情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

개인정보보호기술의 최신 동향과 향후 전망

남 기 효*, 박 상 중**, 강 형 석**, 남 기 환**, 김 성 인***

요 약

최근 우리나라는 개인정보 침해사고 및 프라이버시 침해를 통한 여러 가지 사회문제가 급속도로 증가하고 있으며, 이에 따라 개인정보보호를 위한 다양한 연구 및 기술개발이 이루어지고 있다. 본 논문에서는 국내외에서 다양한 방향으로 연구가 진행되고 있는 개인정보보호기술에 대해 새로운 분류방법을 제시하고, 이를 바탕으로 최신의 동향과 향후 전망에 대해 기술한다.

Ⅰ. 서 론

최근 우리 사회는 타인의 명의도용, 보이스 피싱 등 "개인정보 침해사고"가 끊임없이 발생하면서 개인정보 침해가 심각한 사회문제로 대두되고 있다. 뿐만 아니라 개인정보 침해사고는 인터넷을 통한 악성 댓글 등과 같이 개인의 프라이버시를 침해하고, 개인에게 각종 정신적의 피해를 입히는 등의 "프라이버시 침해사고"로 확대되고 있다.

개인정보 침해사고 및 프라이버시 침해사고는 다른 일반 정보보호 침해사고와는 다르게 개인에게 직접적으로 경제적, 정신적 피해를 주는 것이 특징인데, 이러한 사고를 발생시키는 기술적 측면의 원인으로는 외부의 불법적인 접근을 통한 개인정보 유출, 내부자의 부주의 또는 의도에 의한 개인정보 유출, 웹사이트 등을 통한 개인정보 노출 등 3가지로 요약할 수 있다.

금년에 발생한 H 통신사의 고객정보 600만건 유출, A 사이트 1,081만 가입자 정보 유출, G 정유사 1,125만 회원정보 유출 등과 같이 최근에도 심각한 개인정보 유출사고가 빈번하게 발생하고 있으며, 웹사이트를 통한 개인정보의 노출은 매년 수십만에서 수만 건에 이르는 사례가 지속적으로 확인되고 있다. 특히 한국정보보호진흥원(KISA)의 개인정보 침해 접수건수도 2006년 18,206건에서 2006년 23,333건, 2007년 25,956건 등으로 매년 증가하고 있다[1].

최근 이러한 국내 환경의 특성에 따라 개인정보보호에 대한 다양한 요구가 끊임없이 발생하고 있으며, 이에 부응하여 개인정보보호를 위한 다양한 연구 및 기술개발이 수행되면서 국내 개인정보보호기술도 급속히 발전하고 있다.

본 논문에서는 최근 국내에서 진행되고 있는 다양한 연구들을 포함한 개인정보보호기술에 대해 새롭게 분류한 기준을 제시하고, 이를 바탕으로 국내 개인정보보호기술의 동향과 향후 전망을 기술한다.

Ⅱ. 개인정보보호기술의 분류

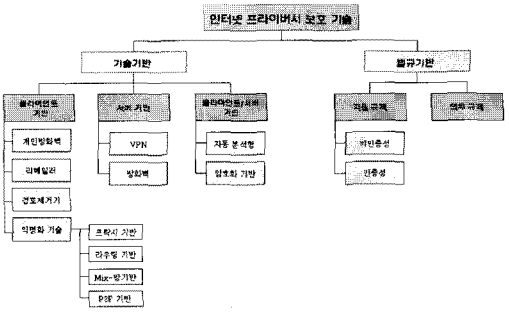
앞에서 설명한 바와 같이 개인정보 침해사고는 외부의 불법적인 접근, 내부자의 부주의 또는 의도적인 유출, 웹사이트를 통한 개인정보 노출 등의 3가지 원인으로 개인정보가 외부에 유출 또는 노출되어 발생한다.

따라서 개인정보보호는 보호하고자 하는 자산이 개인정보라고 하는 측면에서 생각하면 정보보호와 밀접한 관계를 가지고 있다. 하지만 개인정보는 정보주체가 생존하는 동안 지속적으로 유효성을 가질 수 있다는 점에서 중요하며, 각 국가별 법률과 제도에 따라서도 보호를 강제화할 수 있는 개인정보의 범위가 다르므로 법률, 제도, 정책 등과 밀접한 관계를 갖고 있다는 것이 일반 정

* (주)위너다임 이사(nkh@wdigm.co.kr)
** 고려대학교 정보경영공학전문대학원({happylife},{hyungsuk1},{namkh}@korea.ac.kr)
*** 고려대학교 정보경영공학부 교수(tennis@korea.ac.kr)

보보호와 다른 점이다.

