정 보 보 호 학 회 지
제28권 제6호, 2018. 12

방위산업기술 자료의 외부 반출 시 보호 방안

장 경 준*

요 약

방산업체는 물리적 망분리를 의무적으로 구축하고 군사기밀 및 방위산업기술을 보호하는 정보보호체계를 운용 중이다. 그러나, 물리적 망분리를 운용하더라도 다양한 경로로 방위산업기술 자료가 외부로 반출되어 불법적인 유출이 발생할 수 있다. 본 논문에서는 물리적 망분리 시스템의 문제점을 진단해 보고 방위산업기술 자료가 협력업체 등 외부로 반출되는 경우와 출력물에 의해 유출되는 경우에 대해 유출 방지 방안을 제시하였다.

Ⅰ. 서 론

우리나라 국방과학기술 수준이 발전함에 따라 현재 세계 9위권으로 평가받고 있으며 방산수출액도 ‘06년 2.5억불에서 ’14년 이후 매년 30억불을 넘어 크게 증가하고 있다. 이와같이 방산수출 및 기술이전 등의 증가로 대외 기술유출 가능성이 점차 증대됨에 따라 방위사업청에서는 산업스파이와 해킹 등으로부터 방산기술을 보호하기 위해 지난 ‘15년 12월 방위산업기술보호법을 제정하기에 이르렀다[1]. 또한 방위산업기술을 주로 보유하고 있는 방산업체에 대해서는 물리적인 망 분리를 강제하여 방위산업기술 보호에 만전을 기하고 있다[2].

방위산업기술 자료는 그 특성상 방위사업청・국방과학연구소 등 군 관련 기관 및 협력(하도급)업체들과 공유를 필요로 한다. 어떤 업체도 수주한 방산물자를 100% 자체 단독생산이 불가능하며 하도급 등 협업을 통해 부품을 조달할 수 밖에 없다. 군 관련 기관이나 방산업체들은 물리적인 망 분리는 물론 내부망의 방위산업기술 자료는 암호화 되어 해킹 등 비 정상적인 방법으로 유출되어도 안전하다. 그러나 하도급 업체로 넘어가면 기본적인 방화벽도 없는 업체가 다수로 사실상 보안의 사각지대이다.

대기업의 기술자료를 확보하기 위한 해커들의 공격방법이 최근 협력사를 통한 우회해킹 기법으로 전환되고 있는데 이는 대기업과 방산업체들은 정보보호시스템을 지속적으로 강화하고 있는 반면 중소기업이 대부분인 협력(하도급 포함)업체들은 보안수준이 매우 낮기 때문이다. 따라서 대기업과 방산업체는 현재의 보안수준을 지속적으로 유지 발전시켜야 하고 협력업체를 통한 방위산업기술 보호를 위한 대책을 보강할 필요가 있다.

본 논문에서는 물리적인 망분리를 완료한 방산업체를 기준으로 취약점을 분석해 보고, 방위산업기술 자료가 협력업체 등 외부로 반출되는 경우와 출력물에 의해 유출되는 경우에 대해 유출 방지 방안을 살펴본다.

Ⅱ. 현 실태와 문제점

2.1. 중소 하도급 업체 보안 수준

중소벤처기업부와 대・중소기업・농어업협력재단에서 발간한 ‘17년 중소기업 기술보호 수준 실태조사를 보면 표 1과 같다. 표에서 나타나듯이 중소업체는 대기업과 비교해 보안수준이 매우 낮다는 것이 명확히 드러난다. 또한 명지대학교에서 수행한 방산관련 업체들의 기술보호 수준 진단 결과에 의하면[3], (방산업체는 대기업과 중소업체로 양분하였고 방산업체의 하도급 업체는 조사표본 247개 업체중 중소기업이 약 99%인 245개였음) 방산 대기업은 64.7%가 해킹 및 자료유출방지를 위해 정보보호시스템을 구축하고 있어 비교적 양호하였으나 방산 중소기업은 30.8%로 저조하였으며 방산 하도급업체는 DRM과 같은 고가의 시스템은 차지하더라도 가장 기본적인 방화벽도 25.9% 밖에 설치하지 않아 정보통신 시스템을 통한 기술유출에 무방비 상태임을 보여주고 있다.

