개인 정보 개선 방안에 대한 연구(국내외 비교 분석)

이도균 · 김학수

강원대학교 IT특성화대학 컴퓨터정보통신공학 전공

Comparative Study on Improvement of Personal Information

Do-kyun Lee · Harksoo Kim

Kangwon National University

E-mail : ldk1127@naver.com · nlpdrkim@kangwon.ac.kr

요 약

개인 컴퓨터의 보급과 인터넷의 발달로 인하여 정보화시대가 도래했다. 그에 따라 각종 정보들이 넘치게 되었으며 개인과 기업에서는 정보보호에 많은 주의를 기울이게 되었다. 하지만 IT 강국이라 일컫는 우리나라에서는 개인정보 유출사건이 끊임없이 일어나고 있다. 그럼에도 불구하고 사회 전반적으로 개인 정보 보안 문제를 소홀히 하는 인식이 퍼져있다. 따라서 본 논문에서는 외국의 개인 정보에 대한 인식과 유출 사례 그리고 대응 방법을 분석한다.

ABSTRACT

Due to the spread of personal computers and the development of network, the information age has come and a variety of information has been flooded. Accordingly, individuals and companies have been a lot of attention to information security. However personal information leaks have been happening constantly in Korea. Nevertheless, awareness of security of personal information have been treated carelessly in society. In this paper, we will survey foreign awareness of personal information, specific cases for information leaks, and coping methods.

키워드

개인 정보, 정보 유출, 보안, 대응 방법

Ⅰ. 서 론

현대 사회에서 개인정보는 공공기관의 대국민 서비스, 기업의 영업활동 등 많은 분야에 걸쳐 그 활용범위가 증가하고 있다. 단순히 신분을 확인하는 수단에서 벗어나 이제는 새로운 부가가치를 창조하는 핵심자원으로 변화하고 있다. 기업들은 비즈니스, 고객관리, 마케팅 등 개인정보를 적극 활용하고 있다. 그러나 이러한 사회 변화에서 많은 부작용이 발생하고 있으며, 급속도로 기술이 빠르게 발전되고 있는 것에 반해 이에 사회적, 윤리적 규범을 정립하지 못하는 사회적 부조화 현상이 초래되고 있다. 대표적인 것이 바로 개인정보 유출로 인한 침해이다. 실제로 정보통신망을 통하지 않고서는 풍족한 현대의 삶을 제대로 영위할 수 없다. 하지만 이런 정보 통신망을 이용하기 위해서는 일정한 개인정보를 통신망 관리자에게 제공하여야만 한다. 통신망을 관리하는 자가 개인의 정보를 침해할 수 있는 위치에 있으므로 우리는 잠재적인 개인정보의 침해 상태 속에서 살고 있다고 할 수 있다[1].

개인정보 유출 사건에는 외부 침입에 의한 유출과 내부 유출에 의한 두 가지 갈래가 있다. 외부 침입은 외부의 해커가 침입하여 개인 정보를 탈취해가는 반면 내부 유출은 관계자가 내부에서 개인 정보를 빼돌리게 된다. 본 연구는 우리나라와 외국의 외부와 내부의 두 가지 갈래에 의한 개인정보 사건을 비교 분석하여 문제점에 대응하는 방안을 모색하려 한다.

Ⅱ. 국내의 개인 정보 사건

표1은 2008년부터 있었던 주요 개인 정보 유출 사건의 시기와 유출 기관, 유출 경로를 나타냈다.

인터넷 쇼핑몰부터 대형 IT 기관까지 다양한 기관에서 개인정보 보안 사고가 발생한 것을 볼 수 있다.

표 1. 국내의 주요 개인정보 유출 사건

시기	유출기관	유출 경로
2008년 2월	옥션	외부 침입
2008년 9월	GS칼텍스	내부 유출
2011년 4월	현대캐피탈	외부 침입
2011년 5월	SK커뮤니케이션즈	외부 침입
2011년 11월	넥슨	외부 침입
2012년 7월	KT	외부 침입
2014년 1월	국민,롯데,농협	내부 유출

개인 정보를 다루는데 익숙하고 다른 기업들보다 우위에 있을 것이라고 생각했던 기관들의 정보 유출 사고는 국민들에게 큰 불안감을 가져다주었다. 뿐만 아니라 개인 정보 유출로 인한 범죄 집단의 보이스 피싱, 스팸 피해와 같은 2차 피해를 무시할 수 없게 되었다.

