논문 2012-1-6

개인정보보호 동향과 보호대책

정연서*

An Investigation of Privacy Information Protection and Security

Youn-Seo Jeong*

요 약

최근, 전세계적으로 악성소프트웨어들에 의한 해킹공격이 증가하고 있으며, 개인정보 오남용 및 유출사고 등으로 개인정보보호의 중요성이 높아지고 있다. 이에 따라 우리 정부에서는 2011년 법을 제정하고 시행을 하였다. 본 논문에서는 개인정보보호법의 주요내용들을 살펴보고 관련기술과 제품들에 대하여 조사정리하고 마지막으로 개인정보보호를 위한 방안들에 대하여 제시하였다.

Abstract

The world has seen an unusual increase in hacking attacks, mostly originating from an increase in malwares activities. And, with the frequent abuse and a leakage of personal information recently the importance of the protection of personal information has been increasingly emphasized. The government enforced the act on the privacy protection in 2011.

In this paper, we investigate issue of the act on the privacy protection and relevant technologies and equipments for protection of personal information. Lastly, we present plans for protection of personal information.

한글키워드 : 개인정보, 개인정보보호

1. 서 론

인터넷 문화 확대와 스마트폰의 보급으로 인해 인터넷 접근과 사용은 일상화되어 가고 있다. 최근 TV 시청시간보다 인터넷 사용시간이 앞선 조사결과도 나오고 있으며[1] 스마트폰의 확산으로 인한 사용시간은 더욱 증가할 것으로 예측되고 있다.

보유수량이 급증[1]하고 있는 스마트폰[2]은 단순한 전화기가 아닌 새로운 미디어 장치로 자리잡았으며 방송, 신문, PC기반 유선인터넷 등 기존 미디어의 소비시간을 흡수하며 미디어 이용 변화를 촉진시키고 있다. 스마트폰 이용자를 대상으로 진행한 '미디어별 이용시간 점유율' 조사결과에 따르면, '인터넷' 이용시간 점유율은 스마트폰 사용 전에 비해 13% 증가하고 PC기반 유

* 한국전자통신연구원
(email: jys847@etri.re.kr)
접수일자: 2012.5.23 수정완료: 2012.6.21

1) 2011년 4억 9140만대, 전년대비 61.3% 증가

선인터넷의 점유율은 오히려 감소하고 있는 것으로 나타났다[3].

표 1. 미디어별 이용시간 점유율 - 스마트폰 이용 행태 조사(2010.10)

미디어형태	스마트폰 사용전	스마트폰 사용후
모바일인터넷	-	23
PC인터넷	43	33
잡지 및 인쇄물	7	5
종이 신문	8	6
라디오	15	13
TV	28	21

그러나, 이러한 이용확대는 개인들의 정보유출이라는 부작용을 가져오고 있다. 사이트 가입시 주민등록번호를 개인인증에 주로 이용하고 있는 우리나라의 경우 유출정보를 이용하여 금전적인 피싱 등에 이용되고 있어 다른 국가에 비해 피해가 심각한 수준이다. 개인정보침해신고 건수는 지속적으로 증가하고 있으며 최근 3년간 개인정보침해 사고의 피해 규모는 총 10조 7천억원(KISA 자료)에 이르는 것으로 나타나고 있다[4].

수년간의 준비를 거쳐 개인정보보호법이 제정되고 계도기간을 거쳐 2012년 4월 본격적으로 시행되고 있다. 국내 언론사에서 국내 기관 및 기업을 대상으로 한 설문조사에서 '내부 직원에 의한 개인정보 유출(585명, 46.5%)이 가장 유려되고 있는 보안위협으로 나타나고 있다. 그 다음으로는 '해킹에 의한 개인정보유출(528명, 42%)'이며 이어 내부기밀과 핵심정보 유출로 나타나고 있다[5].

