

主題

정보통신부문에서의 개인정보 보호 정책 현황과 발전과제

한국정보보호센터 주덕규, 박광진

차 례

- I. 개요
- II. 각국의 개인정보보호 정책 현황
- III. 국내 개인정보 수집 및 취급현황
- IV. 향후 발전과제

I. 개 요

전자상거래의 급속한 확산은 디지털경제시대의 기업경영에 새로운 가능성을 제시하고 있다. 즉, 전자상거래의 경우 정보기술을 활용하여 인터넷상에서 상거래를 하면 유통비용의 절감 등에 의한 효율적인 사업활동은 물론 신속하고 정확한 시장조사가 이루어지기 때문에 이용자에 대한 서비스를 향상할 수 있다. 기업들은 데이터베이스 마케팅과 같이 정보통신 기술을 효과적으로 활용함으로써, 소비자에

게 차별화된 제품 및 서비스를 제공할 수 있게 되었으며, 그 결과 치열한 경쟁에서 경쟁 우위를 획득할 수 있게 되었다. 그러나 소비자가 자신에 관한 개인정보가 자신의 동의없이 전자상거래를 이용하는 과정에서 쉽게 수집 및 취급되고, 제3자에게 광범위하게 제공된다는 사실을 알게되면 전자상거래 이용에 대한 거부감이 유발될 수 있으며, 사업자가 적절한 보호 장치를 갖출 것으로 기대한 신뢰마저 손상당하게 된다.¹⁾

따라서 인터넷상에서 개인정보가 유출되는 것을

1) 실제로 1999년 가을 미국 WSJ지와 NBC가 실시한 공동 여론조사에서는 이들이 제시한 21세기에 당면할 8가지 우려사항 중에서 개인정보 유출이 1위(29%)를 차지하여, 개인정보 유출이 응답자들의 가장 큰 우려 대상인 것으로 나타났고, 미국 비즈니스위크 조사('98.3.)에 따르면 인터넷 전자상거래를 자제하는 소비자의 기피이유 중 하나는 자신의 개인정보 및 통신정보의 유출에 대한 우려라고 밝히고 있다. 또한, 1997년 3월 Boston Consulting Group의 보고서는 9,300명의 인터넷 이용자를 조사한 결과, 70%가 넘는 이용자가 전화나 우편에 비해 프라이버시 침해의 우려를 더 느끼고 있으며, 41%가 넘는 이용자는 개인 정보의 등록 요구를 받게 되면 더 이상의 이용을 하지 않고 있고, 27%가 넘는 이용자는 거짓 정보를 등록하면서 계속 이용하는 것으로 밝히고 있다.

우려하여 인터넷 사용 및 전자상거래에 대한 소비자의 불안·불신감을 해소시켜 전자상거래 활성화를 도모하는 차원에서도 적극적인 개인정보보호조치가 한층 더 요구된다. 인터넷 프라이버시 보호는 인터넷을 이용하는 이용자들의 개인정보가 함부로 오·남용되는 것을 막음으로써 개인의 존엄과 인격이 훼손될 수 있는 가능성을 줄이고 이용자들이 안심하고 인터넷을 이용할 수 있게 함으로써 그 이용촉진에도 기여하게 될 것이다. 개인정보가 활용되는 각 단계에서 정보 프라이버시가 침해되는 경우는 학자에 따라 상이하지만 크게 수집, 이차적 사용, 오류, 부당한 액세스의 네 가지로 나눌 수 있다.

1. 수집 (Collection)

데이터베이스 마케팅을 위한 개인정보 수집 단계에서의 정보 프라이버시를 보호하기 위해서는 불필요한 개인정보의 수집은 원칙적으로 제한되어야 하고, 합법적이고 정당한 절차에 의해 데이터 주체(소비자)의 인지나 동의를 얻은 후에 수집되어야 한다. 소비자의 동의 또는 허가를 획득한 개인정보의 이용은 정보 프라이버시를 침해할 가능성이 크게 줄어들고, 개인정보 사용에 대한 소비자의 신뢰를 확보하는데 기여한다. 그러나 수집한 고객정보, 편집리스트와 같은 외부고객정보를 소비자들의 동의 없이 제 3자에게 제공하는 경우에는 소비자들의 정보 프라이버시를 크게 침해할 여지가 있다.

2. 이차적 사용 (Secondary Use)

특정한 목적을 위하여 수집된 개인정보가 정보 제공자의 동의 또는 허가 없이 다른 목적으로 재사용되는 개인정보의 이차적 사용은 정보통신기술의 발전과 개인정보가 기업 경영에 중요한 자원이 된다고 인식되면서 상업적으로 사용하려는 경향이 증가하고 정보중개업을 전문으로 하는 기업이 발생함에 따

라 개인정보의 이차적 사용은 더욱 심각한 문제로 대두되기 시작하였다. 정보중개업은 대가를 지불하고 수집한 개인정보의 소유권이 중개업자에게 있기 때문에 이 소유권을 바탕으로 정보를 제 3자에게 판매 또는 대여하는 영업 활동을 수행한다. 그러나 소비자들이 이러한 이차적 사용에 대해 동의 또는 허가하지 않은 경우 이는 소비자들의 정보 프라이버시를 심각하게 침해하게 된다. 그리고, 비록 문화적 가치와 정보 프라이버시에 대한 우려 수준의 차이가 크지 않다 하더라도 각 국가의 프라이버시 보호 법률이 상이하기 때문에 개인정보의 국가간 이동(Transborder Data Flow) 역시 심각한 정보 프라이버시 침해를 초래할 수 있다.

