웹에서의 개인정보보호 방안

우성희

한국교통대학교

Privacy and Security on the Web

Sung-hee Woo

Korea National University of Transportation

E-mail : shwoo@ut.ac.kr

요 약

인터넷은 정보의 바다로 불려 질 만큼 엄청난 정보를 가지고 있지만 개인정보를 수집하여 악의적인 행동을 하는 각종 웹사이트에 제공함으로써 개인정보 유출 뿐 아니라 경제적 손실을 야기할 수 있다. 현재의 정보기술은 인터넷뿐만 아니라 모바일이나 개인용 단말기에서도 정보를 얻을 수 있기 때문에 개인정보의 유출은 엄청난 속도로 퍼져나갈 수 있다. 따라서 웹페이지 상에서 개인정보는 개개인을 구별하는 기본적인 정보로서 그 중요성이 더욱 증가 되고 있는 반면 개인정보 유출로 피해 사례 또한 증가하고 있다. 따라서 본 연구에서는 웹상에서의 최근 개인정보 침해 사례와 그 원인 및 보호 방안을 검토 및 분석한다.

ABSTRACT

The Internet is referred as sea of information, which provides huge information, but personal information is collected for malicious behavior and provided to various web sites via internet. This can lead to economic losses as well as the disclosure of personal information. We can easily get personal information from device, such as mobile and private terminal, as well as internet, and then it can be spread very quickly. The personal information leakage and damage cases are also increasing, while the importance of personal information on the web page to distinguish the individual as the basic information is growing.
In this paper we review and analyse recent invasion of privacy practices on the web and its causes, and technical and administrative protections

키워드

개인정보보호, 침해사례, 웹에서의 정보보호, 침해원인

Ⅰ. 서 론

인터넷은 정보의 바다로 불려 질 만큼 엄청난 정보를 가지고 있지만 개인정보를 수집하여 악의적인 행동을 하는 각종 웹사이트에 제공함으로써 개인정보 유출 뿐 아니라 경제적 손실을 야기할 수 있다. 현재의 정보기술은 인터넷뿐만 아니라 모바일이나 개인용 단말기에서도 정보를 얻을 수 있기 때문에 개인정보의 유출은 엄청난 속도로 퍼져나갈 수 있다. 따라서 정보화 시대가 진행됨에 따라 웹페이지 상에서 개인정보는 개개인을 구별하는 기본적인 정보로서 그 중요성이 더욱 증가 되고 있다. 최근 주요 개인정보 유출 사례의 가장 큰 피해는 네이트와 싸이월드 회원 3500만 명의 정보가 유출된 사건이다. 이것은 전 국민의 3분 2에 해당하는 대규모의 이용자 정보가 유출된 사건으로 정보통신 강국을 자처하던 우리나라는 큰 혼란에 빠졌었다. 1차적 피해를 막는 것뿐만 아니라 유출된 개인정보가 악용 되어 2차적인 피해를 일으킬 수 있기 때문에 개인 정보 보호에 대한 중요성을 깨닫는 계기가 되었다. 또한 행정안전부는 인터넷상에서 불필요한 주민번호 수집과 사용으로 인하여 발생하는 주민번호 유·노출 등의 문제점을 해결하기 위하여 인터넷상 주민번호 대체수단인 ‘공공 I-PIN(Internet-Personal Identification Number) 서비스를 개발·보급하고

있다. 공공 I-PIN 서비스는 인터넷상 개인 식별번호를 의미하며, 홈페이지 회원가입, 글쓰기 시 주민번호를 사용하지 않고도 본인임을 확인할 수 있는 개인정보 보호서비스로 2008년 8월, 민간 분야의 아이핀과 통합·연계되어 서비스를 제공하고 있다. 본 연구는 웹상에서의 최근 개인정보 침해 사례와 그 원인 및 보호 방안을 검토 및 분석한다.

