

# PC의 개인정보보호법 대응 방안

서미숙\*, 박대우\*\*

요약

최근 해킹 및 개인정보 유출로 인한 관공서 개인정보 취급에 대한 사회적 불신감 팽배, 신뢰도 저하 문제가 발생하고 있다. 개인정보보호법, 정보통신망법의 강화에도 불구하고, 업무에 활용된 명부 등이 저장된 위치를 기억하지 못하여 그대로 방치되고 있으며, 자료공유시스템 등 웹사이트를 통해 열람(접근)된 개인정보파일이 개인 PC내 임시 파일로 PC의 하드디스크에 저장되어 있다. 개인정보보호법은 2011년 3월 29일 공포되었고, 9월 30일부터 전면 실시되었다. 본 논문에서는 PC의 개인정보를 검색하고 검색된 파일을 암호화, 파일숨김을 하여 파일을 안전하게 보관하게 하며, 사용기간이 지난 파일의 경우 완전삭제를 하여 PC에서 개인정보보호법에 대응 방안을 제시한다.

## I. 서론

2011년 8월 한국엠포는 회원전체에 해당하는 36만 명의 이름·ID·암호화 하지 않은 비밀번호·주민등록번호를 정보통신망을 통해 누출하였다.

개인정보보호법규를 위반한 한국엠포에 과징금 3천 300만원 및 과태료 900만원을 부과하고 개인정보에 대한 기술 관리적 보호조치를 수립 시행 명령을 내렸다고 한다.

본 논문에서는 개인정보보호법 대응을 위하여 개인정보에 대한 기술 관리적 보호조치를 위하여 PC내에 개인정보 검출 및 실시간 개인정보 검색으로 개인정보의 현황 파악, 개인정보 관리 및 사전 유출예방, 개인정보의 효율적 통합관리를 하도록 하여 개인정보보호법 대응의 방안을 연구한다.

회(회원탈퇴, 주민번호 삭제 등)와 관련한 단순 상담 및 처리성 민원이 급증한 것에 기인한다. 유형별로 훼손, 침해, 도용을 제외하고 기술적·관리적 조치 미비로 인한 개인정보 누출 등이 10,958건(전년 대비 606% 증가)으로 가장 많았으며 다른 유형의 증감폭은 크지 않은 것으로 나타났다[1].

## II. 개인정보 침해 신고 및 유출사례

### 2.1. 개인정보 침해상담건수

2011년도 개인정보 침해건수는 총 122,215건으로 전년대비 약 1,228.8% 증가 하였다. 이는 2011년도에 주민등록번호 클린센터('10.7월 이후) 영향으로 동의절



(그림 1) 개인정보 침해신고 상담건수

### 2.2. 개인정보침해 유형별 신고건수

개인정보 침해신고 민원건수를 [정보통신망이용촉진 및 정보보호 등에 관한법률]의 규정에 따른 침해 유형

\* 호서대학교 벤처전문대학원(cowboyiw@hanmail.net)

\*\* 호서대학교 벤처전문대학원(prof\_pdw@naver.com)

(표 1) 유형별 개인정보 침해신고 현황  
(단위: 건)

	2008	2009	2010
고지·명시한 범위를 넘어선 이용 또는 제3자 제공	1,037	1,171	1,202
개인정보 취급자에 의한 훼손·침해 또는 누설	125	158	158
영업의 양수 등의 통지의무 불이행	9	6	22
개인정보관리책임자 미지정	26	10	21
기술적·관리적 조치 미비로 인한 개인정보누출 등	1,321	819	1,551
수집 또는 제공받은 목적 달성 후 개인정보 미파기	294	294	323
동의철회·열람 또는 정정 요구 불응	949	680	826
동의철회, 열람·정정을 수집보다 쉽게 해야 할 조치 미이행	503	603	630
법정대리인의 동의 없는 아동의 개인정보 수집	27	19	35
주민등록번호 등 타인 정보의 훼손·침해·도용	10,148	6,303	10,137
정보통신방법 적용대상 이외의 개인정보침해(신용정보침해 등)	24,144	23,893	38,414
계	39,811	35,167	54,832

별로 분류 하였다.

표 1과 같이 기술적·관리적 조치 미비로 인한 개인정보누출 건수가 1,551로 3번째로 많은 신고가 접수되었다[2].

### III. 기술적·관리적 조치를 위한 개인정보 검색솔루션

현재 개인정보 검색 솔루션은 국내 20여개의 제품이 있다. 이중에 대표적인 제품이 에스엠에스 i-Safer, 소만사의 Privacy i, 지란지교의 pc필터 등이 있다.