3. 오류 (Error)

데이터베이스 마케팅을 위하여 기업은 과거부터 축적된 개인정보를 이용하여 시장을 세분하고 판매 촉진 활동을 수행한다. 그러나, 고의적 또는 우발적으로 발생한 사고에 의해 데이터베이스에 오류가 발생할 수 있다. 개인정보는 정적 사적정보(Static Private Information)와 동적 개인정보(Dynamic Personal Information)로 나눌 수 있다. 이 중 동적 개인정보는 시간이 경과함에 따라 그 내용이 급격하게 변화하는데 이를 데이터베이스에 적절히 반영하지 못 하는 경우 오류를 발생시키고 개인에 대한 허상을 초래하여 정보 프라이버시가 침해하게 된다. 이 문제는 동적인 현실 세계에서 과거 개인정보의 정적인 속성 때문에 더욱 심각해질 수 있다. 결과적으로 오류가 있는 개인정보의 이용은 비효과적인 데이터베이스 마케팅을 초래할 뿐 아니라, 소비자에게는 심각한 프라이버시 침해를 초래한다. 특히, 이렇게 오류가 있는 개인정보가 제 3자에게 판매 또는 대여되는 경우 문제의 심각성은 더욱 커진다.

4. 부당한 액세스 (Improper Access)

정당한 권한을 지니고 데이터베이스에 액세스하는 관계자를 제외하고 해커와 같이 부당하게 데이터베이스에 액세스하는 경우, 단체와 법인 관계자가 다른 목적으로 개인정보를 조작·유출하는 경우도 있다. 특히, 데이터베이스의 파일이 부당하게 액세스되고, 변경 또는 파괴되었는지조차 알 수 없는 경우, 정보 프라이버시 침해는 더욱 심각한 문제가 된다.

II. 각국의 개인정보보호 정책 현황

우리 나라를 상대로 한 외국기업의 개인정보 수집 활동이 활발해지면 법률 제정을 비롯한 개인정보보호 정책을 통하여 개인정보를 보호하지 않을 경우 국내 소비자의 피해가 우려되는 반면, 외국에서 외국 소비자를 상대로 한 국내기업의 개인정보 수집 및 이용은 해당국의 개인정보보호 정책에 크게 좌우되며, 결과적으로 개인정보보호에 익숙하지 않은 국내 기업으로서는 큰 장벽에 부딪히게 된다. 따라서 국민의 프라이버시권을 실질적으로 보호한다는 측면뿐 아니라 인터넷의 신뢰확보를 통한 전자거래의 활성화 및 국제적 전자거래 환경하에서의 국내 기업의 이익 보호를 위해서도 개인정보의 수집과 유통에 관한 최소한의 질서를 법적으로 확립하는 것이 바람직하다.

1. 국외 현황

가. 유럽연합(EU : European Union)

유럽연합은 개인정보보호에 관하여 강력한 정책을 추진하고 있다. 유럽연합의 유럽의회와 유럽이사회는 일반적인 개인 정보 취급에 대한 규정으로 회원국 국민의 기본권과 자유를 보호하고 개인정보 처리와 관련한 프라이버시권을 보호하며 EU 국가간

의 개인정보의 자유로운 유통을 촉진하기 위하여, 1995년 10월 『개인데이터의 처리와 개인데이터의 자유로운 유통에 관련된 개인정보 지침』을 채택하였다. 동 지침은 특별히 전자거래나 인터넷만을 위해 제정된 것은 아니지만, 경제활동이나 행정목적, 기타 모든 영역에 있어서 개인정보를 수집하고 축적, 이전하는 활동에 적용된다. 또한 동 지침은 1998년 10월까지 회원국으로 하여금 다음 원칙에 따라 자국의 프라이버시법을 제·개정할 것을 요구하고 있다. 특히, EU 수준으로 적절하게 개인정보를 보호해 주고 있지 않은 국가로는 개인자료의 이전을 금지하고 있어 EU 회원국과 교역을 하고 있는 다른 국가들에게도 해당 국가의 기존 개인정보보호 법제 및 정책을 변화시켜야 하는 도전을 주고 있다.

1997년 12월에는 동 지침을 보완하기 위하여 『정보통신부문에서의 개인정보 처리 및 프라이버시 보호에 관한 지침』을 채택하였는데, 주로 ISDN(the Integrated Services Digital Network)이나 디지털 이동 네트워크(public digital mobile networks)를 통한 정보통신 서비스에 적용된다. 이 지침은 개인데이터의 처리와 관련한 기본적 인권과 자유, 특히 프라이버시권의 균등한 보호수준을 보장하고, EU에서의 데이터와 통신설비 및 서비스의 자유로운 이동이 보장되도록 각 회원국 규정의 조화 제공을 목적으로 하고 있다.

또한, 1999년 2월에는 인터넷에서의 프라이버시 보호를 위한 각료위원회 권고(No. R(99)5)인 『정보고속도로에서 신상정보의 수집처리와 관련한 개인의 보호를 위한 지침』을 채택하고 있다. 동 지침은 인터넷 이용자와 서비스 제공자(ISP)의 권리와 의무를 담고 있다. 서비스이용자의 권리로 자신들에 관한 어떠한 개인 정보가 수집·처리·저장되는지를 알아볼 수 있으며 특정한 목적을 위하여 필요에 따라 이러한 정보를 변경하거나 삭제하도록 요

구할 수 있음을 규정하고 있다. 서비스 제공자(네트워크 운용자, 네비게이션 소프트웨어 설계자 및 계시판 이용자 포함)의 의무로는 개인정보를 합법적이고도 공정하게 이용하고, 데이터 통합성·기밀성·네트워크 보안을 보장하며 개인정보의 은밀한 수집, 기록 또는 월경 전송을 금지하는 것에 대한 책임을 인식하도록 권고하고 있다.

나. 미국의 자율규제정책

1998년 11월에 미국 상무부는 개인정보보호를 위한 세이프하버 원칙(Safe Harbor Principles)을 제시하였다. 세이프하버 원칙은 7가지 항목으로 구성되어 있는데, 이 원칙을 충족하는 미국기업은 EU 기준에 적합한 개인정보보호에 충실한 기업으로 추정되어 향후 아무런 제재없이 EU와의 개인 데이터를 이전할 수 있도록 하기 위하여, 미국산업계에 이행을 권고하고 한편으로는 EU와 협상하기 위하여 만들어진 것이다. 이 원칙은 1998년 처음 발표된 이래 1999년 11월 15일 "International Safe Harbor Privacy Principles(Draft)"로 수정 제안되고 있다. 세이프하버 원칙에서는 수집하는 개인정보의 유형, 해당 정보의 수집방법, 당해정보의 수집목적, 조직체의 유형, 당해 조직체가 정보주체에게 당해 정보의 이용과 공개를 제한할 수 있는 선택권과 조치를 제공하고 있음을 알려주도록 규정하고 있다. 또한, 미국에서는 표준 프라이버시 준수 운영방안을 제시하고 일정조건을 충족하는 업체에 "TRUSTe"나 "BBB 온라인 마크"와 같은 인증마크를 부여하는 제도를 시행해 오고 있으며, 정부 및 비영리단체는 "Privacy Policy"를 작성하여 홈페이지에 게시함으로써 그들 기관의 개인정보취급 방침 등에 관하여 자세히 설명하고 있다.

