DOI: 10.3745/KIPSTC.2009.16-C.4.461

디지털 프린터의 보안기능 시험/평가방법론 개발

조 영 준[†] · 이 광 우[††] · 조 성 규[†] · 박 현 상[†] · 이 형 섭[†] · 이 현 승[†] · 김 송 이[†] · 차 욱 재[†] · 전 웅 렬[††] · 원 동 호[†††] · 김 승 주[††††]

요 약

현재 기업 및 공공기관에서 주로 사용하고 있는 디지털 프린터는 출력을 비롯하여 복사, 스캔, 팩스 등의 다양한 기능을 통합한 복합 기기로서, 최근에는 산업기술 유출 방지를 위해서 중요 데이터 유출 방지를 위한 보안기능을 구현하고 있다. 이에 일본과 미국에서는 일찍이 디지털 프린터에 대한 공통평가기준(CC, Common Criteria) 평가 인증을 진행하고 있으며, 국내에서도 최근부터 공공기관에 납품되는 제품에 대해 보안적합성 검증을 의무화하고 CC 평가 인증을 시작하고 있다. 하지만, 국내에서는 디지털 프린터에 대한 평가 지식이 부족하여 공통평가기준 평가를 준비하는 개발자 및 평가자가 어려움을 겪고 있다. 따라서 차기 평가 수요가 예측되는 디지털 프린터의 보안기능 기반기술 시험방법 및 평가요소기술에 대한 확보가 절실한 상황이다. 이에 본 논문에서는 국내·외 주요 업체들의 디지털 프린터에 포함되어 있는 보안 기능 및 개발 동향을 분석하고, 각 보안기능별 특성을 파악하여 디지털 프린터 보안기능 평가 및 취약성 시험 방법에 대한 가이드라인을 제시한다.

키워드 : 디지털 프린터, 공통평가기준(CC), 보안기능 시험/평가

Development Testing/Evaluating Methods about Security Functions based on Digital Printer

Youngjun Cho[†] · Kwangwoo Lee[††] · Sungkyu Cho[†] · Hyunsang Park[†] · Hyoungseob Lee[†] · Hyunseung Lee[†] · Songyi Kim[†] · Wookjae Cha[†] · Woongryul Jeon[††] · Dongho Won[†††] · Seungjoo Kim[††††]

ABSTRACT

Digital Printers that are mainly used in enterprises and public institutions are compound machinery and tools which are combined into various functions such as printing, copying, scanning, and fax so on. Digital Printers has security functionality for protecting the important data related with confidential industry technology from leaking. According to the trends, CC(Common Criteria) evaluation and assurance about digital printer is on progress in Japan and USA. Domestically CC evaluation and assurance is started recently. However, the know-how about the digital printer evaluation is not enough and the developers and the evaluators have difficulty in CC evaluation of digital printer products in the country. Therefore, the testing method of digital printer security functionality and evaluation technology is essentially needed for increasing demand for the evaluation afterwards. In this study, we analyze the security functionality and developing trends of digital printer products from internal and external major digital printer companies. Moreover, we research the characters of each security functions and propose guideline for digital printer security functionality evaluation and vulnerability testing methods.

Keywords : Digital Printer, Common Criteria(CC), Security Function Testing/Evaluation

1. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변화하고 있다. 현재 대다수의 기업 및 공공기관에서는 업무의 효율성 증대와 경비 절감을 위해 프린터에 복사기, 스캐너, 팩시밀리 등의 기능을 통합하여, 인쇄/복사/스캔/팩스 외에도 대용량 문서 데이터 저장, 네트워크 통신 등의 기능을 갖춘 기기를 사용하고 있다. 이러한 기기는 디지털 프린터, 디지털 복합기, HCD(Hard-Copy Device), MFD(Multi-Function Device), MFP(Multi-Function Peripheral) 등으로 불린다. 본 논문에서는 이하 디지털 프린터로 통칭한다.

최근에는 산업기술 유출 방지를 위해서 디지털 프린터에 중요 데이터 유출 방지를 위한 보안기능을 구현하고 있다. 이러한 디지털 프린터는 하드디스크나 플래시 메모리 등의 저장장치와 인터넷 또는 전화 회선에 연결되는 통신장치가

※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2009-(C1090-0902-0016)).
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
††† 종신회원 : 성균관대학교 정보통신공학부 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 부교수(교신저자)
논문접수 : 2009년 1월 29일
수 정 일 : 1차 2009년 3월 16일
심사완료 : 2009년 3월 18일

내장되어 있는데, 이로 인하여 데이터에 대한 접근 권한이 없는 자가 특정 문서 파일 등을 출력하거나 팩스, 스캔할 때 저장되는 데이터가 유출되는 등의 보안 문제가 야기될 수 있다. 특히 보안에 민감한 파일이나 문서가 노출될 경우, 기업이나 국가에 큰 손실을 유발할 수 있기 때문에 저장되는 데이터를 암호화하거나 삭제하는 보안 기능 및 사용자에 대한 식별 및 인증, 접근제어 기능 등은 디지털 프린터 시장의 새로운 경쟁요소로 부각되고 있다.

이에 일본에서는 업체들을 중심으로 공통평가기준(CC, Common Criteria) 평가 인증이 활발히 진행되고 있으며, 미국에서는 정부에서 조달기준으로 디지털 프린터에 대한 CC 인증을 요구하고 있다. 또한 초기에 CC 인증을 경험한 주요 디지털 프린터 관련 업체들은 자체적으로 디지털 프린터에 대한 보호프로파일(PP, Protection Profile)을 개발하고 있다. 국내에서는 디지털 프린터 내의 하드디스크 데이터의 완전삭제 기능에 대한 보안적합성 검증을 의무화하고 있다. 하지만 국가적으로 디지털 프린터에 대한 보안 인식은 아직도 미비한 상태이며, CC 인증 사례도 한 건이다. 국내에서 생산되는 디지털 프린터가 해외 수출 및 관련 업체들과의 경쟁에서 뒤처지지 않기 위해서는 CC 인증이 절실한 시점이지만, 디지털 프린터에 대한 인식과 평가 방법에 대한 지식이 부족하여 CC 평가를 준비하는 개발자 및 평가자가 어려움을 겪고 있다.

이에 추후 평가 수요가 급격하게 증가할 것으로 보이는 디지털 프린터의 보안기능 기반기술 시험방법 및 평가요소기술 확보를 위하여 본 논문에서는 2장에서 국내·외의 주요 디지털 프린터 업체 제품에 포함되어 있는 보안 기능 및 주요 업체들의 디지털 프린터 보안기능 개발 동향을 분석하고, 3장에서는 분석된 각 보안기능별 특성을 파악한다. 4장에서는 디지털 프린터 보안기능 평가 및 시험을 위한 시험항목을 도출하고 5장에서는 도출된 시험항목에 따른 시험/평가 가이드라인을 제시한다. 끝으로 6장에서는 결론을 맺는다.

2. 국내·외 디지털 프린터 보안기능 개발 동향

본 장에서는 국내·외 디지털 프린터 보안기능 개발 동향을 분석한다. 이를 위해, 먼저 디지털 프린터 업체들의 개발 동향을 살펴본다. 그리고 국내·외 디지털 프린터 보안기능 관련 시험수행기관 동향을 살펴본다.

2.1 국내·외 디지털 프린터 보안기능 개발 업체 동향 조사

디지털 프린터의 보안기능은 디지털 프린터의 사용자에 대한 인증 및 식별, 하드디스크 완전삭제, 전송되거나 저장되는 데이터의 암호화, 출력문서 보안기능 등이 있다. 이와 같은 디지털 프린터 보안기능을 개발하고 있는 업체들은 보안기능 개발 이후 평가기관에 의하여 공통평가기준(CC: Common Criteria)에 근거하여 보안기능이 제대로 구현되고 시험되었는지를 평가받게 된다. 국내·외 디지털 프린터 관련 보안기능 개발업체의 조사결과는 <표 1>과 같다

〈표 1〉 디지털 프린터 보안기능 개발업체 현황

회사	사이트	인증 횟수
Canon Inc.	www.canon.com	6
Fuji Xerox Co., Ltd.	www.fujixerox.co.jp	28
Hewlett-Packard Development Company, L.P.	www.hp.com	1
Konica Minolta Business Technologies, Inc.	www.konicaminolta.com	30
KYOCERA MITA Corporation	www.kyoceramita.com	4
Lexmark International, Inc.	www.lexmark.com	3
Oki Data Corporation	www.okidata.com	1
Panasonic Communications Co., Ltd.	panasonic.co.jp/pcc/e	3
Ricoh Company, Ltd.	www.ricoh.com	6
SAMSUNG	www.samsung.com	1
SEIKO EPSON CORPORATION	www.epson.co.jp/e	1
Sharp Corporation	sharp-world.com	20
TOSHIBA TEC CORPORATION	www.toshibatec.co.jp	7
Xerox Corporation	www.xerox.com	6

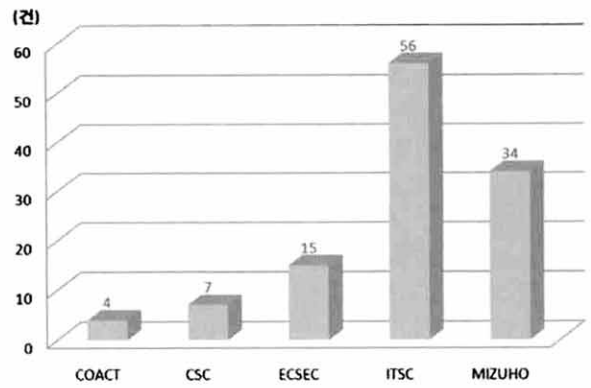
2.2 국내·외 디지털 프린터 보안기능 시험수행기관 동향

최근의 디지털 프린터는 보안기능이 탑재된 IT제품으로 분류되어, 보안 기능성과 이에 적용된 보증수단이 보안기능 요구사항들을 만족하는가에 대한 신뢰도를 확인하기 위해 공통평가기준에 의해 보안성 평가를 받는다. 본 절에서는 디지털 프린터의 보안기능성에 대하여 CC 평가를 수행한 시험수행기관들을 조사하고, 조사된 자료를 바탕으로 현재 디지털 프린터의 CC 평가 인증 진행 현황과 그 의미를 분석한다.

