"개인정보보호 밑 빠진 독에 물 붓기"

개인정보 무방비 노출, 대책시급
…전문가 아니더라도 타인 개인정보 습득 손쉬워

임태훈 연구원/한국데이터베이스진흥센터 연구개발팀

K사에 근무하는 이모씨는 인터넷을 써핑하다가 우연히 모회사의 신입사원 합격자 명단을 보게 되었다. 이 명단에는 신입사원들의 이름과 주민등록번호가 나와있었다. 이씨는 명단에 나와 있는 이름 중에서 김모씨를 골라, 무료로 E-mail 계정을 제공하는 W사에 접속한 후, 인명검색을 했다.

많은 사람들이 이용하는 W사에는, 이씨의 예상대로 합격자 명단에서 골랐던 김씨가 가입되어 있었다. 인명검색으로 이씨는 김씨의 아이디를 쉽게 알아낼 수 있었다. 문제는 비밀번호. 이씨는 주민등록번호를 몇 번 조합해서 비밀번호를 입력한 뒤, 로그인을 시도했지만 에러 메세지가 계속 나타났다. 그러나, 문제는 곧 해결되었다.

이씨는 로그인 아래 있는 버튼 〔비밀번호를 잊으셨나요?〕를 클릭했다. 그러자, 이름과 주민등록번호, 비밀번호를 받을 E-mail 주소를 입력하는 란이 나왔다. 이씨는 김씨의 이름과 주민등록번호, 이씨 자신의 E-mail 주소를 입력하였다.

약 5분 뒤, 이씨는 명단에서 골랐던 김씨의 비밀번호를 자신의 E-mail로 받아볼 수 있었다. 아이디와 비밀번호를 알아낸 이씨는 김씨의 전자우편들을 낱낱이 볼 수 있었다.

친구와 애인의 편지는 물론, 온라인 결제대금 청구서 등의 신용정보도 알아낼 수 있었다. 뿐만 아니었다. 〔개인정보 조회와 수정〕 버튼을 누르고 아이디와 비밀번호를 입력하자, 집 주소 · 직장주소 · 소속 · 전화번호 · 이동통신번호 · 학력 · 취미 · 관심분야 등이 고스란히 드러났다.

이 정도의 정보를 조합하니, 김씨가 대략 어떤 사람인가를 가늠할 수 있었다. 이씨는 온라인 결제대금 청구서를 통해, 김씨가 가입되어 있는 모 이동통신회사를 알아내었고, 곧 사이트에 접속하였다. 대부분의 사람들이 하나의 아이디와 비밀번호를 사용하기 때문에, 이 사이트에도 쉽게 로그인할 수 있었으며, 곧 김씨의 신용카드 번호를 알아낼 수 있었다. 이씨는 김씨의 신용카드 번호로 인터넷 쇼핑몰에서 각종 물건을 구입하고 김씨의 카드번호로 대금을 결제해 버렸다.

위에서 가정한 상황은 이제 뉴스거리도 되지 않을 만큼 소위 "뻔한 스토리"가 되어버렸다. 인터넷 업체들의 보안상태는 이미 깨진 독이 되어버렸고, 회원들의 개인정보는 물이 새듯이 술술 새어나가고 있다.

지난 6월에는 네이버와 엠파스 등의 강력한 검색엔진 덕분(?)에 몇 개의 검색어를 조합 · 검색하였을 때, 타 인터넷서비스업체에 가입되어 있는 회원들의 주소, 전화번호, 이름 등이 그대로 드러나기도 했다.

새어나가는 개인정보를 막기 위해 정보통신부는 대책 마련에 고심하고 있다. 지난 6월 1일부터는 개인정보보호지침이 본격적으로 시행되었다.

개인정보보호지침은 서비스제공업체가 서비스 성격에 맞게 〔개인정보보호방침〕을 마련하여 준수하도록 규정하고 있다. 〔개인정보보호방침〕이란 용어는 개인정보보호정책, 개인정보방침, Privacy Policy, Privacy Statement 등으로도 쓰이고 있다.

서비스제공업체는 이 방침을 홈페이지 메인화면에 링크시켜 이용자들이 언제든지 볼 수 있도록 하고, 방침내용에 쿠키(cookie)의 운영에 관한 사항, 기술적 · 관리적 대책, 개인정보

관련 불만처리에 관한 사항, 개인정보보호방침의 개정에 관한 사항, 개인정보 관리책임자의 소속 · 성명 및 전화번호 기타 연락처, 개인정보의 수집목적 및 이용목적, 개인정보를 제3자에게 제공하는 경우의 제공받는 자 · 제공목적 및 제공할 정보의 내용, 동의 철회 · 열람 또는 정정 요구 등 이용자의 권리 및 그 행사방법, 서비스제공자가 수집하고자 하는 개인정보항목, 수집하는 개인정보의 보유기간 및 이용기간, 기타 아동에 관한 조치사항 등을 포함할 것을 규정하고 있다.

