情 報 保 護 學 會 誌
第18卷 第6號, 2008. 12

기업내부 개인 정보 보호 시스템 개발

박 중 환*, 조 남 욱**, 이 기 혁***, 최 일 훈*

요 약

최근 인터넷 상의 개인 정보 보호가 중요한 사회·경제적 이슈로 부각됨에 따라 기업 내부의 정보시스템에 산재해 있는 개인정보의 보호와 체계적인 관리의 필요성도 대두되고 있다. 하지만 기업내부의 DBMS나 파일서버에 집중적으로 보관 관리되고 있는 개인정보와 달리 분산된 개인용 컴퓨터(PC)에 산재해 있는 개인정보의 효과적인 보호와 관리 방안은 부족한 실정이다. 본 연구에서는 기업 업무 환경 하에서 분산된 PC내에 저장된 개인정보를 효과적으로 관리할 수 있는 시스템(Privacy-i)을 제안하였다. 이를 위해 기업내에 산재한 PC에 저장된 개인정보를 보호하는 개인정보보호 시스템의 요구사항을 분석하고 시스템을 설계를 재시하였으며 하였으며 실제 개발을 통해 개인정보 보호 시스템을 구현하였다. 본 연구를 통해 개인 정보 유출에 대한 관리 책임을 지고 있는 관리 주체인 기업이 PC에 산재하는 개인 정보보호의 필요성을 인식하고 개발된 시스템의 적용함으로써 기업 내 정보 보안 수준을 높이는 계기가 될 것을 기대된다.

Ⅰ. 서 론

정보통신 기술의 발달과 e-business의 활성화로 인해 인터넷 상의 개인정보 보호가 중요한 사회·경제적 이슈로 떠오르고 있다. 특히 최근 옥션 (www.auction.co.kr)의 개인정보유출사태 이후 개인정보보호를 태만시한 조직에 대해서 관리 소홀의 책임을 포괄적으로 지우고 있어 개인정보를 관리하는 조직의 개인정보 보호 관리 방안 마련이 시급하다. 현행법에서 개인정보란 '생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 개인을 식별할 수 있는 정보'로 정의 된다[1]. 개인정보 유출은 개인정보 소유자의 동의 없이 개인의 사적정보가 유용될 위험성으로 인해 이를 방지하기 위한 다양한 법적, 기술적 방안이 마련되고 있으나 개인 정보 유출의 위험성은 정보기술의 발달로 인한 유비쿼터스(Ubiquitous) 컴퓨팅 환경의 도입으로 인해 점점 더 증가하고 있는 추세이다.

문형진 등 은 e-biz 환경에서 개인 정보보호를 위하여 암호화를 기반으로 한 개인정보 보호 방법론을 제안하였다[5]. 송유진과 이동혁은 개인정보 보호를 개인정보 라이프 사이클 관점에서 분석하고 보호하기 위한 프레임워크를 제시하였다[6]. e-business 환경 내에서 개인정보 유출 위험을 분석하고 이를 해결하기 위한 개인정보 정책모델이 제시되었다[10].

최근 유비쿼터스 컴퓨팅이 이슈로 부각되면서 유비쿼터스 환경에서의 개인정보 보호 중요성이 증가함에 따라[6], 유비쿼터스 환경에서 개인정보에 대한 국내외 및 시장동향에 관한 연구[7], 유비쿼터스 환경 하의 여행 시나리오를 설정하고 이에 대한 기술 보호 지원 기술에 대한 연구[2]가 수행되었다. 홍승필과 이철수는 유비쿼터스 환경에서 개인정보 보호 시스템의 설계와 개발을 위한 5단계의 방법론을 제시하였다[9]. 또한, 유비쿼터스 환경의 핵심 기술 중의 하나인 RFID 태그 시스템 상의 개인정보 보호 기법을 제안한 연구가 있다[4]. 개인정보 보호에 대하여 정책적 관점에 대한 연구도 진행되어 왔다. 임태훈 등 은 국내 인터넷 상의 개인정보 보호 실태를 조사 분석하였으며[8], 강성철은 우리나라 개인 정보 보호 실태를 분석하고 개인 정보보호 강화를 위해 법제도 정비와 개인정보 보호 활동 강화를 제안하였다[1]. 하지만 개인 정보 보호에 대한 사회적, 학술적 관심의 증

