情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

기업 비밀정보 유출 방지 및 보호 관점에서의 디지털 복합기 보안 기술 동향 분석

이 광 우*, 김 승 주**

요 약

최근 주요 기업에서 기업 비밀정보가 유출되는 보안사고가 빈번히 발생함에 따라, 기업의 비밀정보 유출 방지 및 보호에 대한 사회적 관심이 높아지고 있다. 기업 비밀정보의 유출은 해당 기업뿐만 아니라 국가적으로도 막대한 손실을 초래할 수 있다는 문제를 가지고 있다. 이러한 문제를 해결하기 위해 각 기업에서는 보호구역의 설정, 출입허가 또는 출입시 휴대품 검사 등의 물리적인 유출 차단 방법을 구축하고 있으며, 기업 기밀문서에 대해서는 DRM(digital right management)을 활용한 문서유출 방지 및 네트워크 트래픽 차단 등 다양한 방법을 적용하고 있다. 하지만, 전자파일 형태로 존재하는 기밀문서는 인터넷 또는 네트워크에 연결된 PC 및 서버를 통해 전자우편(E-mail), 메신저, 게시판 등으로 쉽게 유출될 수 있어 많은 문제점을 가지고 있다. 이러한 시점에서 최근 널리 보급되고 있는 디지털 복합기는 문서 저장을 위한 하드디스크(HDD) 및 네트워크 응용 서비스를 포함하고있어 다양한 보안 취약점에 노출되어 있다. 따라서 기업 비밀정보 유출 방지와 보호를 위해서는 디지털 복합기에 대한 보안 기술 연구가 필수적이다. 이에 본고에서는 기업 비밀정보 유출 방지 및 보호 관점에서 디지털 복합기 개발 현황을 살펴보고, 보안상 문제점을 해결하기 위해 연구되고 있는 디지털 복합기 보안 기술에 대한 동향을 살펴보고자 한다.

Ⅰ. 서 론

최근 주요 기업에서 기업 비밀정보가 유출되는 보안사고가 빈번히 발생함에 따라, 기업의 비밀정보 유출 방지 및 보호에 대하여 사회적 관심이 높아지고 있다. 국정원 산업기밀보호센터의 통계자료에 따르면, 2004년부터 2009년까지 국내의 첨단기술을 해외로 불법 유출하다가 적발한 건수는 총 203건이었으며, 그 수는 매년 지속적으로 증가하고 있다[1]. 또한 기업 비밀정보의 유출 분야도 기존 첨단 전자정보통신 분야에서 자동차, 조선을 비롯한 기계, 화학 등의 전분야로 확대되고 있는 추세이다. 이러한 기업 비밀정보 유출에 따른 피해는 해당 기업에 그치지 않고 국가 경제에 막대한 손실을 초래할 수 있어 심각한 문제를 가지고 있다. 이와 같은 문제를 해결하기 위하여, 각 기업에서는 보호구역의 설정, 출입허가 및 출입시 휴대품 검사 등의 물리적인 유출 차단 방법을 구축하고 있고, 기업 내에서 활용되는 기밀문서에 대해서는 DRM(digital right management)을 기반으로 한 시스템을 구축하여 문서유출을 방지하고자 노력하고 있으며, 네트워크망 분리 및 중요 네트워크 트래픽 필터링을 통해 기밀 정보의 유출을 차단하는 등 다양한 보안 대책을 적용하고 있다. 일반적으로 기업 비밀정보에는 칩, 부품, 시제품, 회계장부 등과 같이 물리적인 장비나 출력된 형태의 문서로 존재하는 것도 있지만, 설계도면, 제품설계서, 마케팅 전략 회의록, 사진 등과 같이 전자파일 형태로 존재하는 것도 있다. 물리적인 장비나 USB 등의 저장매체를 통한 기밀자료의 유출 시도는 출입시 휴대품 검사 과정을 통해 차단할 수 있으나, 전자파일 형태로 존재하는 기밀문서는 사내에서 네트워크에 연결된 PC 및 서버를 통해 전자우편(E-mail), FTP, 메신저, 웹 게시판 등으로 쉽게 유출될 수 있고, 비밀정보가 유출되었을지라도 피해 사실에 대한 인지가