다. 일 본

일본의 경우에 공공부문의 개인정보보호를 위하여 1988년 12월에 「행정기관이보유하는전자계산

기처리에따른개인정보의보호에관한법」을 제정하였으며, 민간부문에서의 개인정보처리시 개인정보보호는 1997년 3월 개정된 「민간부문에서의 전자계산기 처리에 관련된 개인정보 보호에 관한 가이드라인」에 기초하고 있다. 일본의 각 사업자단체는 통산성의 가이드라인을 참고하여 자체적인 가이드라인을 제정하여 운영하고 있다. 1997년 사이버산업연합회의 「사이버산업에서의 개인정보보호를 위한 가이드라인」, 1998년 3월 전자상거래실증추진협의회 「전자상거래에 있어서의 개인정보보호 가이드라인」 등이 그것이다. 한편, 일본은 EU지침에서 규정한 "적절한 개인정보보호 수준 확보"의 한 방안으로서 일본 산업규격인 개인정보보호규격(JIS Q 15001)을 1999년 3월 제정하여 개인정보보호에 관한 인식제고에 노력하고 있다. 또한 EU 등 국제간 거래환경 조성을 위해 개인정보보호의 중요성을 부각시키기 위한 다각적인 노력을 하고 있으며 이와 아울러 통산성 산하 재단법인 일본정보처리개발협회에서는 1998년 4월 1일부터 "개인정보보호 지침"을 근거로 하여 개인정보 취급 관련 전 사업자를 대상으로 민간부문에서 자율적으로 개인정보보호를 위해 프라이버시마크 제도를 시행하고 있다.

한편 일본은 개인정보가 이미 사회전반에 널리 사용되어지는 현재의 시점에서 공공부문과 민간부문에 모두에 적용할 기본법을 제정하기 위하여 2000년 작업결과를 토대로 2001년중에 입법화할 것을 목표로 통산성 고도정보통신사회추진본부 산하에 『개인정보보호연구회』를 구성하여 활동중이다. 『개인정보보호연구회』는 1999년 11월에 발표한 중간보고서에서는 (1) 전 분야를 포괄하는 기본법을 제정, 국민 모두에게 적용할 수 있는 원칙을 확립하고 (2) 신용정보, 의료정보, 전기통신의 3개분야는 개별법을 제정하여 대응하며 (3) 보도·출판, 학술·연구 분야에 대해서는 원칙의 적용을 제외하는 것을 검토한다 등을 주요내용으로 하고 있다.

2. 국내 법제도 현황

우리 나라의 경우 프라이버시 및 개인정보보호와 관련된 국내의 법률로는 공공기관의 컴퓨터로 처리되는 개인정보를 주요 대상으로 하는 1994년에 제정된 「공공기관의개인정보보호에관한법률」과 소비자의 개인정보중 주로 신용과 관련된 정보가 보호대상인 1995년에 제정된 「신용정보의이용및보호에관한법률」 및 인터넷 등의 민간부문에 적용되는 「정보통신망이용촉진등에관한법률」이 있다. 기타 전자서명법, 전자거래기본법, 의료법, 금융실거래및비밀보장에관한법률, 전기통신사업법, 전자거래기본법 등에서 소관분야별 개인정보보호 및 이용에 대한 간략하게 규정하고 있다.

가. 정보통신망이용촉진등에관한법률

인터넷에서의 개인정보의 오남용을 방지하기 위한 조치로서 1999년 2월 개정된 정보통신망이용촉진등에관한법률(이하 "정보통신망이용촉진법"이라 한다)에서 개인정보 수집시에 개인정보 관리책임자의 소속·성명 및 전화번호 기타 연락처, 개인정보의 수집목적 및 이용목적, 개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용, 이용자의 권리 및 그 행사방법, 수집하는 개인정보의 보유기간 및 이용기간을 미리 이용자에게 고지하거나 정보통신서비스 이용약관에 명시하는 의무를 정보통신서비스제공자에게 부과하고 있다. 정보통신망이용촉진법은 OECD의 개인정보보호원칙에 맞춰 인터넷 등 가상공간에서의 개인정보를 보호하기 위하여 이용자의 동의에 기초한 적절한 개인정보 수집·이용·처리·제공 및 이용자의 권리보장을 규정하고 있다.

나. 신용정보의이용및보호에관한법률

신용정보의 오용 및 남용을 방지하고 국민의 프라이버시 보호 및 신용질서를 확립하기 위한 법으로써

신용정보업자와 신용정보집중기관 등 신용정보기관을 대상으로 규율하고 있다. 이 법에서 신용정보를 '금융거래 등 상거래에 있어서 거래 상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보로서 대통령령이 정하는 정보'로 정의하고 있다. 이 법에서는 신용정보의 수집·조사 및 처리, 신용정보의 유통·이용 및 관리, 신용정보주체의 보호 등을 마련하고 있으며, 개인의 정치적 사상, 종교적 신념 기타 신용정보와 무관한 사생활에 관한 정보, 불확실한 개인정보 등에 대한 수집·조사 자체를 금지하는 등 개인정보보호를 위한 규정을 마련하고 있다. 또한 신용정보관련자에 대하여 "업무상 알게된 타인의 신용정보 및 사생활 등 개인적 비밀"을 업무목적 외로 누설 또는 이용하지 못하도록 규정하고 있다.

