Journal of Digital Convergence
Vol. 16. No. 10, pp. 235-241, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.10.235

출력물 보안 관리 시스템을 위한 인터페이스 구축

한정수*, 김귀정
백석대학교 정보통신학부 교수

Interface Construction for Printout Security Management System

Jung-Soo Hon*, Gui-Jung Kim
Division of Information Communication, Baekseok University, Professor

요 약 출력물관리 시스템은 출력시 수집된 출력 로그 내에 개인정보(주민번호, 카드번호)가 존재하는지 패턴을 분석하여 사용자에게 경고 메시지 팝업 전달, 인쇄 강제 종료, 관리자에게 메일 발송 및 별도 로그 관리 기능을 갖추어야 한다. 인증 관리 역시 사용자 PC에 Agent를 설치하여 등록되어 있는 사용자만 프린트가 가능하며, 사용자 정보에 따라 작업이 허가되거나 거절될 수 있도록 제한 기능을 갖추어야한다. 또한 복합기로 프린트/복사/스캔 사용 시 ID카드 인증 후 문서 출력 및 복합기를 사용할 수 있으며, ID카드 미사용시 디바이스에 ID/PW를 입력 인증 후 복합기를 사용할 수 있도록 구축해야한다. 본 연구에서는 기존의 출력물 보안 방법들 보다 더욱 우수한 기술을 갖추고 있는 보안 업체인 (주)와우소프트와 공동으로 인터페이스를 개발하여 기록물관리 시스템을 위한 인터페이스들을 구축하였다. 또한 출력물관리를 위한 필요한 기본 기능들의 인터페이스를 설계하였으며 이를 바탕으로 출력물관리 시스템 구축에 기여하였다.

주제어 : 출력물, 보안, 스토리지, 복합기, 인터페이스, 권한관리

Abstract The printout management system should analyze the pattern of existence of personal information (resident number, card number) in the output log and users should be provided with functions such as warning message pop-up, forced printing termination, mailing to administrator, independently logs management. Authentication management can also be performed only by registered users by installing an agent on a user PC, and it should have a restriction function to permit or deny work according to user information. In addition, when printing/copying/scanning using this equipment, it is possible to use document printing and multifunction copier after ID card authentication and ID/PW should be input to device when ID card is not used. In this study, we developed these interfaces with WOWSOFT co., Ltd, a security company that has better technology than the existing printout security methods, to construct the printout management system. Also we designed the interface of basic functions necessary for printout management and contributed to the establishment of printout management system.

Key Words : Printout, Security, Storage, Printer/Scanner, Interface, Authority management

1. 서론

출력물 보안(printout security)이란 기업 내부에 연결된 PC 에서 인쇄되는 모든 내용(사용자, IP, 인쇄매수, 인쇄원본, 개인정보)을 남기고 각각의 내/외부에 연결된 프린터에 모든 클라이언트를 원격으로 통제/관리함으로써 기업의 인쇄 시스템 관리를 일괄적으로 관리감독 할 수 있어 시스템의 보다 효율적인 통제가 가능한 시스템을 말한다. 출력물은 체계적으로 관리해야하는 기업정보의 자산이다. 정보 유출자 현황은 전직 직원에 의한 유출이

* Corresponding Author : Jung-Soo Han(jshan@bu.ac.kr)
Received September 8, 2018
Revised October 5, 2018
Accepted October 20, 2018
Published October 28, 2018

56.2%, 현직 직원에 의한 유출이 24.6%로 내부자에 의한 유출이 전체의 80% 이상이며, 유출방법에 있어서도 출력물에 대한 유출이 약 40%로 이메일에 의한 유출인 21%보다 많은 비중을 차지하고 있는 것이 현실이다[1].