본 논문에서는 이어서 국내외의 개인정보보호 침해사고와 동향에 대하여 기술하고, 시행되고 있는 개인정보보호법의 주요사항에 대하여 살펴본다. 그리고 마지막으로 개인정보 보호를 위한 방안들에 대하여 제시한다.

2. 개인정보보호 동향

2.1 개인정보 침해사고

일반적으로 인터넷을 이용하고 있는 성인들의 경우 가입한 사이트의 수는 적게는 수십에서부터 수백에 이르고 있다. 공공기관 및 상업기관에 보관된 가입자 정보들은 허술하게 보관, 관리되거나 인터넷 사이트에 노출되어 있는 것이 현실이다. 우리나라의 경우 인터넷사이트 대부분이 회원가입시 주민번호와 개인의 전화번호, 주소 등을 요구하고 있으며 금융기관이나 물품구매 등의 결재가 요구되는 곳에서는 카드 및 계좌번호 등의 금융정보도 안전하게 관리되지 않고 무단으로 보관되고 있는 경우도 많다. 개인정보를 이용한 금전적인 이용가치로 인하여 해당정보의 탈취와 유통에 이르는 조직적인 범죄도 그 수와 기법이 날로 발전하고 있다. 지난 한 해 동안 발생한 개인정보 유출사고로 7월 SK컴즈의 3,500만명, 8월 옵손코리아의 35만, 4월 현대 캐피탈의 170만명, 11월말 넥슨사의 해킹사고로 1,320만명의 회원정보가 유출되는 사고가 발생하였다. 개인정보보호법이 시행되었음에도 불구하고 5월 국내 교육방송사이트의 400만명 회원정보 유출 및 국외 포털사이트 및 개발자 사이트 등의 수많은 가입자 정보 유출사건이 발생하였다.

개인정보 유출에 대한 대응방식도 적극적으로 변해 집단소송 등이 본격화되고 있으며 국내에서도 배상판결이 내려진 경우도 있다. 앞으로 개인정보 유출에 따른 배상으로 인한 기업들의 도산도 빈번하게 나타날 수 있다.

국외의 경우에도 개인정보와 관련한 소송이 빈번하게 발생하고 있다. 영국의 ICO(Informa-tion Commissioners Office)에서는 진료정보가

수록된 하드디스크를 제대로 파기하지 않고 재판매한 업체에 325,000 유로의 벌금을 부과하였고, 미국에서도 개인정보와 의무기록이 저장된 백업 테이프의 분실로 합의금 750,000 달러를 지불하도록 하였다. 페이스북의 이용자 개인정보침해에 대해서는 천만달러의 벌금이 부과되기도 하였다[6].

2.2 세계 각국의 개인정보보호 기구

세계 각국에서는 개인정보를 위한 기구들을 설치하여 자국민들의 개인정보를 보호하고 있으며 주요 각국의 설치현황은 다음과 같다.

2.2.1 미국 - 연방거래위원회 (Federal Trade Commission)

미국은 개인정보보호에 관한 사항을 포괄적으로 규정하고 있는 개인정보보호기본법은 가지고 있지 않지만, 각 영역별로 개인정보보호를 위한 법규범을 마련해 두고 있다. 공공부문과 민간부문의 개인정보보호체계가 분리되고, 민간부문에 있어서도 각 영역별로 입법이 이루어지고 규율됨에 따라 포괄적인 개인정보보호기구는 없으나 공공부문에 있어서는 1974년 프라이버시법(The Privacy Act of 1974)이 적용되어, 미국정부기관에 의해 보유되고 있는 개인정보를 보호하고 있다.

2.2.2 영국 – 정보 커미셔너 (Information Commissioner)

영국(UK)은 1984년부터 정보보호등록관을 설치하여 자국 내에서 이루어지는 모든 개인정보처리행위를 사전 등록함으로써 개인정보를 보호하고 있다. 1998년에는 전면 수정된 정보보호법(The Data Protection Act 1998)에 따라 정보보호커미셔너(Data Protection Commissioner)로 개칭되고, 2000년에는 정보공개법(Freedom of Information Act 2000)에 따라 정보커미셔너(Information Commissioner)로 정립되었다.