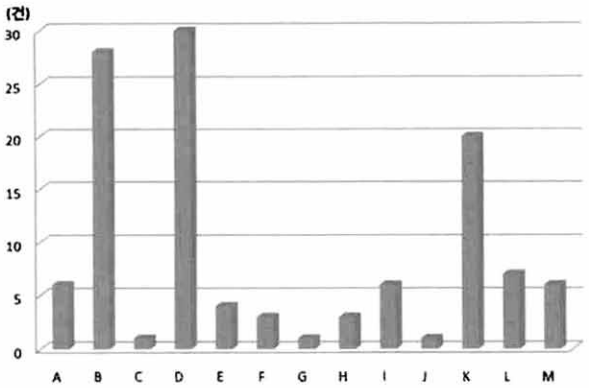
2.2.1 디지털 프린터 보안기능 평가기관 평가 현황

2002년 이후 현재까지 디지털 프린터 보안기능과 관련하여 평가를 수행한 평가기관과 평가 의뢰 업체를 중심으로 평가 현황을 조사한 결과, (그림 1)과 같이 디지털 프린터 보안기능 관련 평가는 일본과 미국에서 주로 진행되고 있음을 알 수 있었다. 특히 일본의 ITSC(48%), MIZUHO(29%), ECSEC(6%)와 미국의 COACT(4%), CSC(13%)는 디지털 프린터 보안기능과 관련된 평가에 있어 독보적인 점유율을 차지하고 있다[6,7].

각 평가기관에 평가를 의뢰한 디지털 프린터 보안기능 개발 업체를 살펴보면, 미국의 COACT에서는 Hewlett-Packard



(그림 1) 평가기관별 디지털 프린터 보안기능 평가현황



(그림 2) 디지털 프린터 보안기능 평가의뢰 업체 현황

와 Lexmark Inc.가 평가를 받았으며, CSC에서는 Sharp와 Xerox가 평가를 받았다. 또한 일본의 ECSEC는 Canon, Xerox, Ricoh 등이 주로 평가를 받았으며[8], ITSC에서는 Fuji Xerox, Sharp, Konica Minolta, Kyocera Mita가 주로 평가를 받았다[9]. MIZUHO는 Konica Minolta와 Sharp의 평가를 주로 수행하였다[10]. 디지털 프린터 보안기능 관련 개발 업체에서 평가받은 제품들을 살펴보면, 디지털 프린터 자체를 평가받은 업체도 있었지만, 보안기능 모듈단위로 평가를 신청한 업체들도 다수 있었다. 또한 디지털 프린터 보안기능 개발 업체들은 기존에 자사의 제품에 대하여 평가를 수행하였던 평가기관에 다시 평가 신청하는 것으로 나타났다.

2.2.2 국가별 평가 동향

2002년부터 현재까지 국가별 디지털 프린터 보안기능 평가 현황을 살펴보면 일본과 미국이 주를 이루고 있다. 현재까지 평가인증을 받은 디지털 프린터 보안기능 관련 평가 116건 중에서 미국이 11건으로 9%의 비율을 차지하고 있고, 일본이 105건으로 복합기 평가의 91%를 차지하고 있다. 복합기 평가를 진행한 주 평가기관으로는 일본의 ECSEC (Electronic Commerce Security Technology Laboratory Inc. Evaluation Center), ITSC(Information Technology Security Center), MIZUHO(Mizuho Information & Research institute, inc. Center for Evaluation of Information Security)와 미국의 COACT, CSC(Computer Sciences Corporation)가 있다.

2.2.3 디지털 프린터 평가 의뢰 업체 현황

디지털 프린터 평가 의뢰 업체의 현황을 살펴본 결과 (그림 2)와 같이 디지털 프린터 보안기능 관련 평가를 의뢰한 다수의 업체 중에서 Fuji Xerox와 Konica Minolta, 그리고 Sharp가 디지털 프린터 보안기능과 관련하여 다수의 평가 인증을 획득했음을 알 수 있다.

- A : Canon Inc.
- B : Fuji Xerox Co., Ltd
- C : Hewlett-Packard Development Company, L.P.
- D : Konica Minolta Business Technologies, Inc
- E : KYOCERA MITA Corporation
- F : Lexmark Inc.
- G : Oki Data Corporation
- H : Panasonic Communications Co., Ltd.
- I : RICOH COMPANY, LTD.
- J : SEIKO EPSON CORPORATION
- K : Sharp Corporation
- L : TOSHIBA TEC CORPORATION
- M : Xerox Corporation

3. 국내 · 외 디지털 프린터 보안기능 분석 및 조사

3.1 국내 · 외 디지털 프린터 제품의 보안기능 조사

보안기능이 탑재된 디지털 프린터에서의 일반적인 보안기능은 크게 패스워드 기반의 인증, 하드디스크 완전 삭제, 그리고 데이터 암호화가 있다. 이러한 기능들은 보안 유출 경로 중의 하나인 출력문서에 대한 보안을 강화하기 위하여 사용자에 대한 식별 및 인증을 통해 지정된 사용자만이 관련 문서를 출력할 수 있도록 하며, 하드디스크에서의 잔여정보에 대한 보안 문제를 해결하기 위하여 특수한 알고리즘을 적용하고 하드디스크에 대한 완전삭제를 구현하여 잔여정보에 대한 보안을 강화한다. 또한 하드디스크에 저장되는 데이터에 대하여 검증된 암호 알고리즘을 기반으로 암호화를 수행하여 내부 데이터에 대한 보호를 수행한다. 대표적인 디지털 프린터 개발업체들이 출시한 제품에서의 보안기능 탑재여부는 <표 2>와 같다.

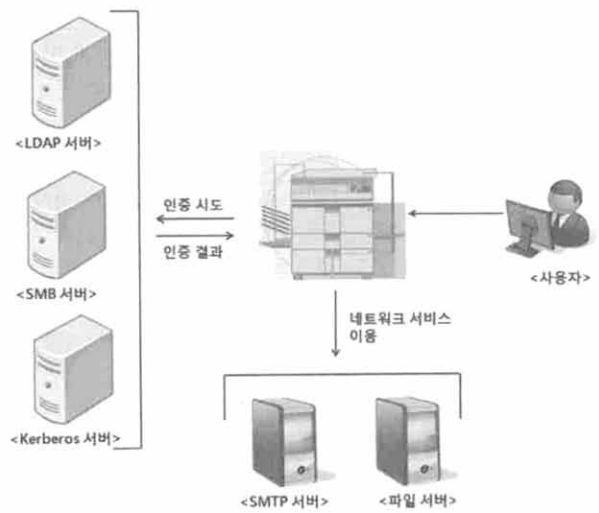
3.1.1 인증

디지털 프린터에서의 인증 및 식별 기능은 기본적으로 문서를 사용하려는 사용자의 신원과 이에 대한 검증 절차를 수행하며, 대부분의 제품에서는 패스워드 기반의 인증 절차를 사용한다. 디지털 프린터에서는 문서에 대한 복사, 스캔, 인쇄, 팩스 등의 기능을 가지고 있으며, 디지털 프린터가 네트워크와 연결되었을 시에는 이를 활용한 편의기능인 스캔 후 이메일 전송 또는 서버 전송 등의 기능 등이 제공된다.

〈표 2〉 디지털 프린터 개발업체 및 기종에 따른 보안기능 탑재 여부(A : 인증 및 식별, B : 암호화, C : 하드디스크 완전삭제)

디지털 프린터 개발업체 및 기종	A	B	C	기타 보안기능
삼성전자 SCX-6X45	O	O	O	- 감사기록 제공
신도리코 Aficio MP 5000/5000B, 4000/4000B	O	X	X	- 워터마크를 이용한 부정출력 방지
신도리코 DGwox	O	O	X	- SSL을 이용한 데이터 보호 - 워터마크를 이용한 부정출력 방지
후지제록스 ApeosPort-II	O	O	O	- 감사로그 제공
후지제록스 DocuCentre-III	O	O	O	- 워터마크를 이용한 부정출력 방지
HP Laserjet 4345	O	O	O	
Kyocera KM-8030	O	O	O	

이러한 기능이 제공되는 복합기에서는 반드시 해당 기능에 대한 사용 권한이 있는지에 대한 확인을 위하여 인증 및 식별 기능을 제공하는데, 이 때 인증서버에 접근하기 위하여 대부분 Kerberos, LDAP, 또는 SMB 등의 프로토콜을 지원한다. 네트워크 자원의 사용을 위한 인증 및 식별 절차에 대한 전체적인 구성은 (그림 3)과 같다.



(그림 3) 네트워크 인증 및 식별을 위한 전체 구성

3.1.2 데이터 접근제어

디지털 프린터에서 수행되는 기본적인 기능인 복사, 스캔, 출력, 팩스 기능은 대부분 하드디스크 또는 메모리에 해당 문서가 저장된 후 기능을 수행하게 된다. 따라서 저장된 중요 데이터에 대한 접근제어 기능이 탑재되며, 이러한 접근제어 및 권한 부여를 위해 인증 및 식별은 필수적이다. 대부분의 디지털 프린터에서는 저장된 문서를 보존용 문서와 일반 문서로 구분하게 되는데, 보존용 파일에 대한 접근 권한은 해당 파일을 저장한 사용자에게만 허용된다. 일반적으로 보존용 파일에 접근할 경우, 사용자 클라이언트 PC에서는 PIN 번호를 설정하게 된다. 해당 문서 출력 시 사용자는 클라이언트 PC 또는 해당 디지털 프린터에 직접 접근하여 문서에 대한 접근 권한이 있음을 증명하기 위해 미리 저장된 PIN 번호를 입력하여 인증 절차를 수행한 후 해당 문서를 출력 또는 전송하게 된다. 디지털 프린터에서 보존용 파일에 대한 접근 및 문서 출력 과정은 (그림 4)와 같다.

(그림 4) 데이터 접근제어 및 문서 출력

3.1.3 하드디스크 완전삭제

최근 출시되는 대부분의 기업용 디지털 프린터에서는 기본적으로 하드디스크 완전삭제 기능을 제공한다. 디지털 프린터에서 사용된 데이터는 대부분 하드디스크에 저장되며, 운영체제의 특성상 데이터 삭제 명령은 데이터 영역을 초기화하지 않으므로 자기적인 특성을 유지하게 된다. 따라서 단순한 삭제만으로는 데이터가 완전히 삭제되지 않으며 복원 유틸리티 등을 사용하면 삭제된 데이터의 복구가 가능하다. 이를 방지하기 위해 디지털 프린터 제조업체에서는 하드디스크 완전삭제 기능을 적용하고 있다.

하드디스크 완전삭제 기술 중 하나를 예로 들면 미 국방성 표준인 DoD 5220.22-M의 "DoD Clearing and sanitizing standard"가 있다. 이것은 매체의 모든 접근 가능한 위치를 단일 문자, 그것의 보수, 그리고 임의의 문자로 세 번을 덮어쓴 후 검증하는 절차를 갖는다.