* (주) 소만사, 연구소 (hinnie@somansa.com;acechoi@somansa.com)
** 교신저자, 서울산업대학교 산업정보시스템공학과 (nwcho@snut.ac.kr)
*** 건국대학교 대학원 박사과정 (kevinlee@sktelecom.com)

가에 비해 기업 업무 환경 하에서 PC단의 개인정보보호에 대한 솔루션의 개발은 아직까지 미흡한 실정이다.

본 연구에서는 기업 내부의 PC에 산재해 있는 개인정보를 보호하기 위한 시스템을 개발하고자 한다. 최근 정보보안전문업체인 (주)소만사의 조사에 따르면, 5년 이상 근속한 개인들의 PC하나에 저장된 개인정보파일이 평균 50여개가 넘는다고 한다. 1000여명의 임직원 기업의 경우 5만 건 이상의 개인정보가 1,000여개의 PC에서 흩어져있는 있는 것이다. 개인 정보 유출에 대한 관리 책임을 관리 조직에 지우는 것이 현재의 추세임을 감안하면 회사 내에서 개인정보가 포함된 파일이 광범위하게 배포되어있는 것을 방기하는 것은 회사의 존립을 위태롭게 하는 사안을 방치하는 것이라고 할 수 있다. 특히 PC는 서버와 달리, 보안수준이 매우 낮아 접근통제가 잘 되지 않고 있으며, 취약점에 대한 적절한 패치가 진행되고 있지 않을 뿐 아니라, 사용자 인증도 허술하다. 또한 전담 관리 인력이 있는 서버와는 달리 관리의 주체가 개인이기 때문에 DBMS나 파일서버에 집중적으로 보관 관리되고 있는 개인정보와 달리 PC에 보관되어있는 개인정보는 외부로 노출될 수 있는 가능성이 높다. 대부분의 기업에서는 개인정보가 포함된 파일을 PC에 보관하는 것을 원칙적으로 제한하고 있으며, 업무용도로 인하여 사용하게 될 경우에도 개인정보가 포함된 파일은 암호화하여 보관하도록 하고 있으나 많은 사용자들이 자신의 PC에 개인정보가 포함된 파일의 소재 파악조차도 안 되고 있는 현실이다. 따라서 이러한 개인정보의 보관 및 삭제 관리에 대한 정책을 강제화할 수 있는 도구의 필요성이 강력하게 대두되고 있다. 본 연구에서는 기업 업무 환경에서 분산된 PC의 개인정보를 효과적으로 관리할 수 있는 시스템(Privacy-i)을 제안한다. 2장에서는 먼저 기업 내부 개인 정보시스템의 요구사항을 분석하고 이를 토대로 시스템 설계를 3장에 제시한다. 실제 구현된 시스템은 4장에 제시하였다.

Ⅱ. 개인정보보호 시스템 요구사항 분석

본 장에서는 먼저 개인용 컴퓨터(PC) 내부의 개인정보보호를 위한 시스템 요구사항을 분석한다. 먼저 개별 PC를 대상으로 한 개인정보보호 요구사항을 제시하고 이를 확장하여 기업내부의 정보를 통합하여 관리하는 기업용 개인정보보호시스템의 요구사항을 제시하고자 한다.