Ⅲ. 국내 개인정보 수집 및 취급현황

본 조사는 한국정보보호센터에서 1999년 10월 22일부터 11월 21일 까지 정보통신서비스제공자, 전기통신사업자 및 일반회사(금융기관, 의료·언론기관, 대기업·중소기업 등) 등 모두 1,000여개의 웹사이트를 대상으로 실시하였다.

1. 개인정보 수집여부

1,000개 사이트 중 약 94%인 936개 사이트가 서비스이용자로부터 최소 한 개 이상의 개인정보를 수집하고 있다. 분야별로 개인정보를 수집하는 비율을 살펴보면, 쇼핑몰의 경우에는 98%인 295개 사이트가, 일반회사의 경우에는 95%인 416개 사이트가, 공공기관의 경우에는 87%인 225개 사이트가 개인정보를 수집하고 있었다.

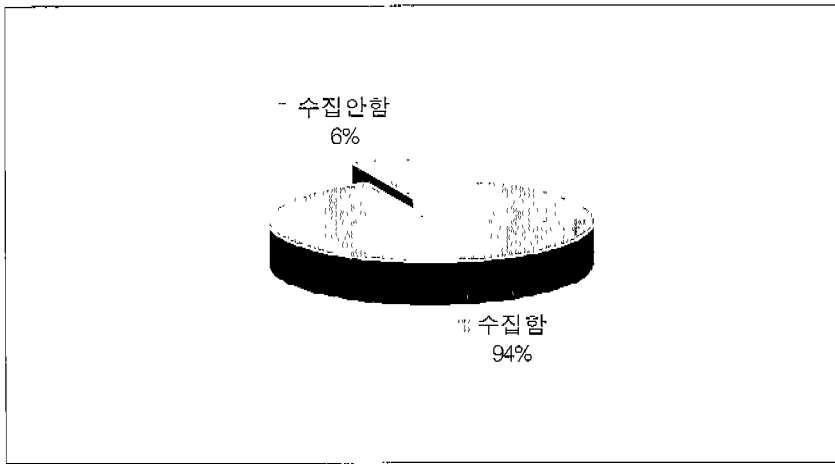


그림 1. 개인정보를 수집하는 웹사이트 비율 (전체)

2. 개인정보 수집항목

어떤 개인에 관한 정보를 알면 그 사람의 사회적, 경제적 지위와 기호 및 선호하는 상품의 양상까지도 파악할 수 있다. 또한, 수집한 개인정보를 통계나 이 익정보로 결합함으로써 개인 프로필의 생성이 가능

하다. 개인정보를 수집하고 있는 웹사이트는 성명, 주민등록번호, 주소, E-mail, 전화번호, 직업, 직 장명, 성별, 거주지, 신용카드번호(계좌번호), 결혼 여부, 기념일, 취미·특기 등 다양한 개인정보를 수 집하고 있었다. 가장 많이 수집하는 개인정보 유형 은 성명(99%), E-mail 주소(86%), 주소(67%),

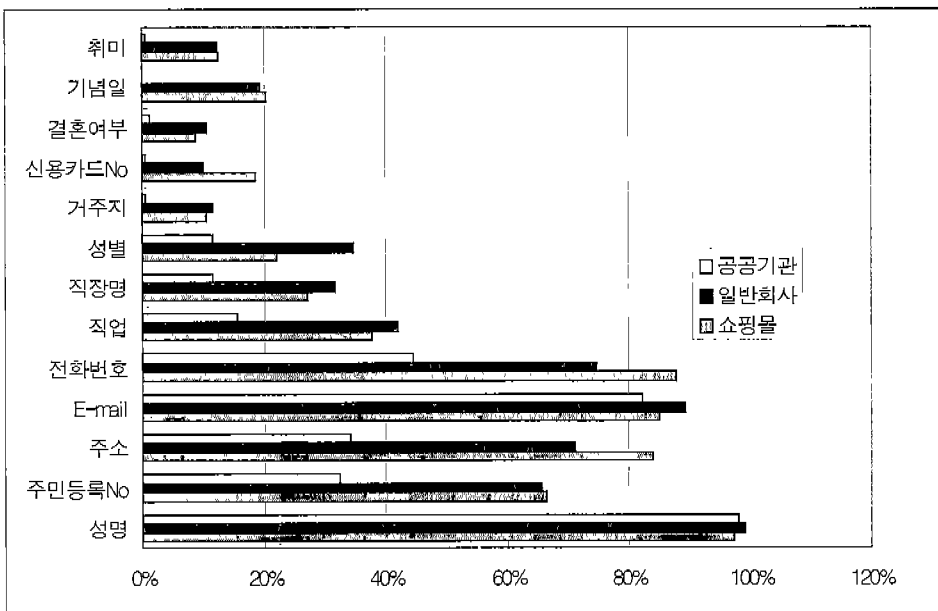


그림 2. 웹사이트에서 수집하고 있는 개인정보의 항목 (전체)

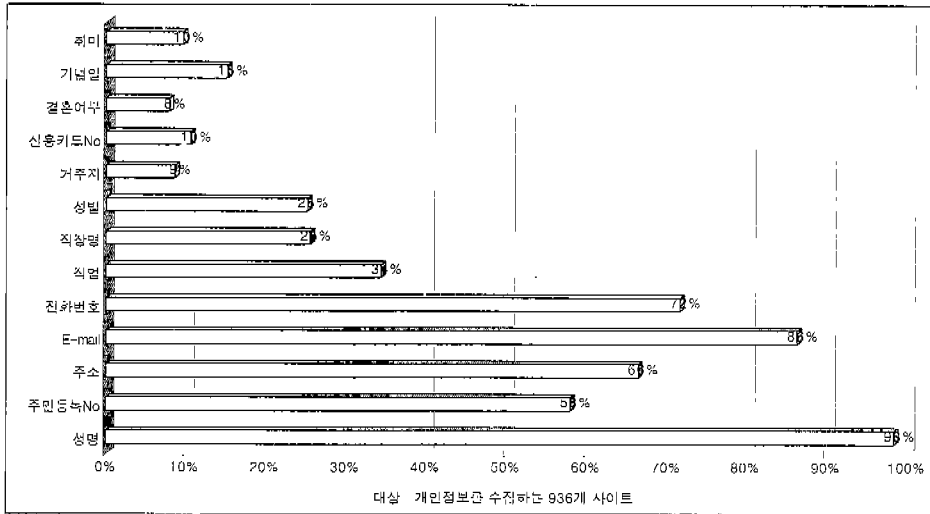


그림 3. 웹사이트에서 수집하고 있는 개인정보의 항목(분야별)

주민등록번호(58%) 등의 개인식별정보였다.