3.1.4 암호화

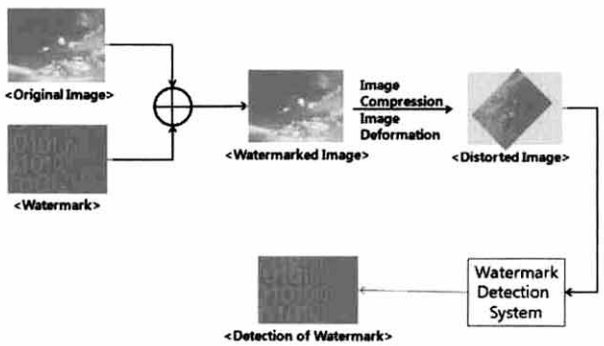
디지털 프린터 내의 하드디스크에는 중요한 데이터가 보관될 수 있다. 그러나 이러한 데이터는 공격자에게 노출될 수 있다. 따라서 하드디스크 내에 저장되는 데이터는 기밀성을 위해 암호화를 필요로 한다. 본 보안기능은 하드디스크에 데이터를 기록할 때 시스템 내부적으로 작동한다. 하드디스크에 기록되는 데이터는 암호화 알고리즘으로 암호화된 후 하드디스크에 기록되며, 하드디스크에 기록된 데이터는 암호화 알고리즘으로 복호화 하여 사용될 수 있다.

3.1.5 기타 보안 기능

기타 보안 기능으로 디지털 워터마킹과 SSL(Secure Socket Layer)를 들 수 있다. (그림 5)에서처럼 디지털 워터

마킹(Digital Watermarking) 기술은 데이터의 복제 및 위조 방지를 위해 사용되는 보안기능이다[1]. 워터마킹은 저작권 보호, 위·변조 판별, 불법복제 추적, 사용자 제어, 내용 보호, 내용 라벨링 등의 기능을 제공한다[2]. 현재 디지털 프린터에서 워터마크 기술을 이용한 위조 및 복제 방지 기술은 신도리코와 후지제록스, Konica Minolta의 일부 제품군에서 활용되고 있다.

SSL은 TCP/IP 상의 응용 계층과 전송계층 사이에서 동작하며, 클라이언트와 서버 사이에서 안전한 채널을 생성해 준다[5]. 디지털 프린터는 자체적으로 내장된 웹 서버를 기반으로 관리자에게 원격 관리 서비스를 제공하고 있는데, 원격에서 송수신되는 중요 정보에 대한 기밀성 및 무결성을 보장하기 위하여 SSL 프로토콜을 이용한다.



(그림 5) 디지털 워터마킹 기술

3.2 국내·외 디지털 프린터 보안기능 시험/분석 방법 조사

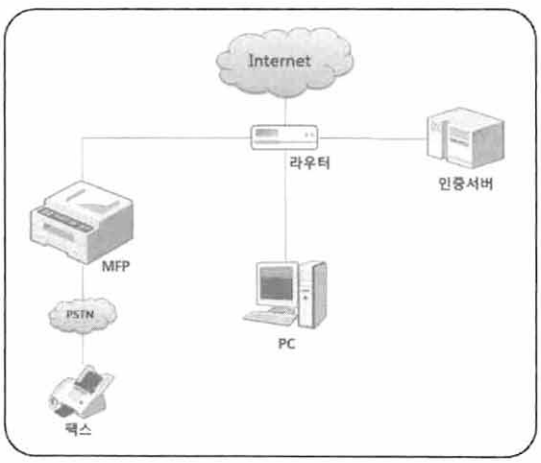
디지털 프린터에 구현된 모든 기능은 완전하게 동작해야 하며, 보안상 취약점이 존재하지 않도록 해야 한다. 이를 위해 디지털 프린터 제품을 출시하기 전에 디지털 프린터에 대한 철저한 시험 및 분석이 이루어져야 한다. 일반적인 시험 및 분석 방법은 시험 준비(Prepare to test), 시험 계획 수립(Test Plan), 시험환경 구축(Build test environment), 시험 수행(Functional specification test), 시험 결과 분석(Test result analysis)의 다섯 단계로 구성된다.

3.2.1 시험 준비

시험을 수행하기 전에 시험 수행을 위한 준비 작업을 수행한다. 그 첫 번째 단계로, 시험의 목적을 명확히 해야 한다. 일반적으로 디지털 프린터를 시험/분석하는 목적은 평가 대상 디지털 프린터를 구성하는 모든 보안 기능이 보안 목적에 맞게 동작하는지 확인하고, 보안기능들이 전체적으로 효용성 있는 하나의 보안 시스템으로 동작하는지 여부를 확인하는 것에 있다. 목적을 명확하게 한 후에는 시험 분석서를 작성하기 위한 작성 기법을 명시해야 한다. 작성 기법에는 정형화된 기법, 준 정형화된 기법, 비정형화된 기법이 있다. 작성 규칙을 명시한 후에는 용어 및 약어를 정리한다. 시험 수행과 관련된 모든 용어 및 약어에 대해 미리 정리함으로써 시험 도중 발생할 수 있는 혼동을 미연에 방지할 수 있다.

3.2.2 시험 계획 수립

시험 준비가 끝나면 시험 계획을 수립한다. 시험 계획을 수립하기 위해, 우선 시험에 필요한 장비를 식별한다. 일반적으로 디지털 프린터 제품의 시험 및 분석에는 디지털 프린터와 시험용 서버, 시험용 PC가 요구된다. (그림 6)은 디지털 프린터, 시험용 PC, 시험용 서버 간의 구성을 나타낸 것이다.



(그림 6) 일반적인 디지털 프린터 시험 구성도

3.2.3 시험 환경 구축

장비 식별이 끝나면 시험 환경을 구축한다. 시험용 서버와 시험용 PC, 디지털 프린터 간의 네트워크를 구축하고, 구축된 네트워크에 대한 세부 사항을 명확히 한다. 또한, 시험 및 분석에 사용되는 응용 프로그램과 드라이버를 선택하여 프로그램명과 버전을 명확히 식별해야 한다.

3.2.4 시험 수행

시험 수행 단계에서는 실제로 디지털 프린터에 대한 시험을 수행한다. 시험 수행은 각 기능별로 나누어서 수행한다. 앞서 설명한 일반적인 보안기능별로 시험 단계를 나누어보면 네트워크 자원 사용을 위한 인증 및 식별, 데이터 접근 제어, 하드디스크 완전삭제, 암호화, 디지털 워터마킹, SSL로 나눌 수 있다. 시험은 가능한 모든 경우의 수를 염두에 두고 모든 상황에 대해 시험을 수행해야 한다. 각 시험은 <표 3>과 같은 시험서 양식에 따라 수행하고 그 과정과 결과를 명확히 기록한다.

〈표 3〉 시험서 작성 양식

목 록	내 용
시험목적	시험을 하는 목적
시험환경	시험이 이루어지는 환경
종속관계	본 시험의 수행을 위해 선 수행 또는 후 수행되어야 하는 시험 식별
시험절차	본 시험이 이루어지는 상세 과정
예상결과	본 시험으로 인해 예상되는 결과
실제결과	본 시험이 수행된 후 나온 결과

3.2.5 시험 결과 분석

시험이 종료되면 시험 결과를 분석한다. 우선 시험 결과를 분석하기 쉬운 형태로 정리/가공한다. 다음으로 디지털 프린터의 모든 보안 기능에 대하여 시험이 이루어졌는지를 확인하기 위해 시험 일치성 분석이 이루어져야 한다. 마지막으로 예상 결과와 실제 결과가 다른 시험항목에 대해서는 기능 수정 및 보완 작업을 수행한다.

3.3 국내·외 디지털 프린터 관련 표준화 동향 조사

본 절에서는 국내·외에서 진행되었던 프린터 관련 표준을 소개하고, 각 표준에서 정의한 자산과 위협 및 그에 대응하는 보안기능에 대해 알아본다.

3.3.1 CIAC-2304

국외에서는 디지털 프린터에 대한 취약성 및 위협 분석이 이미 수행되었다. 미국에서는 정부 주도하에 1995년 CIAC-2304 Data Security Vulnerabilities of Facsimile Machines and Digital Copiers 보고서를 통해 팩시밀리와 복사기에 대한 위협을 분석하였다. CIAC-2304에서는 팩스와 복사 기능에 대한 취약성을 분석하였으며, 분석된 취약성은 <표 4>와 같다.

〈표 4〉 CIAC-2304에서 보고된 취약성

분류	취약성
팩스	메시지 인증이 불가하여 공격자가 중간에서 데이터를 위변조 할 수 있음
	가입자의 전화번호나 서비스 제공자의 ID를 위변조할 수 있음
	팩스 기기에 대한 인증이 되지 않을 경우, 전화번호를 스푸핑할 수 있음
	팩스 전송 시, 암호화하지 않는 경우 도청을 통해 중요 데이터가 유출될 수 있음
	잘못된 팩스 설정이나 사용자의 부주의로 인해 시스템이 취약해질 수 있음
	하드웨어 자원의 한계로 인해 저장된 데이터가 삭제될 수 있음
복사	네트워크를 통해 저장 데이터 유출될 수 있음
	인쇄할 데이터를 위변조하여 인쇄될 수 있음

3.3.2 IEEE P2600

IEEE P2600은 디지털 프린터 내부에 저장된 사용자 데이터와 시스템 관리 데이터, 물리적인 디지털 프린터 자원, 디지털 프린터 운영 펌웨어 등을 디지털 프린터가 보호해야 할 자산으로 정의하였다. IEEE P2600에서는 디지털 프린터가 안전하게 보호해야할 자산의 중요도에 따라 운영 환경을 네 가지로 분류하고 있으며, 각 운영 환경에 따라 위협을 도출하였다. 도출한 위협은 보호해야 할 사용자 데이터, 자원, DoS(Denial Of Service)위협, 다른 공격에 이용될 위협, 보안 기능으로 나누어 정의한다. <표 5>는 IEEE P2600에서 보고된 취약성에 대해 정리한 것이다.