2.1 외부 침입 사례

2008년 대형 인터넷 쇼핑몰 옥션에서 1860만명의 개인정보가 유출되었고 2011년에는 인터넷 포털 사이트 네이트에서, 최근엔 통신회사 KT의 홈페이지가 해킹을 당하여 1200만명의 개인정보가 유출됐다. 2008년부터 20여건의 사고가 발생하였고 2억 5000만 여건의 개인정보가 유출되었다. 대부분이 중국에서 일어난 시도이다. 이처럼 외부에서 개인 정보를 탈취할 목적으로 일어나는 해킹 사고가 끊임없이 일어나 늘 화제가 되고 있다.

2.2 내부 유출 사례

기업의 정보 유출 경로가 바뀌고 있다. 해커의 외부 침입 사례가 주를 이루었었지만 최근에는 기업 내 조직원들에 의한 내부 유출의 사고가 많아졌다. 2009년에는 정유회사 GS칼텍스의 1100만건의 개인정보를 내부직원이 판매하여 유출되는 일이 있었고 특히 2014년에는 국민은행, 롯데카드, 농협 등의 카드 3사에서 1억 건이 넘는 고객의 개인 정보가 내부에서 유출되었다. 뿐만 아니라 국내의 상당수의 커다란 금융업체들은 개인정보의 내부 유출을 겪었다. 내부에서 유출되는 개인 정보의 규모는 해킹과 같은 외부 침입 사건에 비하여 압도적으로 크기 때문에 내부 유출을 더욱 유의해야 한다.

III. 외국의 개인 정보 사건

3.1 외부 침입 사례

개인 정보 유출은 국내뿐만 아니라 외국에서도 번번이 일어난다. 외국 역시 IT 기업 뿐만 아니라 다양한 기관에서 개인 정보 보안 사고가 발생했다는 것을 찾아 볼 수 있다. 2007년 미국의 소매유통업체 TJX 계열사에서 1억건의 개인정보가 유출되었다. 2008년에는 대만에서 주요기관의 컴퓨터를 해킹해 총통을 비롯한 5천만 건의 개인정보가 유출되었으며 2009년 미국의 카드회사 하틀랜드 페이먼트 시스템즈에서 두 번째 규모에 이르는 1억 3천만건에 이르는 개인정보가 유출되었다. 2014년에는 프랑스의 최대 이동통신사와 독일 이메일에서 개인 정보가 탈취 당하는 사고가 발생했고 12월 미국에서 대형 마트 Target에서 단말기 해킹으로 약 1억건 이상의 정보가 유출되었다.

3.2 내부 유출 사례

2007년 미국 금융서비스 회사 Certegy Check Sevices사에서 개인 정보 관리 책임자에 의하여 개인 정보가 정보 브로커에게 넘겨졌다. 2012년에는 중국 상하이 로드웨이 D&B사에서 규모가 가장 큰 카드사 정보 유출이 발생했다. 1억 5천만건의 개인 정보가 내부 직원에 의하여 유출되었다.

IV. 국내외 대응 비교

4.1 외부 침입에 대한 대응 비교

국내에서는 2008년 옥션에는 보안 조치와 기술 상황을 비추어 과실이 없다고 판단하였다. 네이트에는 과태료 600만원을 부과하였고 최근 KT 해킹 관련하여 보안 담당자가 불구속 입건되었다.

미국 유통업체 TJX는 곧바로 유출 사실을 공개하고 피해자들에게 추가 비용 발생분을 배상 해야했고 유출에 대한 책임으로 집단 소송에 약 2조에 가까운 비용과 벌금을 지출하고 있다. Target 역시 정보 유출 사실을 일반에 공개했고 관련 있는 고객에 대해 카드 교체를 지원하며 1년간 도용 방지 프로그램을 무료로 제공했다. 독일의 정보통신 안전국은 진원지를 파악해 범인 색출에 열을 올리고 있다.

4.2 내부 유출에 대한 대응 비교

GS칼텍스는 유출 직후 회수되어 피해가 발생되기 어렵다는 이유로 집단 청구에 대한 배상 채

임을 묻지 않았다. 카드 3사는 과징금 처분을 받지 않고 단지 3개월 영업 정지 처분을 받았다.

미국의 경우 TJX와 Certegy Check Services사는 당사자간 화해 권고를 통해 피해 보상에 합의하여 추가 피해 발생시 일어나는 비용과 새 계좌 개설 비용을 보상하기로 했다. 법원이 집단 소송이 발생했을 때 적극적인 화해를 권고하기 때문이다. 미국은 집단소송제와 징벌적 손해배상제 활성화 되어있다. 집단소송제는 기업의 불법행위로 인하여 피해를 입은 경우 피해자 중의 1인 또는 수인이 대표 당사자가 되어 수행하는 손해배상 청구소송이며[2] 징벌적 손해배상제는 가해자가 불법행위를 행한 경우 법원이 피고를 징벌하고자 하는 목적에서 다액의 배상금 지불을 명하는 제도이다[3]. 피해자들과 합의를 이끌어내지 못하고 집단소송에서 패하는 경우 징벌적 손해배상제에 의거하여 막대한 보상체계를 통하여 법적인 제도가 잘 완비하여 정보유출을 사전에 방지, 재발에 방지하려는 모습을 볼 수 있다.