2.2.3 프랑스 - 국가정보처리 · 자유위원회 (Commission Nationale Informatique Libertes)

프랑스에서는 1974년 공공부문과 민간부문에서 이루어지는 정보처리 기술의 발달에 대비한 개인의 사생활과 자유보호를 위한 방안을 강구하기 위한 위원회가 법무부 내 설치하고 정보처리 축적 및 자유에 관한 법률을 제정하고 국가정보처리자유위원회(CNIL : Commission nationale de l'informatique et des libertes)를 설립하였다.

2.2.4 독일 – 연방 프라이버시 커미셔너 (Bundesbeauftragter fur den Datenshutz)

1970년 Hessen 주의 정보보호법과 1974년 Rheinland Pfalz주의 정보남용금지법에 이어, 1977년 연방정보보호법(Bundesdatenschutzgese-tz)을 제정하였다. 현재 연방과 주 차원에서 각각 개인정보보호법이 마련되어 있고, 이를 바탕으로 개인정보보호기구들이 설치되어 활동하고 있다.

그리고 캐나다, 호주, 그리스, 스웨덴 등의 국가들에서도 개인정보를 보호하기 위한 관련 법과 기구들을 만들어 운영하고 있다.

우리나라의 경우는 기존의 개별법으로 시행되던 공공기관의 개인정보보호에 관한 법률, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 교육정보시스템의 운영 등에 관한 규칙, 의료법, 신용정보의 이용 및 보호에 관한 법률 가운데 개인정보보호와 관련된 법을 통합 일원화한 개인정

보보호법을 수년간의 분비 끝에 제정하고 시행하고 있다. 개인정보 열람, 정정, 삭제 및 처리정지권 보장, 개인정보 유출시 통지 및 신고제도, 집단분쟁제도, 권리침해 중지를 요구하는 단체소송 도입 등을 내용으로 담고 있으며 이용자들의 피해구제책을 강화하는 내용을 담고 있다. 그리고, 개인정보보호관리체계 인증제도(PIMS: Personal Information Management System)를 도입하여 기업이 개인정보 보호 활동을 체계적 · 지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준이상의 기업에 인증을 부여하고 있다. 신고접수와 분쟁처리를 위해 한국인터넷진흥원(KISA)내 개인정보침해신고센터를 설립하여 운영하고 개인정보분쟁위원회를 통해 관련된 분쟁조정을 처리하고 있다.

3. 개인정보보호법 규정

개인정보보호법에서는 크게 개인정보와 영상정보의 보호지침에 대하여 다루고 있다. 개인정보는 살아있는 개인의 정보로 성명, 주민등록번호 등을 통하여 개인을 알아 볼 수 있는 정보로 해당 정보를 다른 정보와 쉽게 결합하여 알아 볼 수 있는 정보들도 포함된다. 상호, 영업소재지, 대표자 및 임원정보, 자산정보, 영업실적 등 법인 및 단체 정보 등은 포함되지 않는다. 그리고 CCTV 등 영상정보들에 관한 설치, 운영, 공개, 관리 규정들을 규정하고 있다.

3.1 적용대상 및 처벌규정

공공부문은 국회, 법원, 헌법재판소 등 헌법기관과 국가인권위원회, 중앙행정기관 및 소속기관, 지방자치단체, 공사 공단, 공기업 등 약 28,000개 모든 공공기관이 적용된다. 또한, 약 350만개 72개 업종, 모든 사업자도 법 적용대상이다. 일반법의 성격을 가지므로 포털, 망사업자, 병원, 금융기관, 제조업, 서비스업, 택배사, 1인사업자, 꽃가게, 공인중개사, 약국, 정유소 등이 모두 포함된다. 개인정보보호법을 위반하면 최대 10년 이하의 징역 또는 1억원 이하의 벌금이 부과되며 개인정보를 목적외에 이용하거나 제공할 경우 5년이하의 징역 또는 5천만원 이하의 벌금이 부과된다. 주민등록번호 등 개인 고유식별정보는 원칙적으로 사용을 금지하고 있으며 위반시 5년이하 징역 또는 5천만원 이하의 벌금이 부과되며 이에 따라 주민번호외의 수단으로 회원가입 방법을 제공하고 개인들의 가입정보를 암호화 등의 안전조치 마련이 의무화 되며 위반시 3천만원 이하의 과태료가 부과된다[7].

