

교회 홈페이지에서 개인정보 보호에 관한 연구

김종민 (고신대학교 인터넷비즈니스학과 교수)

I. 서론

일반적으로 개인정보란 개인의 이름, 주소, 전화번호, 나이, 성별, 주민등록번호와 같이 개인을 식별할 수 있는 개인에 대한 일반적인 정보를 말하는데, 이외에도 다른 정보들과 결합되어 특정 개인을 구별하고 그 사람의 신체적, 정신적, 사회적 상태를 판단하거나 사실 확인이 가능한 정보도 개인정보에 포함된다[1].

이러한 개인정보는 홈페이지를 통해 쉽게 노출되기도 하는데, 개인정보 노출이란 일반 인터넷 이용자가 해킹 등 특별한 방법을 이용하지 않고 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 인터넷에 방치되어 있는 것을 말한다[2]. 이와 같이 개인정보가 홈페이지에서 노출되는 이유는 홈페이지 관리자, 개발자, 사용자가 개인정보 보호에 대한 인식이 부족한 것에서 출발한다고 볼 수 있다. 개인정보는 정보화 시대에서 매우 중요한 자산이며 우리가 관심을 가지고 보호해야 할 중요한 대상이라고 할 수 있다. 홈페이지에서 개인정보가 보호되지 못하고 노출되어 악용될 경우 2차, 3차 피해가 발생하게 되므로 홈페이지에서의 개인정보 보호에 대한 관심을 가져야 할 것이다. 홈페이지에서 개인정보가 보호되기 위해서는 개인정보가 수집과 활용, 폐기 등의 과정에서의 동의와 함께 지침에 따른 엄격한 관리가 필요하며, 개인정보가 외부로 노출되지 않도록 보안기술을 적용해야 하고 관리자나 사용자의 부주의로 개인정보가 홈페이지에서 공개되지 않도록 지속적으로 관심을 갖고 관리하여야 한다.

본 연구에서는 교회홈페이지를 대상으로 개인정보 보호 상태에 대해 점검하였다. 교회별 개인정보 보호 실태를 평가하기 위해서 10개의 항목으로 구성된 평가 항목을 정의하였으며, 평가 항목에 따라 각 홈페이지를 평가하고 분석하여 교회 홈페이지 운영에서의 문제점을 파악하였으며 향후 대응방안을 제시하였다.

II. 교회 홈페이지에 대한 개인정보 보호 실태 평가

1. 평가 대상과 방법

본 연구에서는 교회 홈페이지에 대한 개인정보 보호 상태를 점검하기 위해 20개 교회의 홈페이지를 평가 대상으로 선정하였다. 이때 평가 대상은 그룹 A와 그룹 B로 나누었는데, 그룹 A는 규모가 큰 교회이고 그룹 B는 규모가 작은 교회이며, 각 그룹별 10개씩 교회 홈페이지를 평가 대상으로 선정하였다.

평가 항목은 개인정보를 획득하고 활용, 처리 절차에 대한 부문, 정보 보안과 관련된 부문 그리고 홈페이지 관리 부문으로 크게 나누었으며, 해당 부문별 평가 항목을 <표 1>에서와 같이 총 10개의 평가 항목으로 정의하였다. 평가를 위해서 해당 평가 항목의 준수여부를 조사한 후, 준수할 경우 1점을 할당하는 방식으로 한 개의 교회 홈페이지에 대해 총 10점 만점으로 채점하였다.

<표 1> 평가 항목 목록

구분	평가 항목
개인정보의 획득과 처리 방침	① 개인정보 수집, 이용, 목적을 제시하고 동의획득 절차가 있는가?
	② 개인정보 제3자제공시 제공 받는 자, 제공이용목적, 제공 항목, 보유 및 이용 기간 등을 제시하고 동의획득절차가 있는가?
	③ 개인정보 파기에 관한 절차가 명시되어 있는가?
	④ 주민등록번호나 민감 정보를 수집하는가?
정보 보안	⑤ 보안프로토콜을 적용하고 있는가?
	⑥ 로그인시 비밀번호의 체계가 보안수준에 적합한가?
	⑦ 홈페이지 회원 가입 시 주민등록번호 대체 수단이 있는가?
홈페이지 관리	⑧ 게시글에 개인정보를 포함하는가?
	⑨ 외부 검색엔진을 통해 개인정보가 노출되는가?
	⑩ 사용자들에게 개인정보 관련 유의사항 안내문이 있는가?