분야별로 살펴보면, 거주지, 결혼여부, 기념일, 취미·특기 등의 부가정보를 공공기관의 경우 (1.8%)가 일반회사(35%)나 쇼핑몰(33%)보다 훨씬 적게 수집하고 있음을 알 수 있다.

3. 개인정보 수집항목 수

개인정보를 수집하는 사이트 중 39%가 4개이하의 개인정보를 수집하고, 46%의 사이트가 5~8개

의 개인정보를 수집하고 있으며, 9개이상의 개인정보를 요구하는 곳도 15%에 달하고 있다. 그러나 분야별로 살펴보면 상당한 차이가 있다. 7가지 이상의 항목을 수집하는 경우가 일반회사는 52%, 쇼핑몰은 41%에 달했으나 공공기관은 단지 9%만이 7가지 이상의 항목을 수집하고 있다. 또한, 4가지 이하의 항목을 수집하고 있는 경우가 공공기관이 72%인 반면 쇼핑몰은 25%, 일반회사는 22%에 불과하였다. 이것으로 보아 공공기관이 보다 적은 항목의 개인정보를 수집하고 있으며, 서비스 제공에 필요한

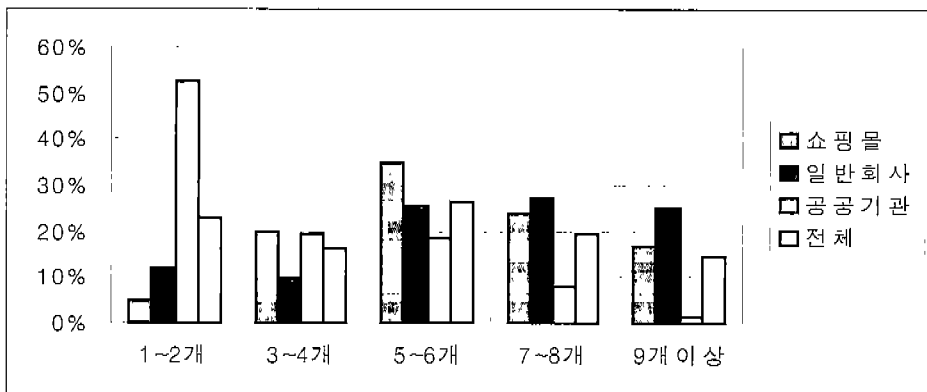


그림 4. 입력을 요구하는 개인정보 항목 수 (전체)

범위 내에서 개인정보를 수집하고 있음을 보여주고 있다.

4. 개인정보 필수입력 요구 항목

서비스제공을 위한 개인정보는 서비스를 위한 필수항목과 부가서비스를 위한 부가정보로 구분할 수 있다. 필수입력 요구항목은 서비스제공자가 반드시 입력하도록 요청하는 항목으로서, 서비스 제공 및 이용을 위하여 필요한 정보이며, 이를 입력하지 않을 경우 서비스제공이 거부되는 항목이다. 부가정보는 굳이 입력하지 않아도 해당 서비스를 이용하는데 지장은 없으나, 입력하면 생일축하, 인생설계, 바이오리듬 확인 등의 부가서비스를 제공받을 수 있는 항목이다. 필수입력사항을 구분하여 입력하도록 하는 것은 개인정보의 입력을 서비스이용자에게 선택하게 하는 것으로 정보 프라이버시 보호에 중요한 사항이다.

이 조사에서는 「필수입력사항」 등으로 명시한 경우에 한하여 필수입력 요구항목으로 분류하였다. 필수입력 요구사항을 구분하고 있는 사이트는 전체

45%인 426개였다. 나머지 55%의 사이트에서는 반드시 입력하여야 하는 필수정보인지 입력하지 않아도 되는 사항인지를 구분할 수가 없었다. 분야별로는 쇼핑몰, 일반회사, 공공기관 모두가 비슷한 비율(43% ~ 50%)로 필수입력사항을 구분하고 있음을 알 수가 있었다.

5. 개인정보를 수집하여 제공하는 서비스

전체적으로는 회원모집 및 관리를 위한 경우(60%)가 가장 높았고, 정보제공의 경우(51%)와 상담·질의·의견게시의 경우(47%) 등의 순이었다. 회원모집은 정보제공, 물품주문 뿐만 아니라 기타 사항인 구인·구직, 채팅, 동호회, 미팅·결혼추천, 전문가등록, 설문조사, 경품추천 등 광범위하게 이루어져, 웹사이트는 회원확보를 통한 개인정보수집을 선호하고 있는 것으로 나타나고 있다. 이것은 인터넷 가상공간에서 무료 서비스를 제공하면서 확보한 회원 수를 하나의 기반 자원으로 인식되고 있는 현실을 반영한 것으로 보여진다.