개인정보보호기술은 이와 같이 정보보호의 측면과 정책적인 측면을 모두 고려해야 하며, 또한 현재 다양한 방향으로 지속적인 연구가 이루어지고 있어서 이를 정확히 분류하는 것은 매우 어려운 일이다. 하지만 개인정보보호기술을 보다 체계적이고 구조적으로 이해하기 위해 현재의 기술을 포함하여 전체적인 기술을 분류하는 것은 의미 있는 일이다. Abedelmounaam[7]은 2003년에 이미 인터넷 프라이버시 보호기술을 [그림 1]과 같이 분류한 바 있다.



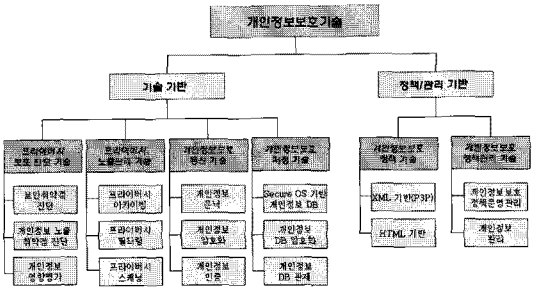
〔그림 1〕 인터넷 프라이버시 보호기술 분류[7]

[그림 1]의 분류 기준은 기존 정보보호기술 중 개인정보보호를 위해 적용되는 일부 기술과 웹 정보보호기술, 법규 기반의 규제항목 들을 포함한 것으로 최근 국내에서 다양하게 연구되고 있는 기술 중 다수의 기술이 포함되지 않아 이 분류기준을 따르기에는 많은 문제점이 있다.

따라서 본 논문에서는 최근 국내에서 활발한 연구 및 기술개발이 진행되고 있는 여러 분야의 개인정보보호기술을 중심으로 새롭게 개인정보보호기술을 분류한다.

[그림 2]는 현재 국내외적으로 다양한 연구가 진행되고 있는 개인정보보호기술을 중심으로 새롭게 개인정보보호기술을 분류한 것이다. 이 논문에서는 [그림 2]에서 알 수 있는 바와 같이 개인정보보호기술을 각 기술이 갖는 중요한 측면에 따라 크게 기술기반과 정책 및 관리 기반으로 분류하였다. 그리고 각 기반별로 는 중요한 프로세스에 따라 1차 분류하여 부분기술을 지정하였다. 또한 각 부분기술별로는 기술이 달성하게 되는 주요기능을 중심으로 세부 기술을 분류하였다.

이 그림에서 프라이버시보호 진단기술은 보안취약점에 의한 개인정보 노출 및 유출 위험, 웹페이지 설계 오류를 통한 소스코드 등에 나타나는 개인정보의 노출 위험,



〔그림 2〕 프라이버시 보호기술 분류

기관 또는 시스템의 전체적인 개인정보 유출 위험 등을 진단하는 기술을 의미한다. 그리고 프라이버시 노출관리 기술은 외부 송신 또는 웹 서비스 등록 시 개인정보 또는 프라이버시 침해정보 노출을 방지하기 위해 전체 정보를 저장하거나 사전차단, 사후 점검하는 기술을 모두 포함하며, 프라이버시 보호를 위한 스팸 필터링 기술도 여기에 포함된다. 또한 개인정보보호 통신기술은 안전한 개인정보 유통을 위해 적용되는 SSL, 응용보안 등과 같은 보안기술에서부터 안전기관으로부터 인증된 가상주민번호를 이용하여 서비스를 이용하는 i-PIN 기술도 포함된다. 개인정보보호 저장기술은 안전한 개인정보 저장을 위해 적용되는 데이터베이스 보안을 위한 다양한 기술을 의미하며, 개인정보보호정책기술은 최근 우리나라에서도 국내 표준화를 수행한 P3P(Platform for Privacy Preferences Project) 등과 같이 정책에 기반을 두고 있는 기술을, 개인정보보호 정책관리기술은 사전에 정한 개인정보보호 정책에 따라 개인정보가 운영/관리되고 있는지, 저장매체, 출력물을 통해 개인정보가 유출되지 않는지 등을 관리하는 기술을 의미한다.

다음 Ⅲ장에서는 [그림 2]에서 명시한 기술 중에서 최근 국내에서 활발히 연구 및 기술개발이 이루어지고 있는 주요 기술들에 대해서 설명한다.

Ⅲ. 국내 개인정보보호기술 동향

국내에서는 최근 개인정보보호에 대한 많은 연구가 다양한 방향으로 이루어지고 있으며, 그 중 많은 연구결과는 상용화 수준에까지 이르는 등 급속한 발전을 거듭하고 있다. 이 논문에서는 개인정보보호기술의 최근연구 및 기술개발 결과들의 기술현황과 문제점을 앞의 [그림 2]에서 제시한 기술 분류에 따라 설명한다.