* 성균관대학교 정보보호그룹 (kwlee@security.re.kr)
** 성균관대학교 정보통신공학부 부교수(skim@security.re.kr)

어렵고, 단발성 범죄로 기술 유출에 대한 증거 확보 및 추적이 어렵다는 문제점을 갖는다. 따라서 산업 스파이들의 주요 기밀정보 유출 수단이 되고 있다.

이러한 시점에 최근의 기업 환경에서는 업무 효율성 향상, 편리성 증대, 사무기기 공간의 최소화 측면에서 기존 스캐너, 복사기, 팩시밀리, 프린터를 하나로 통합한 디지털 복합기가 널리 보급되고 있다. 특히 디지털 복합기는 기존 스캐너, 복사기, 팩시밀리, 프린터의 기능뿐만 아니라, 문서 저장을 위한 하드디스크(HDD)와 다양한 네트워크 응용 서비스를 포함하고 있는 복합 기능 제품으로써, 기존 기능들이 결합되면서 각각의 기기가 가지고 있는 문제점을 비롯하여 예기치 못한 다양한 보안 위협을 포함할 수 있다.

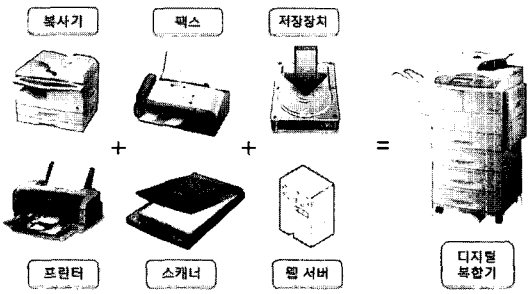
예를 들어, 산업 스파이들은 디지털 복합기 내에 탑재되어 있는 하드디스크 및 메모리를 분리하여 저장장치 내의 기업 기밀정보 유출을 시도할 수 있으며, 팩시밀리 기능을 제공하는 팩스 카드를 통해 디지털 복합기 내에 저장되어 있는 정보를 유출할 수 있다. 따라서 최근 디지털 복합기가 기업 비밀정보 유출을 일으킬 수도 있는 정보기기로 주목받고 있다.

이러한 보안상 문제점들을 해결하기 위해 디지털 복합기 관련 업체 및 연구기관에서는 다양한 보안 대책을 수립하고, 해당 기능을 탑재하고 있으며, IEEE P2600 Working Group 등의 표준화 작업반을 구성하여 디지털 복합기에 대한 보안 대책을 수립하기 위해 많은 노력을 기울이고 있다. 이에 본고에서는 기업 비밀정보 유출 방지 및 보호 관점에서 디지털 복합기의 문제점을 살펴보고, 이러한 문제를 해결하기 위해 연구되고 있는 디지털 복합기 보안 기술들에 대한 국내·외 연구 개발 동향을 살펴보고자 한다.

Ⅱ. 디지털 복합기 개요

현재 대다수의 기업 및 공공기관에서는 업무의 효율성 증대와 경비 절감을 위해 기존 스캐너, 복사기, 팩시밀리, 프린터를 하나로 통합하여, 인쇄/복사/스캔/팩스 기능이 가능하고, 대용량 문서 데이터 저장 및 다양한 네트워크 응용 서비스(웹 서버, FTP 등) 기능을 제공하는 디지털 복합기를 널리 사용하고 있다.