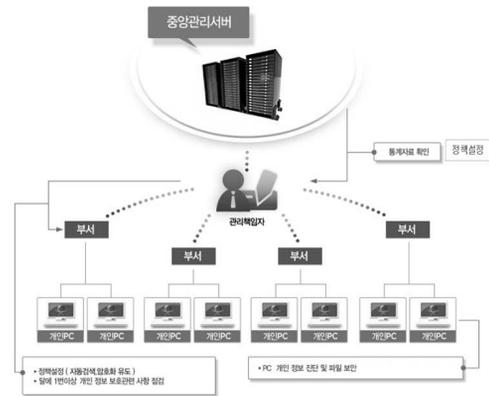
개인정보 검색솔루션은 사용자 PC 내 저장된 개인정보 식별을 통해 개인정보 관리 및 사전 유출 예방을 위한 개인정보 검색 및 PC에 보유중인 개인정보를 자동으로 검출하여 유출 가능성이 있는 개인정보 파일에 대한 보호조치가 가능하며 개인정보보호법(‘11. 9. 30 시행) 제29조(안전조치 의무) 관련 직원 PC에서 사용 중

인 개인정보파일의 보유 규모 파악 및 체계적 보호 조치 시행이 가능하다[3].

본 논문에서는 이중 에스엠에스의 i-Safer를 연구하였다.

#### 3.1. 시스템의 구성도

개인정보 검색솔루션의 시스템의 구성도는 그림 2와 같다.



(그림 2) i-Safer의 시스템 구성도

#### 3.2. 특징 및 기대효과

##### 3.2.1 특징

i-Safer의 특징은 실시간 개인정보 검색으로 개인정보 유출을 예방할 수 있으며, 웹메일, 웹하드, P2P, FTP, 메신저, 저장매체 등을 통해 개인정보 포함 파일을 전송할 경우 실시간 감지하여 경고를 하며, 개인정보 또는 중요파일에 대한 접근 차단 및 숨김 기능, 파일의 데이터를 복구 불가능하도록 완전삭제 기능 등이 있다.

##### 3.2.2 기대효과

- 검색을 통해 개인정보 관리 및 사전 유출예방.
- 개인정보의 효율적 통합관리.
- 개인정보 현황 파악 가능.
- 개인정보보호법 대응.

### IV. i-Safer의 기능

i-Safer의 기능은 개인정보검색 기능, 파일보안 기능, 파일삭제 기능, 실시간 개인정보 감시 기능, 서버에서 클라이언트 관리 기능과 같이 크게 5가지로 볼 수 있다.

#### 4.1. 개인정보 검색

개인정보 검색기능은 그림 3처럼 주민등록번호, 외국인등록번호, 면허 번호, 전화번호, 여권번호, 사업자등록번호, 계좌번호, 이메일, 신용카드, 주소, 새주소 등의 패턴으로 검색이 된다. 또한 다양한 종류의 전자문서 지원하며, ZIP, 7Z, ALZ, BZ2, RAR등 압축파일 검색도 가능하다. 뿐만 아니라 검색한 파일정보를 DB에 저장하여 재검색시 빠른 검색을 할 수 있다.



(그림 3) i-Safer의 개인정보 검색

#### 4.2. 파일 보안 및 완전삭제

파일보안의 기능은 3가지 기능이 있다. 첫 번째로 메뉴나 우클릭을 통하여 개인정보 또는 기타 보안을 요하는 파일에 대한 커널 레벨의 접근 차단 및 숨김 기능으로 악성코드로부터 보호 접근 차단이 가능하다.

두 번째로 파일을 암호·복호화 기능(국정원 검증 모듈 사용)이 있어 안전하게 개인정보를 관리할 수 있다.

그리고 사용기간이 지났거나 불필요한 파일을 완전 삭제 하는 기능이 있다.

##### 4.2.1 파일의 암호화

그림 4에서 검색된 파일을 우클릭이나 도구의 암호화를 클릭하여 암호화 할 수 있으며 이때 암호는 국정의

지침 대로 AREA로 암호화가 된다.

i-Safer에서는 국가정보원 지정 암호화 모듈 탑재(이니텍의 INISAFE Net)하였다.



(그림 4) 파일의 암호화

##### 4.2.2. 파일의 숨김

개인정보 또는 기타 보안을 요하는 파일에 대한 접근 차단 및 숨김 기능, 파일/폴더 단위의 접근 차단 및 숨김 기능, 차단/숨김 파일에 대한 리스트 관리, i-Safer를 제외한 다른 방법으로 개인 정보 파일에 대한 접근이 불가능하며, 부팅 및 안전모드 부팅 후 숨김 파일에 대한 접근 차단이 가능하다. 또한 커널 레벨의 접근 차단 및 숨김 기능으로 악성코드로부터 보호가 가능하다.