〔표 1〕 프라이버시 노출관리 세부기술 비교

세부기술	특징
프라이버시 아카이빙 기술	In-bound 또는 Out-bound를 통해 유출입되는 데이터 중 특정 영역 또는 프라이버시 정후의 정보만을 저장하여, 추후 검색하는 기술
프라이버시 필터링 기술	In-bound 또는 Out-bound를 통해 유출입되는 데이터 중 개인정보 또는 프라이버시 침해정보 패턴을 검사하여 유출입을 차단하는 기술
프라이버시 스캐닝 기술	특정 시스템에 대해서 개인정보 또는 프라이버시 침해정보 포함여부를 검사하고 관리하는 기술

1. 프라이버시 보호진단기술

프라이버시보호 진단기술은 보안취약점에 의한 개인정보 노출 및 유출 위험, 웹페이지 설계 오류를 통한 소스코드 등에 나타나는 개인정보의 노출 위험, 기관 또는 시스템의 전체적인 개인정보 유출 위험 등을 진단하는 기술을 의미하며, 최근 개인정보보호가 모든 기관 및 시스템에 필수적으로 요구되는 사항으로 부각함에 따라 그 필요성이 커지고 있다.

1.1 보안취약점 진단기술

보안취약점 진단기술은 일반 정보보호분야에서 이용되는 다양한 보안취약점 진단기술을 의미한다. 통신망 및 시스템 운영환경 변동에 따라 보안취약점도 지속적으로 증가하고 있으며, 이렇게 변화하는 보안취약점 진단기술은 개인정보보호를 위한 보안취약점 진단기술에 그대로 적용할 수 있다.

1.2 개인정보 노출취약점 진단기술

개인정보 노출취약점 진단기술은 설계 또는 운영단계에서 발생할 수 있는 개인정보 노출 취약점을 진단하는 기술을 의미한다. 이 기술 중 일부 기술은 일반 정보보호분야에 속하는 기술과 동일하지만, 다른 일부 기술은 일반 정보보호와는 상관없이 최근의 개인정보보호에 대한 요구에 따라 나타나게 되었다. 개인정보 노출취약점 진단기술의 대표적인 기술로는 일반 정보보호 분야에서 최근 이슈가 되고 있는 악성코드 탐지기술, 피싱/파밍 사이트 탐지기술 등을 들 수 있으며, 정보보호 분야에 속하지 않은 기술로는 웹사이트 운영단계에서 공개된 소스코드를 통한 개인정보 노출 취약점 진단기술을 들 수 있다. 특히 소스코드를 통한 개인정보 노출 취약점 진단기술은 2006년 행정안전부가 실시한 공공기관 웹사이트 개인정보 노출진단연구결과에서 보고된 후, 근래 신규 웹사이트 구축 시 필수적으로 진단하는 항목이 되고 있다[6].

1.3 개인정보 영향평가기술

개인정보 영향평가기술은 새로 구축되는 정보시스템이나 현재 운영 중인 시스템에 대해서 시스템 운영이 프라이버시에 미칠 영향을 조사, 예측, 검토하여 침해위험을 평가하는 기술을 의미한다. 이 기술은 1989년 데이빗 플래허티(David Flaherty)의 '감시사회에서의 프라이버시 보호(Protecting Privacy in Surveillance Societies)'란 저서에 처음으로 그 개념이 제시되었으며, 그 이후 1991년 미국 뉴욕 주 "공공서비스 위원회의 통신상의 프라이버시에 대한 정책(Statementof Policy on Privacy in Telecommunication)"과 같은 개인정보 영향평가를 위한 공식 가이드라인이 제시되면서 본격적으로 다양한 평가기술이 개발되고 있다. 국내에서는 한국정보보호진흥원(KISA)이 2005년부터 개인정보영향평가제도(PIA: Privacy Impact Assessment)를 운영하면서 정보보호컨설팅기관을 중심으로 다양한 평가기술에 대해 활발한 연구가 진행되고 있다[1].

2. 프라이버시 노출관리 기술

프라이버시 노출관리 기술은 최근에 출현하여 매우 빠르게 연구와 기술개발이 이루어진 기술이다. 이 기술은 기존의 네트워크 운용기술이나 데이터 처리기술 등을 그 기반으로 하고 있으나, 국가의 개인정보보호 정책과 다양한 응용 프로그램 등 운영환경 등과 맞물려 각 상황에 적합한 다양한 형태로 기술이 개발되었으며 현재에도 지속적으로 발전하고 있다[4].