이러한 기기는 디지털 프린터, 디지털 복합기, HCD (Hard-Copy Device), MFP(Multi-Function Printer),



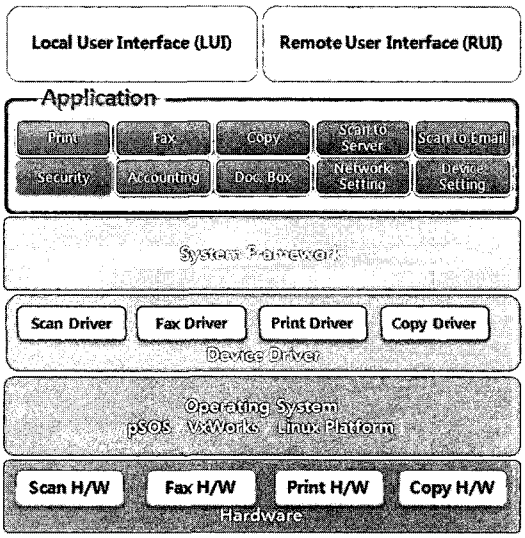
〔그림 1〕 디지털 복합기의 정의

MFD (Multi-Function Device), MFP(Multi-Function Peripheral) 등으로 불리고 있다.

최근의 디지털 복합기는 기존 제품의 단순한 조합이 아닌 다양한 하드웨어 및 소프트웨어를 장착하여 그 성능이 나날이 발전하고 있다. 디지털 복합기에 접속할 수 있는 네트워크 인터페이스의 경우, 기존에는 RJ45 인터페이스를 이용한 네트워크 연결이 유일한 접속 수단이었던 반면, 최근에는 홈 네트워크 기술과 무선 디바이스 기술의 발전으로 인하여 WiFi, 802.11g 무선 네트워크, USB 및 블루투스(Bluetooth)를 이용한 출력 기능을 갖추고 있다. 또한 80 기가바이트 이상의 대용량 하드디스크를 탑재하고 있어, 대용량의 문서 저장이 가능하고, 필요시 언제든지 원하는 문서를 디지털 복합기 내에서 검색하여 출력할 수 있는 기능을 제공하고 있다. 이에 더하여, 최근 출시되고 있는 기업용 디지털 복합기는 ScantoEmail, ScantoFTP 등 다양한 네트워크 응용 서비스를 제공하기 위해 디지털 복합기에 자체웹 서버를 탑재하고 있고, 컬러 LCD 및 터치스크린을 통해 현재 상태를 확인하고 원하는 명령을 수행할 수 있으며, 다양한 응용 프로그램을 이용하여 PC를 통한 문서편집이 없이도 원하는 곳으로 원하는 형태의 파일을 전송할 수 있는 기능까지 가지고 있다. 이처럼 디지털 복합기가 PC의 기능을 모두 포함하고 엔터프라이즈급 서버의 역할까지 담당함에 따라, 기업의 경비 절감은 물론 업무 효율성 증대에도 많은 기여를 하고 있다.

최근 출시되고 있는 복합기 제품의 내부 구조는 다음 그림과 같다.

디지털 복합기는 최하위 계층으로 스캔, 팩스, 출력 기능을 제공하는 하드웨어 장치를 가지고 있으며, 그 위에 하드웨어를 제어하기 위한 운영체제를 포함하고 있다. 기존의 운영체제는 실시간 처리를 위해 pSOS, VxWorks 등과 같은 RTOS(real-time operating system)