따라서 기업들의 출력비용은 반드시 관리해야 할 경상경비로 취급되고 있다. 개인이 취급하는 정보량 증가, 프린터 보급률 및 속도의 증가, 그래픽 위주의 문서형태로 종이 문서의 출력과 출력비용은 매년 증가하고 있다. 기업 내 유통되는 문서 중 41%가 내용 검토 및 교정, 업무정보 등 참고용이며 23%가 회의자료, 업무공지 등 일회용으로 사용되고 있다. 따라서 관리되지 않는 종이문서는 전체의 64%를 차지 하고 있다[2-5].

내부자에 의한 정보유출사고, 특히 인쇄 출력물을 통한 정보 유출이 심각하여 DRM 등을 통해 정보보안과 병행하여 출력 보안을 하고 있으나 실효성이 적다. 또한 다양한 프린터에 대하여 기계 변경 없이 출력 보안 적용이 어렵고, 기업내부의 주요문서 출력 및 복사, 팩스 전송을 통한 산업기밀 유출 방지를 위해 다양한 방안이 동원되고 있으나 대부분 사고 발생 후 유출경로 추적에 중점을 두고 있어 그 대처 방안이 주요 연구되고 있다[6-8].

본 논문에서 제안한 연구는 빠른 스캔기능을 통한 종이문서 전자문서화, 종이문서 보관을 위한 공간 및 시간 절약, 종이문서 관리의 중앙집중화를 통한 효율성 증가, 종이문서 원본증명을 통한 보안 및 유출 방지, 정부 기록물 가이드라인 및 법규 준수 등을 활용한 출력물 보안 시스템을 설계하였다.

2. 관련연구

2.1 출력물 보안 종류와 장단점

현행 전자문서 유출방지를 위한 대응책이라 도입하고 있는 방법은 문서보안 솔루션, DLP 솔루션, 문서중앙화 솔루션, 개인정보보호 솔루션 등의 경우 각 개발사가 상이하여 도입 전후 관리 및 보안, 구축 및 유지보수 비용 등 많은 문제점이 대두되고 있다. 문서암호화(DRM)는 문서단위의 암호화 기능을 어플리케이션을 통하여 진행하는 방법으로서 어플리케이션 및 OS에 영향이 많을 뿐 아니라 키값 관리가 어려운 단점이 있으며, 구축 및 유지보수 비용이 크다[9].

온/오프라인 유출통제(DLP)는 PC기반 유출경로를 통제하는 API 방식으로 저장매체/네트워크/프린트 등을 모니터링 하는 방식으로 사용된다. 그러나 이 방식은 다양한 유출경로통제에는 한계가 있으며, 사후 모니터링 개념으로만 사용되고 있다. 또한 로그관리와 조회의 어려움을 갖고 있다. 문서중앙화 방식은 PC내 로컬영역 저장을 금지하며 로컬저장통제 API와 네트워크API를 이용한 중앙저장소를 활용하는 것이다. 그러나 이 방식은 네트워크 단절시 업무가 중단되며, 전체 네트워크 속도저하 문제가 있으며, 외부 해킹 등으로 대규모 피해가 발생하는 단점이 있다[10].

Table 1. Printout Security Problems

Item	Method	Problems
Log Record	How to record and manage the history of document viewing, printing, and copying	Accessor tracking is possible in an accident, Not be blocked in advance
Pass Word	The password of the person in charge is needed for document viewing, outputting, and copying, and the method of focusing on security before the accident	It helps to prevent security accidents of outsiders, More then 80% of technology leak is a former and present position
PW info. output	When outputting and copying, it can encrypt the information such as the date and time at the top and bottom of the document, and identify the leakage path in an accident	Due to industrial secrets, pre-accident actions are important. It's impossible to recover the damage in case of an accident.
Non-copyable special paper	Use special paper to prevent copying of the original contents	In addition to not being able to copy necessary work, it can not prevent the leak of the original

기타 전자문서 보안 제품군에는 기능별 보안 통제를 이용하는 프린트 워터마킹, 개인정보검색 및 통제, 모바일 오피스 보안, PC업무영역 가상화 통제, 화면캡처 방지, 문서 2차 유통 통제 등이 있는데 이들은 선택적 구축이 용이하지만 타 솔루션과의 연계가 불가능하며, 운영상 통합보안관리의 어려움이 있어서 기업환경을 고려하여 도입해야 한다. Table 1은 출력물 보안의 문제점을 보여주고 있으며, 출력물보안의 필수 기능은 Table2에 4가지 기능으로 정리할 수 있다[11,12].