〈표 5〉 IEEE P2600에서 보고된 취약성

분류	위협
사용자 데이터	일반적인 방법으로 사용자 데이터에 접근함
	전화회선이나 관리 포트를 통해 사용자 데이터에 접근함
	스니핑을 통해 사용자 데이터에 접근함
	위장을 통해 전송되는 사용자 데이터를 변경 또는 삭제함
	인쇄된 형태의 사용자 데이터를 획득함
	저장장치에 저장된 사용자 데이터를 삭제 또는 유출함
자원	서버 보안이나 과금을 피하기 위해 시스템과 P2P로 연결함
	제어나 과금을 우회하기 위해 불법 장치를 사용함
DoS 위협	가능한 네트워크 연결을 모두 열어 네트워크 인터페이스에 대한 서비스 거부 공격을 시도함
	인쇄 처리의 루프를 유발하는 인쇄 파일로 인해 인쇄 기능에 대한 서비스 거부 공격을 시도함
	팩스 회선을 방해하여 팩스 기능에 대한 서비스 거부 공격을 시도함
다른 공격에 이용	네트워크 서비스를 통해 IT 환경을 공격함
	디지털 복합기의 네트워크 서비스를 이용하여 조직 내부 망에 서비스 거부 공격을 시도함
	팩스 연결을 통해 디지털 복합기 내부에 접근함
보안 기능	관리 데이터를 스니핑하여 정당한 사용자로 위장함
	관리 데이터를 변경 및 삭제하여 정당한 사용자로 위장함
	감사 기록에 접근하여 정당한 사용자와 시스템 내부에 대한 지식을 얻음
	디지털 복합기의 설정 값을 변경하여 추후 공격에 이용함
	인가되지 않은 애플릿을 설치하여 추후 공격에 이용함

4. 공통평가기준을 활용한 디지털 프린터 보안기능별 기반기술 시험항목 도출

본 장에서는 위에서 분석한 국내·외 디지털 프린터의 보안 기능을 공통평가기준을 기반으로 시험/평가 하기위한 항목을 도출한다. 이를 위해 공통평가기준의 시험 클래스(ATE)와 취약성 클래스(AVA)를 참조한다. 공통평가기준에서 시험 클래스는 평가 제품의 보안기능이 설계 설명대로 동작하는지 확인하는 것에 중점을 두고 있다. 취약성 클래스는 평가 제품의 개발이나 운영 중에 악용 가능한 취약성이 발생할 가능성을 다룬다. 공통평가기준 v3.1에서 <표 6>에서 보는 것과 같이 시험 클래스와 취약성 클래스는 다음과 같은 패밀리를 포함한다. 이 중 ATE_COV, ATE_DPT, ATE_FUN은 개발자가 작성한 문서와 개발자가 수행한 시험과 관련된 패밀리이며 ATE_IND와 AVA_VAN은 평가자가 시험/취약성과 연관되는 패밀리이다. ATE_FUN은 개발자가 수행한 시험의 정당성과 관련된 패밀리로 개발자의 문서를 통해 이를 확인하는 것이다. 또한 AVA_VAN은 잠재된 취약성에 대한 시험과 관련된 패밀리이다. 이는 모든 보안기능에 대해 <표 5>, <표 6>에서 보고된 취약성과 대표적인 취약성 분석 사이트인 National Vulnerability Database (NIST)(http://nvd.nist.gov/), SecurityFocus→bugTraq (http://www.securityfocus.com/vulnerabilities), Secunia (http://www.secunia.com), CVE(Common Vulnerability and Exposures)

〈표 6〉 시험/취약성 클래스와 패밀리

클래스	패밀리	설명
ATE	COV	보안 기능이 기능명세에 따라 시험되었는지를 입증
	DPT	보안 기능 시험의 상세 수준을 다룸 (내부 인터페이스 직접 시험)
	FUN	시험 문서내의 시험항목이 정확하게 수행되고 문서화되었음을 보증
	IND	평가자가 위 시험을 검증하고 추가적인 실험을 수행
AVA	VAN	잠재적 취약성에 대해서도 시험 (기능 무력화 및 우회 시험)

(http://cve.mitre.org/), Black hat (http://www.blackhat.com) 등을 통해 시험한다. 이에 본 논문에서는 ATE_COV, ATE_DPT, ATE_IND에 해당하는 항목에 대해 시험항목을 도출한다.

4.1 잔여정보 보호 기술

잔여정보의 데이터 복구를 막기 위한 보호 기술로 사용된 데이터 영역에 덮어쓰는 과정을 반복하여 이전에 사용된 데이터의 복구를 막는 방법이 있다[4]. 공통평가기준에 따라 완전삭제와 관련된 시험항목은 <표 7>과 같이 도출할 수 있다.

〈표 7〉 시험/취약성 클래스에 대응되는 잔여정보 보호 기술

클래스	패밀리	설명
ATE	COV	잔여정보 보호 기술에 대해 개발자가 적합한 시험을 수행했는지 확인 - 완전삭제를 수행하는 기능 리스트 생성 - 저장매체 식별 - 완전삭제 알고리즘 식별
	DPT	개발자가 수행하는 잔여정보 보호 기술에 대한 시험 확인 - 완전삭제 알고리즘 소스 코드 확인
	IND	- 포렌식 툴을 이용한 데이터 복구 여부 확인

4.2 보안인쇄 기술

보안인쇄 기능의 시험항목은 두 가지 목표를 바탕으로 도출한다. 우선 해당 기능이 가져야 할 보안요구사항을 충실히 반영하고 있다는 것을 입증하기 위한 시험을 수행하고, 기능의 동작이 정확하고 명세서와 일치하여 결함(fault)이나 결점(defect)이 없음을 확인하는 시험을 수행한다. 보안인쇄 기술과 관련된 시험항목은 <표 8>과 같다.

〈표 8〉 시험/취약성 클래스에 대응되는 보안인쇄 기술

클래스	패밀리	설명
ATE	COV	보안인쇄 기술에 대해 개발자가 적합한 시험을 수행했는지 확인 - 보안인쇄를 수행하는 기능 리스트 생성
	DPT	개발자가 수행하는 잔여정보 보호 기술에 대한 시험 확인 - PIN에 대한 시험 - 보안적용 대상에 대한 기밀성 확인
	IND	- PIN의 길이나 입력횟수의 초과 시 차단 여부 확인

4.3 위조/복제 방지 기술

위조 및 복제 방지 기능을 시험하기 위해서는 두 가지 요소가 식별 되어야 하는데, 첫 번째는 위조 및 복제 방지 기능이 완전히 원본 문서의 복사, 출력 또는 스캔을 방지하기 위한 목적인지 아니면 복사본을 명시하기 위함인지를 명확히 식별하는 것이다. 전자의 경우, 도출된 세부 시험항목이 모두 해당되지만, 후자의 경우에는 세부 시험항목이 일부 적용되지 않을 수 있다. 두 번째로 식별되어야 하는 요소는 위조 및 복제 방지 기능이 수행되는 환경에 대한 식별로써, 해당 기능이 복사, 스캔, 출력 및 팩스 전송 등 디지털 프린터의 기본 기능 중 어떤 기능에서 사용하는지 식별하는 것이다. 이러한 환경 식별이 명확히 이루어진 후, 위조 및 복제 방지기능의 정상 동작여부를 판별한다. 공통평가기준에 따라 위조/복제 방지 기술과 관련된 시험항목은 <표 9>와 같다.

〈표 9〉 시험/취약성 클래스에 대응되는 위조/복제 방지 기술

클래스	패밀리	설명
ATE	COV	위조/복제 방지 기술에 대해 개발자가 적합한 시험을 수행했는지 확인 - 위조/복제 방지를 수행하는 기능 리스트 생성
	DPT	개발자가 수행하는 위조/복제 방지 기술에 대한 시험 확인 - 디지털 워터마크의 실제 반응 확인 - 워터마크를 통해 실제 주요 기능 차단 여부 확인
	IND	- 디지털 워터마크 훼손, 변조 시 동작여부 확인

4.4 출력 접근제어 기술

출력 접근제어 기술은 다른 사용자로부터 자신의 신원 정보를 이용하여 자신의 출력물을 보호하는 기술이다. 따라서 사용자 인증은 출력 접근제어 기술의 핵심이다. 출력 접근제어 기술의 안전성을 평가하기 위해서는 디지털 프린터에 구현된 인증 절차 및 메커니즘이 적절한지 여부와 인증 실패 시 대처 방안 및 인증서버에 대한 안전성 평가가 필요하다. 이를 통해 출력 접근제어 기술이 공격에 안전하다는 것을 입증한다. 공통평가기준에 따라 사용자 인증을 사용한 출력 접근제어 기술에 대한 시험항목은 <표 10>과 같다.

〈표 10〉 시험/취약성 클래스에 대응되는 출력 접근제어 기술

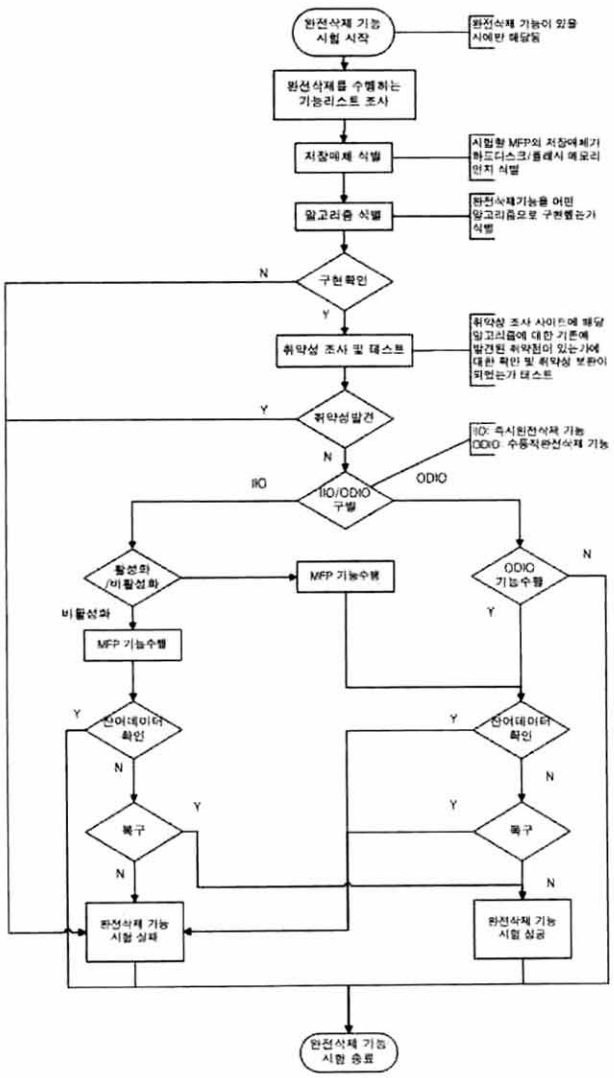
클래스	패밀리	설명
ATE	COV	출력 접근제어 기술에 대해 개발자가 적합한 시험을 수행했는지 확인 - 출력 접근제어를 수행하는 기능 리스트 생성
	DPT	개발자가 수행하는 출력 접근제어 기술에 대한 시험 확인 - 사용자별 접근제어 정책 확인 - 인증 메커니즘, 인증서버 동작 시험
	IND	- 인증 메커니즘의 적합성 확인 - 인증 서버의 안전성 확인

5. 공통평가기준을 통한 디지털 프린터 보안기능별 기반기술 시험 방법 개발

본 장에서는 4장에서 도출한 시험항목을 바탕으로 공통평가기준에 따라 시험항목에 따른 시험목적을 도출한 후, 세부 시험방법에 대해 개발한다. 개발자가 제공하지 않는 기능에 대해서는 시험/평가 하지 않으며 제공하는 기능에 한해서 다음과 같은 시험이 이루어져야 한다.