##### 4.2.3. 파일의 삭제

검색된 파일 또는 원하는 파일을 선택하여 파일의 데이터를 복구가 불가능하도록 완전삭제를 한다[3]. 이때 파일/폴더, 임시파일, e-mail영구삭제 지원이 가능하며, Kr-Random, Kr-Random-00-FF, Quick Erase-FF, DoD\_Short, DoD\_5220.22-M, Gutmann Wipe의 다양한 삭제방법을 지원한다.

또한 컴퓨터를 사용이 익숙하지 않은 사람의 실수로 컴퓨터의 시스템 파일의 삭제를 막기 위하여 Windows 폴더, 시스템파일보호 기능이 지원된다.

4.3. 서버에서 클라이언트 관리 기능

실시간 검색할 전자문서의 확장자, 검색옵션 설정, 실시간 검색된 전자문서 개인정보DB 저장, 개인정보가 감지된 파일에 대한 메시지 알림 기능이 있으며 그림 5 처럼 화면 우측 하단에 알림창이 뜬다.



(그림 5) 실시간 알림창 감지

4.4. 서버에서 클라이언트 관리 기능

서버에서 클라이언트 관리, 통신 프로토콜 암호화 지원, 사용자 및 부서별 관리 기능, Client PC에서 수행할 작업 할당 기능, 관리자서버를 통해 키워드 및 패턴을 등록, 수정, 삭제 가능, 서버에서 모든/일부 에이전트를 대상으로 주기적인 예약 검색을 설정, 개인정보취급자와 비취급자에 따라 개인정보검출, 암호화정책 별도 적용 가능하다.

또한 PC에 탑재치 이상의 개인정보파일이 추가 저장 되는 경우 실시간으로 e-mail, SMS로 관리자에게 통보, 기존인사DB의 회원 연동이 가능, Client PC에서 수행할 작업 할당 기능, 하드웨어 변동사항 파악, 검색항목 관리 기능(키워드 및 패턴 등록), 검색결과 통계기능 제공하여, 그림 6처럼 미 검색자, 미 접속자 검출이 가능하다.

VI. 결 론

개인정보보호법이 시행되고 있음에도 불구하고 개인정보에 대한 인식 부족 및 지속적인 유출 사고와 신고가 접수 되고 있다.

개인정보 유출과 방지를 위한 가장 중요한 부분이 보



(그림 6) 실시간 감시하여 경고 메시지

안 인식과 자신의 PC관리이다. PC보안(내부정보 유출 방지)은 최근 서버 이외에 PC의 해킹사고가 증가하고 있고 PC보안사고 대부분이 내부자에 의한 자료 유출 및 위·변조 등의 피해사고로 그 필요성이 커지고 있다. PC의 개인정보나 산업기밀 자료를 암호화 및 파일 숨김, 완전 삭제를 하여 안전하게 관리를 하게 되면 개인정보보호법 및 대응이 가능하며 유출을 최소화 할 수 있을 것이다.

향후 연구에서는 PC의 개인정보 보호 및 유출 차단에 대한 연구도 지속적으로 필요할 것이다.

참고문헌

- [1] 방송통신위원회, “한국인터넷진흥원 개인정보침해 신고센터 접수자료,” 2012년 7월.
- [2] 한국인터넷진흥원, <http://www.krcert.or.kr/>, 2012년 7월.
- [3] 서미숙, 박대우, “개인정보의 패턴 추출과 완전삭제 방법에 관한연구,” 2012년 8월

〈著者紹介〉



**서미숙 (Mi-Sook Seo)**

정회원

2003년 8월 : 한국방송통신대학교  
컴퓨터학과 (공학사)

2011년 3월 ~ 현재 : 호서대학교  
벤처전문대학원 융합공학과 석사  
과정

<관심분야> 정보보호, 완전삭제,  
Hacking, Forensic



**박대우 (Dea-Woo Park)**

정회원

1998년 2월 : 숭실대학교 컴퓨터  
학과 (공학석사)

2004년 2월 : 숭실대학교 컴퓨터  
학과 (공학박사)

2004년 2월 : 숭실대학교 겸임교수

2006년 2월 : 정보보호진흥원(KISA)  
선임연구원

2007년 3월 ~ 현재 : 호서대학교  
벤처전문대학원 교수

<관심분야> Hacking, CERT/CC,  
침해사고대응, e-Discovery, For-  
ensic, 사이버국방, 정보보호, 유비  
쿼터스 네트워크 보안, WiBro 보  
안, VoIP보안, 스마트폰 및 이동단  
말 보안