개인정보보호지침은 이전까지는 권고안의 성격에 그쳤으나, 6월 1일부터는 정보통신망이용촉진 등에 관한 법률에 근거하여 최고 500만원까지의 과태료를 부과할 수 있게 되었다.

실제로 정보통신부는 지난 6월 8일부터 17일까지 개인정보침해신고센터에 신고된 300개 인터넷 사이트를 대상으로 개인정보보호규정 준수실태를 조사하여 13개 업체에 2백~3백만 원의 과태료를 부과하고, 위반정도가 경미한 249개 업체에는 시정명령을 내렸다.

이들 13개 업체는 이용자의 개인정보를 수집하면서 개인정보 관리책임자의 성명과 연락처, 정보수집 및 이용목적, 제3자 제공 여부, 동의철회 등 이용자 권리와 행사방법 등을 미리 이용자에게 알려주거나 이용약관에 명시하지 않았다.

단속내용과 같이, 인터넷 서비스제공업체가 개인정보보호지침을 무시하여 이용자가 피해를 입는 유형은 대략 서비스의 내용과 무관하게 개인정보를 과다하게 요구하는 경우, 이용자의 동의 없이 광고주 등 제3자에게 개인정보를 제공하는 경우, 이용자의 동의철회 및 회원탈퇴 요구에도 개인정보를 삭제하지 않는 경우, 서버보안장치의 미비로 해킹 등을 통해 개인정보가 외부에 노출되는 경우 등이다.

이러한 업계의 현실에 대해, 인터넷 서비스업체들은 개인정보보호지침이 제대로 전달되지 않았으며, 지침의 내용도 현실과 차이가 크다고 주장하고 있다.

게다가 9월 1일부터 개인정보보호지침과 마찬가지로 [정보통신망이용촉진등에관한법률]에 근거를 두고 있는 정보통신서비스 정보보호지침이 별도로 시행되고 있어 업체들의 혼란은 더욱 커질 것으로 예상된다.

정보통신서비스 정보보호지침은 정보통신서비스제공자, 정보시스템운영자, 이용자 등이 지켜야 할 구체적인 사항을 규정하고 있으며, 이 규정에 따라 정보통신서비스 제공자는 해킹 · 컴퓨터 바이러스 피해를 막기 위해 방화벽 등 정보보호장비를 설치해야 한다.

정보통신서비스 정보보호지침에서 다루고 있는 정보의 개념이 개인정보보호지침의 정보 개념보다 포괄적이라고 할 수 있다. 개인정보보호지침은 개인정보 관리책임자를 지정하고 개인정보방침을 제정하여 게시하도록 규정하고 있으며, 정보통신서비스 정보보호지침은 정보보호 책임자와 시스템 운영자를 지정하고, 정보보호내부방침을 마련하도록 규정하고 있다.

그러면, 개인정보보호를 위해 인터넷 서비스업체가 가장 서둘러야 하는 것은 무엇일까 ? 먼저, 개인정보보호방침을 마련해야 한다.

개인정보보호지침 규정에 따라, 일단 회원을 모집하는 사이트들은 모두 개인정보보호방침을 첫 화면에 게시하여야 한다. 개인정보보호방침은 개인정보보호를 위한 일종의 의지표현이라고 할 수 있다. 개인정보보호방침의 구문을 작성하는데 어려움을 느낀다면 한국데이터베이스진흥센터가 표준화과제로 작성한 표준 개인정보보호방침을 이용하면 된다.

일단 개인정보보호방침을 홈페이지 첫 화면에 게시하였으면, 두 번째로 회원가입을 받을 때 몇 가지 주의를 기울여야 한다. 개인정보는 반드시 필수입력사항과 선택입력사항으로 나누어 수집해야 하며, 선택입력사항을 입력하지 않은 회원에게도 동일한 서비스를 제공하여야 한다. 그리고, 인종 및 민족, 사상 및 신조, 출신지 및 본적지, 정치적 성향 및 범죄기록, 건강상태 및 성생활에 관련된 정보는 이용자의 인권을 침해할 수 있으므로 가능한 한 수집하지 말아야 한다.

세 번째로 개인정보의 수집목적 또는 제공받은 목적을 달성하면, 즉시 개인정보를 폐기하도록 한다. 즉, 탈퇴한 회원이나 정보제공에 대한 동의를 철회한 이용자에 대해 그들의 개인정보를 가능한 한 빨리 삭제해야 한다는 것이다.