2.1 프라이버시 아카이빙 기술

외부에 유출 또는 시스템에 등록되는 프라이버시 정

보를 저장하고, 검색하는 기술을 의미한다. 이 기술은 정보유출 방지를 위한 아카이빙 기술을 적용하고 있으나, 현재의 아카이빙 기술은 저장된 정보 중 필요로 하는 특정 정보를 검색하는 데 걸리는 시간이 가장 큰 기술적 한계이므로, 이를 해결하기 위해 프라이버시 보호 정책에 따라 특정 범위 또는 패턴을 따르는 콘텐츠에 대해서만 아카이빙을 수행하도록 함으로써 개인정보 또는 프라이버시 침해정보에 대한 검색이 용이하도록 하는 아카이빙 기술이나 이에 따라 검색속도를 증가시키는 기술에 대해 지속적으로 연구가 이루어지고 있다.

2.2 프라이버시 필터링 기술

외부에 유출 또는 시스템에 등록되는 정보를 검사하여 특정 패턴에 대해 차단하는 기술을 의미한다. 일반적으로 정보유출 방지를 위한 필터링 기술을 적용하지만, 최근 기술은 기존의 키워드 검사에 따라 필터링을 하는 것이 아니라 프라이버시 보호와 운영 합리성을 위해 정책과 여러 조합별 규칙을 이용하여 필터링을 수행하는 기술이 개발되어 수행되고 있다[4]. 또한 이 기술에는 프라이버시 보호를 위한 스팸 필터링기술도 포함되는데, 스팸 필터링의 정확도를 향상시키기 위해 다양한 인공지능 기법을 적용한 연구가 최근까지 지속적으로 수행되고 있다[8].

프라이버시 필터링은 보다 상세하게는 개인정보 필터링기술, 프라이버시 침해정보 필터링기술, 스팸 필터링기술 등 3가지로 나눌 수 있으며, 이 세 가지 기술 중 개인정보 필터링기술과 프라이버시 침해정보 필터링기술은 특정 패턴을 비교하는 시그니처 기반의 기술만이 개발되어 있고, 스팸필터링기술은 시그니처, 휴리스틱, 블랙리스팅 등의 비학습 기반 필터링 기술에서 베이지언, KNN (K-Nearest Neighbor), SVM(Support Vector Machine), 신경망 등 다양한 학습 기반 알고리즘을 적용한 필터링 기술이 개발되고 현재도 지속적으로 연구되고 있다[8].

2.3 프라이버시 스캐닝 기술

현재 운영 중인 PC, 내부 시스템, 내외부 웹사이트 등에 포함된 개인정보 또는 프라이버시 침해정보를 검색하는 기술을 의미한다. 이 기술은 시스템 검색 및 웹사이트 검색 기술을 주로 활용하고 있으며, 특히 웹사이트를 대상으로 한 프라이버시 스캐닝 기술의 경우, 인터넷의 특성 상 이 웹사이트를 통해 노출된 개인정보가 포함된 웹페이지가 외부 웹사이트에 링크될 수 있으므로, 외부 링크를 검사하는 기술까지 포함된다. 또한 최근에는 스크립트 형 웹사이트와 같이 웹사이트마다 다르게 개발되어 스캐닝이 어려운 웹사이트에 대해서도 스캐닝을 수행하는 가상화 기술까지 개발이 진행되고 있다[4].

3. 개인정보보호 통신기술

최근에는 정보의 유통과정에서 개인정보가 유출되는 사고가 빈번하게 나타나고 있으며, 이에 따라 통신경로상의 개인정보보호를 위해서 안전한 개인정보통신을 위한 기술이 개발되고 있다.

3.1 개인정보 은닉 기술

통신 과정에서 개인의 익명성을 보장하는 익명화 기술 등은 다양한 형태로 개발되어 있으나, 현재 우리나라에서 활발한 기술개발이 이루어지고 있지는 않다.

3.2 개인정보 암호화 기술

현재 SSL 인증서 방식과 응용 프로그램 방식 등 다양한 형태로 개인정보 암호화 기술이 개발되어 있으며, 지속적으로 기술이 발전하고 있는 분야 중 하나이다. 특히 최근에는 무선 서비스를 위한 PKI 경량화기술 개발 등 국제경쟁력 측면에서 기술적 우위를 점하고 있어 앞으로도 지속적으로 발전이 예상되는 분야이다.

3.3 개인정보 인증 기술

개인정보 인증기술은 개인정보를 이용한 다양한 인증기술을 의미하는 것으로, 일반 인증기술에서 신용평가기관을 통한 본인확인인증 또는 성인인증, i-PIN 이나 G-PIN 등 대체인증, ID-연계(federation)기술 등을 모두 포함하는 기술을 의미한다.

최근에는 i-PIN 기술이 대표적인 개인정보 인증기술로 많은 형태로 개발되고 있다. i-PIN 기술은 2005년 7월 가이드라인 발표 이후, 현재에 이르기까지 많은 방법에 대한 기술 개발이 이루어지고 있으며, 한국정보보호진흥원을 중심으로 국제표준화가 추진되고 있다[1]. 또한

G-PIN에 사용되는 ID-연계(federation)기술은 ITU-T에서 ID 관리 국제표준화가 진행되고 있으며, 우리나라에서는 한국전자통신연구원(ETRI)에서 활발한 활동을 하고 있다.