Table 2. Printout Security Required Function

Function	Contents
Watermark Edit & Manage	Support various watermarks such as logo, image, output information (id, time, IP). Provide an editor that allows to specify the slope, density, and location of the watermark.
History management	Manage the output history in image or text form and check the original. It is possible to trace output by various history management such as document print date and time, outputter, printer info.
Various printer support	Support all printer models that support various printer drivers.
Management function	Support output-policy, user-management and various history management with administrative web(document security management

2.2 종이 기록물 전자문서화 및 보안관리 폐기

국가기록원은 기록관리업무 중 표준화 현황을 제시하고 있다. 기록관리 표준은「기록물관리 표준화 업무 운영규정」(국가기록원 훈령 제127호, 2017.5.17.개정)에서 규정한 적용범위에 따라 국가표준과 공공표준으로 구분되어있다. 기록물 평가/폐기 절차는 비전자 기록물의 폐기를 위해서 기록물에 포함되어 있는 보안사항, 개인정보 등이 유출되지 않도록 기관 내 파쇄 후 반출을 원칙으로 하고있다. 파쇄는 기록물에 포함되어 있는 내용 판독이 불가능하도록 세절하여야 한다. 기관 내 파쇄가 불가능하여 대상 기록물을 원형 그대로 반출 후 파쇄 또는 용해 처리해야 하는 경우에는 반출 또는 용해 처리 과정에서 폐기 대상 기록물이 유출되지 않도록 해당 공공기간의 직원 중 담당자를 지정하여 폐기 과정을 관리/감독 하여야 한다[13,14].

비전자기록물 폐기 방법은 파쇄와 용해로 진행된다. 파쇄는 기록물 세절 시 보안은 종이가 얼마나 잘 세절되는가에 달려 있으므로, 보안사항, 개인정보 등 민감한 기록은 교차 세절을 통해 내용판독이 불가능하도록 해야 한다. 용해는 용해된 종이가 섬유 구성분을 감소시키므로 제대로 처리하면 매우 안전한 폐기 방법이다.

2.3 기존 출력물 보안 기술

일반적으로 출력물 보안 · 관리 솔루션은 특정 어플리케이션이나 프린터 드라이버에 제약 없이 회사 내 모든 사용자 PC에서 출력되는 출력물에 대해 워터마크를 삽입하고 출력로그 및 원본이미지를 저장/관리하여 중요문서가 외부에 유출될 경우 최단 시간 내에 사용 출처 및 책임 추적을 하기 위한 솔루션이다. 출력물 로그관리에 있어서 사용자의 출력로그는 인쇄정보, 시스템 정보, 원본 이미지, 원본 텍스트를 로깅하여 관리자 툴에서 다양한 검색 조건으로 모니터링하는 방식이다. 출력물 통계관리는 로깅된 출력 로그 정보를 바탕으로 사용자별/부서별/프린터별 또는 기간별로 다양한 출력 통계 데이터를 제공하여 관리자가 손쉽게 출력물 현황을 파악 할 수 있도록 지원한다. 가시적 워터마크는 출력물에 회사CI, 소유권 정보, 출력자 정보 등을 원본 문서에 포함시켜 함께 출력하도록 하여 종이문서의 불법 유출을 사전에 방지하고, 출력자 실명제 확보를 통하여 정보유출을 방지하는 것이다. 개인정보 패턴정보는 문서 출력 시에 개인정보(주민번호, 신용카드번호 등) 패턴이 최초 발견된 경우, 출력을 한 사용자에게는 경고 메시지의 표시와 강제 종료, 관리자에게는 실시간으로 개인정보 문서 출력에 대한 내용의 메일 메시지를 통보. 개인정보 출력한 문서는 출력물 모니터토링 서버에 로그를 저장하여 관라자가 관리하도록 한다[15-17].