2. 평가 항목별 세부내용

본 연구에서 정의한 각 항목별 평가 내용과 방법에 대해 살펴보면 다음과 같다.

- ① 개인정보 수집과 관련하여 정확한 동의절차가 있는가에 대해 평가한다.
- ② 수집된 개인정보를 다른 사람에게 제공할 경우, 목적과 제공되는 개인정보 항목, 그리고 이용기간에 대해 명시하고 동의를 받고 있는지에 대해 평가한다.
- ③ 개인정보를 파기할 경우, 파기 절차에 대해 명시하고 있는지에 대해 평가한다.
- ④ 개인정보 획득 시 주민등록번호 등과 같은 민감한 개인정보를 수집하고 있는지에 대해 평가한다.
- ⑤ 홈페이지에서 민감한 개인정보(아이디, 비밀번호, 회원 가입 시 전송하는 개인 정보 등)가 전송되는 경우, 보안 프로토콜을 적용하여 처리하고 있는지에 대해 평가한다. 본 연구에서는 보안프로토콜의 적용여부를 판단하기 위해 로그인, 회원 가입 과정에 대해 평가하였다.
- ⑥ 비밀번호를 설정할 경우, 안전한 비밀번호 설정 원칙[3]을 고려하였는지 평가한다.
- ⑦ 홈페이지 가입 시 주민등록번호를 대체할 수 있는 다른 개인인증 방법이 있는지에 대해 평가한다. I-PIN 혹은 공인인증서, 기타 다른 대체 인증 방법의 제공여부에 대해 판단한다. 주민등록번호를 수입, 이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(대체수단)을 제공하여야 한다[5].
- ⑧ 홈페이지에서 게시된 글에 개인정보가 포함되어 있는지를 조사하여 평가한다.
- ⑨ 홈페이지에서 사용자들이 글이나 자료를 게시할 경우 개인정보 노출에 대해 유의할 수 있

도록 적절한 안내문을 홈페이지에 공지하고 있는지의 여부에 대해 평가한다.

- ⑩ 구글 검색엔진을 이용하여 교회 홈페이지에서 특정 확장자를 가진 파일(.pdf, .xls, .doc, .hwp 등)을 검색한 후, 검색된 파일에서 개인정보가 존재하는지를 조사한다. 홈페이지 개인정보 노출방지 가이드라인을 보면 이러한 첨부 파일에서 개인정보 노출이 빈번한 것을 알 수 있다[2, 4].

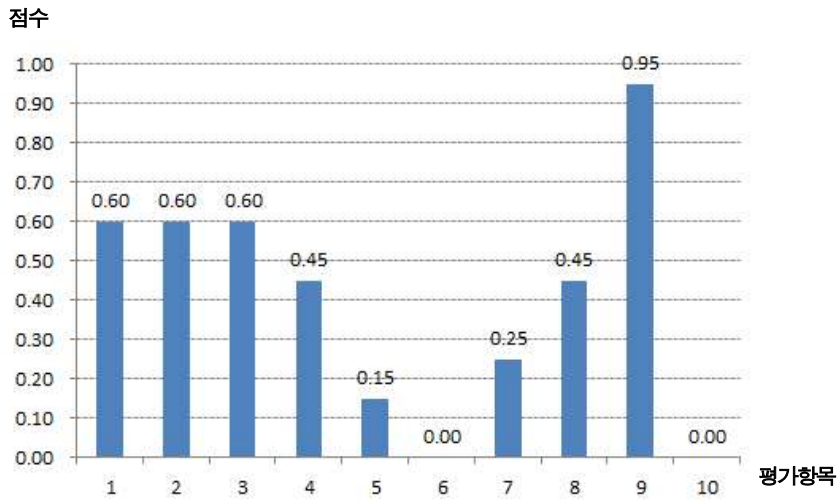
3. 평가 결과 분석

10개의 평가 항목에 대한 각 그룹별 평가 결과(평균값)를 살펴보면 [그림 1]에서와 같이 그룹 A(규모가 큰 교회)에 속한 교회 홈페이지의 경우 4.8점, 그룹 B(규모가 작은 교회)의 경우 3.3점을 나타냈으며, 전체 교회에 대한 평가 결과는 4.1점으로 낮게 나타났다. 그룹 A의 경우 그룹 B에 비해 평가 결과가 상대적으로는 높았지만 두 그룹 모두 개인정보 보호에 있어서는 아직 미흡한 것으로 평가되었다.