II. 개인정보 침해현황 및 사례

최근 급격한 정보통신기술의 발전과 초고속 인터넷의 보급으로 전자거래등 인터넷을 기반으로 하는 산업이 급성장하고 있고 기업들의 고객정보의 보유량은 핵심경쟁력이 되고 있다. 그러나 본인의 동의 없는 개인정보 수집 또는 제 3자 제공 등 개인정보의 오남용 사례가 같이 증가하여 유비쿼터스 컴퓨터 사회에서의 개인정보 유출 및 사생활 침해의 가능성이 상존하게 되었다. 개인정보가 유출당하는 이유는 개인정보 규모의 급격한 증가가 직접적인 원인이겠으나 개인정보의 보호조치가 적절하게 이루어지지 않아 개인정보 유출 사고도 지속적으로 증가하고 있으며 최근의 개인정보 민원증가 추이와 유출 유형은 다음 그림 1

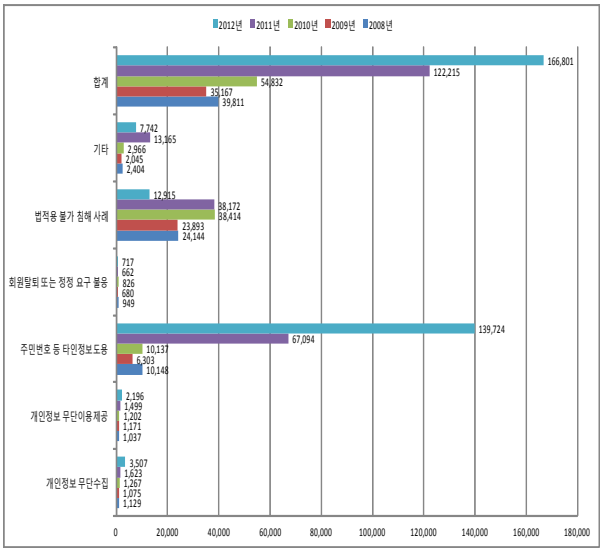

그림 1. 년도별 개인정보 침해내용과 현황

과 같다[1][3].

2012년도 개인정보 침해건수는 총 166,801건으로 전년대비 약 26.7% 증가했다. 주민등록번호 등 타인 정보의 훼손·침해·도용에 관한 침해 신고가 139,724건(전년대비 약 52% 증가)으로 가장 많았으며(전체의 83.8% 차지), 그 다음으로 기술적·관리적 조치 미비 관한 침해신고가 3,855건(전년대비 약 65% 감소)으로 나타났다. 지난해 개인정보침해 신고건수가 16만6000여건에 달하는 등 개인정보 침해 사례가 해마다 크게 늘고 있다. 개인정보보호법 제정 등 정부의 법적 규제 강화에도 불구하고 여전히 불법적인 개인정보 침해 사고가 늘고 있는 것으로 나타났으며 개인정보 침해 사례를 15가지로 분류해 상담현황을 통해 신고유형을 분석한 결과, 지난 10년간 개인정보 침해사례가 전반적으로 증가세를 나타낸다. 특히 2011년 9월말부터 개인정보보호법에 제정돼 시행되고 있지만 최근 3년간(2010~2012) 주요 침해사례[5]는 이와 관계없이 증가한 것으로 나타났다. 특히 주민등록번호 등 타인정보의 훼손 침해 도용의 문제가 전체 침해 사례 중 50.9%의 비중을 차지할 만큼 피해가 심각하다고 지적했다. 최근 3년간 이용자 동의 없는 개인정보 수집도 2010년 1267건에서 2011년 1623건으로 늘어났고 지난해에는 3020건을 기록 2년간 2배 넘게 증가했다. 개인정보 수집 시 고지 또는 명시 의무 불이행도 2010년 75건에서 2011년 53건으로 다소 감소세를 보이다가 지난해에는 368건으로 폭증했다[5].