5.1 잔여정보 보호 기술

완전삭제와 관련된 시험항목으로는 완전삭제를 수행하는 기능 리스트 생성, 저장매체 식별, 완전삭제 알고리즘 식별, 완전삭제 알고리즘 소스코드 확인, 포렌식 툴을 이용한 데이터 복구 여부 확인이 있다. 잔여정보 보호 기능시험의 전체 흐름도는 (그림 7)과 같다.



(그림 7) 잔여정보 보호 기능 시험 전체 흐름도

5.1.1 완전삭제를 수행하는 기능 리스트 생성

개발자가 제공하는 완전삭제 기능에 대해서 시험하기 위해서는 존재하는 기능 리스트를 생성해야 한다. 완전삭제 기능 리스트 생성을 시험하기 위한 시험목적과 시험절차는 <표 11>과 같다.

〈표 11〉 완전삭제 기능 리스트 생성 시험항목

시험목적	완전삭제 기능을 수행하는 디지털 프린터 기능을 식별한다.
시험절차	1. 디지털 프린터의 사용설명서를 참고해서 완전삭제 기능을 수행하는 디지털 프린터 기능을 확인한다. 2. 디지털 프린터의 기능명세서를 참고해서 완전삭제 기능을 수행하는 디지털 프린터 기능을 확인한다. 3. 확인된 기능을 토대로 디지털 프린터 기능 리스트를 생성한다.

5.1.2 저장매체 식별

디지털 프린터의 저장매체 식별 시험항목은 <표 12>와 같다. 디지털 프린터의 저장매체로는 일반적으로 하드디스크와 플래시 메모리가 이용되고 있다.

〈표 12〉 저장매체 식별 시험항목

시험목적	디지털 프린터에 사용된 저장매체를 식별한다.
시험절차	1. 디지털 프린터의 사용설명서에서 저장매체에 대해서 서술하고 있는지 확인한다. 2. 디지털 프린터의 보안목표명세서에 저장매체에 대해서 서술하고 있는지 확인한다. 3. 확인된 저장매체 정보를 바탕으로 디지털 프린터의 저장매체를 식별한다.

5.1.3 완전삭제 알고리즘 식별

디지털 프린터 내에서 이루어지는 완전삭제가 어떠한 알고리즘을 이용하고 있는지 식별해야 한다. 완전삭제 알고리즘 식별 시험항목은 <표 13>과 같다.

〈표 13〉 완전삭제 알고리즘 식별을 위한 시험항목

시험목적	완전삭제 알고리즘을 식별한다.
시험절차	1. 디지털 프린터의 사용설명서에서 완전삭제에 대하여 설명하고 있는지 확인한다. 2. 디지털 프린터의 보안목표명세서에 완전삭제에 대하여 설명하고 있는지 확인한다. 3. 확인된 알고리즘 정보를 바탕으로 디지털 프린터의 완전삭제 알고리즘을 식별한다.

5.1.4 완전삭제 알고리즘의 소스코드 확인

<표 14>에서 시험하는 소스코드 확인은 WhiteBox시험의 일종으로 정보보호제품 평가등급 중 EAL3까지는 수행하지 않아도 된다. EAL4를 요구하는 보안기능을 수행하는 디지털 프린터에서는 보안기능을 확인하는데 소스코드 확인이 필수적이다. 따라서 디지털 프린터의 소스코드 중에서 보안기능에 해당하는 소스코드가 무엇이며 소스코드가 알고리즘에 맞게 설계되어 구현되었는지 명확히 확인해야 한다.

〈표 14〉 완전삭제 알고리즘 소스코드 확인 시험항목

시험목적	완전삭제 알고리즘 소스코드를 확인한다.
시험절차	1. 디지털 프린터에서 사용하고 있는 완전삭제 알고리즘을 확인한다. 2. 해당 완전삭제 알고리즘의 표준을 검색하여 삭제 방법을 확인한다. 3. CC평가 제출물의 하나인 ADV_IMP등과 같이 디지털 프린터의 보안기능을 구현하기 위하여 사용된 소스코드에서 완전삭제에 해당하는 부분을 확인하여 표준알고리즘대로 구현되었는지 확인한다.

5.1.5 포렌식 툴을 이용한 데이터 복구 여부 확인

실제 완전삭제가 이루어지는지 포렌식 툴을 이용하여 시험하는 절차는 <표 15>와 같다. 대표적인 포렌식 툴로는 Logicube, FinalData, WinHex, EnCase 등이 있다.

〈표 15〉 포렌식 툴로 데이터 복구 확인 시험항목

시험목적	포렌식 툴로 삭제된 데이터가 복구되는지 확인한다.
시험절차	1. 기존의 포렌식 툴을 조사한다. 2. 포렌식 툴을 선택한다. 3. 완전삭제 기능이 포함된 디지털 프린터의 기능을 시험해 본다. 4. 기능실행 후 데이터의 복구를 시도해본다.

5.2 보안인쇄 기술

보안인쇄 기능 시험에 대한 전체 흐름도는 (그림 8)과 같다. 보안 인쇄 기술에 대한 시험항목은 보안인쇄를 수행하는 기능 리스트 생성, PIN에 대한 시험, 보안적용 대상에 대한 기밀성 확인, PIN의 길이나 입력횟수의 초과 시 차단여부 확인이 있다.

5.2.1 보안인쇄를 수행하는 기능 리스트 생성

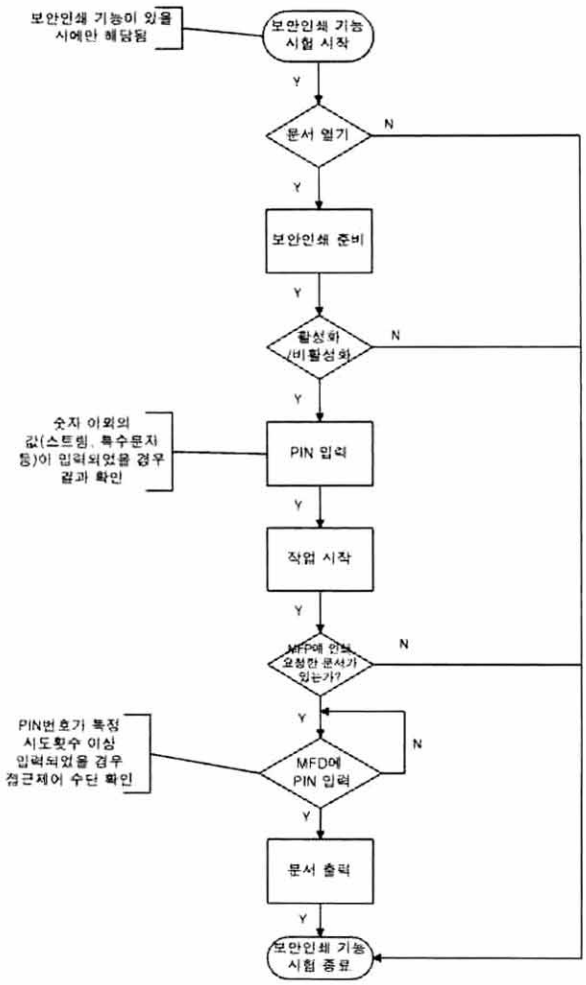
개발자가 제공하는 보안인쇄 기능에 대해서 시험하기 위해서는 존재하는 기능 리스트를 생성해야 한다. 보안인쇄 기능 리스트 생성을 시험하기 위한 시험목적과 시험절차는 <표 16>과 같다.

〈표 16〉 보안인쇄 기능 리스트 생성 시험항목

시험목적	보안인쇄 기능을 수행하는 디지털 프린터 기능을 식별한다.
시험절차	1. 디지털 프린터의 사용설명서를 참고해서 보안인쇄 기능을 수행하는 디지털 프린터 기능을 확인한다. 2. 디지털 프린터의 기능명세서를 참고해서 보안인쇄 기능을 수행하는 디지털 프린터 기능을 확인한다. 3. 확인된 기능을 토대로 디지털 프린터 기능 리스트를 생성한다.

5.2.2 PIN에 대한 시험

PIN에 대한 시험목적과 시험절차로는 <표 17>과 같다. 본 시험 시 명세서 및 설명서에서 서술하고 있는 지원 포맷을 확인해야 하며 지원 포맷 내에서 PIN을 입력하여 제대로 출력되는지 확인해야 한다. 또한 명세서 및 설명서에서 서술하고 있는 미지원 포맷으로 PIN을 입력하였을 경우 에러메시지 출력 여부를 확인해야 한다.



(그림 8) 보안인쇄 기능 시험을 위한 흐름도

〈표 17〉 PIN에 대한 시험항목

시험목적	PIN 입력 시 숫자 외에 특정 문자의 입력을 차단하는지 확인한다.
시험절차	1. 보안인쇄 설정 화면으로 들어간다. 2. PIN 대신 특정 문자열을 입력한다. 3. PIN이 제대로 입력되는지 확인한다.

5.2.3 보안 적용 대상에 대한 기밀성 시험

보안 적용 대상에 대한 기밀성 시험과 관련된 시험목적과 시험절차는 <표 18>, <표 19>, <표 20>에서 서술하고 있다.

〈표 18〉 보안 적용 대상에 대한 기밀성 시험항목 1

시험목적	PIN이 디지털 프린터로 전송되는 과정에서 기밀성이 유지되는지 확인한다.
시험절차	1. 보안인쇄 설정 화면으로 들어간다. 2. 규칙에 맞는 PIN을 입력하고 인쇄를 시작한다. 3. PC에서 프린터로 가는 패킷을 캡처하여 PIN이 노출되는지 확인한다.

<표 18>과 관련된 시험 시 PIN이 암호화 되어 전송되는지 확인하여야 하며 암호화되어 있다면 암호화에 사용된 알고리즘의 적절성을 확인해야 한다. 또한 전송 과정 중 특정 부분에서 암호화 시 사용된 키에 대한 정보가 노출되는지 확인해야 한다.

<표 19>와 관련된 시험 시 PIN이 디지털 프린터 내에 저장되어 있는지 확인해야 하며 이 때, 암호화 되어 저장되는지 확인해야 한다. 또한 암호화에 사용된 알고리즘의 적절성을 확인해야 하며 특정 부분에서 암호화에 사용된 키가 노출되는지 확인해야 한다.

〈표 19〉 보안 적용 대상에 대한 기밀성 시험항목 2

시험목적	PIN이 디지털 프린터에 안전하게 보관되는지 확인한다.
시험절차	1. 보안인쇄 설정 화면으로 들어간다. 2. PIN을 입력한다. 3. 디지털 프린터로 가서 앞에서 설정한 PIN을 입력하고 문서를 출력한다. 4. 디지털 프린터 내의 하드디스크를 분리, 하드디스크 내에 저장된 PIN을 찾는다. 5. PIN이 노출되는지 확인한다.