* 명지대학교 산업대학원 융합보안학과 객원교수 (jkj4290@naver.com)

〔표 1〕 중소기업/중견기업/대기업 기술보호 역량점수 결과

구 분	중소기업 점수(점)	중견기업 점수(점)	대기업 점수(점)
2017년	51.3	60.3	67.9
2016년	49.3	59.4	67.2
2015년	47.6	-	66.8
2014년	45.6	-	65.6
2013년	43.3	-	65.5
2012년	34.9	-	62.4
2011년	42.6	-	75.4

2.2. 하도급업체를 통한 보안사고 사례

2.2.1. 정보보호시스템 취약점 이용

‘09.3월경 경남 소재 000 방산업체 연구소에 근무하던 차장 △△△은 ○○○ 성능개량 사업을 分社하여 추진하도록 임무를 고지 받아 창원지역에 하도급업체를 설립, 부품을 납품하면서 자신이 근무하던 000방산업체 연구소(통제구역)에 근무인과를 위요, 3년간 무단으로 출입하면서 방산기술을 유출하였는데 유출 수법을 보면 중식시간에 모든 연구원들이 한꺼번에 나가고 화면보호기가 5분후에 가동된다는 점을 이용, 연구원들에게는 “긴급한 통화만하고 금방 가겠다”고 한 후 연구원들이 모두 나가면 자신이 필요로 하는 자료가 있는 연구원 PC로(15년 정도 근무하여 각 연구원 PC에 어떤 자료가 있는지 알고 있는 상태) 이동하여 USB・외장형 하드・메일 등을 이용하여 자료를 빼돌린 후 사무실과 自家에 각각 보관하다 사무실에 보관하던 자료가 악성코드에 의해 유출되었다.

2.2.2. 하도급업체 퇴사자를 통한 방산기술 유출

‘13 ~ 15년간 경기 양주소재 00정밀은 임직원들이 퇴사를 하면서 경쟁업체 및 협력업체 등과 공모하여 방산기술자료를 개인 USB에 담아 유출하였으나 이를 인지한 회사측에서 알고도 수사 의뢰 및 보안대책 강구 등의 보안대책을 강구하지 않고 방치하다 동일한 유형의 기술유출사고가 다시 발생한바 있다.

2.2.3. 하도급업체 무선공유기를 통한 방산기술 유출

‘13.11. 무인항공기 관련 부품을 생산하는 방산관련 업체 000의 경우 무선인터넷을 사용하지 않도록 하는 회사 방침을 어기고 임직원 1명이 개인 무선공유기를 무단반입한 후 접속용 비밀번호 없이 인터넷을 사용하다가 보안컨설팅 간 현장에서 적발된바 있는데 무선인터넷 공유기능을 이용하여 개발 중인 UAV 설계도 수백 장을 아무런 통제 없이 외부로 유출할 수 있었던 사고이었다.

2.2.4. 외국지사를 이용한 자료 유출

‘13.10. 방산관련업체 OOO사는 중국지사 직원을 통해 내부 서버가 북한에 해킹된 사실이 밝혀졌다. OOO사는 군 지휘통제체계 등의 사업을 수주한 회사로 다량의 방산기밀을 보유하고 있었다. 북한이 OOO사의 중국지사 직원을 포섭하여 해당 직원의 계정과 권한으로 VPN을 통해 1년간 200여 차례 본사 전산망에 침투하였고 다량의 정보가 유출된 것으로 추정되고 있다. 이 사고는 외국인 직원에 대한 내부통제, 자료접근관리 등이 미흡한 사례이다.

2.2.5. 악성코드에 의한 방산자료 유출

‘13년 5월경 군의 주요 전투체계 개발을 담당하는 방산관련업체 OOO사는 군 사업을 위해 자사 외부에 사무실을 임대하여 군 사업수행 팀을 운영하고 있었는데 사무실이 자사 네트워크 외부에 위치한 관계로 방화벽 외에는 별다른 정보보호 시스템이 없는 상태에서 북한 해커가 동사 연구원 PC에 악성코드를 감염시키고 동 악성코드가 공유폴더를 통해 사무실 파일서버로 사용되는 VDI 서버로 침투하여 해군 OOOO 체계 소스코드 등 방산기술 자료를 유출하였다.