3.2 개인정보 관리

개인정보보호를 위해 대상기관에서는 보관 하거나 수집할 개인정보의 분석과 수집절차, 처리방침, 이용방안, 제공과 개인정보 자료들에 대한 접근권한 부여와 통제, 접근기록 유지, 개인정보 파기방법 및 절차 등의 관리적 보호조치 방안을 수립하고 이를 이행하기 위한 기술적, 물리적 보호조치를 세워야 한다. 그리고, 개인정보가 유출되었을 경우에는 정보주체들에게 이를 알리고 대응조치를 신속하게 취해야 과태료나 소송 등에 의한 피해를 최소화할 수 있다. 개인정보의 안정성 확보조치 기준에 포함된 보호조치 항목들에는 접근권한 관리, 접근통제 시스템 설치 · 운영, 개인정보 암호화, 접속기록보관, 보안프로그램 설치, 개인정보 보관장소의 출입통제 등이 있다.

3.3 영상정보 관리

CCTV의 경우 목욕실, 화장실, 발한실, 탈의실 등 사생활 침해 장소에는 설치가 금지되고 범죄

예방, 시설안전, 화재예방 목적으로만 설치 가능하다. 그리고 CCTV가 설치되어 녹화되고 있음을 알리는 안내판을 부착하여야 한다. 당초 설치 목적을 벗어나 함부로 조작하거나 다른 곳을 비추거나 하면 안되며 영상정보의 무단 유출・공개 금지되며 개인영상정보를 제공하는 경우 본인 확인 후 필요 최소한으로 제공하고 타인 영상은 모자이크 처리를 한 후 제공하여야 한다. CCTV 운영관리 방침수립・공개하고 영상정보의 접근통제 방침을 만들어 안전하게 보호될 수 있도록 보관하여야 한다.

4. 개인정보보호 방안과 솔루션

4.1 개인정보보호 방안

개인정보보호법에 준하여 보호조치를 마련하기 위해서 먼저 개인정보 취급방침과 내부관리계획을 마련하고, 개인정보처리관리자(CPO: Chief Privacy Officer)를 임명하여야 하고 조직의 개인정보처리 시스템 접근권한 규칙(정책)을 수립하여야 한다.

4.1.1 개인정보 취급방침 수립

개인정보를 취급하는 사업체에서는 개인정보처리관리자를 임명하고 내부적으로 개인정보의 보호를 위한 방안을 수립하여야 하며 시행하기 위한 절차를 마련한 후 기관의 개인정보취급 방침을 수립하고 이를 공지하고 실천하여야 한다. 개인정보 처리방침에는 처리목적, 처리 및 보유 기간, 정보주체의 권리·의무 및 그 행사방법 등에 관한 내용들을 포함해야 한다.

4.1.2 내부관리계획 수립 및 시행

개인정보가 분실이나 도난, 유출, 변조, 훼손되지 않도록 안전성을 확보하기 위하여 취하여야 하는 세부적인 기준을 수립하여야 하며, 개인정보의 안전한 처리를 위하여 내부관리계획을 수립하고 시행하여야 한다.

내부관리계획에는 개인정보보호 책임자의 의무·책임에 관한 사항, 개인정보 처리단계별 기술적·관리적 보호조치에 관한 사항, 정기적 자체감사에 관한 사항, 개인정보취급자에 대한 교육 등 개인정보보호를 위해 필요한 사항이 포함되어야 한다.

