

개인정보 유출 방지를 위한 명함 자동화 설계 연구

박종열* · 박대우*

*호서대학교 벤처대학원

Cards Automated Designed Research for Personal Information Leak Prevention

Jong-Youel Park* · Dea-Woo Park*

*Hoseo Graduate School of Venture

E-mail : parkjy4567@daum.net · prof_pdw@naver.com

요 약

본 연구는 명함 제작할 때 인쇄 기획사 컴퓨터에 명함신청 정보가 파일로 저장되어 있어 개인 정보 유출의 위험성이 항상 존재한다. 명함신청 파일에 들어가는 조직정보, 이름, 휴대폰번호, 이메일 주소 등의 정보는 암호화 되어 있지 않아 쉽게 접근이 가능하다. 이 연구에서는 명함신청의 프로세스를 자동화 하여 명함신청 파일에 들어가는 정보를 암호화 하고 명함 신청 프로세스를 간소화 하여 담당자의 업무를 최소화 하고 인쇄소와 직접적으로 연계하여 명함 인쇄 완료 후에 인쇄 파일을 자동으로 삭제하는 방법을 연구 한다.

ABSTRACT

This paper proposed have been the business card information to the computer when creating business card printing agency saved to a file, there is always the risk of personal information leakage. Application file organization information into the card, the name, phone number, email address information, such as is capable of easily accessible because it is not encrypted. This paper proposed it encrypts the information entered on the Business Card application file to automate the process of the card application and simplifying the business card application process minimizes the work of staff and linked directly to the print shop how to automatically delete the print file after the completion of business card printing and research.

키워드

Card Automatic, Information Disclosure, Personal Information

I. 서 론

우리나라 대표 기업인 KT 홈페이지 해킹 및 개인정보 유출 사건이 2014년 3월 25일 발생하였다[1]. KT의 개인정보유출 해킹사고는 해커가 정상적으로 KT홈페이지에 로그인하여 정상로그인 정보 값(쿠키)을 전송하여 로그 분석 툴인 파로스 프로그램일 이용하여 정상 로그인 정보 값(쿠키)와 타인의 고객센터 서비스 계약번호로 KT에 값을 변형하여 개인고객정보를 엑셀 파일로 다운로드한 사례이다. 이와 비슷하게 기업 및 개인이 명함을 제작시 기업의 정보와 개인의 메일 아이디, 이름,

휴대번호, 이메일 등의 개인정보가 유출되고 있는 실정이지만 별다른 대책을 세우지 못하고 있는 실정이다. 일반적으로 명함 제작 의뢰시 인쇄 기획사 PC에 파일 형태의 명함 신청 회사의 개인정보가 저장되어 있어 유출 될 수 있는 위험에 항상 존재하고 있는 실정이며 이를 해결할 수 있는 방법론이 현재는 없는 실정이다.

국가정보원 산업기밀센터에서 발표한 통계자료에 따르면, 최근 5년간 발생한 국내 핵심기술 유출 사건은 209건이며 이중 60.8%가 전직직원, 19.6%가 현직원원에 의해서 발생되었다. 유출 경로로는 카드형 USB, 외장하드, 스마트폰 등이 사

용되었다[2].

본 연구에서는 개인정보 유출을 방지하기 위한 데이터베이스의 암호화 기술, 네트워크의 암호화 처리 기술, 명함 자동화 시스템의 자동 처리 기술을 설계하는 방법을 제시한다.

본 연구의 구성은 다음과 같다. 제 2장에서는 개인정보 유출 방지를 위한 명함 자동화 솔루션을 설계 하기 위하여 솔루션 개발 기술에 대한 선행연구를 검토하고, 제 3장에서는 개인정보 유출 방지를 위한 명함 자동화 시스템의 구성 및 인터페이스 관련된 사항을 설명한다. 제 4장에서는 명함 자동화 솔루션 설계에 대하여 설명하고, 제 5장에서는 본 논문의 결과를 요약하고 향후 연구방향을 제시한다.

II. 관련연구

개인정보 유출방지를 위한 보호 기술은 개인정보 침해기술인 PIT (Privacy Invading Technology) 와 개인정보 강화 기술인 PET(Privacy Enhancing Technology) 로 분류할 수 있다. PIT유형에는 모바일 장치의 GPS를 이용한 개인의 위치 자료 취득, PC와 태블릿PC, 스마트폰등 쿠키정보를 이용하여 정보를 확인하고 개인정보를 취득하고 프로파일링 기술을 응용하여 또 다른 개인정보를 취득하는데 이를 안전하게 보호 할 수 있는 기술이 요구된다[3][4].

개인정보를 강화하는 기술인 PET는 개인정보에 관한 수집을 최소화 시키고 개인정보의 익명화, 개인정보 데이터에 대한 접근제어 제공 및 사용자에 의한 직접적인 개인정보 통제는 물론 데이터 추적 등 다양한 개인 정보 보호 기술을 말한다[5].