<표 20>과 관련된 시험 시 보안문서가 디지털 프린터 내에 암호화되어 저장되는지 확인해야 하며 암호화에 사용된 알고리즘의 적절성을 확인해야 한다. 또한 특정 부분에서 보안문서를 암호화 하는데 사용된 키에 대한 정보가 노출되는지 확인해야 한다.

〈표 20〉 보안 적용 대상에 대한 기밀성 시험항목 3

시험목적	보안문서가 디지털 프린터에 안전하게 보관되는지 확인한다.
시험절차	1. 보안인쇄 설정 화면으로 들어간다. 2. 규칙에 맞는 PIN을 입력하고 인쇄를 시작한다. 3. 디지털 프린터 내의 하드디스크를 분리, 하드디스크 내에 저장된 보안문서를 조사한다. 4. 보안문서의 기밀성이 유지되는지 확인한다.

5.2.4 PIN의 길이나 입력횟수의 초과 시 차단 여부 확인

<표 21>과 관련된 시험 시 명세서 및 설명서에서 서술하고 있는 PIN의 입력 범위를 확인해야 하며 입력 범위 내에서 PIN을 입력하여 제대로 출력되는지 확인해야 한다. 또한 명세서 및 설명서에서 서술하고 있는 입력범위를 벗어나는 PIN을 입력하였을 경우의 에러메시지 출력 여부를 확인해야 한다.

〈표 21〉 PIN의 지정 길이 초과 시 입력 차단 시험항목

시험목적	PIN 입력 시 지정된 길이를 벗어나는 값을 입력하였을 경우 입력을 차단하는지 확인한다.
시험절차	1. 보안인쇄 설정 화면으로 들어간다. 2. 지정된 PIN의 길이를 초과한 값을 입력한다. 3. PIN이 제대로 입력되는지 확인한다.

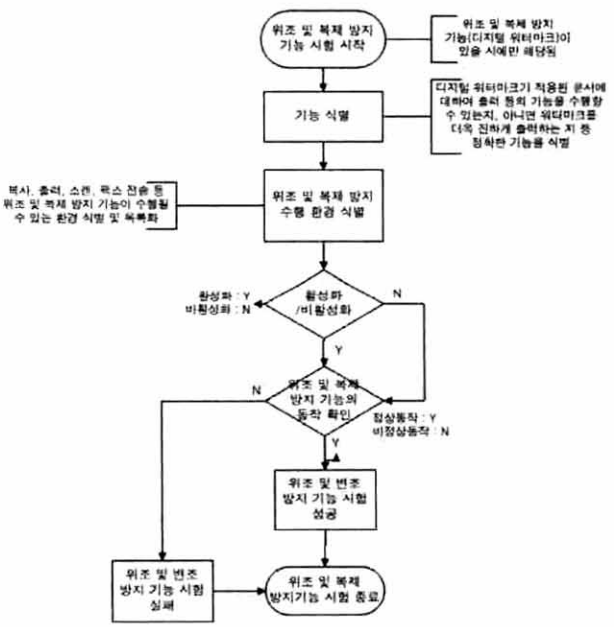
<표 22>와 관련된 시험 시 명세서 및 설명서에서 서술하고 있는 PIN 입력 허용 횟수를 확인해야 하며 입력 허용 횟수 내에서 PIN을 입력하여 제대로 출력되는지 확인해야 한다. 또한 PIN 입력 횟수가 명세서 및 설명서에서 서술하고 있는 허용 횟수를 넘어서는 경우의 에러메시지 출력 여부를 확인해야 한다.

〈표 22〉 PIN의 지정 입력횟수 초과 시 차단 시험항목

시험목적	디지털 프린터 상에서 PIN 입력 시 지정된 횟수를 초과하였을 경우 입력을 차단하는지 확인한다.
시험절차	1. 보안인쇄 설정 화면으로 들어간다. 2. 지정된 범위 내의 PIN을 입력한다. 3. 인쇄를 시작하고, 디지털 프린터에 이전 단계에서 입력한 PIN 외의 PIN을 입력한다. 4. 3의 과정을 반복한다. 5. 에러메시지 또는 출력 여부를 확인한다.

5.3 위조/복제 방지 기술

디지털 워터마크를 활용한 위조 및 복제 방지 기술에 대한 시험항목은 위조/복제 방지를 수행하는 기능 리스트 생성, 워터마크의 실제 반응 확인, 워터마크를 통해 실제 주요 기능 차단확인, 그리고 워터마크 훼손 변조 시 동작여부 확인으로 구성될 수 있다. 위조/복제 방지 기술 시험을 위한 전체 흐름도는 (그림 9)와 같다.



(그림 9) 위조/복제 방지 기술 시험을 위한 흐름도

5.3.1 위조/복제 방지를 수행하는 기능 리스트 생성

개발자가 제공하는 위조/복제 방지 기능에 대해서 시험하기 위해서는 존재하는 기능 리스트를 생성해야 한다. 위조/복제 방지 기능 리스트 생성을 시험하기 위한 시험목적과 시험절차는 <표 23>과 같다.

〈표 23〉 위조/복제 방지 기능 리스트 생성 시험항목

시험목적	위조/복제 방지 기능을 수행하는 디지털 프린터 기능을 식별한다.
시험절차	1. 디지털 프린터의 사용설명서를 참고해서 위조/복제 방지 기능을 수행하는 디지털 프린터 기능을 확인한다. 2. 디지털 프린터의 기능명세서를 참고해서 위조/복제 방지 기능을 수행하는 디지털 프린터 기능을 확인한다. 3. 확인된 기능을 토대로 디지털 프린터 기능 리스트를 생성한다.

5.3.2 디지털 워터마크에 대한 디지털 프린터의 실제 반응 시험

<표 24>는 디지털 프린터에서 실제 워터마크가 출력되는지 확인하는 시험절차이다.

출력된 디지털 워터마크가 입력된 스트링 또는 이미지 파일과 일치하는지 확인하기 위하여 스트링의 경우 특수문자 및 기호에 대한 정상 출력여부를 시험해야 하며 제한된 스트링의 크기를 초과하여 입력 한 후, 에러 메시지 또는 정상출력 여부를 확인한다. 또한 다양한 폰트의 스트링에 대한 워터마크 출력 여부를 확인해야 하며 이미지 파일의 경우, 지원하는 이미지 포맷 및 미지원 이미지 포맷에 대해서도 정상출력 여부를 확인해야 한다. 제한된 이미지의 크기를 초과하여 입력한 후, 에러 메시지 또는 정상 출력 여부를 확인해야 한다.

〈표 24〉 디지털 워터마크의 실제 반응 확인 시험항목

시험목적	실제 디지털 워터마크가 설정에 따라 정상적으로 출력되는지에 대한 여부를 확인한다.
시험절차	1. 명세서 및 설명서에서 제공하고 있는 워터마크 출력방법을 그대로 따라한다. 2. 명세서 및 설명서와 차이점이 있는지 확인한다. 3. 출력된 디지털 워터마크가 입력된 스트링 또는 이미지 파일과 일치하는지 확인한다. 4. 출력 용지의 크기 및 종류 변경에 따른 워터마크의 정상 출력 여부를 확인한다. 5. 상기 수행한 절차 및 에러 메시지 출력 등의 전체 동작과정이 명세서 및 설명서에서의 서술과 동일한지 확인한다.

5.3.3 디지털 워터마크를 통해 실제 주요기능 차단 여부 확인

디지털 워터마크가 인쇄된 문서에 대해 복사, 스캔, 출력, 팩스 전송 등의 기능이 차단되는지 여부를 확인하기 위한 시험방법은 <표 25>와 같다.

5.3.4 디지털 워터마크 훼손/변조 시 동작여부 확인

<표 26>과 <표 27>은 디지털 워터마크 기술의 훼손/변조 시 동작여부를 시험하기 위한 시험목적과 시험절차이다.

<표 26>과 관련된 시험 시 짧은 길이의 스트링 또는 특수문자 및 기호를 워터마크로 사용할 경우와 작은 크기의 이미지 파일을 워터마크로 사용해 본 경우에 대해서도 확인해야 한다.

〈표 25〉 디지털 워터마크를 통한 실제 주요 기능의 차단여부 확인 시험항목

시험목적	디지털 워터마크가 인쇄된 문서에 대해 복사, 스캔, 출력, 팩스 전송 등의 기능이 실제 차단되는지에 여부를 확인한다.
시험절차	1. 명세서 및 설명서에서 제공하고 있는 워터마크 출력방법을 그대로 따라한다. 2. 워터마크가 적용된 문서에 대하여 복사, 스캔, 출력, 팩스 전송 등의 기능을 수행한다. 3. 워터마크가 적용된 문서에 대하여 복사, 스캔, 출력, 팩스 전송 등의 단일 기능에 대하여 반복 수행한다. 4. 상기 수행한 복사, 스캔, 출력, 팩스 전송 등의 기능이 정상적으로 수행되는지 확인한다. 5. 상기 수행한 절차 및 에러 메시지 출력 등의 전체 동작과정이 명세서 및 설명서에서의 서술과 동일한 지 확인한다.

〈표 26〉 디지털 워터마크 훼손 및 변조를 통한 원본 손상여부 확인 시험항목

시험목적	디지털 워터마크 훼손 및 변조 시, 원본에 충분한 손상이 가는지 확인한다.
시험절차	1. 디지털 워터마크가 특정 영역에 치우쳐 있으면 해당 영역에 대한 위조, 변조 및 삭제가 가능해지므로 워터마크가 문서 전 영역에 걸쳐 골고루 퍼져 있는지를 확인한다. 2. 디지털 워터마크가 인쇄되지 않은 부분을 통해 문서 내용이 충분히 파악 가능한지를 확인한다. 3. 일정 길이 이상의 스트링 또는 일정 크기 이상의 이미지 사용 권고하는지에 대한 내용을 확인한다. 4. 일정 길이의 스트링 또는 일정 크기의 이미지에 대하여 디지털 워터마크가 원본문서의 위조 및 복제 방지를 충분히 방지하는 지 확인한다.