최근에는 전문 해커조직이 보안이 강화된 대기업이나 금융기관 침투가 어렵자 하도급이나 협력업체를 통한 우회침투가 강화되고 있다는 언론보도가 계속되고 심지어는 2차 협력업체를 통해 공인인증서를 유출(‘16.3.11 중앙일보)해 가는 등 협력(하도급)업체를 통한 보안사고가 지속적으로 증가할 것으로 예상된다.

2.3. 망분리 시스템에서 외부반출 방산기술 자료 관리상 문제점

방산업체가 물리적 망분리를 하고 문서암호화(Enterprise- Digital Rights Management) 시스템을 적용하였더라도 외부로 반출되는 기술자료는 평문으로 내보내는 경우가 많다. 이러한 문제가 발생하게 된 이유는 국방부 망분리 가이드라인[2] 중 7번 조항인 “해외지사 및 하도급업체 등 외부로 전송하는 방산자료는 암호화 등의 보안대책을 강구해야 하며 방산정보 보호를 위해 필요한 정보보호시스템 등을 설치해야 한다.”는 부분을 잘못 해석해 발생한 문제라고 보여진다. 본래 이 가이드라인을 만든 목적은 방위사업기술보호법에 의해 지정된 방위산업기술자료나 방산기밀을 외부로 보낼 때 네트워크 구간에서 해킹에 의한 방산기밀 유출을 방지하고 업무상 관계가 있는 업체(인원) 외에는 자료가 유출되지 못하도록 하기 위해서 만든 것이다.

망분리 업체들은 이 가이드라인을 지키기 위해 내부망(방산망)에서 사용하는 DRM을 외부 DRM(하도급업체에 동일한 DRM 라이선스 부여로 암호화 자료 공유 허용)으로 확장해 사용하거나 외부 반출문서 암호화 추적・관리시스템을 이용해서 구축하였다. 외부DRM 형태로 구축한 경우 비용 등의 문제로 1차 하도급업체만 라이선스를 주고 타 방산업체나 방사청 등 방산관련기관에는 라이선스를 줄 수 가 없어 하도급 업체를 제외한 타 방산업체나 방산관련 기관으로 방산자료를 보낼 때는 암호화 문서를 복호화 한 후 평문 이메일로 보내고 있어 가이드라인을 위배함은 물론 망 분리 본래 목적에도 어긋난다는 것이다. 국방부에서는 “방산자료(문서, 도면, 압축파일 등)는 DRM을 일괄 적용”하도록 하고 있는데 이는 해킹에 의해서 자료가 탈취되더라도 열어보지 못하도록 하기 위함이다.

또 다른 문제는 방산기술자료를 암호화하여 1차 협력업체에 보낸다고 하더라도 업무의 특성상 동 자료가 2차, 3차 하도급 업체로 재전송 할 필요가 있으며 이 경우 이러한 2, 3차 업체가 모두 동일한 DRM시스템을 갖추고 있어야 한다는 것이다. 이렇게 되면 비용의 급증은 물론 다른 DRM과의 충돌 등으로 업무 수행이 거의 불가능하다는 것이 현장 실무자들의 의견이다.

또한 방산기술자료를 인터넷 PC를 이용해 평문 이메일로 보내다 보니 관계자들의 업무 분망과 관심소홀 등으로 해킹의 위험성이 높은 인터넷 PC에 평문 방산기술자료가 누적되고 있어 망분리를 한 의미가 없어지고 있다는 것이다.