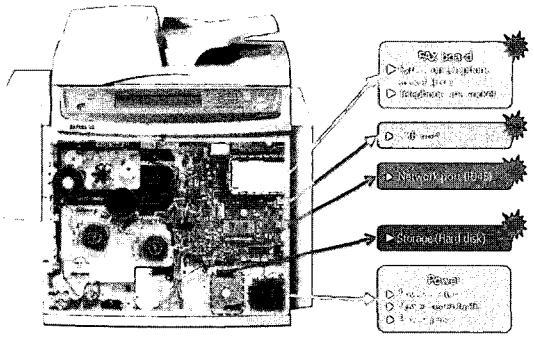


〔그림 2〕 디지털 복합기의 논리적 내부 구조

을 탑재하는 것이 대세였으나, 최근에는 임베디드 하드웨어 기술 및 소프트웨어 기술이 발전함에 따라 임베디드 리눅스를 탑재하는 디지털 복합기가 증가하고 있다. 그 상위 계층으로는 각 하드웨어 장치들을 관리하기 위한 디바이스 드라이버(Device Driver)가 존재하며, 그 위에는 디지털 복합기 서비스를 제공하기 위한 기본 토대가 되는 시스템 프레임워크와 어플리케이션 계층이 있다. 어플리케이션 계층에 탑재된 어플리케이션들이 실제 사용자에게 제공되는 디지털 복합기 기능이 된다. 이러한 어플리케이션에는 출력, 팩스, 복사, Scan ToServer, ScanToEmail, 출력량 정보, 문서 저장함, 네트워크 설정, 장치 설정 등이 있으며, 보안 기능 역시 포함될 수 있다. 이러한 어플리케이션 계층의 설정은 디지털 복합기 자체에 존재하는 터치스크린 LCD인 LUI(Local User Interface)나 RUI(Remote User Interface)를 통하여 접근할 수 있다.

이와 같이 디지털 복합기는 다양한 서브시스템이 통합된 제품으로 설계상 보안을 신중하게 생각하지 않을 경우에는 다양한 취약점에 노출될 수 있어 디지털 복합기의 설계의 중요성이 강조되고 있다. 다음 그림은 디지털 복합기 상에서 취약점이 발생 가능할 수 있는 물리적 인터페이스를 나타낸다.

디지털 복합기가 제공하는 주요 기능인 인쇄, 복사, 스캔, 팩스의 기능은 주로 문서 출력과 관련된 것으로, 디지털 복합기의 기능이 복잡하고 다양해짐에 따라 산



〔그림 3〕 보안 취약성이 발생 가능한 디지털 복합기의 물리적 인터페이스

업스파이가 디지털 복합기를 통해 사내 주요 기밀문서의 인쇄, 복사, 스캔 과정에서 인터넷망 또는 전화망(PSTN)을 통해 기밀정보를 유출될 수 있다는 문제점이 존재할 수 있다. 또한 디지털 복합기 내의 하드디스크는 탈부착이 가능하므로, 하드디스크 자체를 유출할 수 있는 문제점이 존재한다. 이러한 문제점들을 해결하기 위해, 최근 각 디지털 복합기 제조업체에서는 보안 기술을 향상시키기 위해 많은 노력을 기울이고 있다.

Ⅲ. 디지털 복합기 보안 기술 개발 동향

본 장에서는 국내·외 디지털 복합기 보안 기능 개발 동향을 분석한다. 이를 위해, 먼저 디지털 복합기 업체들의 개발 동향을 살펴본다.

3.1 국내·외 디지털 복합기 보안 기능 개발 업체 동향 조사

디지털 복합기의 보안 기능은 크게 사용자 인증 및 식별, 하드디스크 완전삭제, 감사기록 저장, 전송되거나 저장되는 데이터의 암호화, 출력문서 보안 기능, 자체 무결성 시험, 접근권한 제어 등으로 나눌 수 있다. 국내·외 디지털 복합기 관련 보안 기능 주요 개발업체는 [표 1]과 같다

3.2 국내·외 디지털 복합기 제품의 보안 기능 조사

보안 기능이 탑재된 디지털 복합기에서의 일반적인 보안 기능은 크게 패스워드 기반의 인증, 하드디스크 완전 삭제, 그리고 데이터 암호화가 있다. 이러한 기능들