본 연구에서는 개인정보에 대한 철저한 암호화를 통하여 개인정보 유출에 따른 문제점을 해결하고 인쇄소와 기업과 IT기술을 융합하여 서비스가 진행 될 수 있게 설계하고 인쇄소는 자동화된 솔루션을 이용하여 신청된 명함을 자동 처리하고 기업은 업무 프로세스를 간소화 하고 기존 방법에서 유출 될 소지가 높은 개인정보를 보호하는 방향의 명함 자동화 솔루션을 설계하는 방법을 연구한다.

III. 명함 자동화 설계 방안

3.1 개인정보 유출 방지를 위한 설계 방안

개인정보 유출 방지를 위한 명함 자동화 시스템은 개인 및 임직원이 명함을 신청하면 기업의 관리자가 이를 승인하고 명함 자동화 시스템인 인쇄 관리 서버에서 자동으로 인쇄소에 발주가 들어가고 인쇄가 완료 되면 자동으로 주문한 명함의 내용은 삭제를 할 수 있게 시스템을 설계한다.

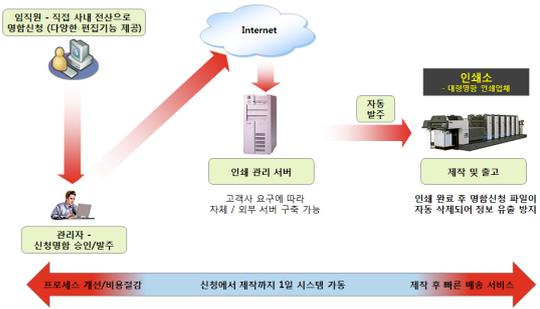


그림 1.명함 자동화 구성도

3.2 명함 자동화 시스템의 간결화 설계 방안
회사에서는 업무 프로세스를 간결화 하고 인쇄소는 자동으로 만들어진 시스템을 이용하여 명함 자동 처리를 하고 시스템에서는 자료를 암호화 하고 완료되면 정보를 자동 파기하도록 설계한다.



그림 2.명함 자동화 업무 흐름

IV. 명함 자동화 구현 방안

기존의 명함 처리 방식은 기존의 복잡한 처리 과정과 기획사 및 인쇄소에서 조직 및 개인정보가 유출될 위험이 있으며 수기 신청으로 인한 누락 위험, 담당자의 효율적 업무수행이 곤란하고 인사발령 및 조직변경 등 대량 제작 시 업무과다 등 여러 가지 문제점들이 노출되고 있는 실정이다.

명함 자동화 시스템은 기업에서 업무를 간결화 하고 개인별 신청 및 승인만 하면 자동화된 시스템을 이용하여 인쇄소에 명함 신청이 완료 되어 바로 인쇄작업에 착수 하고 인쇄가 완료되어 발송 처리가 완료 되면 자동으로 신청되었던 명함 파일은 자동으로 삭제할 수 있게 구현한다.

V. 결 론

개인정보 유출을 방지하기 위한 명함 자동화 시스템은 기업에서는 업무의 효율성을 높이고 담당자는 업무량을 감소 할 수 있으며 관리가 용이해지고 개인정보 유출에 대한 걱정을 하지 않아도 된다. 인쇄소는 별도의 개인정보를 관리하지 않고 자동 시스템에서 명함을 인쇄하고 배송 함으로써

업무가 간결하고 제작기간이 단축되고 대량 생산이 가능하며 전국적인 명함 처리가 가능해지며 인쇄가 완료 되면 자동으로 개인정보를 파기하여 기업, 인쇄소 모두 개인정보 보호에서 안전할 수 있는 방법을 제시하였다.

향후연구로는 명함 자동화 시스템 설계를 기반으로 실제 구현하는 모델이 필요하고 명함 자동화 시스템에서 사용자가 직접 명함을 수정하고 보정 할 수 있는 시스템 연구와 명함 이외의 인쇄가 필요한 항목들을 추가하여 신청 할 수 있는 시스템 연구가 필요하다.

참고문헌

- [1] Yonhapnews, “KT 개인정보 유출 해킹사고 개요”, http://www.yonhapnews.co.kr/photos/19910_00000.html?cid=GYH20140325000900044&from=search
- [2] NIS, “industry confidential protection center Industry and security information knowledge spill statistics“, <http://service4.nis.go.kr/servlet/page?cmd=preservation&menu=AAA00#.U4k8c3lZp9A>
- [3] 최병훈, “웹 환경의 개인정보보호 시스템 설계에 관한 연구,” 석사학위논문, 동국대학교, 2010년 2월
- [4] 정영만, 이창훈, 정재욱, 원동호, “SNS 상에서 개인 정보 보호를 위한 Paillier Encryption Scheme 적용 기술 제안,” 한국정보보호학회 하계학술대회 발표집, 22(1), pp. 120-123, 2012년 6월
- [5] G.W. van Blarckom, J.J. Borking, J.G.E.Olk, “Handbook of Privacy and PrivacyEnhancing Technologies : The case of Intelligent Software Agents,” PISA, pp.33-53, May. 2003.