4. 개인정보보호 저장기술

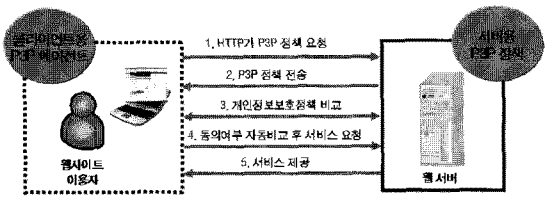
개인정보보호 저장기술은 일반적인 데이터베이스 보안기술을 기반으로 하고 있으며, 특히 최근에는 데이터베이스 전체에 대한 보호가 아닌 개인정보가 포함된 특정 필드에 대한 보호기술에 대한 연구가 활발히 추진되고 있다.

이 기술에 속한 세부 기술 중에서 Secure OS 기반의 개인정보 DB나 개인정보 DB 관제 기술은 일반 데이터베이스의 보안기술과 유사하여 개인정보보호를 위한 별도의 연구로 이루어지고 있지는 않으나, 개인정보 데이터베이스 암호화 기술은 일반 데이터베이스 암호화 기술과는 다르게 전체 데이터베이스 중 개인정보가 포함된 데이터베이스 일부를 암호화하는 개인정보보호기술의 관점에서 개인정보보호 저장기술 중 가장 활발히 연구가 수행되고 있다. 즉 최근에는 개인정보 데이터베이스의 암호화에 따른 인덱싱 및 검색방법에 대해 많은 연구가 수행되었으나, 보안성과 성능 측면에서 문제가 있으므로 이 분야는 앞으로도 많은 연구가 필요하다.

5. 개인정보보호 정책기술

우리나라는 개인정보를 수집하는 모든 웹사이트에 개인정보보호정책을 의무적으로 고지하도록 하는 등 HTML 기반의 개인정보보호정책기술은 오랫동안 일반화되어 왔다. 특히 HTML 기반의 개인정보보호정책은 국내 법적으로 각 웹사이트가 개인정보 처리에 관해 의무적으로 고지해야 하는 사항을 포함하고 있는데, 웹사이트 수가 기하급수적으로 증가하고 다양한 웹 서비스가 등장함에 따라 인터넷 이용자들이 각 웹사이트의 개인정보보호정책을 충분히 인지하지 못한 상태에서 자신의 개인정보를 제공함으로써 개인정보에 관한 많은 분쟁을 야기하게 되었다. 이는 HTML 기반의 개인정보보호정책이 일반 텍스트 형태로 구성되어 이용자가 허락할 수 있는 수준의 정책인지를 확인하기 위해서는 정책의 내용을 정확히 분석해야 하는데, 이는 실제로 인터넷 이용 환경에서 많은 불편을 초래하여 이용자가 간과하는 경우가 많기 때문이다. 뿐만 아니라 HTML 기반의 개인정보보호정책은 그 세부 내용에 대한 자동분석도 어려운 한계가 있다.

한편, 웹 분야의 국제 표준화기구인 W3C(World Wide Web Consortium)는 개인정보보호정책을 자동분석이 가능한 언어인 XML로 구현하는 개인정보보호정책 국제표준인 P3P 1.0을 표준을 2002년에 발표한 바 있으며, 2006년에는 각 국가별 법규를 "Extension"이라는 확장형 엘리먼트를 이용하여 규격에 반영할 수 있는 확장형 P3P 규격인 P3P1.1을 발표하였다. [그림 3]은 P3P의 운용 프로세스를 나타낸다[2].



〔그림 3〕 P3P의 운용 프로세스

우리나라는 HTML 기반의 개인정보보호정책기술의 문제를 극복하기 위해 정부 중심으로 XML 기반의 개인정보보호정책기술에 대한 연구를 시도하게 되었으며, 그 결과 P3P1.1 규격에 국내의 개인정보보호 관련 법률이 정한 개인정보보호정책 의무고지사항을 표현함으로써 자동분석이 가능한 개인정보보호정책을 구성할 수 있는 한국형 P3P 규격 수립을 추진하게 되었다. 이를 위해서 한국정보보호진흥원은 2005년 한국형 P3P 연구전담반을 구성하고 개인정보보호전문가를 중심으로 P3P 규격 분석 및 국내 법률에 대한 집중적인 연구를 수행하는 등 꾸준한 활동을 하였으며, 이에 따라 2007년에는 P3P 국내 표준 규격인 "개인정보보호정책 설정 및 협상 규격"을 수립하게 되었다[3]. 한편, P3P 국내 표준은 개정된 정보통신망법의 시행규칙 3조 3항에 "개인정보취급방침의 전자적 표시방법"으로 법제화되었으며, 개인정보보호정책이 자동분석이 가능한 언어로 구현됨에 따라 향후 다양한 방법으로 개인정보 관리 응용기술로 발전할 것으로 전망된다[1].