〔표 1〕 디지털 복합기 보안 기능 개발업체 현황

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

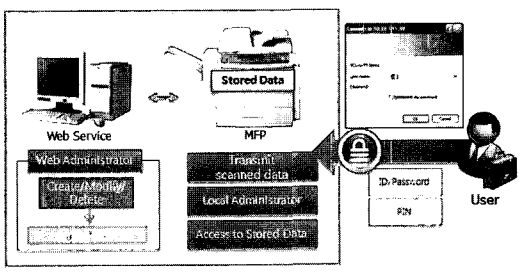
〔표 2〕 디지털 복합기 기종에 따른 보안 기능 탑재 여부

디지털 복합기 개발업체 및 기종	인증 및 식별	암호화	완전 삭제	기타 보안 기능
삼성전자 SCX-6X45	O	O	O	- 감사기록 제공
신도리코 Aficio MP 5000/5000B	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	

은 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 잔여 정보에 대한 보안 문제를 해결하기 위하여 특수한 알고리즘을 적용하여 하드디스크에 대한 완전삭제를 구현하여 잔여 정보에 대한 보안을 강화한다. 또한 하드디스크에 저장되는 데이터에 대하여 검증된 암호 알고리즘을 기반으로 암호화를 수행하여 내부 데이터에 대한 보호를 수행한다. 대표적인 디지털 복합기 개발업체들이 출시한 제품에서의 보안 기능 탑재여부는 [표 2]와 같다.

3.2.1 인증

디지털 복합기에서의 인증 및 식별 기능도 기본적으로 문서를 사용하려는 사용자의 신원과 이에 대한 검증 절차를 수행하며, 대부분의 제품에서는 패스워드 기반의 인증 절차를 사용한다. 디지털 복합기에서는 문서에 대한 복사, 스캔, 인쇄, 팩스 등의 기능을 가지고 있으며, 디지털 복합기가 네트워크와 연결되었을 시에는 이를 활용한 편의기능인 스캔 후 이메일 전송 또는 서버 전송 등의 기능 등이 제공된다. 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 4]와 같다.



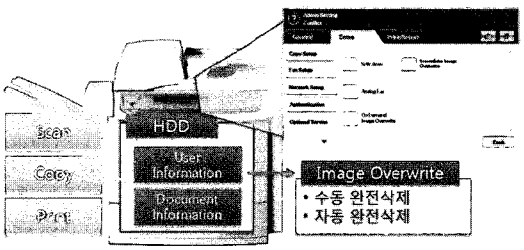
〔그림 4〕 네트워크 인증 및 식별을 위한 전체 구성

3.2.2 데이터 접근제어

디지털 복합기에서 수행되는 기본적인 기능인 복사, 스캔, 출력, 팩스 기능은 대부분 하드디스크 또는 메모

리에 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 복합기에서는 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 복합기에 직접 접근하여 문서에 대한 접근 권한이 있음을 증명하기 위해 미리 저장된 PIN 번호를 입력하여 인증 절차를 수행한 후 해당 문서를 출력 또는 전송하게 된다.

3.2.3 하드디스크 완전삭제



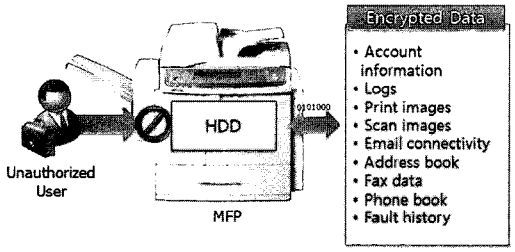
〔그림 5〕 하드디스크 완전삭제 기능

최근 출시되는 대부분의 기업용 디지털 복합기에서는 기본적으로 하드디스크 완전삭제 기능을 제공한다. 디지털 복합기에서 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 복합기 제조업체에서는 하드디스크 완전삭제 기능을 적용하고 있다.

하드디스크 완전삭제 기술 중 하나를 예로 들면 미국방성 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.

3.2.4 암호화

디지털 복합기 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 보안 기능은 하드디스크에 데이터를 기록할 때 시스템 내부적으로 작동한다. 하드디스크에 기록되는 데이터는 암호화 알고리즘으로 암호화 된 후 하드디스크에 기록되며, 하드디스크에 기록된 데이터는 암호화 알고리즘으로 복호화하여 사용될 수 있다.