Ⅲ. 보안 대책

외부로 반출되는 방산기술자료를 관리대장에 수기로 기록하는 방식은 기록하는 사람에 전적으로 의지하게 되고 실제 반출된 방산기술자료가 얼마나 복사되어 유포되는지 반출자가 확인할 수 없다. 따라서 이러한 방식은 다분히 형식적이라고 볼 수 있으며 사람에 의한 관리가 아닌 시스템적으로 자동화하는 것만이 진정한 방산기술자료 보호대책이라고 할 수 있겠다. 여기서 두 가지 전제가 있는데 첫 번째는 네트워크로 유포되는 방산기술자료의 암호화 추적관리 방안과 출력해서 반출(유출)하는 경우의 보안관리 대책이다.

3.1. 네트워크를 통한 방산기술자료 반출시 보안대책

3.1.1. 기술적 요구 조건

(1) 문서, 설계도, 동영상, 소스코드 등 다양한 형태의 파일을 암호화 하여 필요한 업체나 기관에 DRM 솔루션 라이선스가 없어도 송・수신 할 수 있어야 한다.

(2) 송신자 측에서는 수신자의 이름과 IP, 고유주소(MAC Address) 등이 실시간 확인 가능하여야 하며 제 3자 배포, 출력・복사 등 방산기술 자료의 사용 이력에 대한 추적관리가 가능하여야 한다.

(3) 협업이 필요 없고 특정인에게만 방산기술자료를 송신하여 재 배포를 차단하고자 할 경우 특정 수신자의 PC에만 자료가 저장되고 이 자료는 이동식 저장매체나 이메일 등 어떠한 방법으로도 유출이 불가능하여야 한다.

(4) 송신자의 실수로 제 3자에게 잘못 전달된 방산기술자료는 송신자가 원격으로 파기가 가능하여야 한다.

(5) 수신자가 고의 또는 해킹 등에 알지 못하는 방법으로 제3자에게 배포되더라도 파일이 암호화 되어 있어 열람이 불가능 하여야 한다.

(6) 네트워크 송수신 구간에서 방산기술자료(패킷)를 절취하더라도 암호화 되어 있어 열람이 불가하여야

한다.

(7) 수신자는 방산기술자료 편집 후 원본 송신자(업체, 기관)에게만 보낼 수 있으며 실수 또는 고의로 제3자에게 보내더라도 방산기술자료 열람이 불가하여야 한다.

(8) 수신자에 의한 프린팅 출력 통제가 가능하여야 한다.

(9) 화면 촬영을 통한 방산기술자료 유출방지를 위해 화면 워터마킹이 되어야 한다. 기존 문서에 표시되는 워터마킹은 제3자가 화면촬영을 하여 유출할 경우 문서 작성자가 자신의 PC에서 유출된 것이 아니라고 부인하면(문서를 여러명이 공유한 경우) 어떤 PC에서 유출된 것인지 추적이 사실상 불가하다. 따라서 화면에 워터마킹을 하여 최종 유출자의 PC를 추적할 수 있도록 하여야 한다. 그림 1은 화면 워터마킹의 예시다.