6. 개인정보보호 정책관리기술

개인정보보호 정책관리기술은 기술적인 측면보다는 관리적인 측면에 더 중심을 두고 있다. 현재 개인정보보호 정책관리기술은 각 기관 또는 기업이 운영하고 있는 개인정보보호정책에 따라 개인정보가 보호되고 있는지를 지속적으로 보장할 수 있는 방법 및 절차를 의미하며, 개인정보 관리기술은 각 기관 또는 기업에서 수집하여 저장 및 관리하는 개인정보를 안전하게 관리하기 위한 관리적 방법을 의미한다. 최근까지 이를 위한 다양한 방법이 연구되고 있으며, 아직까지는 기술적 측면보다는 관리적 측면에서 각 기술별 목적을 달성하기 위한 프로세스 또는 노하우의 개념에 머무르고 있다. 따라서 이 기술은 개인정보보호기술의 발전과 더불어 기술적인 측면에서 지속적으로 발전할 것으로 예상된다.

Ⅳ. 개인정보보호기술의 발전전망

현재 개인정보보호기술은 일반 정보보호기술의 발전, 유무선망 통합 · 웹2.0 등 서비스 운영환경 변화, 개인정보보호를 위한 국가정책의 강화 등의 요인으로 인하여 급속한 변화와 발전을 거듭하고 있다. 개인정보보호기술은 새롭게 출현하고 있는 다양한 보안 위협과 외부환경 등을 고려할 때, 가상화, 지능화, 경량화, 고성능화, 고기능화, 통합화 등 6가지의 방향으로 발전할 것으로 전망되며, 본 논문에서는 이 방향에 초점을 맞추어 향후 개인정보보호기술 발전 전망을 설명한다.

1. 프라이버시 보호진단기술(가상화 및 통합화)

프라이버시보호 진단기술은 시스템 설계단계 뿐 아니라 운영단계에서 새롭게 나타날 수 있는 보안 위협을 진단할 수 있는 상시 진단 또는 제어기술로 발전할 것으로 예상된다. 특히 보안 위협의 위험도를 진단하기 위해 시스템 내부에 안전하다고 확신하지 않는 모든 요소에 대해 가상화 기술로 프라이버시 침해 가능성을 분석하거나 안전하다고 확신하는 요소만을 허용하는 화이트리스팅 방법 등으로 기술이 발전할 것으로 전망된다. 그 중에서도 악성코드 및 피싱/파밍 사이트 진단 등의 문제를 해결하기 위한 기반기술로써 다양한 서비스 환경에서 가상 실행을 통해 프라이버시 침해 위험을 판단하는 가상화 기술이 지속적으로 발전할 것으로 예상된다. 또한 개인정보 영향평가는 새롭게 출현하는 프라이버시 침해 위협에 부응하여 대응책으로써 여러 요소가 통합된 평가기술이 지속적으로 개발될 것으로 예상된다.

특히 최근 인터넷의 구축기술은 다양한 형태로 발전하고 있으므로 웹사이트가 구축되는 다양한 환경 변화에 부응하여 개인정보 노출취약점 진단기술도 여러 가지 형태로 지능화될 것으로 예상된다.

2. 프라이버시 노출관리 기술(지능화, 가상화)

프라이버시 노출관리 기술은 프라이버시 보호기술 중 앞으로 가장 많은 발전이 전망되는 분야이다. 특히 이 기술은 최근 프라이버시 침해 뿐 아니라 기밀정보 유출사고와 맞물려 다양한 콘텐츠 보안기술로 발전할 것으로 예상된다.

2.1 프라이버시 아카이빙 기술

현재까지의 프라이버시 아카이빙 기술은 일반 아카이빙 기술과 프라이버시 정보 검색기술이 결합된 형태이며, 저장된 정보 중 프라이버시 침해 정보에 대한 검색 성능이 최대의 기술적 한계가 되고 있다. 따라서 향후 프라이버시 정보 검색 성능을 개선하기 위한 아카이빙 기술이 개발될 것으로 전망된다.

2.2 프라이버시 필터링 기술

현재의 프라이버시 필터링 중 개인정보 필터링기술은 특정 패턴을 갖는 정형화된 개인정보만을 필터링하는 시그니처 기반의 필터링기술이며, 향후 개인정보보호에 대한 정부의 강력한 정책에 따라 비정형화된 개인정보 필터링을 위한 목적으로 다양한 필터링 기술이 개발될 것으로 전망된다.