또다른 보안 기술은 시스템은 출력물 내에 개인정보를 실시간으로 모니터링하고, 개인정보가 검색된 출력물 인쇄를 차단하여, 출력물을 통한 개인정보 유출을 원천적으로 방지하는 출력물 개인정보보호 솔루션이다. 이는 출력 후 Web 또는 App을 통해서 중요 정보의 출력 인증으로, 출력물 방치로 인한 개인정보의 유출 및 유실의 가능성을 제거하여 안전한 출력물 유통 환경을 제공 및 다양한 제조사가 생산한 출력장치와 완벽하게 호환되어 출력물 통합 관리가 가능하고, 인쇄 절감 관리 기능까지 제공하여 운영 비용 절감 효과까지 기대할 수 있는 기술이다[18].

이 기술에 필요한 기능은 Fig. 1이 설명하고 있다. Pull Printing 기능은 본인 인증을 스마트폰 등으로 할 수 있고, 원하는 시점/원하는 장비에서 출력할 수 있으며, 대기시간이 지나면 출력 자동 취소된다. 이는 프린터 벤더나 종류에 상관없이 Pull Print 기능을 지원해야한다. 보안정책 관리 기능은 오프라인 로그인 유효기간, 로그전송 옵션, 로그 전송 옵션, 텍스트 및 이미지 로그 전송 옵션, 워터마크 사용자 선택 옵션 등을 설정해야한다. 인쇄물 패턴 검사 기능은 사내에서 출력되는 문서들에 대해 패턴 검출 기준을 설정하여 중요정보를 포함한 문서를 관리하는 기능이다. 중요정보검출문서 출력 제어 기능은

중요 정보 검출 기준에 따라 인쇄허용, 차단, 결재 후 인쇄 기능, 마스킹 시 인쇄 허용, 결재 후 마스킹 적용/미적용 등 옵션 제공, 출력 결재 요청 및 출력 결재 승인 완료에 대한 실시간 알림 기능 제공하는 것이다. 끝으로 인쇄 승인 기능은 모든 인쇄물에 대한 출력시 결재 신청 및 승인 가능, 출력시 워터마크 해제 신청 및 승인 가능, 특정 애플리케이션에서 출력시 인쇄 신청 및 승인 가능, 일반 문서 혹은 보안 문서 출력시 인쇄 신청 및 승인 가능 등의 기능들을 지원하는 기술이다[18,19].

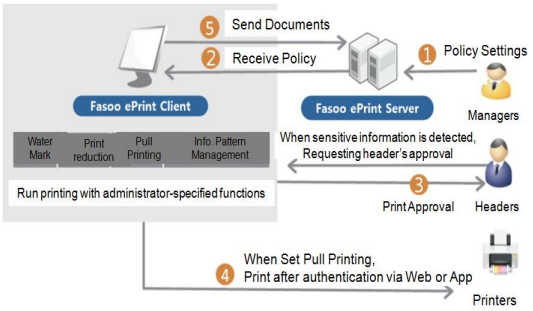

Fig. 1. Security System Process

3. 출력물 보안 시스템 인터페이스 설계

본 논문에서는 출력물 보안 시스템을 위한 인터페이스를 설계하였다. Fig. 2에서처럼 출력물 관리는 크게 기록물관리, 통계, 운넝관리의 3가지로 구성하였으며, 기록물 보관함, 통계조회, 권한관리, 메뉴관리, 스토리지관리 등으로 구성하였다. 특히 운영관리는 기록물 관리를 위한 핵심요소가 된다. 권한관리는 기록물들을 일기, 쓰시 등 권한을 부여할 수 있도록 하여 그 권한을 해당자에게 줄 수 있다. 사용자 관리는 등록된 사용자들을 관리하며 보안에 필수 요소가 된다. 이 시스템을 구축하기 위한 기본 인터페이스를 설계하였다.