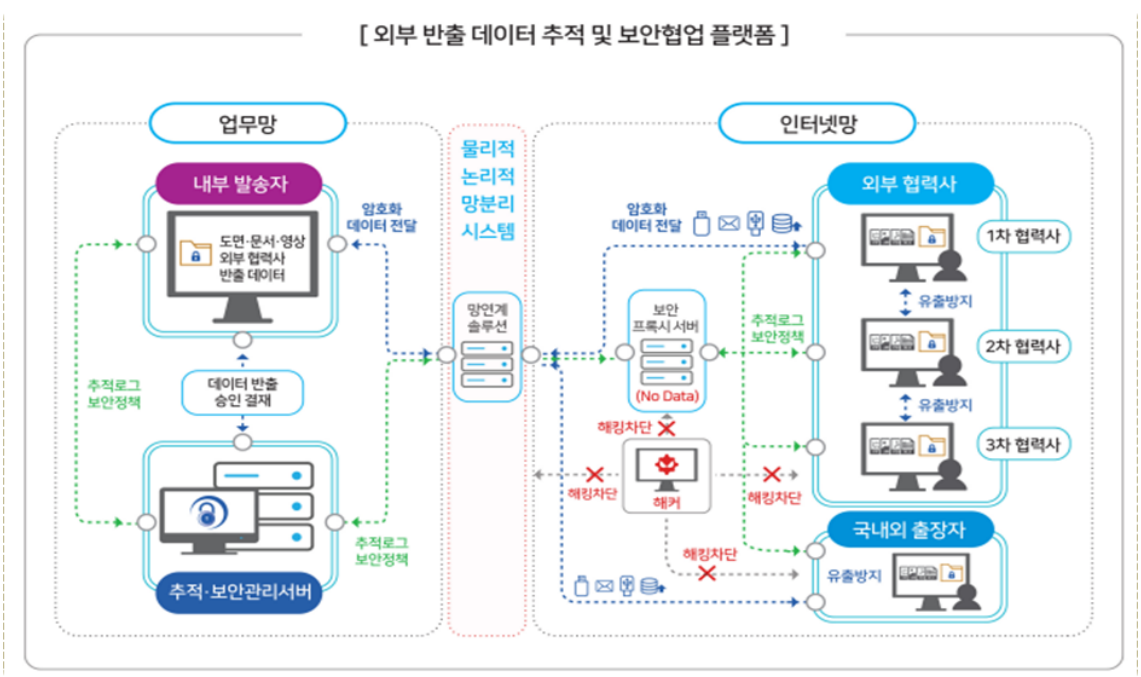
(10) 내부망(방산망)의 방산기술자료를 외부로 반출하는 경우는 오로지 결재를 통해서만 가능하도록 구축되어야 한다.

(11) 하도급 업체와 협업이 필요한 경우 그림 2와 같이 원도급 업체와 하도급 업체간 라이선스와 관계없이 방산기술자료는 암호화 된 상태에서 송·수신 및 편집이 가능하여야 한다.

〔그림 1〕 화면 워터마크 예시

3.1.2. 정책적인 요구사항

(1) 수신자측에서 방화벽, DRM 등의 보안시스템을 운용하고 있는 경우 암호화 파일이 *.exe나 zip과 같은 형태로 가는 경우 방화벽에서 차단을 하고 문서



〔그림 2〕 외부반출 데이터 추적 및 보안협업 플랫폼

편집 후 저장과정에서 DRM 솔루션간 충돌이 발생하므로 송신자측의 암호화 문서를 예외처리 해주어야 하는 과정이 필요하다. 이는 개별업체간 해결이 불가능하므로 방위사업청이나 국방부에서 지침하달을 통해 시행이 가능하도록 하여야 한다.

(2) 망 분리 상태에서의 암호화 문서 송·수신은 복호화 과정(DRM별 상이)을 거쳐야 하므로 사용자들이 불편을 이유로 암호화 문서수신을 거부하는 경우가 발생하고 있는데 국방부·방위사업청 등 군 관련 기관이나 업체 차원에서 사용자 보안교육을 통해 암호화 문서 사용을 적극 권장하는 지침제정과 교육이 필요하다.

3.2. 출력물에 의한 방위산업기술 유출방지 대책

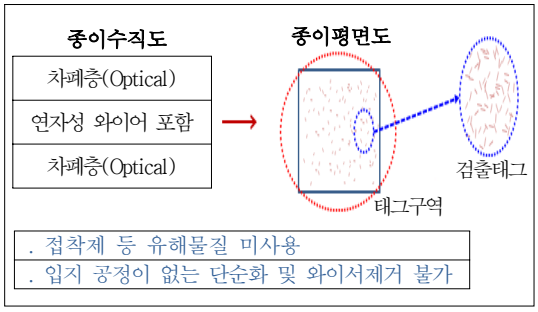
방산기술 자료 유출의 또 다른 경로는 자료를 출력해서 가져가는 것이다. 대부분의 업체들을 보면 컴퓨터를 이용한 자료유출 방지를 위해 많은 비용을 투자하여 정보보호시스템을 구축하고 있지만 내부직원이 출력하여 가져가는 것을 방지하는 대책은 거의 마련하지 않고 있다. 이는 내부 직원을 신뢰하고 또한 기술적인 문제나 비용 부담이 크기 때문인데 국가정보원 산업기밀보호센터의 자료를 보면 전·현직 등 내부직원에 의한 유출이 80% 비율을 보이는 것으로 보아 내부직원을 신뢰만 할 수도 없는 현실이다.