〔그림 6〕 데이터 암호화 기능

3.2.5 기타 보안 기능

기타 보안 기능으로 디지털 워터마킹과 SSL(Secure Socket Layer) 통신이 있다. 디지털 워터마킹(Digital Watermarking) 기술은 데이터의 복제 및 위조 방지를 위해 사용되는 보안 기능이다[1]. 워터마킹은 저작권 보호, 위·변조 판별, 불법복제 추적, 사용자 제어, 내용 보호, 내용 라벨링 등의 기능을 제공한다[2]. 현재 디지털 복합기에서 워터마크 기술을 이용한 위조 및 복제 방지 기술은 신도리코, 후지제록스, Konica Minolta 등의 일부 제품군에서 활용되고 있다. SSL은 TCP/IP 상의 응용 계층과 전송계층 사이에서 동작하며, 클라이언트와 서버 사이에서 안전한 채널을 생성해준다[5]. 디지털 복합기는 자체적으로 내장된 웹 서버를 기반으로 관리자에게 원격 관리 서비스를 제공하고 있는데, 원격에서 송수신되는 중요 정보에 대한 기밀성 및 무결성을 보장하기 위하여 SSL 프로토콜을 이용한다.

Ⅳ. 디지털 복합기의 신뢰성 및 안전성

디지털 복합기 보안 기능을 개발하고 있는 업체들은 보안 기능 개발 이후 평가기관에 의하여 공통평가기준(CC: Common Criteria)에 근거하여 보안 기능이 제대로 구현되고 시험되었는지를 평가받을 수 있다. 본 장에서는 국내·외 디지털 복합기 보안 기능 관련 시험수행기관 동향을 살펴본다.

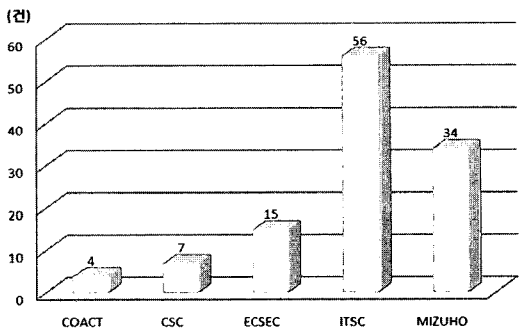
4.1 국내·외 디지털 복합기 보안 기능 시험수행기관 동향

최근의 디지털 복합기는 보안 기능이 탑재된 IT 제품으로 인식되어, 보안 기능성과 이에 적용된 보증수단이 보안 기능 요구사항들을 만족하는가에 대한 신뢰도를 확인하기 위해 공통평가기준에 의해 보안성 평가를 받는다. 본 절에서는 디지털 복합기의 보안 기능성에 대하여 CC 평가를 수행한 시험수행기관들을 조사하고, 조사된 자료를 바탕으로 현재 디지털 복합기의 CC 평가 인증 진행 현황을 살펴본다.

4.1.1 디지털 복합기 보안 기능 평가기관 평가 현황

2002년 이후 현재까지 디지털 복합기 보안 기능과 관련하여 평가를 수행한 평가기관과 평가 의뢰 업체를 중심으로 평가 현황을 조사한 결과, [그림 7]과 같이 디지털 복합기 보안 기능 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 복합기 보안 기능과 관련된 평가에 있어 독보적인 점유율을 차지하고 있다[6][7].