Ⅴ. 문제 분석과 개선 방안

5.1 문제 분석

개인 정보 유출 사건은 국내를 비롯하여 해외에서도 빈번하게 일어나는 사건이다. 그런데 개인정보의 유출 경로에 따라 미국, 유럽 등의 서양과 한국, 중국 등 아시아의 사건 규모에 차이가 있는 것을 볼 수 있다.

표 2. 아시아와 서양의 유출 경로를 통한 비교

	유출 경로	사건	규모
서양	외부 침입	미국 TJX	1억
		미국 하틀랜드	1억3천만
		미국 Target	1억
	내부 유출	미국 certegy	850만
아시아 (한국,중국)	외부 침입	옥션	1860만
		SK커뮤니케이션즈	1200만
		대만	5천만
	내부 유출	카드3사	1억
		GS칼텍스	1100만
		중국 로드웨이	1억5천만

표 2는 아시아와 서양을 유출 경로를 통하여 비교해 보았다. 서양에서는 시스템 보안상의 약점을 통한 해커의 외부 침입에 의한 문제가 두드러지는 반면 아시아에서는 외부 침입 뿐만 아닌 국내 카드 3사와 중국 로드웨이 D&B사 등의 사례와 같은 내부 유출에 의한 문제가 함께 두드러지고 있다.

대응 방법을 비교해보면 서양에서는 엄격한 법적 제도를 구축해놓은 한편 한국과 중국 등의 아시아에선 엄격한 제도가 구축되어 있지 않은 모습이다. 특히 우리나라의 개인 정보 유출 사건과 대응을 분석해보면 개인 정보에 대한 중요성을 인식하지 못하는 모습을 보인다. 해마다 증가하는 사건의 피해와 심각성에도 불구하고 느슨한 처벌이 이어지고 있다. 이것은 기업, 기관들의 개인 정보 보호에 관한 노력에 관심을 줄게 만들고 개인 정보 유출 사건은 계속하게 일어나게 되는 현상으로 이어졌다. 미국의 대형 마트의 대처와 국내의 금융업계, 통신업계를 비교해 보면 느슨한 법적 제도와 보여주기 식의 행정, 처벌과 같은 우리 사회의 문제점을 명확히 파악 할 수 있다.

5.2 개선 방안

끊임없는 개인 정보 유출 사고는 IT강국인 우리나라가 보다 더 선진국이 되기 위해서 뛰어넘어야 할 산이고 과제이다. 고객의 개인 정보를 다루는 사회와 기업에서는 느슨한 법적 제도와 솜방망이 처벌로 인하여 개인 정보의 중요성을 인식하지 못하고 있다. 이것은 사회와 기업의 문제만이 아니라 소비자들도 인식해야하는 문제이다. 기업의 일원들은 사소한 개인정보일지라도 관리자의 허가를 필요로 하는 엄격한 방식으로 바뀌어야 하고 기업은 개인 정보가 중요한 자산이라는 것을 깨달아야 한다. 그리고 사회적 차원에서 개인 정보에 관련된 엄격한 법적 제도를 마련해야 개인 정보 유출 대란이 반복되지 않을 것이다.

Ⅵ. 결 론

본 논문에서는 국내의 정보 유출 사례와 외국의 정보 유출 사례를 외부 칩입과 내부 유출이라는 경로를 통하여 비교, 분석했다. 국내의 사례와 외국의 사례를 비교, 분석함으로써 국내의 문제점을 찾아서 분석해 보았고 문제점에 대응할 개선 방안을 제시했다.

향후에는 개인 정보 사용에 대한 법적 제도와 사회적으로 개인 정보의 중요성을 인식하기 위한 방안이 연구가 필요하다.

참고문헌

[1] 염기남, “개인정보보호제도 운영실태와 개선 방안에 관한 연구”, 전북대학교 행정대학원, 2013
[2] 김은희, “소송위험과 감사시간의 관련성 : 집단소송제도 도입 전.후 비교”, 한양대학교 대학원, 2009
[3] 정우식, “징벌적 손해배상”, 경북대학교 대학원, 2013