여기서 소개하는 기법은 보안복사 용지를 이용한 내부자료 유출방지시스템이다. 유사한 시스템이 개발되어 있으나 비용이나 효율성 문제 등으로 많이 사용하지 않고 있는 현실을 감안, 최근 새로 개발된 보안복사용지 시스템을 이용하여 내부자료 유출방지 기법을 소개한다.

3.2.1. 기존의 보안복사용지 문제점

보안용지란 특정 방식 센서에만 반응하는 물질을 용지 내에 삽입함으로써 센서가 장착된 게이트 등을 통과할 때 신호를 줄 수 있는 것으로, 아모르퍼스나 그와 유사한 비정질(non-crataline state 또는 amorphous), 자성물질(합금), 나노사이즈의 금속와이어, 자기공명의 특성을 가진 소재의 물질을 사용하여 특정주파수에 공진하여 물질의 특성을 구별할 수 있는 신호를 발생하는 용지를 말한다. 그러나, 이러한 보안대상 복사물(방산기술 자료 등)이 반드시 기능성 용지에 복사되어야하는 데에도 불구하고 기능성 용지 이외의 일반용지를 복합기의 급지장치에 넣고 보안대상 복사물을 복사하는 경우는 이를 외부로 유출하더라도 출입문 등의 센서에 의해 센싱(sensing)이 되지 않는 문제점도 발생하였다. 또한 종래 기술의 문제점은 보안용지 여부를 검출하는 센서가 복합기 내에 설치되어 있어 각종 인쇄장치의 구성요소(구동 모터, 스캐닝 구동 장치, 메인보드) 등의 전자기적 간섭으로 인한 노이즈 발생으로 인하여 정확한 검출력이 떨어지고 보안복사용지의 겉면에 태그가 부착되어 있어 사용자가 태그의 존재여부를 알 수 있고, 고의적으로 태그를 훼손하여 문서를 유출할 수 있는 문제점이 있었다.

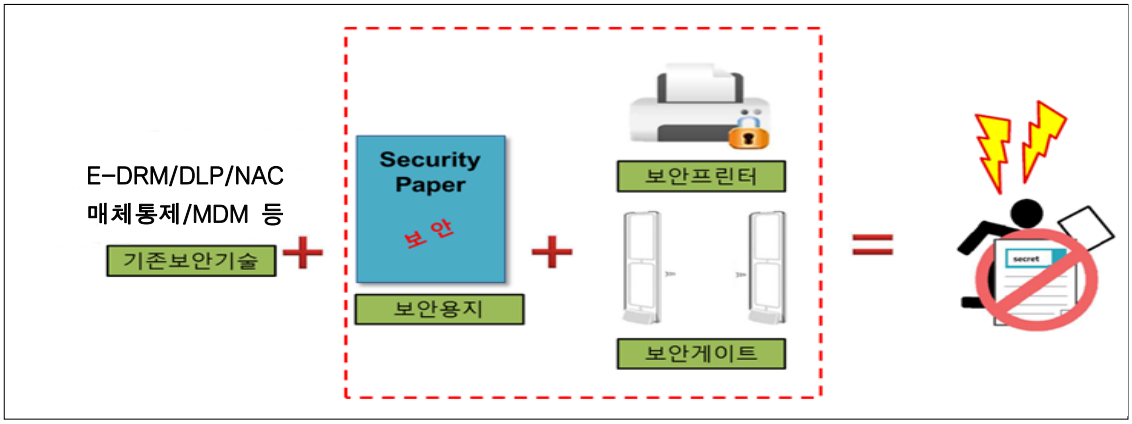
또한 컴팩트화 되는 복합기 구조 설계로 내부에 센서를 설치하기가 어려워 보안 복사지 전용 복합기를 제조함에 따른 비용의 증가로 업체에서 사용하기가 부담스러웠다. 최근 이러한 문제점을 해결한 특수 보안용지가 나왔는데 개념도는 그림 3과 같다. 복합기 모델에 제한 없이 간단한 센서 부착만으로 사용할 수 있어 기존의 복합기를 교체할 필요가 없으며 비용이 대폭 절감되는 효과가 있다. 또한 이 복합기는 일반 복사용지를 사용할 경우 출력이 되지 않는다.