4.1.3 접근 권한의 관리

임의의 무단 접근을 차단하기 위해 개인정보를 수집, 처리하고 있는 개인정보처리시스템에 대한 접근권한은 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하고 관리하여야 한다. 관련 근무인력의 변동이 있을 경우 지체 없이 접근권한을 변경 또는 말소하여야하며, 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 최소 3년간 보관하여야 한다.

4.1.4 접근통제 시스템 설치 및 운영

개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립, 적용하여야 하며, 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하여야 한다. 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 업무용컴퓨터에 조치를 취하여야한다.

4.1.5 개인정보의 암호화

개인정보처리자 개인정보를 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 반드시 암호화 하여야 한다. 비밀번호 및 바이오 정보들은 암호화하여 관리하여야 하며, 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 고유식별정보를 제공하는 경우에도 암호화하여야 한다. 그리고, 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장/보관하여야 한다.

4.1.6 접속기록의 보관 및 위·변조 방지

개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하여야 하며, 접속기록이 위·변조, 도난, 분실되지 않도록 접속기록을 안전하게 보관하여야 한다.

4.1.7 보안 프로그램 설치 및 운영

개인정보처리자는 개인정보처리시스템 또는 업무용 컴퓨터에 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 한다.

4.1.8 물리적 접근 방지

개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

또한, 개인정보가 포함된 서류, 보조저장매체 등은 잠금장치가 있는 안전한 장소에 보관하여야 한다.

4.2 보호솔루션

개인정보보호와 관련된 솔루션은 현재까지 출시된 대부분의 정보보호 솔루션이 모두 관련되어 있으며, 기존의 제품기능에 개인정보보호와 관련 기능을 추가하여 특화된 제품들로 출시하는 경우도 있다. 암호화, 전송암호화, 접근제어, 네트워크 보안, 안티바이러스, 웹방화벽, 계정관리 등에서 사용기록저장 관리, 문서세단기, 시건장치에 이르기까지 모두 포함되고 있다. 주요 솔루션들을 다음과 같다.

4.2.1 개인정보암호화 솔루션

저장되는 개인정보 데이터의 기밀성을 유지하기 위해 관련 데이터를 암호화하여 저장하고 관리하는 솔루션이다.

4.2.2 접근제어 솔루션

저장된 개인정보(DB)를 권한이 부여된 경우에만 접근을 통제 및 관리하는 솔루션. 개인정보의 접근, 저장, 전송 등의 전과정을 감시 통제한다.

4.2.3 사용자인증 및 계정, 접근권한 관리 솔루션

부여된 권한에 따른 접근 인·허가 및 개인정보의 접근 및 사용내역을 모니터링하고 관리한다.

4.2.4 네트워크 감시솔루션

네트워크 내부의 서버나 단말들을 내외부의 해킹과 침입으로부터 보호하고 패킷감시를 통해

개인정보 외부 유출을 모니터링한다.

4.2.5 위·변조방지 솔루션

온라인으로 제공되는 정보와 전자문서들의 무결성과 서버내 저장파일의 위・변조를 방지한다.

4.2.6 서버보안 솔루션

웹서버, 어플리케이션 서버, 파일서버 등의 정보를 보호, 웹페이지가 위・변조 혹은 유출되거나 외부로부터 감염된 악성파일의 유포를 사전에 감시・예방 및 방지한다.

4.2.7 자료파기솔루션

수집된 개인정보의 처리목적이 달성(용도폐기)된 경우 정보 폐기, 종이문서의 파쇄와 HDD 등 저장장치의 폐기관련 솔루션이다. 문서세단기 및 디가우징 장비 등이 있다.

4.2.8 개인정보 보유진단 솔루션

개인업무용 컴퓨터와 서버들에 대한 개인정보 자료 보관상태를 검색하여 내부정책에 따라 폐기 혹은 안전하게 보관, 관리한다.