각 평가기관에 평가를 의뢰한 디지털 복합기 보안 기능 개발 업체를 살펴보면, 미국의 COACT에서는 Hewlett-Packard와 Lexmark Inc.가 평가를 받았으며, CSC에서는 Sharp와 Xerox가 평가를 받았다. 또한 일본의 ECSEC에서는 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]. 국내에서는 한국시스템보증(주)이 삼



〔그림 7〕 평가기관별 디지털 복합기 보안 기능 평가현황

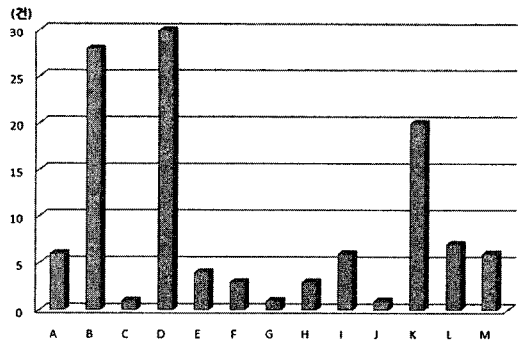
성전자 복합기 평가를 완료한 바 있다. 디지털 복합기 보안 기능 관련 개발 업체에서 평가받은 제품들을 살펴보면, 디지털 복합기 자체를 평가받은 업체도 있었지만, 보안 기능 모듈단위로 평가를 신청한 업체들도 다수 있었다. 또한 디지털 복합기 보안 기능 개발 업체들은 기존에 자사의 제품에 대하여 평가를 수행하였던 평가기관에 다시 평가 신청하는 것으로 나타났다.

4.1.2 국가별 평가 동향

2002년부터 현재까지 국가별 디지털 복합기 보안 기능 평가 현황을 살펴보면 일본과 미국이 주를 이루고 있다. 현재까지 평가인증을 받은 디지털 복합기 보안 기능 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. 반면에 국내에서는 한국시스템보증(주)이 1건의 복합기 평가를 완료한 바 있다.

4.1.3 디지털 복합기 평가 의뢰 업체 현황

디지털 복합기 평가 의뢰 업체의 현황을 살펴본 결과 [그림 8]과 같이 디지털 복합기 보안 기능 관련 평가를 의뢰한 다수의 업체 중에서 Fuji Xerox와 Konica



〔그림 8〕 디지털 복합기 보안 기능 평가의뢰 업체 현황

Minolta, 그리고 Sharp가 디지털 복합기 보안 기능과 관련하여 다수의 평가인증을 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

V. 디지털 복합기 연구 및 표준화 동향

본 절에서는 국내·외에서 진행되었던 디지털 복합기 연구 현황 및 표준화 동향을 소개하고, 표준화 연구에서 정의한 자산과 위협을 살펴본다.

5.1 국내 디지털 복합기 연구 동향

현재 국내에서는 삼성전자가 유일하게 디지털 복합기 개발에 참여하고 있다. 삼성전자는 2008년 12월 디지털 복합기로는 국내 최초로 CC 평가 인증을 획득한 바 있으며, 현재 다양한 보안기능이 탑재된 B2B, B2C 모델을 연구 및 제품화하고 있다. 또한 IEEE P2600 Working Group에 참여하여 활발한 표준화 활동을 하고 있다.

국내 학계에서는 성균관대학교가 삼성전자와 산학협력을 통하여 불법토너 방지 기술, 데이터 암호화 모듈, 하드디스크 완전삭제 등의 개발에 참여하고 있으며, 디지털 복합기상에 존재할 수 있는 취약점을 사전에 최소화하기 위해 디지털 복합기에 대한 보안 취약성 침투 시험을 수행하고, 제품의 보안성을 향상시키기 위한 컨설팅을 수행하고 있다.

5.2 국외 디지털 복합기 연구 및 표준화 동향

국외에서의 디지털 복합기 보안 기능 관련 연구로는 CIAC-2304 보고서 및 IEEE P2600 표준화 작업이 있다.

5.2.1 CIAC-2304

국외에서는 디지털 복합기에 대한 취약성 및 위협 분석이 이미 수행된 바 있다. 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 3]과 같다.