〔그림 3〕 개량형 보안복사용지 (출처: JMC)

3.2.2. 보안복사용지를 이용한 보안대책

개량된 보안복사용지는 용지자체에 특수처리 된 분말을 이용, 자성을 부여함으로써 보안게이트 통과시 비프음에 의한 경고로 방위산업기술자료의 무단유출을 방지한다는 개념이다. 방산기술자료는 경우에 따라 분산보관 되어 있을 수도 있겠으나 대부분 연구소 등 특정장소에 보관되어 있을 것이다. 중요한 것은 비밀합동보



〔그림 4〕 보안복사용지를 이용한 유출방지시스템

관소 같이 방산기술의 보관 장소를 사전에 지정해야 한다는 것이다. 지정된 장소에서 출력할 때는 보안복사용지를 사용토록 하여 내부직원이 임의로 방산기술자료를 유출하지 못하도록 하여야 한다. 물론 정상적인 외부 배포가 필요한 경우라면 승인권자의 승인을 받아 내부 보안규정 절차에 따라 반출하면 된다. 이 내부자료 유출방지시스템의 운용목적은 내부직원이 임의로 방산기술자료를 출력하여 반출하는 것을 방지하는데 있다. 그림 4는 보안복사용지를 이용한 내부자료 유출방지 시스템 개념도를 보여주고 있다.

물리적 망 분리나 DRM · DLP 등 기존의 보안시스템은 출력물에 의한 유출을 방지할 수 없으므로 출력물 유출방지시스템을 더한다는 개념으로 보안복사용지는 기존의 일반 복사지와 크게 구별이 되지 않아야 한다. 즉 보안태그가 육안으로 식별 가능하거나 종이의 재질이 확연히 차이가 난다면 사용자들이 쉽게 사용을 기피하거나 보안태그를 제거하여 외부반출을 시도할 것이다. 방산기술이 보관된 사무실에는 보안프린터 외에 일반 프린터나 복사기가 있어서는 아니되고 일반 용지로 출력을 시도 시 출력이 불가하여야 한다. 일반 복사용지 사용시 경고음 또는 관리자에게 통보되도록 함으로써 외부유출 시도를 원천적으로 차단하여야 한다. 방산기술이 보관된 사무실 출입문에는 보안게이트를 설치하고 보안게이트를 통해서만 출입이 이루어져야 한다. 신발에서부터 사람 머리 위 까지 센서가 감지를 하여야 하며 보안복사용지가 감지될 경우 경고음이 울려야 한다. 보안복사용지가 낱장으로 가방 또는 옷 속에 숨겨 나가도 보안게이트에서 감지되어야 한다.

Ⅳ. 결 론

방위산업기술 자료를 보호하기 위해서는 현재의 물리적 망분리 시스템 운용만으로는 부족하다. 본 논문에서는 외부 반출 방위산업기술 자료에 대한 암호화 추적 관리와 출력물에 의한 반출을 차단하는 보안 대책을 제시하여 방위산업기술자료의 유출 방지 방안을 제시하였다.

참 고 문 헌

[1] 법률 제15052호 “방위산업기술보호법”, 2017. 11
[2] 국방부 훈령, “방위산업보안업무훈령”, 2018. 2
[3] 명지대학교 방산보안연구소, *“방산관련업체 기술보호역량 진단연구”*, 방위사업청 연구용역 보고서, Jan. 2016.

〈저 자 소 개〉

장 경 준 (Kyung Jun Jang)
정회원
2017년 2월~현재 : 에스원 고문
2016년 1월~현재 : 이노티움 부사장
2015년 5월 ~ 2017년 2월 : 방위사업청 보안자문위원
2015년 3월~현재 : 명지대학교 산업대학원 객원교수
2014년 9월~현재 : 리자드방산보안지원센터 운영
1979년 5월~ 2014년 8월 : 국군기무사령부
관심분야 : 방산보안, 정보보호