쇼핑몰의 경우는 물품 주문 및 배달(72%)이 주요 제공하는 서비스였으며, 이는 또한 회원모집 방

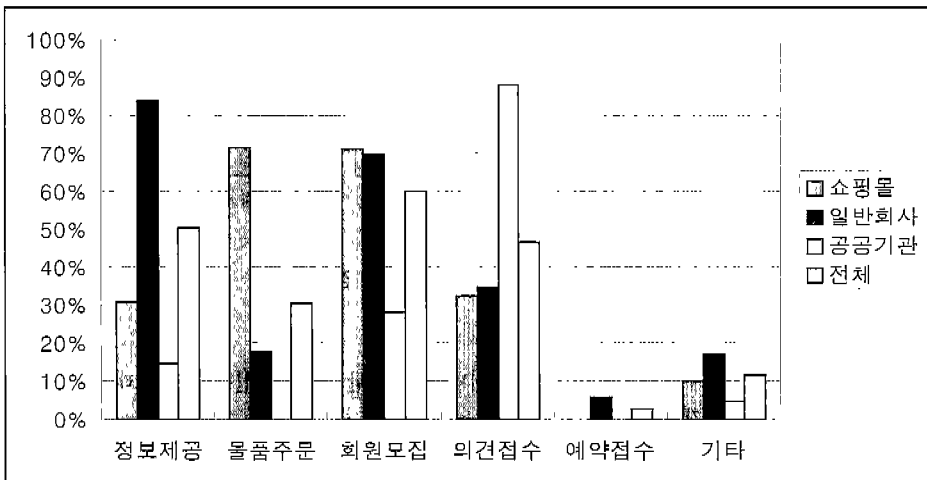


그림 5. 개인정보를 수집하여 제공하는 서비스의 종류

식(71%)을 선호하고 있음을 보여주고 있다. 쇼핑몰에서는 정보제공(31%)이나 상담·질의(32%) 등의 서비스는 상대적으로 저조함을 보여주고 있다. 일반회사의 경우에는 정보제공(84%)을 주요 서비스로 하되, 역시 회원모집 방식(70%)을 선호하고 있었다. 반면에 행정·공공기관들은 상담·의견제시·불만접수(88%)를 주요 서비스로 제공하고 있으며, 회원모집형태(28%)는 미미한 편이었다. 행정·공공기관에서 회원모집형태가 미미한 것은 필수항목만을 주로 요구하는 것과도 일치하고 있다.

6. 개인정보 취급방침의 고지

개인정보취급방침이란 서비스제공자가 서비스이용자의 개인정보 수집 및 이용에 대한 방침을 설명·고지하고, 개인정보 수집에 대한 동의를 받는 일련의 절차를 설명해주는 것이다. 미국에서는 대부분 서비스이용약관과 링크되어 있으며 이용약관과

동일하게 취급되기도 한다. 개인정보취급방침을 주로 게시하는 장소를 조사한 결과 홈페이지의 첫 화면에 아이콘이나 하이퍼링크의 『개인정보취급방침』 형태로 게시하고 있는 경우는 단지 11개 사이트(1%)에 불과하였고, 39%가 개인정보를 입력받는 곳에, 15%가 약관에 게시하고 있었다. 44%의 사이트는 개인정보취급방침을 전혀 게시하고 있지 않았다. 개인정보취급방침의 게시는 하나의 계약사항임과 동시에 2000년 1월 1일부터 시행하여야 할 의무사항이며, 향후 목적의 사용·제공 등으로 인한 법적 분쟁의 원인이 될 수 있으므로 개인정보보호방침 게시에 보다 적극적으로 나서야 할 것으로 보인다.

7. 개인정보보호를 위한 기술적 조치

개인정보에의 접근제어를 위하여 패스워드를 사용하고 있는 경우는 71%인 663개 사이트였고, SET²⁾이나 SSL³⁾과 같은 암호프로토콜을 사용하

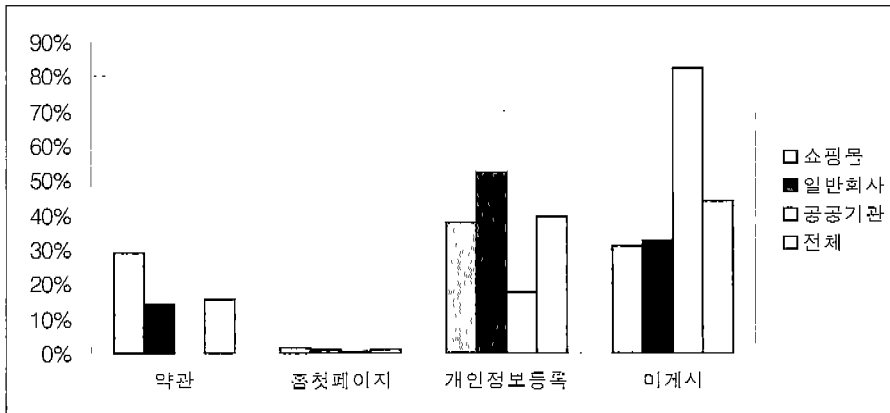


그림 6. 개인정보취급방침 게시 장소

- 2) SET(Secure Electronic Transaction)은 인터넷을 이용한 안전한 신용카드 거래의 표준화를 위하여 비자카드·마스터카드 등이 개발한 프로토콜이다.
- 3) SSL(Secure Socket Layer)은 1994년 미국의 넷스케이프사에 의해 최초로 개발되었으며, 현재 버전 3.0에 이르고 있다. 전송 계층 사이에서 클라이언트와 서버간의 안전한(Secure) 채널을 형성해 주는 역할을 수행한다.

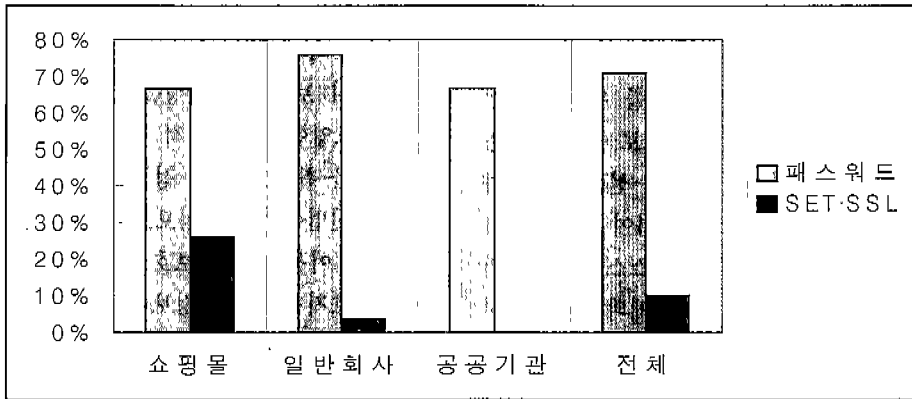


그림 7. 개인정보보호를 위한 기술적 조치 (복수조사)