III. 웹페이지에서의 개인정보 침해 원인

2008년 국가정보보호백서에 따르면 정보보호 제품 사용현황에서 침입차단시스템 45.9%, 침입탐지시스템 9.5%를 차지하며 특히, 인터넷을 이용하는 성인의 경우 일생의 2/3를 개인정보 피해를 입었고, 전 세계적으로 사이버범죄 금전 피해는 1,100억 달러 수준이다. 또한, 개인정보 피해자별 평균 손실 금액은 197달러이고, 모바일 이용자의 31%가 스팸문자를 수신하는 것으로 나타났다. 뿐만 아니라 인터넷 이용성인 10명 중 1명꼴로 모바일 사이버 범죄를 경험한 것으로 조사됐다. 이와 같이 개인정보 침해사고가 끊이지 않고 발생하고 있는 가운데 기업의 개인정보가 대량 유출돼 2차 피해까지 심각한 상황이다. 최근에는 국내의 경우 인터넷을 통해 개인정보를 사고파는 불법거래까지 이뤄지고 있으며, 금융기관에서 수집한 개인정보 유출로 인해 금융거래 이용자는 자신도 모르게 돈이 빠져나가는 사건이 발생하는 등 피해가 심각하다. 이러한 웹 사이트상에서 개인정보침해의 원인은 기술적 측면에서 통신·인터넷 사업자의 개인정보보호 책임성 부족이라고 할 수 있고 관리적 측면에서 본다면 해킹에 대한 대응 부족이다. 개인정보 탈취를 위한 해킹은 네트워크(전송구간), 사업자 서버, 이용자 PC에서 발생한다. 사업자의 정보보호 투자 및 전문가 부족으로 해킹 사실을 조기인지하지 못하거나 신속한 초등 대응이 미흡하기 때문이다.

사업자의 개인정보보호 책임성 부족과 해킹에 대한 부족으로 인해 웹페이지에서 나타나는 구체적인 침해의 원인과 특징[4]는 아래의 표 1과 같다. 개인정보 노출의 원인에는 개인정보처리자의 부주의, 민원인 부주의, 홈페이지 설계오류 등이 대표적이며 표 2와 같이 각 형태별로 다양한 유

형의 개인정보 노출이 발생하고 있다. 이러한 개인정보 노출 발생의 원인[2]는 표 3 같이 크게 4가지 원인으로 볼 수 있다.

표 1. 웹페이지에서 구체적 개인정보 침해의 원인과 특징

침해원인	특징 및 예시
홈페이지 방문 시 사용자가 감염을 인식하지 못하는 경우	윈도우 운영체제 등 프로그램을 업데이트를 하지 않거나 해커가 특정 사이트의 서버를 해킹해 악성코드를 삽입할 경우, 사용자가 홈페이지를 방문시 악성코드에 자동으로 감염
웹하드와 P2P사이트 등의 전용 프로그램	해커가 웹하드 사이트의 운용서버를 해킹해 정상프로그램과 교체하고 악성프로그램을 업로드시, 사용자는 컨텐츠 다운로드 프로그램 실행 시 악성코드를 자동으로 전송받음
이 메일의 첨부파일 또는 본문에 링크된 사이트 접속 유도	메일의 보낸 사람을 경찰청으로 사칭해 '참고인 출석 요구' 등의 문구를 넣고, 자세한 내용을 살펴보도록 '확인' 링크를 걸어 클릭하도록 유도
사용자의 메신저 계정을 탈취하여 등록된 친구들에게 악성코드 자동 전파	메신저 대화창의 파일을 공유하거나 쪽지 전송 등으로 감염을 유도
SNS에서 이용되는 단축 URL 조작	이벤트 안내 메시지 등으로 관심을 끌어 악성코드가 있는 단축 URL을 게시하고, 클릭하도록 유도해 감염
정상앱을 위장한 모바일 악성코드	웹사이트에서 해당 페이지를 보기위해 필요한 프로그램을 설치할 때, 악성코드가 포함된 프로그램이 자동 설치되도록 함

표 2. 형태별로 다양한 유형의 개인정보 노출

구분	주요내용	조치사항	조치주체
게시글에 개인정보 포함	개인정보처리자 부주의, 민원인의 개인정보 보호 인식부족 등에 의해 홈페이지 게시물에 개인정보가 포함되어 노출되는 형태	콘텐츠를 즉시 삭제 또는 해당 개인정보 일부 *(마스킹)처리/게시판에 개인정보 작성/방지를 위한 경고 문구 삽입/노출 차단 S/W 적용	홈페이지 관리자, 개인정보처리자
첨부파일에 개인정보 포함	게시판의 첨부파일에 개인정보가 노출되는 형태	게시판에서 해당 게시물 삭제 후, 개인정보를 제거한 파일을 다시 업로드	홈페이지 관리자, 개인정보처리자
소스코드 및 URL등에 개인정보 포함	모든 홈페이지에서 기본적으로 공개되는 소스코드 또는 URL에 개인정보가 포함되는 형태	웹사이트 수정	홈페이지 관리자
외부 검색엔진 통한 개인정보 노출	구글 등 포털의 검색로봇 수집에 따른 개인정보 노출	홈페이지에 있는 개인정보를 삭제/구글자동삭제 시스템을 이용한 저장정보 삭제 요청/필요시 검색엔진 배제표준이나 메타 태그 적용	홈페이지 관리자

표 3. 개인정보 노출 원인과 세부사항

노출원인	사 례
개인정보처리자의 부주의	.웹의 공지사항 작성할 경우 개인정보가 포함된 게시물 .웹에 첨부 파일을 업로드시 개인정보포함 유무 확인안함
민원인・고객 부주의	.웹에 민원인이 게시글 작성하면서 신속한 민원처리를 위해서 의도적 혹은 부주의로 본인이나 타인의 개인정보가 포함된 글 등록
홈페이지 설계 오류	. 게시판 소스코드에 작성자 정보를 개인정보로 이용하도록 설정한 경우 .홈페이지 게시판에 비밀번호가 설정되어 해당 화면의 소스보기를 통해 게시물에 작성된 글의 내용확인 가능 .조직 구성원들의 소개, 조직 내 개인홈페이지 혹은 게시물의 정보를 구분하기 위해서 웹페이지 주소(URL)에 개인정보 이용하는 경우
외부 검색엔진 노출 이용	현재 외부 검색엔진 중 구글 검색엔진은 전세계적으로 가장 강력한 성능을 가진 검색엔진으로 명의도용 의도를 가진 자가 활용하는 좋은 창구가 됨

Ⅳ. 웹페이지에서의 개인정보 보호 방안

웹페이지를 통해 개인정보가 노출되지 않도록 하기 위해서는 개인정보가 노출되는 근본적인 원인을 분석하여 기술적, 관리적인 측면의 세부 방안을 강구하고, 이를 상시적으로 점검, 준수, 보완하는 것이 무엇보다 중요하다. 표 4는 웹페이지에서 개인정보 세부 보호 방안[2]이다.

개인정보 보호를 하기 위해서는 개인정보 취급・관리 범위의 명확화가 필요하다. 먼저 개인정보처리자 개개인의 업무 범위를 명확하게 정하고 개인정보처리자 변경 시에 업무에 대한 인수인계가 정확하게 이루어져야한다. 홈페이지 관리자는 개인정보 노출방지를 위해 서비스 중인 웹페이지를 확실히 점검하고, 그 이외의 방치된 홈페이지는 없는지 확인해야한다. 또한 개인정보 보호를 위해서는 관련법에 관해 숙지 및 이해가 필요하다. 홈페이지에서 개인정보가 노출되지 않도록 하기 위해서는 관련법(개인정보보호법, 시행령, 관

표 4. 개인정보 세부 보호 방안

구분	종합대책	세부사항
기술적 측면	홈페이지 설계 검토	설계오류에 의한 개인정보 노출 위험 진단
		보안취약점에 의한 개인정보 노출 위험 진단
	개인정보보호 시스템 운영	개인정보 노출 차단을 위한 S/W 적용(또는 게시판 글 등록 시 필터링을 위한 정규표현식 적용)
		필요 시 검색로봇 배제 표준 적용
관리적 측면	정보 노출관리 범위의 명확화	휴먼 홈페이지 장비, 홈페이지 게시자 지정
	개인정보 노출 관리	개인정보노출방지 관리지침 준수
		개인정보 노출 상시점검
	개인정보 노출 방지 교육	개인정보처리자 교육
		홈페이지 이용자 주의사항공지

련 고시 등)에 대한 숙지 및 이해가 필요하다. 웹페이지 관리자와 개인정보처리자의 유의사항과 웹페이지 설계 시 유의사항에 대해 구체적인 사항들[2] 표 4 ~표 7과 같다.