이는 대다수의 인터넷 사이트가 지키지 않고 있는 문제로, 회원이 탈퇴한 이후에도 계속해서 개인정보를 보유하고 있는 사이트가 많다. 개인정보보호지침은 수집목적이 달성된 후, 개인정보가 담긴 문서를 분쇄기로 폐기하고, 서버에 담긴 기록은 복원할 수 없게 삭제하도록 규정하고 있다.

그리고, 개인정보를 광고업체나 제휴회사와 공유하는 경우,

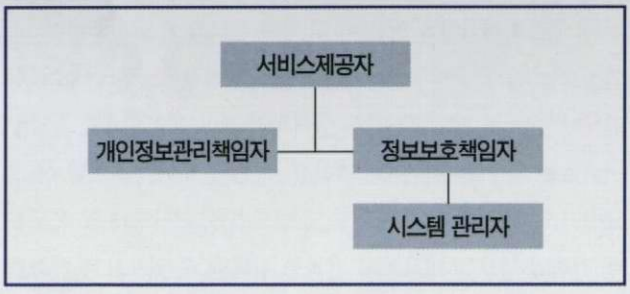
회사가 합병하게 되는 경우, 개인정보의 처리를 외부업체에 위탁하는 경우, 이를 회원들에게 고지하고 이에 대한 동의를 얻어야 한다.

이상은 외부에 보여지는 개인정보보호 조치였고, 이보다 더욱 중요한 것은 내부적으로 정보보호조직을 구성하여 게시한 개인정보보호방침을 지키도록 최선의 노력을 다하는 것이다. 업체 내부에 정보보호조직을 구성하는 것은 정보통신서비스 정보보호지침의 규정에 따른 것이다.

서비스제공자는 정보통신서비스 정보보호지침 제4조에 따라, 정보통신서비스의 안정성과 정보의 신뢰성을 확보하는데 관련된 업무를 총괄하는 "정보보호책임자"와 정보통신서비스에 이용되는 컴퓨터 등 각종 장치를 관리하는 "시스템 관리자"를 지정하여야 한다.

또 개인정보보호지침 제22조에 따라 개인정보의 수집, 이용 및 처리 등의 취급에 관해서 실질적인 권한을 가진 사람을 개인정보 관리책임자로 지정하여야 한다. 따라서, 정보보호조직은 다음과 같은 모습을 갖게 된다.

<그림> 정보보호조직 구성도



정보통신서비스제공자는 제공하는 정보통신서비스에 적합한 정보보호 조치사항을 계획, 구현, 승인, 감독할 수 있는 정보보호조직체계를 수립해야 하며, 정보보호책임자와 시스템 관리자, 개인정보 관리책임자를 지정하고 업무를 관리 · 감독해야 한다.

소규모의 영세한 서비스제공자의 경우, 정보보호책임자와 시스템 관리자를 1인으로 지정할 수 있으며, 이 경우 업무의 구분을 명확히 하여야 한다.

서비스제공자는 이용자의 개인정보를 보호하기 위해 대표자를 최고 관리책임자로 지정하고, 실질적인 관리를 위해 개인정보 취급 부서의 장을 개인정보 관리책임자로 지정할 수 있다.

개인정보 관리책임자를 복수로 지정할 수 있으며 이 경우, 책임자 간의 역할 분담을 명확히 하여야 한다. 정보통신서비스의 최종책임자는 서비스제공자이므로 정보보호에 관한 모든 책임은 서비스제공자에게 있으며, 수립된 내부방침에 따라 정보보호책임자, 개인정보 관리책임자, 시스템 관리자가 이를 준수하여 정보보호 업무를 수행하고 있는지 확인하고, 적절한 시정조치를 취하여 이들을 관리 · 감독해야 한다.

정보보호책임자, 개인정보 관리책임자, 시스템 관리자가 인사이동 되거나 퇴직하는 경우, 이들에 대한 계정을 삭제하고 접속을 제한하는 등 적절한 보안조치를 취하여야 하며, 현재의 정보보호책임자와 시스템 관리자 이외에는 정보보호에 관련된 자료 및 정보시스템에 접근하는 것을 제한하여야 한다.

정보통신서비스 정보보호지침 제 8조에 따르면 정보보호책임자라 함은 정보통신서비스에 대한 안전 · 신뢰성 확보를 위하여 이러한 정보보호 업무를 계획 · 구현 · 운영 · 감독하는 주체를 의미한다.

정보보호책임자는 실제적으로 정보보호 업무의 1차적인 책임이 있으며 직접적으로 관리하는 주체가 된다. 정보보호책임자는 시스템 관리자의 업무 중 정보보호와 관련된 세부업무를 지도 · 감독하고, 서비스와 관련된 모든 정보의 불법적인 유출 · 변조 · 파괴를 방지하기 위해 취하는 모든 정보보호 행위에 대한 관할 업무를 수행한다.