〔표 3〕 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

5.2.2 IEEE P2600

IEEE P2600 Working Group은 디지털 복합기 관련 업체들이 모여 구성한 표준화 작업반으로 현재 대다수의 주요 복합기 업체가 참여하고 있다. 이 표준화 활동에서는 디지털 복합기 상에서 발생할 수 있는 위협을 분석하고, 해당 위협을 해결하기 위한 보안 대책을 제시하고 있으며, 디지털 복합기의 보안기능을 평가하기 위하여 공통평가기준(CC)에 기반한 평가기준인 보호프로파일(Protection Profile)을 마련하는 등 많은 노력을 기울이고 있다.

IEEE P2600은 디지털 복합기 내부에 저장된 사용자 데이터와 시스템 관리 데이터, 물리적인 디지털 복합기 자원, 디지털 복합기 운영 펌웨어 등을 디지털 복합기가 보호해야 할 자산으로 정의하였다. IEEE P2600에서는 디지털 복합기가 안전하게 보호해야할 자산의 중요도에 따라 운영 환경을 A,B,C,D의 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 등으로 나누고 있다.

〔표 4〕 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 불법장치를 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 내부망에 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

Ⅵ. 결 론

기업의 비밀정보를 유출하기 위한 산업 스파이가 증가함에 따라 각 기업의 보안 담당자들은 다양한 보안 방법을 도입하여 기업 비밀정보의 유출을 방지하고 차단하기 위해 노력하고 있다. 이러한 측면에서 볼 때, 디지털 복합기는 문서의 복사, 인쇄, 스캔 및 팩스 등의 업무상 필수적인 처리를 수행하며, 특히 사내에서 중요 기밀문서를 다룰 가능성이 크므로 디지털 복합기에 대한 보안을 확보하는 것이 기업 비밀정보의 유출 및 방지를 위하여 매우 중요하다. 하지만 최근 출시되고 있는 디지털 복합기는 장치의 특성상 항상 네트워크에 연결되어 있으므로 디지털 복합기의 보안을 유지하기가 어렵다. 따라서 각 디지털 복합기의 보안 기능을 향상시키기 위하여 다양한 보안 기능을 탑재하고 있으며, 그 성능은 현재 엔터프라이즈급 서버에 가까울 정도로 발전하고 있다.

향후 디지털 복합기가 기업 내에서의 보안 취약점으로 존재하지 않기 위해서, 디지털 복합기 개발업체는 현재 디지털 복합기를 도입하고 있는 업체에서 가지고 있는 문제점을 잘 파악하고, 해당 문제를 해결하기 위한 안전한 솔루션을 개발해야 하며, 설계 단계에서부터 보안을 고려하여야 할 것이다. 또한 기업 내 보안 관리자는 디지털 복합기에서 제공하는 보안 기능을 명확히 파악하여 해당 기업에 맞는 제품 및 솔루션을 도입해야 한다. 마지막으로 공공기관에서 사용되는 디지털 복합기는 다수의 개인정보를 다루게 되므로 국가적으로 민감한 사항이 될 수 있다. 따라서 이에 대한 보안성을 향상시키기 위해, 평가기관에서는 디지털 복합기에 대한 평가 기술을 조속히 확보해야 할 것이다.

참고문헌

[1] 한국특허정보원, "디지털 워터마킹의 기술개발 현

황 및 기업 분석", 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/".
[11] 국가정보원, "http://service4.nis.go.kr/servlet/page".

〈著者紹介〉

이 광 우 (Kwangwoo Lee)
학생회원
2005년 2월: 성균관대학교 정보통신공학부 (공학사)
2007년 2월: 성균관대학교 컴퓨터공학과 (공학석사)
2007년 2월~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
<관심분야> 암호이론, 보안성 평가, 전자투표, 정보보호제품 취약점 분석

김 승 주 (Seungjoo Kim)
종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: 한국정보보호진흥원 팀장
2004년~현재: 성균관대학교 정보통신공학부 교수
2001년~현재: 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현재: 교육인적자원부 유해정보차단 자문위원, 디지털 콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현재: 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부자문위원, 전자정부 서비스보안위원회 사이버 침해사고대응 실무위원회 위원
<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET