

---

# 웹 환경에서의 분산형 개인정보보호를 위한 솔루션

김대유\* · 김정태\*\*

Solution for Distributed User's Privacy Under Web Environment

Kil-dong Hong\* · Jung Tae Kim\*\*

## 요 약

개인정보란 살아있는 개인에 관한 정보로 성명, 주민등록번호 및 영상을 통하여 개인이 알아볼 수 있는 정보를 말한다. 기존의 방법인 하드웨어 필터를 이용한 하드웨어 형태가 아닌 웹 분산형 방식으로 웹 브라우저와 웹 서버 간의 상호 동작 방식으로 개인정보를 점검할 수 있는 방법을 제안하였다. 사용자 단에서 게시판에 작성된 글은 웹 브라우저내의 자바스크립트로 첨부된 문서를 웹 서비스단에서 문서처리기로 개인정보의 누출을 해결할 수 있는 방법을 제안하였다.

## ABSTRACT

Personal information is defined information related to users' privacy data. It can be verified information through social security number, image, and means relating to individual can verify. Such personal information is in accordance with the privacy act in law for the collection and usage in enterprises and institutions. However, it can be induced privacy problem when it is exposed information without attention. This user's inadvertent disclosure of personal information has occurred due to social engineering and intelligent cyber-crime occurred in order to solve these problems. A variety of protection solutions for personal information have been developed. Web privacy filtering firewall and solutions related with server have been developed among developed many solutions, web privacy filtering and firewall solutions is proposed in this paper.

## 키워드

개인정보보호, 필터링, 방화벽, 정보 노출

## Key word

Privacy, Filtering, Firewall, Information exposure

---

\* 정회원 : 목원대학교 IT공학과 막사과정

\*\* 종신회원 : 목원대학교 전자공학과 (교신저자, jtkim3050@mokwon.ac.kr)

접수일자 : 2012. 09. 12

심사완료일자 : 2012. 09. 29

**Open Access** <http://dx.doi.org/10.6109/jkiice.2013.17.2.317>

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.  
Copyright © The Korea Institute of Information and Communication Engineering.

## I. 서 론

인터넷 환경의 발전으로 인하여 국내외적으로 법률을 제정하여 개인정보를 보호하고자 하는 노력이 전세계적으로 각 나라별로 실시되고 있다. 이러한 개인정보는 개인의 부주위, 홈페이지 등에 개인정보를 개방된 형태를 저장하여 외부의 해커 혹은 비인가된 자들이 임의로 자료를 위변조 하는 결과를 초래하고 있다. 2011년 9월 30일부터 개인정보보호법을 시행하였다. 개인정보보호법 시행령으로 사업자·기업·기관에서는 개인정보 이용 약관을 작성하고 이를 운영해야 한다. 그러나 기존의 방식인 필터링을 이용한 방법 및 기존의 방화벽에 개인정보 검색엔진을 탑재 하는 등의 방법을 사용하여 완벽한 해결방안이 되지 않고 있는 실정이다[1-3].

## II. 연구 동향 및 관련 연구

### 2.1. 국내현황

국내의 개인정보보호기술은 개인정보보호에 특화된 기술보다는 기존 정보보호기술을 개인정보보호에 적용하는 수준에 머무르고 있다. 따라서 클라이언트 기반의 개인방화벽, 서버기반의 방화벽 및 VPN, 클라이언트와 서버기반의 암호화기반 기술 등이 개인정보보호를 위한 목적으로 적용되고 있고, 개인정보보호를 위한 전문기술이 개발된 사례로는 개인정보보호정책의 기반 플랫폼 기술인 P3P 기술, 개인정보 검색기술, 개인정보 인증기술, 홈페이지 개인정보 노출 점검 및 차단 기술, 홈페이지 변조를 통한 스파이웨어 삽입탐지 기술 등이 있다.