정보보호책임자는 주기적으로 정보시스템 및 네트워크의 보안취약점을 점검 · 분석하여, 그 결과를 서비스제공자에게 보고한다.

또, 정보보호책임자는 물리적, 기술적 통제에 관한 기준을 정하고 이를 시행하여야 한다. 물리적 통제는 시건장치 · 지문인식 등의 인증제품과 같이 전산실에 대한 접근통제장치 등을 사용하여 출입을 통제하는 것이며, 기술적 통제는 침입차단(방화벽)시스템 등을 사용하여 외부 불법접근으로부터 내부 정보시스템을 보호하는 것을 의미한다.

해킹 · 바이러스 침투 등 침해사고의 발생에 대비하여 비상연락망, 응급조치에 관한 절차, 복구대책을 포함하는 비상계획을 수립 · 시행한다.

주기적으로 주요 정보시스템에 대한 접속기록(로그파일)을 분석하여 서비스 이용실태와 부정행위 여부를 점검하고, 침해사고, 오류나 부정행위가 발생하였을 경우, 서비스제공자에게 신속히 보고한다.

바이러스 유포나 해킹 등의 침해사고로 정보통신서비스에 중대한 피해가 있거나 개인정보 유출 등 이용자에게 피해가 확산될 경우, 모든 이용자에게 현황과 대응책을 신속하게 알린다.

시스템 관리자는 정보보호 업무를 제외하고, 서비스를 제공하는데 이용되는 컴퓨터 및 주변기기, 라우터, 스위치, 허브와 같은 네트워크 운영체제, 소프트웨어 및 데이터 파일장비 등 각종 장치를 설치 · 운용하는 업무를 담당한다.

이용자에 대한 비밀번호 관리지침 등은 정보보호책임자의 지시에 따라 시스템 관리자가 수행하게 된다.

마지막으로, 개인정보 책임자는 개인정보와 관련된 내부지침을 준수하도록 충분한 기술적 · 관리적 보호조치를 실시하여야 한다.

개인정보 관리책임자는 교육훈련, 내부규정의 정비, 안전대책의 실시, 실천준수계획의 제정 등의 업무를 수행하게 된다. 개인정보 관리책임자는 이용자의 불만사항 접수 및 처리에 대한 책임을 지게 되며, 개인정보를 취급하는 직원에 대해 충분한 교육훈련을 실시하여야 한다.

개인정보 처리를 외부에 위탁하는 경우, 개인정보 관리책임자는 해당 위탁받은 자의 개인정보 관리상황을 지속적으로 확인해야 한다.

정보통신망이용촉진 등에 관한 법률 제32조 제1항 제6호에 의하여 개인정보 관리책임자를 지정하지 아니한 자는 500만원 이하의 과태료에 처한다. 서비스제공자와 정보보호책임자, 시스템 관리자, 개인정보 관리책임자의 역할을 표로 정리하면 다음과 같다.

<표> 정보보호조직 구성원의 역할

정보보호조직	역할
서비스제공자	정보보호조직체계 수립
	각종 정보보호장치 마련
	정보보호책임자, 시스템 관리자, 개인정보 관리책임자의 지정과 감독
정보보호책임자	시스템 관리자 · 개인정보 관리책임자 감독
	시스템 및 네트워크의 점검
	물리적 · 기술적 통제의 기준설정
	정보보호 사고 대비업무
시스템 관리자	컴퓨터 및 네트워크 등 장비 관리
	이용자 비밀번호 및 ID 관리
	주기적 백업
개인정보 관리책임자	개인정보의 보호대책 마련
	이용자 불만사항 처리
	교육훈련, 안전대책 실시
	개인정보 처리 위탁시 관리상황 확인 등

이제 인터넷 서비스업체들은 시장에서 살아남기 위해서라도 개인정보보호에 앞장서 이용자의 신뢰를 확보해야 한다. 이용자의 개인정보보호는 정부의 규제정책이 아닌 시장논리에서 이루어져야 한다.

비슷한 종류의 서비스를 제공하는 사이트들이 매일 우후죽순처럼 생겨나고 있는 현 시점에서 회원들은 독이 깨져있는 사이트에 물을 부으려 하지 않을 것이다. 깨진 독을 새 독으로 바꾸고 물이 새고 있지는 않은지 수시로 점검해야 보다 많은 회원을 확보할 수 있다.

개인정보보호지침,
DB이용자정보관리지침에 관한
문의 및 표준개인정보보호방침 제공
한국데이터베이스진흥센터 연구개발팀
임태훈; T 318-5050 (111),
E-mail : taehoon@dpc.or.kr