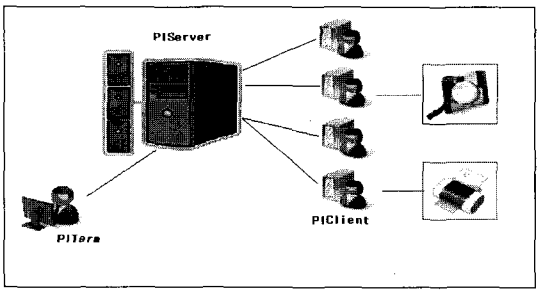
PC 내부의 개인정보 보호를 위해서는 먼저 PC에 산재되어 있는 각종 개인 정보들을 효과적으로 검색하여 보관하는 기능이 우선되어야 한다. 검색대상 파일은 텍스트 파일 뿐만 아니라 메일 등에 포함되어 있는 파일, MS-word, Powerpoint 등의 오피스웨어 및 압축파일 등을 포함해야 한다. 검출된 개인 파일은 암호화를 통해 보호되어야 하기 때문에 암호화 강제 기능이 요구되며 암호화 파일은 공인 받은 암호화 포맷을 지원해야 한다. 소유권한이 없는 개인정보는 시스템이 삭제를 권고(alerting) 혹은 강제할 수 있어야 하며 사용자가 원하는 패턴(id/pwd 패턴, 키워드 패턴 등)을 추가적으로 등록할 수 있는 기능이 요구된다. 또한, 효과적인 정보보호를 위해서는 주기적 검색, 속도, 설치 및 삭제 용이성 등이 요구된다. 이러한 요구 사항을 요약하면 [표 1]과 같다.

만약 개별 PC 만을 대상으로 개인정보보호 시스템을

〔표 1〕 개인 컴퓨터용 개인정보 보호 시스템 요구 사항

항목	내용
개인정보 보관 검출	주민번호, 계좌번호, 여권번호, 핸드폰번호, 카드번호 등 개인정보를 식별할 수 있는 정보를 특정한 횟수(예: 5회)이상 포함한 파일을 찾을 수 있어야 한다.
패턴 추가 및 편집기능	사용자가 원하는 패턴(예: id/pwd 패턴, 키워드 패턴)을 추가적으로 등록하고, 새로 나온 패턴 등은 온라인으로 업데이트 되어야 한다.
파일 및 메일 분석기능	• 텍스트 파일뿐만 아니라 메일(OUTLOOK 포함)에 포함되어 있는 개인정보 또한 검색할 수 있어야 한다. • MS-word, Powerpoint, Excel, 훈글 등의 오피스웨어를 포함한 추가적인 포맷들도 지속적으로 지원되어야 한다. • 압축파일에 대한 검색기능과 다단계 압축파일에 대한 검색기능을 제공해야 한다.
암호화 강제기능	개인정보가 포함된 것으로 검출된 개인정보 보관파일은 암호화되어서 보관할 수 있도록 해야 한다. 암호화 파일은 인증받은 암호화 포맷을 지원해야 한다.
개인정보 삭제 강제기능	소유권한이 없는 개인정보는 삭제를 권고(alerting) 혹은 강제할 수 있어야 한다.
기타 기능	• 속도 및 성능: 대용량 데이터파일을 빠른 시간에 검색할 수 있어야 한다. • 주기적 자동 검색기능 • 설치 및 삭제 용이성 • Text 추출기능 • 파일 Password 분석기능

설계한다면 [표 1]에서 제시한 요구사항을 만족하는 시스템을 설계하는 것으로 충분할 것이지만, [그림 1]과 같이 다수의 PC로 구성된 기업 내부의 개인정보 보호를 목표로 한다면 추가적이 요구사항의 도출이 필요하다.