Fig. 3은 폴더 생성기 이다. 폴더 위치는 탐색기에서 폴더를 생성할 부모 폴더의 위치를 선택하고, 새로 생성할 폴더의 이름을 입력하여 생성되는 인터페이스이다. 폴더명을 빈값으로 설정하여 생성할 수는 없다. 또한 부모 폴더에 동일 폴더명을 가진 폴더를생성할 수 없고, 폴더명에 특수문자 (< >: " / ! ? *) 를 포함할 수 없다. 이름 규칙에 어긋나지 않게 입력하면 폴더가 생성된다. 문서 생성 form은 탐색기에서 문서를 생성할 부모 폴더의 위치를 선택하여, 새로 생성할 문서의 이름을 입력하여 새로운 문서를 생성할 수 있다.

Fig. 2. Security System Structure

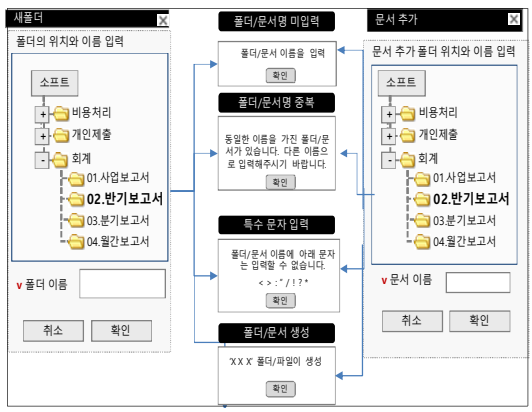

Fig. 3. Folder Creation Form Interface

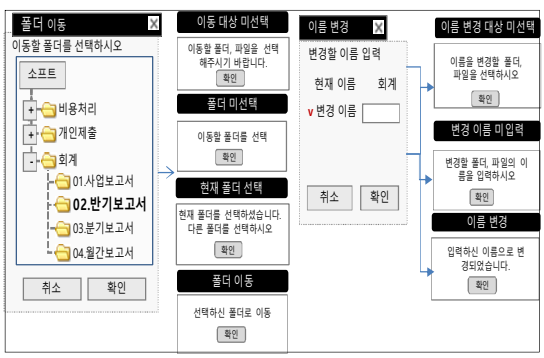

Fig. 4. Folder Moving Form Interface

Fig. 4의 폴더 이동 form은 폴더 선택 시 폴더의 이름의 폰트가 'Bold' 로 변경되도록 하였다. 이동할 폴더를 선택하지 않거나 현재 폴더를 선택한 경우에는 이동시킬

수 없고, 선택한 폴더로 이동이되면 팝업 창이 닫히도록 하였다. 이름 변경 form은 변경할 폴더, 파일을 선택하여 편경이 가능하도록 하였다.

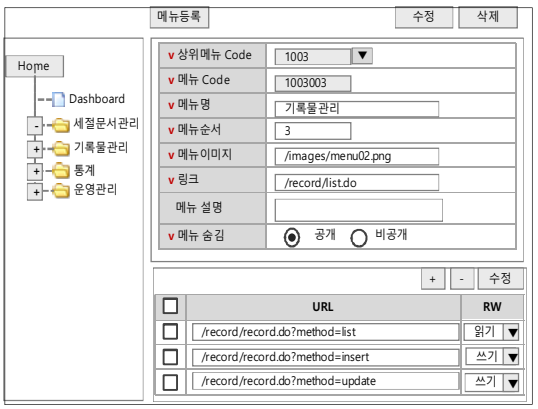

Fig. 5. Menu Management Form Interface

Fig. 5의 메뉴관리는 메뉴 리스트로 등록된 메뉴가 트리구조로 생성 되도록 하였고, 메뉴의 상세 데이터를 이용해 등록, 수정, 삭제 작업이 가능하도록 하였다. 메뉴 URL은 선택한 메뉴에 속한 URL의 리스트가 '+'가 하위 URL Row 가 생성되며, '-' 는 URL Row의 첫번째 내용의 체크박스가 체크된 Row 삭제되며, RW는 메뉴의 읽기, 쓰기 권한을 줄수 있도록 하였다. 메뉴등록은 현재 선택된 메뉴의 하위에 추가된다. 이때 필수 필요 값은 메뉴 code(상위메뉴 값으로 저장), 메뉴명, 메뉴순서, 메뉴이미지, 링크, 메뉴 설명, 메뉴 숨김여부로 결정되고, 수정기능은 등록된 메뉴의 데이터를 변경가능하다. 이때 필요 값은 상위메뉴 code, 메뉴 code, 메뉴명, 메뉴 순서, 메뉴이미지, 링크, 메뉴설명, 메뉴 숨김 여부 등의 옵션을 갖도록 하였다. 메뉴의 다른 메뉴의 하부메뉴로 변경시 상위메뉴로 변경 가능하도록 하였다. 삭제 역시 등록된 메뉴를 삭제하기 위해서는 메뉴 Code를 이용하며, 팝업창에서 메뉴명은 상위메뉴 Code를 이용하면 된다.

Fig. 6의 스토리지추가 form에서 경로는 스토리지로 추가할 경로를 텍스트 박스에 직접 입력하면 경로에 해당하는 폴더가 존재 여부 확인 결과와 디스크 사용 용량 관련 정보를 화면에 표시할 수 있도록하였으며, 경로를 입력 후 추가할 스토리지 영역 정보 확인하면 스토리지가 추가된다. 경로확인은 스토리지로 추가할 경로를 입력하면 스토리지 정보(전체 용량, 사용율)를 획득하여 팝업창에 표시될 수 있도록 하였다. 스토리지관리는 4가지 방식으로 기능을 설계하였다. '경로 확인'을 한번도 선택하지 않은 상태에서 '확인'을 선택한 경우, '경로 확인'을 선택하여 전체용량 사용율이 표시된 이후 '경로' 항목에 사용자가 입력한 값을 변경 후 '확인'을 선택한 경우, '경로 확인'이나 '확인'을 선택한 시점에 입력한 경로의 파티션이 삭제되었거나 쓰기 권한이 거부된 경우의 4가지로 스토리지추가 관리할 수 있는 기능을 설계하였다.

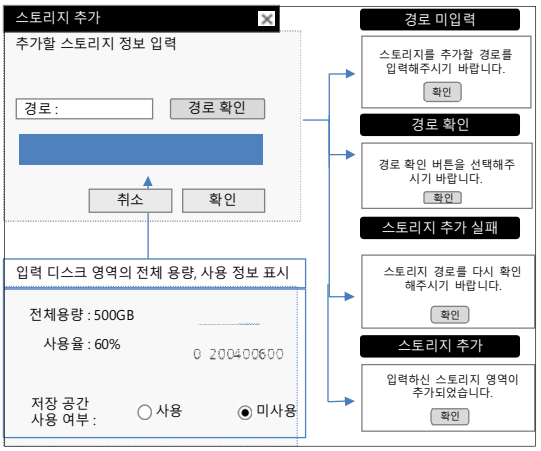

Fig. 6. Storage Addition Form Interface

일시	전체 용량 (6TB)	e:₩ (2TB)	f:₩ (2TB)	g:₩ (2TB)
2018년01월	4239.36 GB (69%)	1392.64 GB (68%)	1433.61 GB (70%)	1413.12 GB (69%)
2018년02월	3502.08 GB (57%)	1126.40 GB (55%)	1187.84 GB (58%)	1187.84 GB (58%)
2018년03월	3809.28 GB (62%)	1228.80 GB (60%)	1290.24 GB (63%)	1290.24 GB (63%)
2018년04월	3317.76 GB (54%)	1064.96 GB (52%)	1146.88 GB (56%)	1105.92 GB (54%)
2018년07월	3256.32 GB (53%)	1024.00 GB (50%)	1003.52 GB (49%)	1228.80 GB (60%)
2018년08월	2949.12 GB (48%)	921.6 GB (45%)	1024 GB (50%)	1003.52 GB (49%)
2018년09월	3133.44 GB (51%)	962.56 GB (47%)	1085.44 GB (53%)	1085.44 GB (53%)
2018년10월	2641.92 GB (43%)	921.61 GB (45%)	942.08 GB (46%)	778.24 GB (38%)

Fig. 7. Statistics Form Interface

Fig. 7의 통계조회 form은 통계종류와 검색기간을 선택하면 디폴트 검색 결과로 1월부터 오늘날짜가 포함된 달까지 조회가능하다. radio/combo를 이용한 통계종류

필드는 일별 사용량, 월별 사용량 중 선택하여 조회 가능하도록 하였다.

4. 결론

종이 기록물 행정 시스템은 사용자가 검색이나 이력관리 등을 하며 종이문서 개별관리를 하는 것이다. 사용자가 문서를 제출하면 각 부서에서는 스캔, 생성, 저장, 폐기관리를 한다. 각 부서는 처리한 문서들은 관련부서로 보내고, 사무처에서는 종이 기록물 통합관리를 하게 된다. 통합관리는 문서의 검색, 변경, 삭제, 이력관리 등을 할 수 있어야 한다. 중앙전산소에는 관리서버와 행정서버가 있는데 행정 정보, 이미지 정보, 사용자 정보를 다룬다. PC에서 출력 시 출력물의 이미지와 추출이 가능한 텍스트, 출력 정보를 서버로 송신하여 출력물 DB에 저장하고 이를 통해 관리자가 모니터링이 가능하도록 별도 관리해야한다.

또한 출력물관리 시스템은 출력시 수집된 출력 로그 내에 개인정보(주민번호, 카드번호)가 존재하는지 패턴을 분석하여 사용자에게 경고 메시지 팝업 전달, 인쇄 강제 종료, 관리자에게 메일 발송 및 별도 로그 관리 기능을 갖추어야 한다. 인증 관리 역시 사용자 PC에 Agent를 설치하여 등록되어 있는 사용자만 프린트가 가능하며, 사용자 정보에 따라 작업이 허가되거나 거절될 수 있도록 제한 기능을 갖추어야한다. 또한 복합기로 프린트/복사/스캔 사용 시 ID카드 인증 후 문서 출력 및 복합기를 사용할 수 있으며, ID카드 미사용시 디바이스에 ID/PW를 입력 인증 후 복합기를 사용할 수 있도록 구축해야한다.

본 연구에서는 기존의 출력물 보안 방법들 보다 더욱 우수한 기술을 갖추고 있는 보안업체인 (주)와우소프트(대표 배종상)[20] 공동으로 인터페이스를 개발하여 기록물관리 시스템을 위한 인터페이스들을 구축하였다. 본 연구에서는 출력물관리를 위한 필요한 기본 기능들의 인터페이스를 설계하였으며 이를 바탕으로 출력물관리 시스템 구축에 기여하였다.

REFERENCES

[1] G. N. Pham, K. R. Kwon, E. J. Lee & S. H. Lee. (2017). Selective Encryption Algorithm for 3D Printing Model Based on Clustering and DCT Domain. *Journal of Computing Science and Engineering, 11(4),* 152-159. DOI : 10.5626/JCSE.2017.11.4.152

[2] J. H. Shin & I. S. KIm. (2015). Study on Detection Technique of Privacy Distribution Route based on Interconnection of Security Documents and Transaction ID. *Journal of the Korea Institute of Information Security & Cryptology 25(6),* 1435-1447. DOI : http://dx.doi.org/10.13089/JKIISC.2015.25.6.1435

[3] L. S. Ho, S. E. A, H. S. Young, L. S. Ha & Pang Sechung. (2015). *Printed Matter Security and Print Control System Using Print Data Collecting and Analysis*. Proceedings of Symposium of the Korean Institute of communications and Information Sciences, 783-784.

[4] S. G. Kim & W. S. Yoo. (2015). Development of a 3D Printing Open-market System for Copyright Protection and Remote 3D Printing. *Journal of the Korean Institute of Industrial Engineers, 41(3),* 253-258. DOI : http://dx.doi.org/10.7232/JKIIE.2015.41.3.253

[5] J. K. Baek & J. P. Park. (2013). A Study on Personal Information Control and Security in Printed Matter. *Journal of the Korea Academia-Industrial cooperation Society, 14(5),* 2415-2421. DOI: http://dx.doi.org/10.5762/KAIS.2013.14.5.2415

[6] J. S. Park & J. C. Ha. (2012). Vulnerability Analysis of Security Document Management in Multi Function Peripheral and Its Countermeasure. *The Journal of Korean Institute of Information Technology, 10(6),* 133-143. UCI : http://uci.or.kr/G704-001947.2012.10.6.009

[7] T. W. Lee. (2012). *A Study on Design and Implementation of Printer Security Integrated Management System*. Master dissertation. Konkuk University, Seoul.

[8] M. S. Yim. (2018). An Exploratory Research on Factors Influence Perceived Compliance Cost and Information Security Awareness in Small and Medium Enterprise, *Journal of tne Korea Convergence Society, 9(9),* 69-81.

[9] S. K. Cho & M. J. Jun. (2012). Privacy Leakage Monitoring System Design for Privacy Protection. *Journal of the Korea Institute of Information Security & Cryptology, 22(1),* 99-106.

[10] H. J. Lee & D. H. Won. (2011). A Protection Profile for E-Document Issuing System. *Journal of the Korea Institute of Information Security & Cryptology, 21(6),* 109-117.

[11] I. J. Suk. (2016). *Implementation of mobile printing*

system for security enhancement in the BYOD based mobile office environment. Master dissertation. Soongsil University, Seoul.

[12] W. X. Liu, Y. L. Chen, N. F. Liao. (2011). Study of printing security based on grating phase encodin, *JOURNAL OF OPTOELECTRONICS LASER, 22(11)*.

[13] S. J. Simske, M. Sturgill, J. Aronoff & M. Vans. (2010). Factors in a Security Printing & Imaging Based Anti-Counterfeiting Ecosystem (Focal), *International Conference on Digital Printing Technologies, 26*.

[14] RFC 1157 *Simple Network Management Protocol (SNMP)*, http://www.faqs.org/rfcs/rfc1157.html

[15] L. Lin & W. He. (2008),Status Quo of Security Printing-A Panoramic View at DRUPA, *International Conference on Digital Printing Technologies, 24*.

[16] S. Simske, P. Mucher & C. Martinez. (2005). *Digital Security Printing: Enabling Product Tracking and Authentication Using Existing Product Lines (Interactive)*, International Conference on Digital Production Printing and Industrial Applications.

[17] Maleshliuski,S.,Gunter,R.(2010),*Security Printing Techniques Based on Substrate and Print- Process Individualities*, TAGA ProceedIngs.

[18] RFC 3805 Printer MIB v2, http://www.faqs.org/rfcs/rfc3805.html

[19] http://www.archives.go.kr/next/data/standardCondition.do

[20] www.wowsoft.com

한 정 수(Han, Jung Soo) [정회원]

- 1900년 2월 : 경희대학교 전자계산공학과(공학사)
- 1992년 2월 : 경희대학교 전자계산공학과(공학석사)
- 2000년 2월 : 경희대학교 전자계산공학과(공학박사)
- 2001년 2월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : UML, 3D 모델링, 기록물보안
- E-Mail : jshan@bu.ac.kr

김 귀 정(Kim, Gui Jung) [정회원]

- 1994년 2월 : 한남대학교 전자계산공학과 (공학사)
- 1996년 2월 : 한남대학교 전자계산공학과 (공학석사)
- 2000년 2월 : 경희대학교 전자계산공학과(공학박사)
- 2017년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 기록물보안, CRM, 의공학, 3D Printing
- E-Mail : gjkim@bu.ac.kr