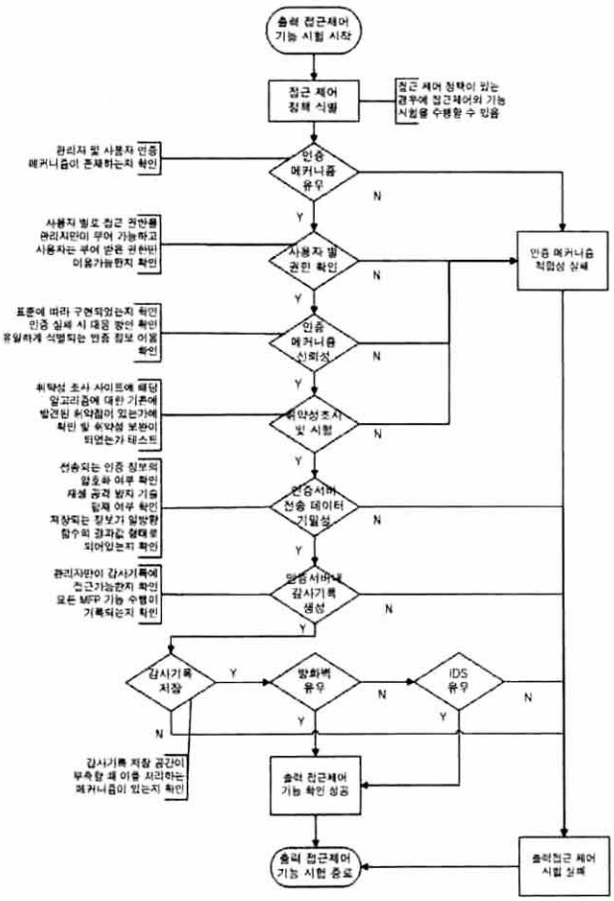
〈표 27〉 디지털 워터마크 변조 시 주요 기능의 정상 동작 여부 확인 시험항목

시험목적	디지털 워터마크의 일부를 변조했을 시 해당 기능의 정상 동작 여부를 확인한다.
시험절차	1. 디지털 워터마크가 적용된 문서에 대하여 일부 변조를 시도한다. 단, 디지털 워터마크가 적용된 원본 문서 내용을 확인할 수 없을 정도의 변조는 시도하지 않는다. 2. 상기 수행한 변조 시도에 대하여 복사, 출력, 스캔 및 팩스 전송 기능이 정상적으로 동작하는지 확인한다. 3. 변조 시도를 복합적으로 적용한 후 2의 과정을 수행한다. 이때에도 디지털 워터마크가 적용된 원본 문서 내용을 확인할 수 없을 정도의 변조는 시도하지 않는다.

<표 27>과 관련된 시험 시 디지털 워터마크에 적용된 스트링 및 이미지 일부를 가리거나 싸인펜 등을 이용하여 인위적으로 변조한 경우에 대해서도 확인해야 한다. 또한 디지털 워터마크가 적용된 문서에 대해 위치를 변경하거나 비스듬하게 놓은 경우에 대해서도 확인해야 한다.

5.4 출력 접근제어 기술

사용자 인증을 사용한 출력 접근제어 기술에 대한 시험항



(그림 10) 출력 접근제어 기술 시험을 위한 흐름도

목은 출력 접근제어를 수행하는 기능 리스트 생성, 사용자별 접근제어 정책 확인, 인증 메커니즘, 인증서버 동작 시험과 인증 메커니즘의 적합성 확인, 인증 서버의 안전성 확인으로 구성된다. 출력 접근제어 기술 시험을 위한 전체 흐름도는 (그림 10)과 같다.

5.4.1 출력 접근제어를 수행하는 기능 리스트 생성

개발자가 제공하는 출력 접근제어 기능에 대해서 시험하기 위해서는 존재하는 기능 리스트를 생성해야 한다. 출력 접근제어 기능 리스트 생성을 시험하기 위한 시험목적과 시험절차는 <표 28>과 같다.

〈표 28〉 출력 접근제어 기능 리스트 생성 시험항목

시험목적	출력 접근제어 기능을 수행하는 디지털 프린터 기능을 식별한다.
시험절차	1. 디지털 프린터의 사용설명서를 참고해서 출력 접근제어 기능을 수행하는 디지털 프린터 기능을 확인한다. 2. 디지털 프린터의 기능명세서를 참고해서 출력 접근제어 기능을 수행하는 디지털 프린터 기능을 확인한다. 3. 확인된 기능을 토대로 디지털 프린터 기능 리스트를 생성한다.

5.4.2 사용자별 접근제어 정책 확인

<표 29>, <표 30>, <표 31>까지는 사용자별 접근제어 정책 확인을 위한 시험목적과 시험절차를 나타낸 것이다.

<표 29>와 관련된 시험 시 관리자 및 사용자 계정 생성 시 입력되는 정보를 확인해야 하며 관리자 모드에서 수행 가능한 작업과 사용자 모드에서 수행 가능한 작업을 확인해야 한다.

〈표 29〉 사용자별 접근제어 정책 시험항목 1

시험목적	관리자 및 사용자의 접근제어 정책을 확인한다.
시험절차	1. 명세서와 설명서에 관리자 및 사용자의 접근제어 정책이 서술되어 있는지 확인한다. 2. 명세서와 설명서에 서술된 내용에 따라 관리자 계정과 사용자 계정을 생성한다. 3. 생성된 관리자 계정과 사용자 계정을 사용하여 각각 인증을 시도한다. 4. 관리자가 수행할 수 있는 작업과 사용자가 수행할 수 있는 작업을 비교한다.

<표 30>과 관련된 시험 시 평가자는 명세서와 설명서에 관리자 모드와 사용자 모드 인증 절차가 서술되어 있는지 확인해야 하며 각각 관리자 모드와 사용자 모드로 인증 시 입력되는 정보와 인증 절차가 서로 상이한지 확인해야 한다.

〈표 30〉 사용자별 접근제어 정책 시험항목 2

시험목적	관리자 및 사용자 인증 메커니즘을 확인한다.
시험절차	1. 명세서와 설명서에 서술된 내용에 따라 관리자 모드와 사용자 모드로 각각 인증을 시도한다. 2. 관리자 모드와 사용자 모드로 인증 시 제공되는 기능의 차이점을 확인한다.

<표 31>과 관련된 시험 시 사용자가 접근 가능한 기능과 관리자가 접근 가능한 기능을 구별하여 확인해야 한다.

〈표 31〉 사용자별 접근제어 정책 시험항목 3

시험목적	역할 별로 부여되는 권한에 대한 적합성을 확인한다.
시험절차	1. 평가자는 관리자 모드와 사용자 모드로 각각 인증을 시도한다. 2. 인증 후 관리자와 사용자가 각각 접근 가능한 기능을 확인한다. 3. 사용자가 접근 가능한 기능 중 관리자가 접근 가능한 기능이 존재하는지 확인한다.

5.4.3 인증 메커니즘, 인증 서버 동작 시험

<표 32>부터 <표 35>는 인증 메커니즘과 인증 서버가 올바르게 동작하는지 확인하기 위한 시험항목에 대한 시험방법이다.

<표 32>와 관련된 시험 시 연속 인증 실패 후 일정 기간 계정 잠금이 수행되는지 확인해야 하며 계정 잠금을 어느 기간까지 설정 가능한지 확인해야 한다. 또한 감사 기록을

바탕으로 연속 인증을 시도한 사용자에 대해 추적성을 제공하는지 확인해야 하며 관리자는 일정한 주기로 감사기록을 검토할 수 있는 기능이 있는지 확인해야 한다.

〈표 32〉 인증 메커니즘 기능 시험 1

시험목적	연속된 인증 실패 후 대응 방안 존재 여부를 확인한다.
시험절차	1. 평가자는 명세서와 설명서에 서술되어 있는 인증 절차대로 잘못된 인증을 연속적으로 수행한다. 2. 연속 인증 실패 후 추가 인증 시도 시 인증 기능 제한 메시지를 출력하는지 확인 한다. 3. 메시지 출력 후 같은 계정을 사용해서 추가 인증을 시도한다. 4. 해당 계정으로 추가 인증을 시도 할 수 없음을 알리는 메시지를 출력하는지 확인한다. 5. 인증 실패 후 관리자에게 감사 기록이 전송되는지 확인한다. 6. 일정 기간이 지난 후 재인증을 시도한다. 7. 일정기간이 지나기 전 디지털 프린터 재부팅 후 인증을 시도한다.

<표 33>의 경우 사용자가 관리자에 의해 설정된 권한 이외의 모든 기능을 수행하여 작업이 이루어지는지 확인해야 하고 인증을 거친 사용자가 다른 사용자로 위장 가능한 지 확인해야 한다. 또한 인증 과정을 여러 번 수행할 경우 위와 같은 결과가 발생하는지 확인해야 한다.

〈표 33〉 인증 메커니즘 시험항목 2

시험목적	인증을 거친 사용자 별 접근 권한 설정을 확인한다.
시험절차	1. 사용자 별 권한 부여(인쇄, 복사, 팩스 등)를 오직 관리자만이 설정할 수 있는지 확인한다. 2. 인증 받은 사용자가 관리자가 설정한 권한만 이용할 수 있는지 확인한다.

<표 34>의 경우 비정상적인 행동이 탐지된 후 이를 관리자에게 알리는지 확인해야 하며 해당 작업이 보류되고 관리자의 확인을 거쳐 수행되거나 해당 작업이 삭제되고 이를 통보하는지 확인해야 한다.

〈표 34〉 인증 메커니즘 시험항목 3

시험목적	인증을 거친 사용자의 비정상적인 행동 탐지를 확인한다.
시험절차	1. 인증을 거친 사용자가 권한이 없는 작업에 대해 지속적인 시도가 있을 시 이를 처리하는 동작의 유무를 확인한다. 2. 인증을 거친 사용자의 평소와 다른 패턴의 업무가 확인 될 때 이를 처리하는 프로세스 존재 유무를 확인한다.

<표 35>와 관련된 시험 시 인증 과정에서 이용하는 함수를 신뢰할 수 있는지 확인해야 하며 인증 정보가 함수를 몇 번 통과한 뒤 저장되는지 확인해야 한다.

〈표 35〉 인증서버의 기능 시험항목

시험목적	인증서버 내에 저장되는 인증정보가 함수를 사용한 결과 값 형태로 저장되어 있는지 여부를 확인한다.
시험절차	1. 인증서버 내 함수 탑재 여부를 확인해야 한다. 2. 평가자는 명세서 및 설명서에서 서술하는 인증 정책대로 계정을 생성한다. 3. 평가자는 자신이 생성한 인증정보와 인증서버 내 저장되는 자신의 계정 정보를 확인한다. 4. 인증정보가 함수를 거치는지 확인한다. 5. 인증정보가 저장되는 폴더를 관리자 외에 일반 사용자가 접근가능한지 확인한다.

5.4.4 인증 메커니즘의 적합성 확인

<표 36>~<표 38>은 인증 메커니즘의 적합성 확인을 위한 시험목적과 시험절차를 나타낸 것이다.

<표 36>과 관련된 시험 시 평가자는 인증 메커니즘에 사용되는 알고리즘을 확인해야 하며 취약성 조사 사이트에서 해당 알고리즘에 대한 취약점을 확인해야 한다. 또한 인증 실패 시, 인증서버 내에서 인증 시도 횟수를 감산하는지 확인해야 한다.