표 5. 웹페이지 관리자의 유의사항

웹페이지 관리자의 유의사항	
관리부주의로 개인정보 노출 유의	백업DB를 연동시킬 때, 백업DB 내에 개인정보가 포함되어 있는지를 사전에 확인하여 제거한 후 연동시켜야 함
접근권한 관리에 유의	개인정보처리시스템을 이용할 권한이 있는 사용자만 접근하도록, 업무 목적 이외의 불필요한 접근을 최소화하고, 인사이동 발생 시 인가되지 않는 접근을 차단하기 위해 접근권한 철저히 관리
암호화 및 접속 기록 관리에 유의	고유 식별번호, 비밀번호, 바이오정보 등을 정보통신망을 이용해 내외부로 송·수신할 경우, 암호화, 특히 비밀번호는 일방향 암호화 처리

표 6. 개인정보처리자의 유의사항

개인정보 처리자의 유의사항	
개인정보파일 관리지침을 준수	.행정안전부의 「표준개인정보보호지침」에 따라 개인정보파일의 관리 .개인정보파일대장을 작성 및 관리·보관 .홈페이지에 글을 게재 전에 자료에 개인정보가 포함되어 있는지 검사
개인정보파일 패스워드 및 암호화 설정이 필요	개인정보가 포함된 파일에 대해서 패스워드 설정 및 별도 암호화, 각 회사의 내부관리규정에 명시 및 이행도록 함
PC점검계획 수립 및 업무 인수인계 시 유의사항에 주의	.인수인계 되는 PC의 개인정보 복구 또는 재생되지 않도록 파기 .홈페이지및 관리자페이지 등에 ACL(Access Control List)를 등록하여 접근통제 조치 .하드디스크 3회 이상 덮어쓰기, 디가우져(소자장비)를 이용한 디스크 영구삭제, 촌공장비 등 물리적 하드디스크 파쇄
개인정보보호 교육 안내	개인정보처리자 및 홈페이지 관리자가 개인정보 노출 위험에 대한 상시교육

표 7. 홈페이지 설계 및 개발시 유의사항

홈페이지 설계 및 개발시 유의사항	
정보보호의 필요성 인식	.설계 및 개발과정부터 개발자가 개인정보호의 중요성에 대해 인식, 수집에서 파기까지 흐름 판단하여 설계 및 개발
웹페이지 설계 검토에 주의	웹페이지 설계부터 충분히 검토, 이미 구축된 홈페이지도 노출위험이나 보안취약점 진단, 위험요소 정확히 파악, 발견 시 수정
설계 및 개발단계에서의 유의	.개인정보처리방침을 홈페이지 메인 화면에 공개함 .개인정보처리방침 및 약관이 개정시 정보주체에 현행약관과 적용일자와 개정사유 명시 .전년도 말 기준 직전 3개월간 그 인터넷 웹페이지를 이용한 정보주체의 수가 하루 평균 1만명 이상인 개인정보 처리자는 아이핀, 휴대폰 인증, 공인인증서 등 주민번호 외의 회원가입을 의무적으로 제공

Ⅴ. 결 론

현대는 급속한 정보화에 따라 불가피하게 제공되는 개인정보가 다양한 형태로 본인의 의지와는 관계없이 노출됨으로 인해 부당하게 개인의 사생활이 침해당하는 정신적 피해와 함께 물질적 손해가 발생하는 등의 심각한 사회문제로 대두되고 있다. 개인정보침해의 가장 큰 원인은 개인정보를 이용하는 사람의 부주의이다. 최근 개인정보 침해가 대두되면서 점차 개인정보 보호의 필요성이 대두되고 있지만, 개인 정보는 침해를 입기 전에 미리 예방하는 것이 최선이다. 따라서 정부는 대중들에게 개인정보 보호에 관한 교육의 기회를 제공해야 한다. 교육에는 개인정보를 통해 나타날 수 있는 금전적, 심리적 피해와 이를 사전에 예방하는 방법을 알려주고, 침해를 당했을 때의 대처방법 등의 내용을 포함하고 있어야 한다. 교육을 통해서 인식의 전환이 이루어져야지만, 개인정보를 이용하는 모든 사람이 이용할 때 주의하기 때문이다. 따라서 본 연구에서는 웹상에서의 최근 개인정보 침해 사례와 그 원인 및 보호 방안을 검토 및 분석하였다.

참고문헌

[1] 강동구, “웹사이트의 개인정보 수집 및 보호 정책이 이용자 태도에 미치는 영향에 관한 연구”, 2012.
[2] 행정안전부, “개인정보노출방지 가이드라인”, 개인정보보호과, 2012. 07.
[3] 방송통신위원회, 한국인터넷 진흥원 개인정보 침해신고센터 접수자료, 2012.
[4] 인터넷 보안뉴스 자료, 2013년 5월 9일.
[5] 한국정보화진흥원, “빅 데이터 시대 위험기반의 정책”, 2012.