#### 2.1.1. P3P 기술

개인정보보호정책에 관한 국제표준인 P3P 기술을 국내에 도입·적용하기 위한 노력의 일환으로 정보통신부는 2005년 6월부터 한국형 P3P연구전담반반을 구성하여 국내 개인정보보호 관련 법규를 W3C의 P3P 확장규격으로 포괄하여 기술적으로 표현한 한국형 P3P규격(안)을 작성한 바 있다. 또한 이 결과로 2005년 12월에는 한국정보보호진흥원(KISA)에서는 이 한국형 P3P규격(안)을 적용한 서버용 P3P 개인정보보호정책 생성기 개발을 완료 하였으며 KT에서는 W3C규격을 준수한 P3P

기반 에이전트를 개발 하였다. 금년에는 행정자치부에서 공공기관 웹사이트에 한국형 P3P를 보급하기 위해서 대전시청의 “공공기관 통합ID관리 시스템 구축”사업 내에 P3P생성기 및 관리시스템 개발을 포함하여 금년 말 구축을 목표로 사업을 진행하고 있다. 한편, 한국정보보호진흥원은 한국형 P3P규격(안)을 보다 발전시킨 형태로 P3P국내 표준화 작업을 진행하고 있다 [4, 5].

#### 2.1.2. 개인정보 검색 기술

개인정보 검색기술은 개인이 자신의 개인정보를 이용한 명의도용을 점검하기 위해서 자신의 개인정보의 이용 정보를 검색하는 기술을 말한다. 이 기술을 이용한 서비스로는 한국 신용평가정보에서 제공하는 크레딧뱅크 서비스와 서울신용평가정보에서 제공하고 있는 사이렌24 서비스를 들 수 있다.

#### 2.1.3. 개인정보인증기술

개인정보 인증에 관한 기술의 대표적인 예로 국내의 주민번호 대체기술을 들 수 있다. 이 기술은 인터넷 사이트 회원가입이나 성인인증 시에 주민등록번호를 대신 사용할 수 있는 주민등록대체수단을 이용하는 기술로, 2005년 주민번호 대체수단 마련에 대한 공청회를 실시한 이후로 금년 상반기에 공공기관 등에 1개 이상의 대체수단 사용을 권고하고 있으며, 금년 하반기 또는 내년에 대형 포털이나 게임 사이트 등을 중심으로 법제화를 추진 할 계획이다.

#### 2.1.4. 홈페이지 개인정보 노출점검 차단 기술

최근 홈페이지 관리자의 부주의나 이용자의 실수 등으로 인하여 홈페이지를 통한 개인정보 노출사고가 빈번히 발생하고 있는데, 특히 24개 공공기관에서 홈페이지를 통한 노출사고가 발생하면서 이에 대한 대응책으로서 최근에 대두되기 시작한 기술이다. 이 기술은 홈페이지 개인정보 노출 필터링 기술과 스캐닝 기술로 크게 분류할 수 있으며, 필터링 기술은 웹 서버 내부 또는 외부에 설치하여 웹 서버에 등록되는 콘텐츠 중 개인정보가 포함되어 있으면 이를 차단하는 기술을 말하며, 스캐닝 기술은 웹 서버 또는 웹 서버 정보를 크롤링하고 있는 검색엔진 등을 스캐닝하여 개인정보 노출 여부를 점검하는 기술이다.

2.2. 국외현황

현재까지 국내외적으로 다양한 형태의 개인정보보호기술에 관한 연구가 진행되었으나, 개인정보보호기술에 관한 종합적이고 체계적인 분석은 거의 이루어지지 않고 있다. 최근의 분석 결과 중에서 가장 많이 인용되는 개인정보보호기술의 분류는 다음 그림과 같이 **Abdelmounaam**이 **IEEE Security&Privacy**에서 발표한 체계를 따르고 있다. 그러나 이 분류체계는 인터넷 환경에 제한적으로 적용되는 프라이버시 보호 기술들을 표현하고 있다는 한계가 있을 뿐 아니라, 인터넷 환경에서도 최근에 국내에 나타나고 있는 다양한 형태의 침해유형에 대한 대응책으로서의 개인정보보호기술이 포함되어 있지 않다는 단점이 있다 [6, 7].