<표 37>과 관련된 시험 시 인증에 사용되는 정보를 확인해야 하며 인증 실패 메시지가 인증 실패에 대한 정보 외의 다른 추가 정보를 제공하는지 확인해야 한다. 또한 인증서버 내 인증 시도 횟수에 대한 설정 기능 존재 유무를 확인해야 한다.

〈표 36〉 인증 메커니즘 적합성 시험항목 1

시험목적	인증 메커니즘의 신뢰여부를 판단한다.
시험절차	1. 네트워크 인증 방식이 신뢰할만한 방식인지 확인한다. 2. 취약성 조사 사이트에 해당 알고리즘에 대한 기존의 취약점이 존재하는지 확인한다. 3. 취약점 발견 시 해당 취약점에 대한 보완이 이루어졌는지 판단한다. 4. 보완 대책 부재로 인한 인증 실패 시 대응 방안을 확인한다.

〈표 37〉 인증 메커니즘 적합성 시험항목 2

시험목적	인증 실패시 대응 방안 존재 여부를 확인한다.
시험절차	1. 평가자는 사용 가능한 인증정보를 이용해서 잘못된 인증을 시도한다. 2. 인증 실패 메시지 출력 여부를 확인한다. 3. 인증서버에서 인증 실패 횟수를 계산하는지 확인한다. 4. 인증 실패 후, 평가자는 인증 시도 전과 비교하여 접근 가능한 기능 및 권한이 동일한지 확인한다.

<표 38>과 관련된 시험 시 명세서 및 설명서에서 서술하고 있는 지원 가능한 인증정보 포맷을 확인해야 하며 사용자 인증 정책이 존재하는지 확인해야 한다. 또한 인증 시

사용되는 인증정보가 사용자의 정보를 바탕으로 생성하는지 확인해야 하며 시스템을 사용하는 모든 사용자가 서로 다른 인증정보를 사용하는지 확인해야 한다.

〈표 38〉 인증 메커니즘 적합성 시험항목 3

시험목적	유일하게 식별 가능한 인증정보사용 여부를 확인한다.
시험절차	1. 계정 생성 시 패스워드 및 기타 인증관련 정책을 사용자에게 공지하는지 확인한다. 2. 평가자는 서로 다른 권한을 가진 두 개의 계정을 생성하고 두 계정 모두 동일한 인증정보를 사용한다. 3. 중복된 인증정보에 대한 경고 메시지를 출력하는지 확인한다. 4. 경고 메시지 출력 후 인증정보 재설정을 요구하는지 확인한다.

5.4.5 인증서버의 안전성 확인

<표 39>~<표 41>은 인증서버의 안전성을 확인하기 위한 시험목적과 시험절차이다.

<표 39>와 관련된 시험 시 평가자는 명세서 및 설명서에서 서술하는 인증 절차 외에 다른 방법의 인증이 가능한지 확인해야 하며 인증 시도 시 입력하는 사용자 정보와 인증서버 내 저장되어 있는 사용자 정보를 확인해야 한다. 또한 인증 시도 전 암호 모듈 작동 여부를 확인해야 하며 재생공격(Replay Attack)에 대한 방지 기능이 있는지 확인해야 한다.

〈표 39〉 인증서버의 안전성 시험항목 1

시험목적	전송되는 인증정보 암호화 여부를 확인한다.
시험절차	1. 평가자는 명세서 및 설명서에서 서술하는 인증 절차대로 인증을 시도한다. 2. 평가자는 인증을 시도한 호스트에서 전송되는 인증정보를 각종 스니핑 도구를 사용해서 패킷을 도청한다. 3. 도청된 정보 내에 평가자가 입력한 정보가 노출되는지 확인한다.

<표 40>과 관련된 시험 시 감사 기록 저장 공간이 부족할 때, 새로운 감사 기록을 기존의 가장 오래된 기록 위에 덮어쓰거나 이를 예방하기 위해 정기적인 백업 기능을 수행하는지 확인해야 한다. 또한 저장 공간 부족을 예방하기 위해 설정된 용량 초과 시 이를 관리자에게 미리 알려주는 기능이 있는지 확인해야 한다.

〈표 40〉 인증서버의 안전성 시험항목 2

시험목적	감사기록 생성 및 적합한 관리 수행 여부를 확인한다.
시험절차	1. 오직 관리자만이 감사기록에 접근 가능한지 확인한다. 2. 로그인, 로그아웃, 복사, 출력, 팩스, 등의 디지털 프린터의 기능 수행 후, 해당 내용이 감사기록에 생성 되는지 확인한다. 3. 감사기록 저장 공간이 부족할 때, 이를 처리하는 메커니즘이 있는지 확인한다.

<표 41>과 관련된 시험 시 방화벽 또는 침입 탐지 시스템 메커니즘 방식을 확인해야 하며 비정상적 패킷을 탐지할 경우 대응 방안의 여부 및 로그 기록 생성 여부를 확인해야 한다.

〈표 41〉 인증서버의 안전성 시험항목 3

시험목적	방화벽 또는 침입 탐지 시스템 구축 여부를 확인한다.
시험절차	1. 방화벽 또는 침입 탐지 시스템의 여부를 확인한다. 2. 방화벽 또는 침입 탐지 시스템의 동작 여부를 확인한다. 3. 방화벽 또는 침입 탐지 시스템이 동작하지 않을 경우, 이를 해결하는 메커니즘이 있는지 확인한다.

6. 결 론

본 논문에서는 국내·외 디지털 프린터 보안기능 개발 동향과 디지털 프린터 보안기능 시험수행기관 평가 현황을 분석하고, 표준화 동향을 살펴보았다. 이어 국내·외 디지털 프린터에 탑재되어 있는 보안기능을 분석하였으며, 디지털 프린터 보안기능별 기반기술로써 잔여정보 보호 기술, 부정 출력/무단 사용 방지 기술, 위조/복제 방지 기술, 출력 접근 제어 기술을 분석하였다. 그 결과 공통평가기준에 따라 이에 대한 시험항목을 도출하고 해당 기능의 시험 방법을 제시하였다.

최근 디지털 프린터는 컨버전스 시대에 발맞추어 프린터, 스캐너, 복사기, 팩스 등의 기기를 통합하여 사용자에게 사무기기가 차지하는 공간을 줄이게 하고 비용은 감소시키면서 업무효율은 극대화하고 있다. 따라서 디지털 프린터에 대한 수요는 계속적으로 증가하고 있는 추세이다. 이에 따라 디지털 프린터에서 사용하는 보안 기술에 대한 중요성도 강조되고 있다.

이에 본 논문에서 제시한 디지털 프린터에 대한 전반적인 보안기능 설명과 시험방법론은 개발자에게는 보다 안전한 제품을 설계하고 개발하는데 도움을 줄 것이며, 평가자에게는 디지털 프린터를 이해하고, 이에 대한 평가를 적절하게 수행하는데 도움이 될 것이다. 뿐만 아니라 사용자에게는 널리 사용되고 있는 디지털 프린터를 통해서도 개인정보 및 기업 기밀정보가 침해될 수 있음을 경고함으로써 보다 안전한 정보기기 운영 환경 구축과 사용에 도움을 주는데 공헌할 것이다.

참 고 문 헌

[1] 한국특허정보원, "디지털 워터마킹의 기술개발 현황 및 기업분석", 2003.

[2] 정보통신연구진흥원, "디지털 컨텐츠의 저작권 보호 및 인증 기술에 관한 조사연구", 2002.
[3] NIST, "http://security.isu.edu/pdf/nistiadraft.pdf"
[4] 한국정보보호진흥원, "중고 PC 데이터 복구 방지 방법 안내", 2005.
[5] 이진우, 남정현, 김승주, 원동호, "SSL/TLS, WTLS의 현재와 미래", 정보보호학회지 제14권 4호, 2004.
[6] COACT Inc. CAFE Laboratory, "http://www.coact.com"
[7] Computer Sciences Corporation, "http://www.csc.com/solutions/security/offerings/1093.shtml"
[8] Electronic Commerce Security Technology Laboratory Inc Evaluation Center, "http://www.ecsec.jp/english_index.html"
[9] Information Technology Security Center Evaluation Department, "http://www.itsc.or.jp/en"
[10] Mizuho Information & Research Institute, Inc. Center for Evaluatio of Information Security, "http://www.mizuho-ir.co.jp/english/"

조 영 준
e-mail : yjcho@security.re.kr
2008년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 암호이론, 정보보호, 보안평가

이 광 우
e-mail : kwlee@security.re.kr
2005년 성균관대학교 정보통신공학부(학사)
2007년 성균관대학교 전자전기컴퓨터공학과(석사)
2007년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야 : 암호이론, 정보보호, 네트워크 보안, 전자투표

조 성 규
e-mail : skcho@security.re.kr
2008년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)
2008년 ~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 디지털 포렌식, 네트워크 보안, 암호이론

박 현 상
e-mail : hspark@security.re.kr
2007년 한성대학교 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 금융보안, 정보보호

이 형 섭
e-mail : hslee@security.re.kr
2005년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 디지털 포렌식, 금융보안

이 현 승
e-mail : hsrhee@security.re.kr
2008년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 네트워크 보안, 금융보안

김 송 이
e-mail : s2kim@security.re.kr
2006년 강남대학교 지식정보공학부(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 네트워크 보안, 키관리, 정보보호

차 욱 재
e-mail : wjcha@security.re.kr
2005년 서울산업대학교 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 네트워크보안, IPTV, DRM, 정보보호

전 웅 렬

e-mail : wrjeon@security.re.kr

2006년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)

2008년 성균관대학교 전자전기컴퓨터공학과(석사)

2009년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정

관심분야 : 보안성 평가제도

원 동 호

e-mail : dhwon@security.re.kr

1976년~1988년 성균관대학교 전자공학과(학사, 석사, 박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공업대 객원연구원

1988년~2003년 성균관대학교 교학처장, 전지전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

2002년~2003년 한국정보보호학회장

2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT감사 자문위원

2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장

관심분야 : 암호이론, 정보이론, 정보보호

김 승 주

e-mail : skim@security.re.kr

1994년~1999년 성균관대학교 정보공학과(학사, 석사, 박사)

1998년~2004년 한국정보보호진흥원(KISA) 팀장

2004년~현 재 성균관대학교 정보통신공학부 교수

2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원

2007년~현 재 대검찰청 디지털수사 자문위원

2007년~현 재 전자정부서비스보안위원회 사이버침해사고대응 실무위원

2008년~현 재 기술보증기금 외부자문위원

2008년~현 재 수원시 지역 정보화 촉진 협의회 위원

2008년~현 재 한국은행 금융정보화추진분과위원회 자문위원

2008년~현 재 법무부 법률서비스산업 경쟁력강화 위원회 위원

관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET