림 3]은 이러한 발상을 토대로 개인정보 흐름도를 중심으로 한 통합 위험 DASHBOARD를 구성한 사례로써, [그림 3]과 같이 개인정보 흐름도를 가시화하게 되면 전체 조직 내에서 특정 개인정보를 취급하는 전체 시스템에 대한 실시간 모니터링을 할 수 있으며 이는 각 개인정보가 조직 내에서 가지는 위험수준을 한눈에 판단할 수 있도록 도와준다.

즉, 주민등록번호와 같은 특정 개인정보에 대해서 이를 보유하고 있는 서비스 중에 위험 수준이 높은 서비스가 존재할 경우 주민등록번호가 해당 서비스에 의해서 유출될 수 있는 가능성이 있음을 시사하는 것이므로, 이 경우 해당 서비스가 위험 수준이 높은 이유, 즉 이행되지 않고 있는 보안대책이 무엇인지를 쉽게 찾아볼 수 있다면 보안 관리자로 하여금 보다 신속하고 효과적으로 전사적 대응이 가능하도록 할 수 있다.



〔그림 3〕 개인정보 흐름도 모니터링 방안
(SK Telecom 사례)

Ⅲ. 결 론

인터넷과 e-Business의 발전으로 인해서 개인정보에 대한 위협이 날로 커지고 그 심각성에 대한 인식이 높아지고 있다. 개인정보가 유출되었을 경우 당사자 개인이나 유출 요인을 제공한 민간 기업 모두 큰 피해를 입게 되며, 이는 IT산업 자체에 대한 회의를 불러올 수 있다. 따라서 본 연구에서는 민간업체에서 수행할 수 있는 개인정보보호 노력의 일환으로 개인정보영향평가라는 활동을 통해 위험수준을 산정해보고 개인정보 흐름을 분석하여 궁극적으로는 전사적으로 개인정보 위험에 대한 통합 모니터링을 가능하게 하는 방안을 제시하고 있다. 이는 SK Telecom에서의 성공적인 구축사례를 바탕으로 하며, 대량의 개인정보를 취급하는 민간기업에서 각 조직의 특성을 반영하여 적극적으로 접근할 경우 효과적으로 반영할 수 있는 모델이 될 수 있다.

참고문헌

[1] 개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리 모델 연구, 한국정보보호진흥원, 2006. 12
[2] 개인정보보호 기술의 동향, 송유진 외, 주간기술동향 1218호, 2005.10
[3] 인터넷과 개인정보의 보호, 최정열, 한국정보법학회, 2002
[4] 김성언, 개인정보 침해에 관한 조사 연구, 한국형사정책연구원, 2001
[5] 개인정보 수명주기에 따른 개인정보관리 모델에 관한 연구
[6] 한국정보보호진흥원 홈페이지 http://www.kisa.or.kr
[7] 국회 홈페이지, http://www.assembly.go.kr
[8] 정보통신망법 및 시행령, 시행규칙 개정에 따른 개인정보보호 조치사항, 한국정보보호진흥원, 2007.07
[9] 정보통신망법 개인정보보호규정의 적용범위, 한국정보보호진흥원, 2005.11
[10] 기업의 개인정보 영향평가 수행을 위한 가이드, 한국정보보호진흥원, 2006. 1
[11] 김기윤/나관식, 다속성 위험평가기법을 이용한 정보시스템의 위협지수 측정,
[12] 공공기관의 개인정보보호에 관한 효율성 분석, 한국지방자치학회, 2006

〈著者紹介〉

이 기 혁 (Lee Gi Hyouk)
정회원

1988년 2월 : 시립인천대학교 물리학과졸업
1991년 2월 : 한양대학교 공학석사
2008년 3월~현재 : 건국대학교 공학박사 과정중
1994년 5월~현재 : SK Telecom (주)정보기술연구원 재직중
<관심분야> 정보통신공학, 정보통신정책분야,정보보호학,개인정보보호공학등
<저서>유비쿼터스 사회를 향한 기술과 서비스(2005,진한엠엔비)
유비쿼터스 컨버젼스(2004,진한엠엔비)
데이터네트워크 구축론(2000,진한엠엔비)
차세대무선인터넷기술(2003,진한엠엔비)
유무선인터넷의 이해와 활용(2001,진한엠엔비)등 다수

윤 재 동 (Young Jae Dong)

1985년8월 : 단국대학교 무역학과 졸업
1993년 2월 : 고려대학교 경영학 석사
2007년 2월 : 건국대학교 경영학 박사
2007년 3월~현재 : 건국대학교 겸임교수
<관심분야> IT벤처기업, 정보보호학