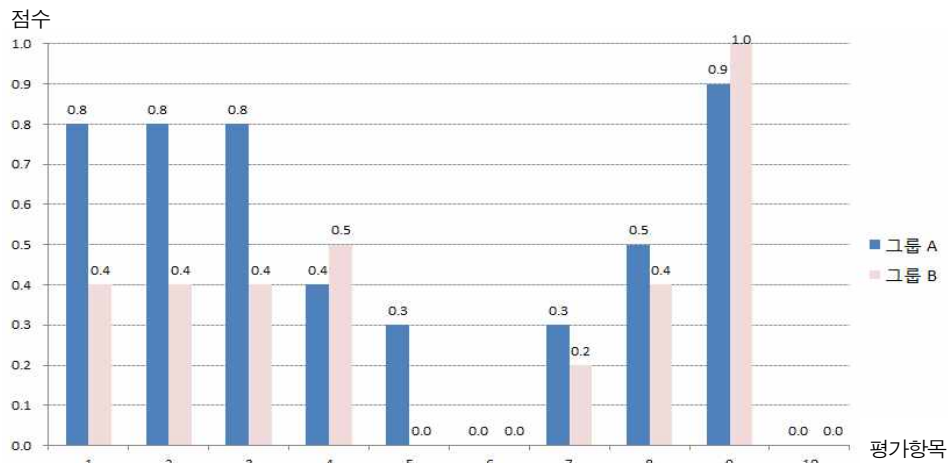
[그림 1]. 그룹별 평가 결과

전체 20개 교회에 대한 각 평가 항목별 결과를 [그림 2]에 나타내었는데, 정보 보안과 관련된 부분(평가 항목 5번~7번)의 경우가 다른 항목에 비해 상대적으로 매우 낮은 값을 나타내는 것을 알 수 있다. 이것은 대부분의 교회 홈페이지에서 정보 전송 보안이나 비밀번호 체계 등에 대해 관심을 갖고 있지 못한 결과이며, 개선이 필요한 부분이다. 개인정보 노출과 안전한 관리를 위한 안내문을 공지하고 있는 교회 홈페이지는 한 곳도 없는 것으로 조사되어 관리자의 관심과 개선이 요구된다.



[그림 2]. 전체 교회에 대한 항목별 평가 결과

그룹별 평가 결과를 평가 항목별로 비교하기 위해 평가 항목별 그룹 점수를 비교하여 [그림 3]에 나타내었는데, 개인정보의 획득과 처리 방침과 관련된 문항(문항 1번 ~ 문항 4번)에 있어서는 그룹 A의 결과가 그룹 B에 비해 상대적으로 우수하였다. 정보 보안과 관련된 문항에 대해서는 두 그룹 모두 취약한 것으로 나타났으며, 그룹 B의 경우 그룹 A보다 더 낮게 평가되었다. 이 부분의 평가 항목에 대해서는 모든 교회 홈페이지가 시급히 개선해야 할 것으로 보인다. 이러한 이유는 대부분의 교회의 경우, 홈페이지 제작에 대한 투자 환경이 상대적으로 열악하고 개발 단계에서 개인정보 보안에 대한 의식이 부족했기 때문으로 판단된다. 한편 정보보안과 개인정보 보호를 위한 홈페이지 안내와 관련된 문항에 대해서는 안내하는 홈페이지가 없는 것으로 조사되어 홈페이지 관리자가 개인정보 보호에 대해 관심을 가질 필요가 있는 것으로 판단된다.



[그림 3]. 평가 항목별 그룹 점수 비교 결과

교회 홈페이지에서 개인정보보호 실태에 조사하고 분석하는 과정을 통해 각 교회에서 다음과

같은 사항에 대해 관심을 가지고 문제점을 개선해야 할 것으로 보인다.

(1) 개인정보를 획득, 사용, 제공하는데 있어서 개인의 동의를 받는 절차를 강화할 필요가 있다. 특히 소규모 교회의 경우, 이러한 동의절차를 무시하는 경우가 많아 시급한 개선이 필요하다고 판단된다. 홈페이지를 운영하고 관리하는 담당자는 가입단계에서 반드시 동의를 받는 절차를 삽입하여 운영할 수 있도록 절차를 개선해야 할 것이다.