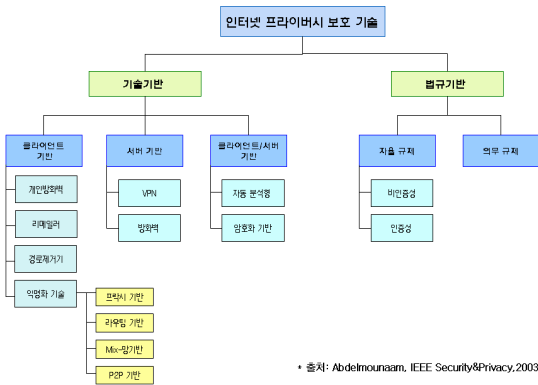


그림 1. 인터넷 프라이버시 보호 기술(국외)  
Fig. 1 Internet Privacy Protection Technology

최근의 개인정보의 침해사고 중에는 홈페이지 불법 변조를 통한 스파이웨어 등 악성코드가 유포되어 개인정보의 침해사고가 나타난다거나 홈페이지 상에 개인정보가 노출되어 이것이 명의도용의 사고로 발전하는 등의 침해사고가 발생하고 있으나, 이 연구에는 이와 같은 최근의 인터넷 환경에서 나타나는 침해사고의 대응책으로서의 개인정보보호기술은 포함되지 않고 있다.

2.3. 관련연구

개인정보보호 솔루션에는 개인용과 기업/기관에서 사용되는 솔루션 제품들이 다양하게 판매되고 있다. 이러한 솔루션은 개인정보가 생성, 복제, 이동, 전송 되는 단계별로 다양한 솔루션을 가지고 있다.

2.3.1. PC형 솔루션

사용자의 PC에서 개인정보가 노출되는 것을 방지하는 솔루션이다. 독립형태로는 개인이 직접 개인정보를 검사하고 조치하는 방식이 있으며 감사형태로는 USB 형태로 개인정보감사형태로 점검하는 방식이 있으며 기관이나 기업에서는 통합 관리형태로 에이전트가 PC에 자동으로 설치되어 서버에서 직접 관리하는 형태가 있다.

2.3.2. 서버형 개인정보점검 솔루션

사업자·기업·기관의 경우에는 개인정보를 다루는 서버시스템 혹은 데이터베이스 시스템에 개인정보가 포함되어있는지 점검하고 관리하는 형태가 있다.

2.3.3. 웹 방화벽형 개인정보점검 솔루션

이는 웹서버를 운영하는 사업자·기업·기관에서 사용되는데 IDS, IPS처럼 웹서버 앞단에 장비를 설치하여 네트워크 송/수신 패킷을 감지하여 개인정보를 필터링하는 솔루션이 있는가하면 JSP, ASP, PHP 형태의 라이브러리를 제공해주는 API 제품군들도 있다.

III. 제안된 웹 개인정보보호 솔루션

기존에 출시되어있는 솔루션들은 서버 내부에서 개인정보점검을 시작하거나 서버외부에 장비를 설치하여 운영하는 방식이다. 이러한 방식은 분산처리가 되더라도 개인정보보호 솔루션을 운영측 내부에서 모두 작동되므로 개인정보보호 솔루션을 증설할 경우 비용부담적인 문제가 많다. 또한 API방식의 경우에는 내부에서 개인정보점검을 할때에 시스템 자원을 소모하기 때문에 서버의 과부하를 일으키는 문제점이 발생하게 된다. 이러한 문제점을 해결하기 위해서 분산형 웹 개인정보보호 컴포넌트를 제안하고자 한다 [8, 9].

3.1. 웹 개인정보보호 솔루션

개인정보보호 솔루션이 여러 가지 형태가 있지만 이것들 중에서도 가장 많이 사용되고 있는것이 바로 웹 서비스이다. 이러한 웹 서비스가 운영되고 있는 기업/기관에서는 개인의 정보를 보호하기 위한 정책을 미리 만들어 놓고 운영하지만 사용자의 부주이나 관리자의 부주

의에 의하여 개인정보가 유출되는 것을 사전에 방지하기 위해서 많이 사용된다. 이러한 솔루션들을 보면 API 형태로 (ASP, JSP, PHP)가 있으며 하드웨어형태로 제공되는 솔루션들이 있다.

### 3.1.1. API 라이브러리

웹 서비스 환경에 따라서 적용되는 방식이 조금씩 다르다. 각 운영되는 서블릿(JSP, ASP, PHP)에 맞춰서 적용되고 있으며 모든 개인정보점검처리를 서버내부에서 처리하는 방식이다. 해당 라이브러리를 설치하려면 운영되는 기업/기관내에서 작업해야 하며 운영되는 환경에 따라서 작업시간이 많이 소요된다.

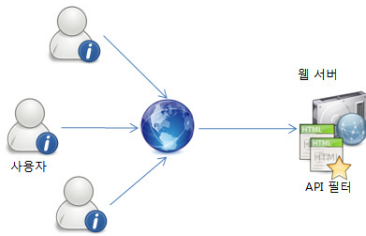


그림 2. API 솔루션 구조  
Fig. 2 Structure of API Solution

### 3.1.2. 하드웨어형

웹 서버 앞단에 IDS, IPS형태로 설치가 이루어지며 SSL인증서를 사용하는 웹 서버의 경우에는 SSL인증서를 하드웨어형 솔루션에 적용을 해야 개인정보보호 솔루션이 정상적으로 동작한다. 또한 웹 서버가 운영되고 있는 시스템 자원(네트워크 대역폭)에 맞춰서 적용을 해야 하며 만약 이것을 초과할 경우 과부하가 발생하므로 운영되는 시스템에 영향을 줄 수 있기 때문이다.



그림 3. H/W 솔루션 구조  
Fig. 3 Structure of H/W Solution

## IV. 제안된 개인정보보호 솔루션 구조

### 4.1. 제안된 웹 환경의 개인정보보호 솔루션

제안된 웹 분산형 개인정보보호 솔루션은 웹 접근성을 고려하여 사용자가 이용하는 모든 단말기에서도 모두 동작하도록 하기 위해서 HTML5를 사용 하였다. 또한 시스템 자원을 효율적으로 사용할 수 있도록 분산 처리형태로 이루어져있으며 적용과 운영 시스템의 영향을 최소화 하는것을 목표로 한다. 제안된 웹 환경의 개인정보보호 솔루션은 사용자가 게시글을 작성할 때에는 정규표현식 패턴을 사용하여 사용자 단에서 직접 점검을 수행하고, 게시글내에 포함되는 첨부파일(상용문서 및 그림)의 경우에는 AJAX를 사용하여 문서처리 서버로 전송한 후 그 결과 값을 점검하도록 하여 분산형 처리 방식을 이용한다.

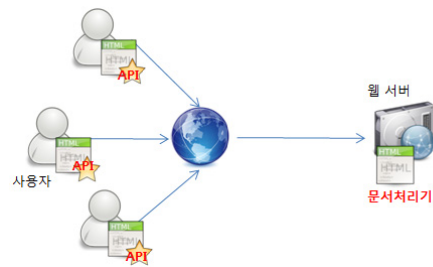


그림 4. 제안된 API 솔루션 구조  
Fig. 4 Structure of Proposed API Solution

제안된 웹 환경에서의 개인정보보호 솔루션은 사용자가 콘텐츠를 등록할 수 있는 웹 페이지에 제안된 방식의 솔루션 라이브러리를 추가하고 몇 가지 설정을 해주면 작업이 완료 된다.

사용자가 게시글을 등록하는 페이지에 방문하고 게시글을 등록할 때 제안된 라이브러리가 동작하며 사용자가 입력하는 컨트롤들의 속성을 확인하고 본문과 첨부파일을 구분한다. 첨부파일이 있는 경우 첨부파일처리기로 파일을 전송하고 텍스트 문서로 변환된 내용을 전달받은 후에 개인정보를 점검하고 개인정보가 포함되어있는 경우 사용자에게 결과 안내메시지를 표시한다.

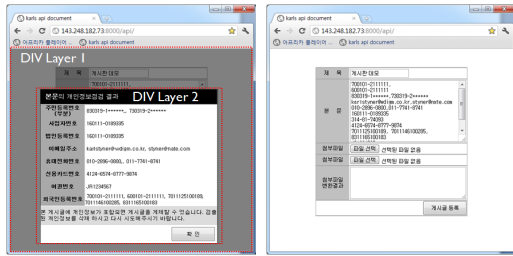


그림 5. 제안된 솔루션의 처리 화면  
Fig. 5 Processing Screen of Proposed Solution

4.2. 제안하는 알고리즘

제안된 웹 분산형 개인정보보호 솔루션은 크게 2가지 형태로 나누어져 있다. 사용자 단에서 처리하게 되는 자바스크립트와 서버단에서 처리하는 문서처리가 있는데, 자바스크립트 형태로 사용자단에서 처리되는 사용자 정의 함수에는 개인정보점검 함수와 첨부파일의 내용이 상용문서인 경우 문서처리로 파일을 전송하여 평문(텍스트)로 변환하는 기능이다. 일반적으로 사용자가 등록하는 본문의 경우에는 개인정보점검 함수로 처리하고 첨부파일이 있는 경우 문서처리에 첨부파일을 송신하고 처리된 결과를 송신하여 개인정보 점검을 하는 방식이다. 개인정보점검의 경우 CPU 자원을 많이 활용하는데 이 부분을 사용자단에서 동작하며 첨부파일이 있는 경우에만 기관 웹 서버 송신하여 처리된 결과를 수신하여 개인정보 점검을 하게 된다. 이렇게 하여 개인정보점검 부분을 분산하여 처리하면 서버의 자원을 소모하는 부분을 사용자단에서 작업하므로 서버의 운영자원을 최소화 할 수 있다.

V. 성능 평가

제안한 개인정보보호 솔루션의 경우에 본문의 경우에는 클라이언트의 시스템 자원을 사용하지만 첨부파일의 경우에는 서버부분에 적용된 문서처리로 처리가 된다. 그러므로 첨부파일을 송신하고 처리결과를 수신하는데 소요시간은 171kb문서로 약 171ms의 시간이 소요되었다. 네트워크 환경에 따라서 처리 지연시간이 변동될 수 있다.

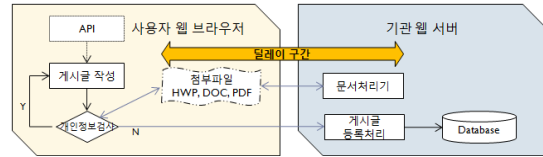


그림 6. 제안된 솔루션의 처리 흐름도  
Fig. 6 Flow of Proposed Solution Processing

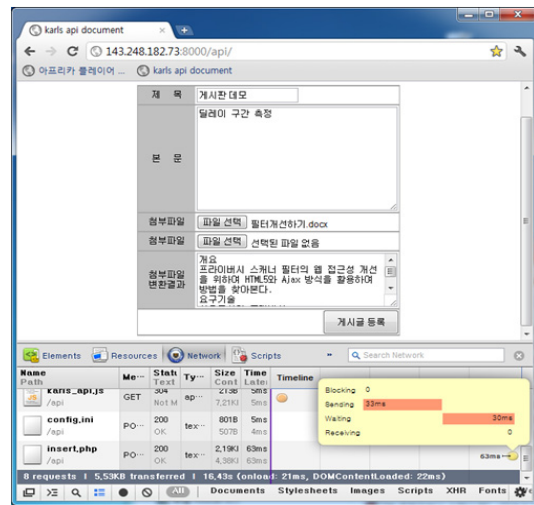


그림 7. 제안된 솔루션의 처리 속도  
Fig. 7 Processing Speed of Proposed Solution

<표1>은 성능 평가를 위한 평가표로서 제안한 방식이 소프트웨어적으로 설계가 되어 구성하기가 쉬운 장점을 가진다.