는 경우는 10%인 90개 사이트에 불과하여, 개인정보의 전송시에 해킹이나 불순목적으로 개인정보에 접근하는 것에 대하여 별다른 조치가 없음을 보여주고 있다. 패스워드나 ID를 사용하더라도 SSL과 같은 안전한 프로토콜을 이용하지 않는다면 쉽게 해킹을 당할 수 있다. 쇼핑몰은 특성상 SET이나 SSL과 같은 프로토콜을 이용하여 안전한 정보의 전송에 관심(26%)을 갖는 것으로 나타나고 있지만, 일반회사(4%)나 공공기관(0%)은 거의 안전한 정보의 전송에는 관심을 갖고 있지 않은 것으로 나타나고 있다. SET의 사용에는 비용이 수반되지만, SSL은 웹사이트 운영자가 약간의 관심만 갖는다면 구현을 할 수 있으므로, 영세한 사업자나 정부·공공기관 등을 위하여 SSL의 사용에 대한 지원방안을 강구하여야 할 것으로 보인다.

8. 쿠키 운영에 대한 설명과 동의

기타 쿠키⁴⁾에 대한 설명을 알려주는 사이트는 전체 1000개 사이트중 2%인 4개⁵⁾에 불과했다. 특히, 쿠키설정이 서비스이용의 전제 조건이 되어 쿠키에 의하여 개인정보(접속정보, E-mail정보 등)를 수집하는 경우 반드시 쿠키 설정에 대한 설명 및 동의를 받도록 하여야 한다. 쿠키는 서비스이용자 본인도 모르게 정보를 수집하는 수단이 될 수 있으므로, 쿠키 설정 여부를 명확히 함으로써 웹사이트에 대한 신뢰를 줄 수 있을 것이다.

표 1. 쿠키에 대한 설명하고 있는 웹사이트

항 목	쇼핑몰	일반회사	공공기관	계
쿠키에 대한 설명	24 (8%)	27 (6%)	0 (0%)	51 (5%)

4) 쿠키는 이용자 사이트에 대한 기본 설정 정보를 보관하기 위하여 웹 사이트가 이용자의 컴퓨터 하드 디스크로 전송하는 소량의 정보이다. 이용자가 접속을 하면 서비스제공자의 컴퓨터는 이용자의 브라우저에 있는 쿠키의 내용을 읽고, 이용자의 추가정보를 자신의 컴퓨터에서 찾아 접속에 따른 성명 등의 추가입력 없이 서비스를 제공할 수 있다. 쿠키는 사용자의 컴퓨터는 식별하지만 사용자를 개인적으로 식별하지는 않는다.

5) 이번 조사에서는 쿠키를 운영하는 서비스제공자중 쿠키운영에 따른 설명과 동의를 받는지 여부를 조사하지 않고, 일률적으로 쿠키에 대한 설명을 하고 있는나를 조사하였기 때문에 오류가 있을 수 있다.

IV. 향후 발전과제

가상공간에서의 프라이버시 보호를 위해서는 정보주체의 개인정보를 공정한 방법으로 수집하고 정당하게 이용하려는 사업자의 노력이 선행되어야 하며, 자신의 프라이버시 보호를 위하여 정보주체가 '정보 자기결정권'에 대해 인식하고 스스로 보호하려는 의지가 반드시 필요하다. 정보주체의 프라이버시 보호에 대한 인식, 사업자의 자율규제노력 및 법적 보호와 개인정보보호를 위한 기술이 유기적으로 구현될 때 효과적인 프라이버시 보호를 기대할 수 있을 것이다. 개인정보보호는 개인 프라이버시 보호와 개인정보의 활용으로 편익 사이에서 적절한 균형을 찾는 것이 중요하다. 정당한 개인정보의 활용은 재화 및 서비스에 대한 정확한 수요자를 발견하도록 하여 자원배분의 효율성을 촉진시키며, 개인 소비자에게도 커다란 이익이 될 수도 있다. 효과적인 개인정보보호를 위하여는 다음과 같은 노력들이 지속되어야 할 것이다.

1. 개인정보취급업자의 자율규제 선행

개인정보를 보호하기 위하여 정보통신망이용촉진법, 신용정보이용및보호에관한법률 등이 제정되어 있으며, 이러한 법에서 규정하고 있는 의무사항을 관련 사업자가 자율적으로 적절한 수준의 개인정보 보호 원칙을 제정하고 실천함으로써 이용자와의 신뢰감을 구축할 수 있다.

또한 경제구조의 복잡화 및 기술진보의 가속화와 개인의 프라이버시 문제를 단순히 법적인 측면에서 보호하고 규제하기보다는 업계 스스로 프라이버시에 관심을 갖고 프라이버시에 관한 이용자의 선호를 찾아내어 그 보호방안을 마련하는 자율규제를 병행하고 프라이버시를 보호하는 적절한 기술을 활용하는 것이 효율적이다. 이미 미국·일본 등에서는 사업자단체 스스로 프라이버시 보호원칙을 수립하고

이용자 등 외부에게 공개함으로써 이용자와의 신뢰감 형성에 주력하고 있으며, 가상공간상의 이용자 프라이버시 보호의 적절성을 나타내는 마크부여제도 등을 도입함으로써 법적 규제와는 별도로 사전적 보호방식을 취하고 있다. 정부가 추진중인 정보통신망이용촉진법상의 개인정보보호 규정의 구체적 준수사항 및 이용자 권익 보호 등을 내용으로 하는 개인정보보호지침은 개인정보취급업자들의 자율규제를 위한 가이드라인으로 활용할 수 있을 것이다.