〔그림 1〕 기업용 개인 정보 보호 시스템 구조

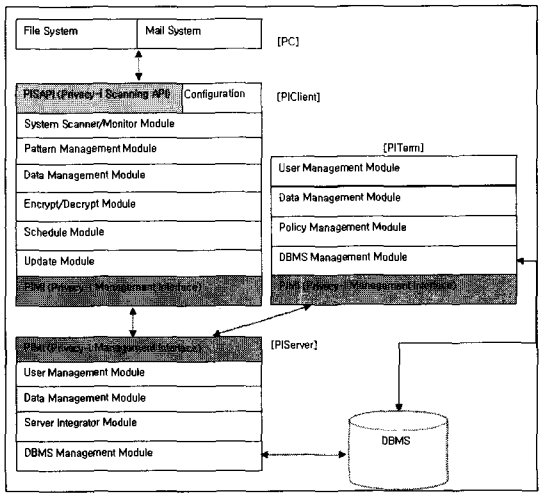
다수의 PC로 구성된 기업 정보 시스템 환경에서는 부서별, 유저별 권한과 개인정보의 중요도에 따른 관리 기능이 우선적으로 요구된다. 또한, 신규 파일과 변경된 파일들을 대상으로 개인정보가 포함되었는지를 상시적으로 모니터링 하는 기능도 요구된다. 부서별, 지역별 리포팅 기능도 필요하며 개인 정보의 중요도, 생성시기, 접근내역 등에 의한 상세한 리포트가 가능해야 한다. 예를 들면, 주민번호가 100건 이상 포함된 파일 중에서 생성 된지 1년 이상 지났으며 최종 접근 후 100일 이상 지체되었지만 암호화되지 않은 파일을 분류하여 리포팅 할 수 있어야 한다.

〔표 2〕 기업용 개인정보 보호 시스템 요구 사항

항목	내용
권한별, 개인정보중요도별 관리 기능	권한을 부여받은 유저외에는 개인정보 파일을 정해진 기간이상 보관하지 않도록 하는 등 역할과 개인정보의 중요도에 따른 보관주기/암호화강제/검사주기/리포팅 주기 등의 정책을 설정할 수 있어야 한다.
상시적인 모니터링 기능	신규 파일과 변경된 파일들을 대상으로 개인정보가 포함되었는지 확인할 수 있어야 한다. 정해진 시기(예: 실시간 혹은 주간)에 검사를 진행하도록 한다.
부서별/지역별 리포팅 기능	부서별/지역별 리포팅이 가능해야 한다. 파일은 개인정보포함 심각도와 생성시기, 최종 접근시기 등으로 분류해서 리포팅 되어야한다.

Ⅲ. 개인정보보호 시스템 (Privacy-i) 설계

본 장에서는 앞서 제시한 요구사항을 토대로 기업 내부의 개인정보 보호시스템 (Privacy-i)의 설계를 제시한다. Privacy-i 는 PC 단에서 저장된 개인정보 검출 및 보호 시스템을 구축할 수 있는 서비스를 제공하며 회사 또는 단체 내의 모든 기밀 정보를 중앙 집중적으로 관리하고 외부로 유출 되는 것을 방지한다. Privacy-i는 다수의 PC와 다수의 사용자가 사용하는 기업 환경에 적합하도록 설계되었으며 PIClient, PIServer, PITerm 의 세 가지 모듈로 구성된다. 전체적인 시스템 설계 아키텍처는 [그림 2]와 같다.



〔그림 2〕 기업용 개인 정보 보호 시스템 (Privacy-i) 아키텍쳐

PIClient 는 사용자 PC 에 설치되며 기본적으로 사용자가 자신의 컴퓨터 디스크 드라이버 내의 파일을 점검하고 관리하는데 사용된다. 또한 PIServer 의 통제를 받아서 사용자PC의 파일을 체크하고 해당 정보를 관리 서버에 보내어 통합 관리를 하도록 도와준다. 만약 사용자가 특정 패턴이 포함된 파일이나 감시 대상 파일을 이동 저장 장치에 이동/복사 하거나, 출력을 하려는 경우 이를 제한하거나 로그로 기록하고, PIServer 를 통해서 관리자에게 이 사실을 알리는 역할을 하게 된다.

PIClient에는 [표 1]에서 제시한 개인 컴퓨터용 개인정보 보호 시스템 요구 사항이 구현되었으며, 검색 및 모니터링 (System Scanner/Monitor Module), 패턴 검증 및 설정 (Pattern Management), 파일 및 검사 기록 관리 (Date Management), 암/복호화 (Encrypt/ Decrypt), 업데이트

및 예약 검사 (Update and Schdeuld) 모듈로 구성된다.