(2) 중요한 개인정보(아이디, 패스워드 등) 전송 할 때 반드시 보안 프로토콜을 사용하여 전송하도록 개발되어야 한다. 많은 교회들이 이 부분에 대해 소홀하고 있는 것으로 조사되었으며 보안 프로토콜을 사용하도록 홈페이지 개발 단계에서 요구하여야 한다.

(3) 대부분의 교회에서는 로그인시 사용하는 비밀번호의 경우, 자체의 규칙에 의해 비밀번호를 결정하도록 하고 있다. 그런데 안전한 비밀번호 설정원칙을 보면 정보주체에 대한 비밀번호의 경우 문자 조합의 경우에 따라 최소 10자리 이상 혹은 8자리 이상으로 규정하고 있다. 이와 같이 비밀번호를 결정할 경우, 안전한 보호가 가능하지만 대부분의 경우 복잡한 비밀번호체계를 꺼리는 관계로 이러한 규칙을 적용하는 교회는 하나도 없었다. 비록 복잡하고 관리에 불편함이 있다고 할지라도 정보주체의 개인정보를 효과적으로 보호하기 위해서는 안전한 비밀번호 설정원칙에 따라 사용자가 비밀번호를 결정하도록 개선해야 한다.

(4) 회원가입 시 주민등록번호를 대신하여 본인 인증을 할 수 있는 대체수단을 가입과정에서 제공하도록 개선해야 한다. 아직도 많은 교회들이 주민등록번호만을 이용하여 본인 확인을 하는 수단으로 사용하고 있는데 이 부분에 대한 개선이 필요하다.

(5) 대부분의 교회에서는 다양한 용도의 게시판을 운영하고 있는데, 이 게시판을 통해 개인정보가 유출될 가능성이 존재하게 된다. 관리자는 사용자들이 교회 홈페이지 이용할 때 개인정보를 업로드 하지 않도록 안내문을 공지를 해야 하며, 사용자는 게시판에 본인 혹은 타인의 개인정보를 올리지 않도록 조심하여야 한다.

III. 결론

정보화시대에 있어서 개인정보는 개인이 보유하고 있는 재산이며 침해당하지 않고 보호받아야 할 대상이다. 홈페이지에서 개인정보는 관리자에 의해, 개발자에 의해, 사용자에게 의해 노출될 수 있으며 이렇게 노출된 개인정보는 다른 범죄에 활용될 수 있어 철저한 관리가 필요하다.

본 연구에서는 20개 교회를 대상으로 10개 항목에 대해 교회 홈페이지에서 개인정보 보호 실태에 대해 평가하였다. 평가 결과 규모가 큰 교회의 경우는 홈페이지 관리에 대한 관심이 비교적 높고 운영 환경도 잘 갖추어져 있어 소규모 교회보다 높은 점수를 받았지만 평가 결과를 볼 때는 개선이 필요하다고 판단된다. 소규모 교회의 경우는 규모가 큰 교회보다 전반적으로 더 낮은 점수를 받아 홈페이지에서의 개인정보 보호에 대해 더 많은 관심을 가져야 할 것으로 보인다. 특히 정보 보안과 관련된 평가 항목에 대해서는 거의 모든 교회 홈페이지가 매우 낮은 점수로 평가되어 시급한 개선이 필요하였다.

홈페이지에서 개인정보의 노출을 막고 효과적으로 보호하기 위해서는 개발자와 관리자가 홈페이지를 설계하고 운영할 때 개인정보 보호와 관련된 원칙들을 잘 준수해야 하며, 관리자와 사

용자의 매우 사소한 부주의로 인해 개인정보가 노출될 수 있기 때문에 개인정보 보호의 중요성에 대한 인식 개선이 필요하다.

참고문헌

- 인터넷윤리실천협의회 (2011). 『인터넷 윤리』. 이한출판사.
행정안전부 개인정보보호과 (2012). “홈페이지 개인정보 노출방지 가이드라인,” 행정안전부.
<http://seed.kisa.or.kr/kor/safepwd/safepwdA.jsp>, 패스워드 선택 및 이용 가이드. (검색일 2012. 10. 15)
행정안전부 (2009). “웹사이트 개인정보노출 방지대책”, 행정안전부.
방송통신위원회, 한국인터넷진흥원 (2012). “개인정보보호 신규제도 안내서”, 방송통신위원회, 한국인터넷진흥원.