또한 프라이버시 침해정보 필터링기술은 최근 인터넷 상의 악성 댓글과 같은 사회문제로 인하여 더욱 강력한 기술발전이 요구되지만, 필터링은 서비스를 제약하는 요인이 많아서 프라이버시 침해 방지의 기능은 대부분 프라이버시 아카이빙 또는 프라이버시 스캐닝 등의 기술을 중심으로 이루어질 것으로 판단된다. 다만 서비스의 개인화 측면에서 프라이버시 필터링 기능을 수

행하는 애플릿기술 등 구현기술은 단기일에 출현할 것으로 예상된다.

마지막으로 스팸 필터링 기술은 현재까지 많은 학습기반 알고리즘이 개발되었지만, 그 결과들은 성능 측면에서 현실에 적용하기에는 많은 한계가 있기 때문에, 알고리즘 정확도를 유지하면서 분류 성능을 향상 시키기 위한 연구가 활발히 진행될 것으로 전망된다. 뿐만 아니라 최근에는 휴대폰을 통한 스팸이 문제가 되고 있으므로, 스팸 필터링 경량화기술에 대한 연구도 함께 진행될 것으로 전망된다.

2.3 프라이버시 스캐닝 기술

프라이버시 스캐닝기술은 최근의 웹사이트가 자바스크립트, AJAX 등 스크립트형 웹으로 변화하고 있으며, FLEX, Flash 등이 웹에 포함되면서 이를 통한 개인정보 및 프라이버시 침해정보의 노출위험이 꾸준히 증가하고 있다. 특히 웹2.0은 인터넷의 개방성을 가장 큰 화두로 하고 있기 때문에 하나의 웹사이트를 통한 개인정보 노출 또는 프라이버시 침해정보 노출 문제의 파급성은 현재보다 훨씬 더 커질 것으로 전망된다. 따라서 프라이버시 스캐닝 기술은 이와 같이 다양한 형태의 웹사이트 및 공유된 웹사이트에서 노출된 개인정보를 자동검사하기 위한 검색기술과 더불어 발전을 계속할 것으로 전망된다. 특히 스크립트형 웹의 효과적인 검색을 위해서 가상 브라우징 등의 가상화기술이 꾸준히 발전할 것으로 예상된다.

3. 개인정보보호 통신기술(경량화)

개인정보보호 통신기술은 최근 모바일 단말기 등을 통한 금융 서비스 이용이 확대되면서 한정된 단말기 자원 내에 다양한 보안기능을 구현하는 보안기능 경량화 기술이 발전할 것으로 전망된다. 특히 이러한 경량화 기술은 1차적으로는 임베디드 소프트웨어와 같이 경량화 구현기술로 실현될 것으로 보이며, 추후 모바일용 TPM (Trusted Platform Module) 등과 같이 하드웨어 형태로 발전할 것으로 전망된다.

4. 개인정보보호 저장기술(고성능화)

개인정보보호 저장기술은 개인정보가 포함된 데이터베이스의 부분 암호화 방법에 대한 기술개발이 현재 집중적으로 수행되고 있다. 이 기술은 개인정보의 암호화 저장 후 데이터베이스에 저장된 개인정보의 정상적인 이용을 위해 데이터베이스를 안전하고 효율적으로 인덱싱하는 기술로 기술적인 진입 장벽이 높으나 향후 지속적인 기술발전을 통해 효율적인 개인정보 데이터베이스 암호화 기술이 개발될 것으로 예상된다.

5. 개인정보보호 정책기술(고기능화)

현재의 개인정보보호 정책기술 중 XML 기반 개인정보보호 정책기술인 P3P는 현재까지 표준화가 지속적으로 진행되고 있으며, P3P1.1규격에서는 P3P의 미래 발전방향으로 다음 4가지를 제시하고 있다[2].

- 개인이 하나의 사이트에서 여러 개인정보보호정책 중 선호하는 개인정보보호 정책을 선택하는 메카니즘
- 방문자가 P3P 정책에 대한 동의를 명시하는 메카니즘
- 방문자와 웹사이트 사이의 정책 동의에 대한 부인방지 메카니즘
- 사용자 에이전트가 서비스를 위해서 개인정보를 전송하는 메카니즘

따라서 향후 개인정보보호 정책기술은 이 방향으로 발전할 것으로 전망된다.

6. 개인정보보호 정책관리기술(통합화)

현재의 개인정보보호 정책관리기술은 기술적인 측면보다는 정책적인 측면에 더 중심을 두고 있지만 앞으로는 기술적인 부분이 매우 강화될 것으로 전망된다. 이 기술은 향후 개인정보보호정책에 따라 개인정보의 관리가 수행되고 있음을 기술적으로 보장하는 통합기술로 발전할 것으로 전망된다.