PIServer 는 각 사용자 PC에 설치된 PIClient 에게 정책을 내려주고 검사 로그를 수신하여 이를 기록하고 자료를 정리하는 등의 역할을 하는 중앙 관리 모듈이며, PIClient의 관리, PITerm 접속 관리, 로그 관리, 사용자 접속 관리, 보안 대상 관리 서버파일에 대한 감시, 사용자 PC의 관리 대상 파일 감시, 서버형 보안 시스템과의 연동 기능이 구현되었다.

PITerm 은 관리자가 PIServer 를 효과적으로 관리하기 위한 모듈이다. 관리자의 PC에서 PIServer 로 접속하여 정책을 설정하고 각 PIClient 를 통해 수집된 로그를 볼 수 있으며, 이러한 로그를 통하여 통계를 내거나 보고서를 만드는 작업을 하는 통합 관리 콘솔이다.

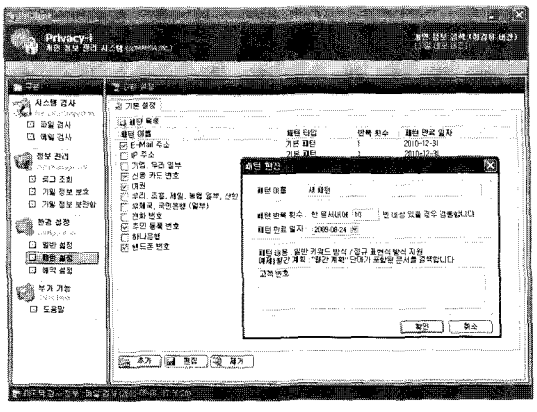
IV. 개인정보보호 시스템 (Privacy-i) 구현

본 장에서는 3장에서 제시한 아키텍처를 토대로 실제 구현된 개인 정보보호 시스템을 예시한다. 먼저 PC 내의 개인 정보 검출 기능을 살펴보면 다음과 같다.

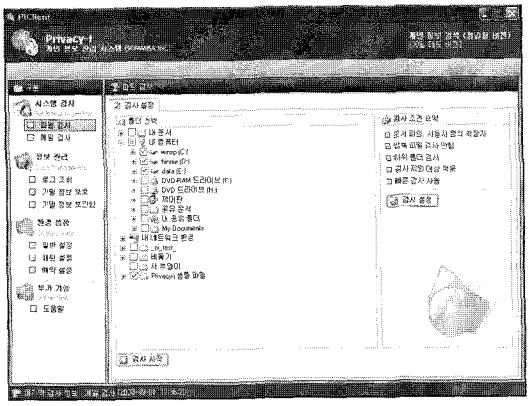
4.1 개인 정보 검출 기능 (파일 검사)

회사 내부의 PC를 대상으로 개인 사용자가 자신의 PC 내부의 개인정보를 검출한다고 하자. 먼저 검사할 패턴 정보를 리스트에서 선택하고 해당 항목을 체크한다. 새로운 패턴을 추가하고자 할 경우 "추가" 버튼을 눌러 패턴 반복 횟수와 패턴 만료 일자, 패턴 내용을 입력하여 추가한다.

상세한 검사가 필요할 경우 검사할 파일 종류와 압축



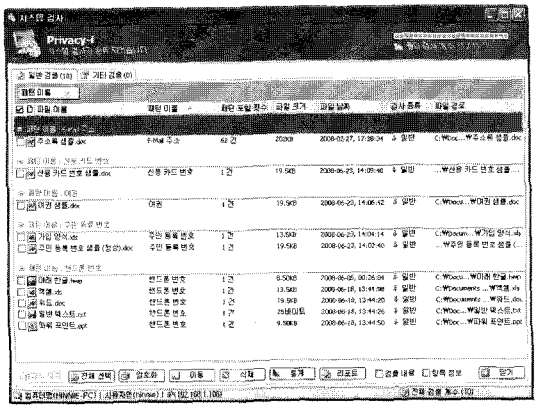
〔그림 3〕 개인정보 검출을 위한 패턴 설정 화면



〔그림 4〕 개인정보 검출(파일 검사) 시작 화면

파일 검사 여부 등을 설정할 수 있으며 개인 정보 패턴 설정과 환경 설정 구성을 마치면 검사할 대상 드라이버 또는 폴더를 설정한 후 "검사 시작" 버튼을 눌러 검사를 시작한다.