4.2.9 접속기록 내역 보관 솔루션

개인정보에 대한 접근권한 부여 및 변경 내역과 접속 내용 등의 기록을 안전하게 보관 유지한다.

4.2.10 암호화전송 솔루션

개인정보 취급자가 외부에서 접속할 경우 VPN이나 전용선 등 안전한 접속수단을 통하여 접근하거나 정보를 전송한다.

4.2.11 출입통제 솔루션

시설 접근통제를 위한 것으로 주요시설이나 공간에 생체인식 출입장치나 CCTV 감시 등으로 강화된 출입통제를 한다.

살펴본 바와 같이 많은 개인정보보호 관련된 솔루션들이 출시되어 있다. 그러나, 무엇보다도 먼저 내부인력에 대한 보호의식이 전제되어야 할 것이며 솔루션들은 선택하기에 앞서 해당기관이나 사업장에서 취급하는 개인정보의 성격과 규모, 기설치 운영되고 있는 시스템(보안시스템 포함)을 분석하고 수립된 개인정보처리지침과 내부관리계획에 맞추어 개인정보보호법에서 제시하고 있는 기준을 부합할 수 있는 솔루션을 선택하여야 비용과 시간 낭비를 줄일 수 있다.

5. 결 론

개인정보의 유출로 인한 피해가 급증하고 있으며 세계 각국에서는 개인 프라이버시 보호를 위한 다양한 대책을 세우고 있다. 우리나라에서도 여러 개별법으로 보호되어 오고 있던 개인정보보호와 관련하여 사각지대를 축소하고 모호한 기준들을 명확하게 위해 개인정보보호법을 시행하였다. 개인정보의 수집단계에서부터 파기까지 전단계에 걸쳐 기본원칙들을 제시하고 있으며 위반시 벌칙과 피해에 대한 구제방법을 강화하여 담고 있다. 이에 따라 공공기관 및 사업자들은 개인정보에 대한 근본적인 인식의 제고와 정보보호를 위한 시스템을 구비하고 보호대책을 수립하여야 한다. 최근 개인정보침해는 점차 지능화 대형화 되고 있으며 유출된 자료들을 이용한 2차

피해사례도 증가하고 있으며 관련한 단체 손해배상청구도 빈번하게 발생하고 있다.

살펴본 바와 같이 스마트폰의 보급 확대와 SNS 등의 사용으로 인해 개인의 정보유출은 더더욱 늘어날 것으로 예견되며 미흡한 조치로 인한 유출은 기관과 기업 모두에게 인사와 금전적으로 큰 손실을 미치게 될 것이다. 그리고, 개인 사용자들도 인터넷상에 무분별한 개인정보의 공개를 삼가하고 다소 취약한 스마트폰 등 개인용 정보기기들의 자료유출에 대비하며 웹사이트의 계정과 암호관리에 좀 더 관심을 기울여야 할 것이다.

참 고 문 헌

[1] 인터넷사용시간, TV 시청시간 앞질러, 중앙닷씨에이 기사, 2010.3.22
[2] IDC 자료 2011년
[3] 닐슨코리안클릭 스마트폰 이용 행태 조사보고서, 2010.10
[4] KISA 연도별 개인정보침해신고 상담건수(정보보호통계)
[5] 보안뉴스 기사, 우리회사 가장 큰 보안위협은?, 2012.7.12 김태형
[6] 개인정보보호 해외 법제 동향, NIA 보고서, 2012.6
[7] 개인 정보보호 종합지원 포털 사이트, http://www.priva cy.go.kr/index.jsp
[8] 정연서 외, 개인정보보호법과 보호방안, 한국SW감정평가학회 춘계학술대회, 2012.5

저 자 소 개

정연서(鄭然瑞)

1996.2 충북대학교 컴퓨터공학과 석사
2001.8 충북대학교 컴퓨터공학과 박사
2001.8-현재 : 한국전자통신연구원

<주관심분야> 네트워크/정보보호 시험평가, 정보보안, 보안성평가