2. 개인정보취급방침의 게시

인터넷에서 개인정보를 수집할 때 서비스제공자(국가, 공공기관, 쇼핑몰, 병원, 인터넷 정보제공자 등)가 수집목적, 이용범위 등의 개인정보관리방침 등을 충분히 설명하고 이용자에게 본인 정보에 대한 통제권(열람·정정·삭제 등)을 부여한다면, 해당 웹사이트에 대한 신뢰도가 높아질 것이며 바람직한 정보의 제공 및 이용 환경이 조성될 것이다. 하지만 이 조사에서 알 수 있듯이 대부분의 웹사이트에서는 이러한 기본적인 고지의무조차도 이루어지지 않고 있는 실정이다. 인터넷 이용의 확산과 관련하여 이러한 기본적인 고지의무의 시행 여부가 인터넷 개인정보 보호의 첫걸음이 될 것이다. 모든 인터넷 홈페이지에 개인정보의 취급정책을 설명하는 게시문을 게시하는 운동을 시작하여야 할 것으로 보인다. 또한 각 사업자들은 자신 회사의 개인정보관리방침을 조속히 수립하여 인터넷 홈페이지에 게시함으로써 이용자들로 하여금 개인정보 유출과 프라이버시 침해에 대한 우려를 일소할 수 있도록 조치를 취하여야 할 것이다.

3. 개인정보침해분쟁 조정(調停)기구의 설립

대부분의 전문가들은 복잡하고 고도화된 정보화 사회에서 전자거래 당사자간의 분쟁은 발생빈도가

더욱 높아질 것으로 전망하고 있다. 이러한 경우 피해자가 직접 법적인 절차를 밟아 문제를 해결하기 위해서는 많은 시간과 비용을 부담해야만 할 것이다. 하지만 복잡한 절차를 거치지 않고 당사자가 서로 동의할 수 있는 독립기관의 조정노력에 의해 이를 해결한다면 신속하고 효과적인 처리가 가능할 것이다. 즉, 당사자만 합의하면 소송에 비해 신속하고 비용도 들지 않는 유용한 제도인 것이다. 따라서 사전에 정보관리자와 정보주체가 동의한 계약을 토대로 제정된 공식적인 규정을 가지고 활동할 독립적인 피해보상 조정기구의 설립이 요망된다.

4. 개인정보보호를 위한 감독기구의 설치

개인정보보호의 오랜 역사를 지닌 유럽 각국이 얻은 결론은 개인정보보호의 성패는 효율적 감독기관에 달려 있다는 것이다. 감독기관은 상대적으로 열세에 있는 정보주체의 권리를 보호하기 위한 책임을 지며, 감시기능을 통해 분쟁의 소지를 사전에 제거할 수 있다. 사업자 및 이용자를 대상으로 한 개인정보 보호 홍보 및 교육을 실시하며 개인정보보호에 관한 인터넷 홈페이지를 작성하여 기술적·관리적 정보를 제공함과 아울러 개인정보침해 신고 창구로 운영한다. 정부는 금년 중에 한국정보보호센터에 가칭 '개인정보침해 신고 및 상담센터'를 개설하여 운영할 예정이다.

5. 모든 일반인을 규율하는 "개인정보보호법"의 제정 여부

민간부문을 규율하는 현행 개인정보보호법제는 '전기통신사업자', '정보통신서비스제공자' 및 '신용정보제공·이용자' 등 적용대상이 사업자중심이다. 따라서 일반인이 타인의 개인정보를 수집하거나 제3자에게 제공하는 경우에는 실질적으로 규율하기는 어렵다. 예를 들어 일반개인 또는 법인이나 단체가 임

의로 개인정보를 수집하여, 제3자에게 제공하는 경우에는 마땅한 처벌법규가 없게 된다. 물론 이를 이용하여 불법적인 용도에 사용되는 경우에는 해당 적용법규가 있는 경우는 다른 문제이다. 결국 현행 개인정보보호법제의 사각지대에서 부당히 침해받고 있는 개인의 정보를 적절하게 보호하기 위하여 모든 일반인을 규율하는 가칭 "개인정보보호법"의 제정여부가 더욱 설득력을 얻게 된다.

※ 참고문헌

- [1] FTC, "Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress" 1999.7
- [2] FTC, "Online Privacy: A Report to Congress" 1998. 6.
- [3] John D. Zelezny, 『COMUNICATIONS LAW』, Wadsworth Publishing Company, 1997.
- [4] National Research Council, "Fostering Research on the Economic and Social Impacts of Information Technology", 1998, National Academy Press.
- [5] 김희은, 『온라인상의 프라이버시 보호에 관한 연구』, (부산대학교 대학원 석사학위논문), 2000. 2.
- [6] 남수정, 김기욱, "소비자의 개인정보보호에 관한 연구"(1998 정보보호우수논문집), 한국정보보호센터, 1998. 12.
- [7] 정보통신정책연구원, 『전산망보급확장과이용 촉진등에관한법률 개정연구만 운영보고서』, 1998.
- [8] 정찬모, "개인정보보호에 관한 국제적 입법동향 및 우리의 대응", 정보통신정책연구원, 1997.

12.

- [9] 주덕규, 『한국의 정보보호법제에 관한 연구』 (송실대학교 대학원 박사학위논문), 1999. 2.
- [10] 하종현, “개인정보보호 제도의 딜레마와 효과적인 도입방안”(1999 정보보호우수논문집), 한국정보보호센터, 1999. 12.
- [11] 한국정보보호센터, 『정보통신망에서의 개인정보 침해사례 분석 및 이용규제방안 연구』, 1998.
- [12] 한국정보보호센터, 『주요국가의 개인정보보호기관 운영상황 연구』, 1998.
- [13] 한국정보보호센터, 『정보통신서비스에서의 개인정보보호에 관한 지침(안) 연구』, 1999.



주 덕 규

1990년 송실대학교 대학원 법학과(법학석사)
 1999년 송실대학교 대학원 법학과(법학박사)
 1996년~현재 송실대학교 법대 강사
 1997년~현재 한국정보보호센터 개발부 선임연구원
 주 관심분야 : 정보보호법제도, 정보보호정책



박 광 진

1982년 동국대학교 전자계산학과(경영학사)
 1988년 한양대학교 대학원 전자계산학과(공학석사)
 1998년~현재 광운대학교 대학원 전자계산학과 박사
 피점
 1983년~1988년 한국전기통신공사
 1988년~1996년 통신개발연구원 책임연구원
 1995년~1996년 정통부 초고속기획단 파견
 1996년~현재 한국정보보호센터 정보화역기능대응팀장
 주 관심분야 : 정보보호정책, 네트워크 보안