설정된 조건(검사 조건, 검사 대상)에 따라 개인정보가 포함된 파일을 검색하며 검사 진행 정도와 폴더 개수, 검사 중인 파일의 이름을 화면 상단에 표시한다. 검사가 완료되면 그림 5에서와 같이 검출된 파일 정보가 리스트에 표시되며 해당 파일에 대해 암호화, 이동, 삭제, 통계, 리포트 기능을 제공한다. 추가적으로 제공되는 검출된 항목의 정보 보기와 상세 보기 기능을 통해 검출된 내용을 상세히 확인할 수 있다.

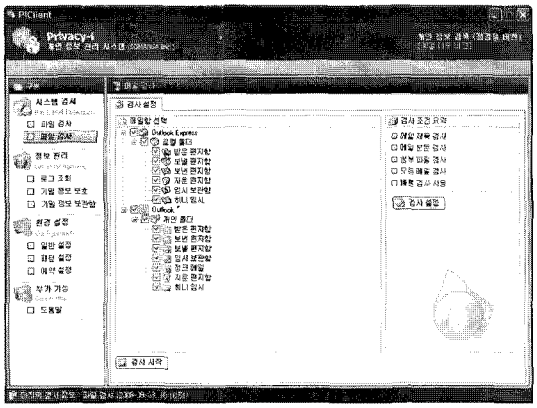


〔그림 5〕 개인정보 검출(파일 검사) 완료 화면

4.2 개인 정보 검출 기능 (메일 검사)

회사 내부의 PC를 대상으로 개인 사용자가 자신의 PC

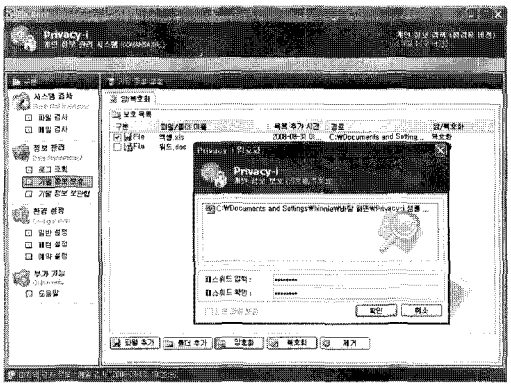
내부의 메일함에서 E-mail 내용이나 첨부 파일에 포함되어 있는 개인정보를 검출하고자 할 경우 OutLook Express와 OutLook의 메일 보관함에서 검사를 원하는 메일함을 선택한 후 파일 검사와 동일한 방법으로 검사를 수행한다.



〔그림 6〕 개인정보 검출(메일 검사) 시작 화면

4.3 개인 정보 관리 기능

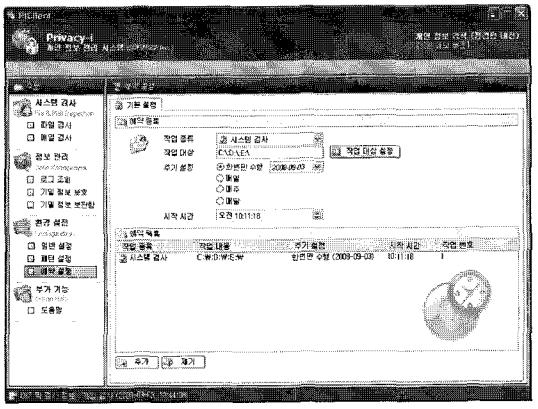
검출된 개인 정보의 관리를 위해 개인 정보가 포함된 파일에 대한 암호화/복호화 기능을 제공한다. 암호화 하고자하는 파일을 선택한 후 비밀번호를 입력하여 암호화를 수행한다