표 1. 성능 평가표  
Table. 1 Evaluation Table

항목	API	H/W	Proposed
Installation	High	Middle	Low
System Load	High	High	Middle
Reliability	Safety	Middle	Safety
Management	Easy	Hard	Easy

적용 및 설치의 경우 기존방식의 API방식의 경우에는 각 분야(JSP,ASP,PHP)의 인력이 필요하다. 또한 적용을 하려면 해당 서버를 분석해야하고 다양한 게시관 환경에서 적용하기에는 어려움이 있다. 또한 H/W방식의 경우 운영되는 네트워크 망을 확인하고 설치를 하게

되는데 운영되는 시스템의 가용성을 확인 한 후 거기에 맞는 장비를 설치해 해야 한다. 또한 H/W의 경우에는 장치 자체에 전기 공급이나 네트워크 혹은 다른 자원을 많이 사용하므로 안전성이나 운영관리에 좋지 않다. 하지만 제안된 방식의 경우 적용방법이 JS스크립트로 간편하게 되며, 한번 적용하면 다른 시스템이 없고 운영되는 웹 서버 자체이므로 다른 관리가 필요가 없다.

## VI. 결 론

본 논문에서는 기존의 하드웨어 기반에서의 문제점을 개선하기 위하여 소프트웨어 기반의 분산처리 알고리즘을 이용한 개인정보보호 시스템을 구현하였다. 또한 기존의 문제점을 해결하기 위해 W3C에서 제정한 HTML5 기술을 응용하여 웹 환경에서의 분산형 개인정보보호 솔루션을 설계한 하여 자료를 송신하고 처리한 결과 수신하는데 소요시간은 171kb문서로 약 171ms의 시간이 소요되어 실시간에 처리됨을 알 수 있었다.

## 참고문헌

- [1] 이영석, 안개일, 김종현, “도메인간 보안 정보 공유를 통한 협력 대응 프레임워크 설계,” 한국정보통신학회논문지, 제15권, 제3호, pp.605-612, 2011.
- [2] 김창수; 정회경, “개방형 네트워크 보안 시스템 구조,” 한국정보통신학회, 제12권, 제4호, pp.643-650, 2008.
- [3] Kim, Sun-Joo, Jo, In-June, “A Derivation of Evaluation Item about Enterprise Security Management,” Journal of Information and Communication Convergence Engineering, vol.8, no.5, pp.544-548, 2010.
- [4] Kim Seok-Soo, “Web Server Cluster’s Load Balancing for Security Session,” Journal of Information and Communication Convergence Engineering, vol.3, no.2, pp.93-95, 2005.
- [5] 여성구, 심미나, 이상진, “웹 로그 데이터에 대한 개인정보 위협분석 및 보안 가이드,” 한국정보보호학회, 제19권, 제6호, pp.135-144, 2009.

- [6] Hui-zhong Shi, Bo Chen and Ling Yu, “Analysis of Web Security Comprehensive Evaluation Tools,” Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on Vol, pp. 285 - 289, 2010
- [7] Bo Song, Shengwen Gong, and Shengbo Chen, “Model Composition and Generating Tests for Web Applications,” Computational Intelligence and Security (CIS), 2011 Seventh International Conference on 2011, pp.568 - 572, 2011.
- [8] 김대유, 김정태, “웹 환경에서의 분산형 개인정보보호를 위한 솔루션”, 한국정보통신 종합학술대회논문집, pp.672-673, 2012.
- [9] 김대유, 김정태, “분산처리를 이용한 웹 환경하에서의 개인정보보호 점검 솔루션 개발”, pp.382-383, 2012.

## 저자소개



김대유(Daeyu Kim)

2008년 2월 : 목원대학교 대학원  
IT공학과 박사과정  
2006년 3월~ : 2013년 2월  
(주)위너다임 정보기술  
연구소 연구원

2013년 2월~현재 : 한국통신인터넷기술  
※관심 분야: 웹보안, 개인정보보호, 네트워크보안



김정태(Jung Tae Kim)

2001년 8월 : 연세대학교 대학원  
전자공학과 박사  
1991년 8월~1996년 2월 : 한국전자  
통신연구원(ETRI)  
선임연구원

2002년 10월~현재 : 목원대학교 전자공학과 교수  
※관심 분야: Network Security, 보안 컨설팅, RFID& USN Security, 통신용 ASIC Design.