V. 결 론

본 논문은 심각한 사회문제로 대두되고 있는 개인정보 침해사고를 방지하기 위한 노력으로 최근 많은 연구가 진행되고 있는 개인정보보호기술에 대한 최신 동향과 향후 전망을 살펴보았다. 앞에서 서술한 바와 같이

개인정보보호기술은 일반 정보보호기술 뿐 아니라 정부의 정책과 법률, 서비스 환경 등의 요소도 기술을 구성하는 매우 중요한 요소라는 점이 일반 정보보호기술과 차이점이다.

초기에 개인정보보호기술은 개인정보 침해사고에 대한 대응책을 일반 정보보호기술을 접목시키는 단편적인 기술에서 출발하였으나, 최근에는 개인정보 침해사고의 경로와 원인을 분석하여 발생 가능한 각종 유·노출의 사고를 방지를 위한 다양한 기술적, 관리적, 제도적 대책을 결합한 방법적 기술로 발전하고 있다.

따라서 향후에는 새롭게 출현하고 있는 다양한 보안 위협과 외부 환경 등을 반영하여 안전한 개인정보보호 사회를 이룩하기 위해서는 가상화, 지능화, 경량화, 고성능화, 고기능화, 통합화 등과 같은 방향성을 가지고 개인정보보호기술에 대해 꾸준히 연구가 이루어져야 할 것이다.

참고문헌

[1] http://www.kisa.or.kr

[2] http://www.w3c.org/p3p

[3] 남기효, "개인정보보호 기술 동향: P3P". 주간기술동향 1250호, 정보통신연구진흥원, pp. 11-18, 2006.

[4] 남기효, "웹 프라이버시 필터링 및 스캐닝 제품 분석". 주간기술동향 1284호, 정보통신연구진흥원, pp. 13-20, 2007.

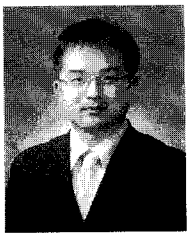
[5] (주)위너다임, *개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구*, 한국정보보호진흥원, 2006.

[6] (주)위너다임, 공공기관 홈페이지 개인정보 노출진단 연구, 행정자치부, 2006.

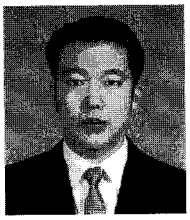
[7] Andelmounaam, "Internet Privacy Security Technology," *IEEE Security&Privacy*, 2003.

[8] Carpinter, J. & Hunt, R., "Tightening the net: A Review of current and next generation spam filtering tools," *Computers & Security 25*, pp. 566-578, 2006.

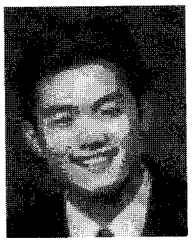
〈著者紹介〉



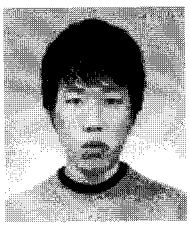
남 기 효 (Kihyo Nam)
종신회원
1993년 2월 : 고려대학교 산업공학과 졸업
1995년 2월 : 고려대학교 산업공학과 석사
1999년 2월 : 고려대학교 산업공학과 박사
1999년 ~ 2002년 : 고려대학교 정보통신기술공동연구소 선임연구원
2002년 ~ 2005년 : 프롬투정보통신(주) 기술기획팀장
2005년 ~ 현재: (주)위너다임 이사
관심분야 : 개인정보보호, 웹 보안, 콘텐츠보호



박 상 중 (Sangjung Park)
2007년 2월 : 부경대학교 시스템경영공학과 졸업
2007년~현재 : 고려대학교 정보경영공학전문대학원 석사과정재학
관심분야 : 개인정보보호, 텍스트 마이닝, 품질경영



강 형 석(Hyung-Seok Kang)
2007년 2월 : 고려대학교 전산학과, 산업시스템정보공학과 졸업
2007년~현재 : 고려대학교 정보경영공학전문대학원 석·박사 통합과정재학
관심분야: 개인정보보호, 텍스트 마이닝, SOA



남 기 환 (Kihwan Nam)
2006년 2월 : 연세대학교 통계학과 졸업
2006년~현재 : 고려대학교 정보경영공학전문대학원 석사과정 재학
관심분야: 개인정보보호, 응용통계

김 성 인(Seong-in Kim)
1970년 2월 : 서울대학교 경제학과 졸업
1973년 2월 : 서울대학교 응용수학과 졸업
1975년 2월 : KAIST 산업공학과 석사
1979년 2월 : KAIST 산업공학과 박사
1979년 ~ 현재 : 고려대학교 정보경영공학부 교수
관심분야 : 인공지능, 응용통계, 미술치료