〔그림 7〕 암호화 수행 화면

4.4 스케줄링을 통한 주기적인 개인 정보 검출

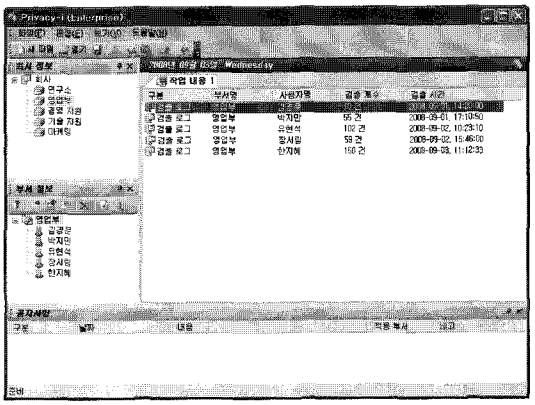
스케줄링을 통한 예약 작업을 통해 특정 시간 또는 주기적으로 개인 정보를 검출한다. 작업 종류, 작업 대상, 주기 설정, 시작 시간을 입력한 후 "추가" 버튼을 눌러 예약 작업을 등록한다.



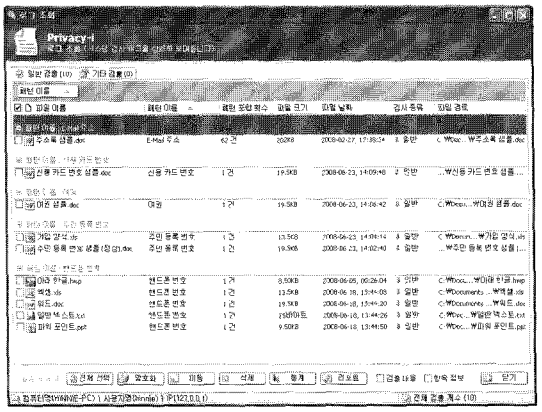
〔그림 8〕 개인 정보 검출을 위한 예약 설정 화면

4.5 중앙 통합 콘솔(PITerm)을 통한 개인 정보 관리

회사 내부의 PC를 대상으로 개인 사용자가 자신의 PC 내부의 개인정보를 검출한 결과를 검색한다고 하자. 먼저 그림 9에서와 같이 "회사 정보"에서 해당 부서를 클릭한 후 사용자 정보 리스트에서 검색하고자 하는 사용자를 선택한다. 해당 사용자의 검출 로그를 표시하는 로그조회 대화상자를 통해 검출 내용을 확인할 수 있다. 추가적으로 부서별/사용자별 검출 통계와 리포트 기능을 통해 중앙 집중적 관리가 가능하다.



〔그림 9〕 중앙 통합 콘솔(PITerm) 화면



〔그림 10〕 특정 사용자의 검출 로그를 보여주는 화면

V. 결 론

본 연구에서는 기업 업무 환경하에서 분산된 PC의 개인정보를 효과적으로 관리할 수 있는 시스템(Privacy-i)을 개발하였다. 이를 위하여 기업 내부 개인정보보시스템의 요구사항을 분석하고 이를 토대로 시스템을 설계를 제시하였으며 실제 개발을 통해 개인정보 보호 시스템을 구현하였다.

본 연구에서 개발된 Privacy-i는 DBMS나 파일서버와는 달리 기업 내부 정보의 외부 유출에 대한 위험성이 상대적으로 크다고 볼 수 있는 개인용 PC의 개인정보 보호를 목적으로 하여 개발되었으며, 실제 구현 사례를 통해 효과적으로 개인정보보호를 실현할 수 있는 시스템을 제안하였다.

본 연구를 통해 개인 정보 유출에 대한 관리 책임을 지고 있는 관리 주체가 PC에 산재하는 개인 정보보호의 필요성을 인식하고 개발된 시스템의 적용 함으로써 기업 내 정보 보안 수준을 높이는 계기가 될 것을 기대된다.

참고문헌

[1] 강성철, "개인정보보호 실태와 정책방향", *한국 인터넷 정보학회*, 1(2), pp.54-58, 2000,

[2] 김윤정, 방혜미, 김명주, "유비쿼터스 컴퓨팅 환경에서 여행 정보 제공 시나리오 및 개인 정보보호 지원 기술 연구", *정보보호학회지*, 16권, 2호, pp.46-52, 2006.

[3] 김한섭, 배수정, 연현정, 황윤철, 이상호, "개인정보 보호를 위한 전자메일 주소 추출 방지 기법", *한국정보과학회 가을 학술발표논문집*, Vol,29, No,2, pp.451-453, 2002.

[4] 남택용, 장종수, 송승원, "유비쿼터스 환경에서의 개인정보 보호 기술", *전자통신동향분석*, 20권, 1호, pp.54-62, 2005.

[5] 문형진, 이건명, 이영진, 이동희, 이상호, "암호기법을 이용한 정책기반 프라이버시보호시스템설계", *정보보호학회논문*, 16권, 2호, pp.33-43, 2006.

[6] 송유진, 이동혁, "개인정보 하이프사이클에 따른 프라이버시 보호 프레임워크", *정보보호학회지*, 16권, 4호, pp.77-86, 2006.

[7] 송유진, 이동혁, 남택용, 장종수, "유비쿼터스 환경에서 개인정보보호의 기술동향", *정보보호학회지*, 16권, 3호, pp.75-86, 2006.

[8] 임태훈, 오상훈, 한국데이터베이스진흥센터, "개인정보보호정책", 제7회 *한국정보관리학회 학술대회 논문집*, 2002.

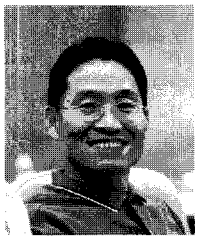
[9] 홍승필, 이철수, "유비쿼터스 컴퓨팅 환경내 개인정보보호 프레임워크 적용 방안", *정보보호학회지*, 16권, 3호, pp.157-168, 2006.

[10] 홍승필, 장현미, "e-Business 환경 내 개인정보 보호 메커니즘적용 방안", *한국 인터넷 정보학회*, 9권, 2호, pp.51-59, 2008.

〈著者紹介〉

박 중 환 (JoongHwan Park)
2000년 2월 : 명지대학교 기계공학과 졸업
2000년 ~ 2006년 : (주)하우리 선임 연구원
2006년 ~ 현재 (주)소만사 선임 연구원
관심분야 개인정보보호, 콘텐츠보호

조 남 욱 (Nam Wook Cho)
1994년 2월 : 서울대학교 산업공학과 졸업
1996년 2월 : 서울대학교 산업공학과 석사
2001년 5월 : Purdue대학교 산업공학과 박사
2001년 ~ 2002년 : Lucent Technologies, USA, Engineer
2003년 ~ 2004년 : 삼성SDS 책임컨설턴트
2004년 ~ 현재 : 서울산업대학교 산업정보시스템공학과
관심분야: 비즈니스 프로세스 관리



이 기 혁 (Lee Gi Hyouk)
정회원
1991년 2월 : 한양대학교 공학석사
2008년 3월 ~ 현재 : 건국대학교 공학박사 과정중
1994년 5월~현재 : SK Telecom (주)정보기술연구원 재직중
관심분야 : 정보통신공학, 정보통신정책분야,정보보호학,개인정보보호공학

최 일 훈 (Il-Hoon Choi)
정회원
1995년 2월 : 서울대학교 계산통계학과 졸업
2006년 8월 : 연세대학교 공학대학원 산업정보경영 졸업
1995년~1998년 : LG소프트
1998년~2000년 : TIBCO (미, 실리콘밸리)
2000년~현재 ㈜소만사
관심분야 : 개인정보보호, 콘텐츠보호