https://doi.org/10.33778/kcsa.2020.20.1.085

군사기밀 유출 사례 분석을 통한 군 내부정보 유출 방지 방안 : 내부자 행위 중심으로★

엄 정 호*, 김 남 욱**

요 약

최근에 발생한 군사기밀 유출 사례 중에는 정보통신망을 이용한 내부정보 유출은 드물다. 그 이유는 군 업무 특성상 국방정보통신망은 자료 전송용 인터넷과 내부 업무용 인트라넷으로 구성되어 있는데 물리적으로 분리되어 있고, 인터넷망을 통해서 자료를 송·수신할 때는 까다로운 절차를 거치게 때문이다. 최근 군사기밀 유출 사례를 분석한 결과 대부분의 유출 경로는 비밀을 복사하여 넘겨주거나 스마트폰으로 촬영하여 전송하거나 기밀 내용을 기억한 후에 발설한 것이다. 그래서 정보통신망을 대상으로 한 군사기밀 유출 차단 또는 탐지하는 기술은 효과적이지 못하다. 본 연구에서는 유출 대상인 군사기밀이 아닌 유출 주체자인 내부자 행위에 중점을 두고 정보유출 방지 방안을 제안하고자 한다. 첫 번째는 군사기밀을 유출하는 행위를 차단하는 예방 대책이고 두 번째는 군사기밀 파일에 의심스러운 접근행위를 차단하는 방안이며, 마지막으로 내부자의 정보유출 행위를 탐지하는 방안이다.

Measures to Prevent the Leakage of Military Internal Information through the Analysis of Military Secret Leakage Cases: Focusing on Insider Behaviors

Jung-Ho Eom*, Nam-Uk Kim**

ABSTRACT

None of the recent cases of military secret leakages have leaked internal information using networks. This is because the Internet and the Intranet are physically separated, and has a difficult process when transmitting and receiving data through the Internet. Therefore, most of the leaked paths are to copy and hand over secrets, shoot and send them with a smartphone, or disclose after remembering them. So, the technology of blocking and detecting military secret leakages through the network is not effective. The purpose of this research is to propose a method to prevent information leakage by focusing on the insider behaviors, the subject of leakage, rather than the military secret. The first is a preventive measure to prevent the leakage behavior of military secrets, the second is to block suspicious access to the military secret data, and the last is to detect the leakage behavior by insiders.

Key words : Information Leakage, Military Secret, Insider, Leakage Prevention, Insider Behavior

접수일(2020년 02월 29일), 게재확정일(2020년 03월 19일)

★ 이 논문은 2019학년도 대전대학교 교내학술연구비 지원에 의해 연구되었음.

* 대전대학교 군사학과&안전융합학부 교수(교신저자)

** 성균관대학교 컴퓨터공학과 박사과정 수료

1. 서 론

최근 공군 중령이 전역 후에 법률사무소에 취업하기 위해서 군사기밀이 포함된 국방 분야 사업계획서를 작성해 법률사무소에 제공한 혐의로 1심에서 징역 8월에 집행유예 1년을 선고를 받은 바 있다[1]. 작년에는 전방 육군부대 정보장교가 경찰서 정보담당 경찰관에게 군 시설, 무기 배치 등이 담긴 군사기밀 문서 수십 건을 모바일 메신저로 주고받은 흔적이 발각되어 1심에서 장교는 징역 3년, 경찰관은 징역 1년에 집행유예 2년을 선고받은 바 있다[2].

군사기밀 유출은 단 한번이라도 발생하면 국방안보뿐만 아니라 국가안보에도 영향을 미칠 수 있기 때문에 군사기밀의 외부 노출을 철저하게 차단해야 한다. 특히, 군 내부자에 의한 군사기밀 유출은 군사작전과 전력증강 사업 등 국가안보와 밀접한 연관을 갖는 내용도 많기 때문에 내부자 보안을 중요시해야 한다. 군의 특수한 업무환경을 고려할 때 기업에서 발생하는 내부자에 의한 정보유출과는 다른 양상을 갖고 있다. 군은 업무용 인트라넷과 정보 검색을 위한 인터넷을 물리적으로 분리하여 사용하고 있다. 그래서 업무용 PC에서 외부로 내부정보를 전송할 수가 없다. 또한, 이동저장매체의 반입이나 사용을 금지하고 있기 때문에 USB와 같은 소형 저장장치를 이용한 정보유출은 거의 불가능하다. 기업에서 설치하여 사용하고 있는 DLP와 같은 내부정보 유출 방지 시스템은 군에서는 큰 효과를 볼 수 없다.

위에서 설명한 정보유출 사례와 같이 군에서의 내부정보 유출 방식은 군사기밀 내용을 보고 다른 보고서에 포함시켜서 유출하는 경우, 스마트폰을 이용한 사진촬영 또는 메모한 후에 모바일 메신저로 전송하는 경우, 그리고 기억 후에 상대방에 발설하는 방식이 주를 이룬다. 국방부는 문서 유출 방지를 위해서 건물 출입문에서 소지품을 검사하고 스마트폰의 건물내 반입을 불허하거나 스마트폰에 사진촬영 금지하는 보안 앱을 설치하여 정보유출에 최선을 다하고 있다. 이렇게 함에도 불구하고 군사기밀 유출은 꾸준히 발생하고 있다.

본 논문에서는 과거 군사기밀 유출 사례를 분석한 결과를 토대로 정보유출 방지 대책을 제안하고자 한다. 방지 대책은 유출 대상인 군사기밀을 대상으로 한 방지 대책보다는 정보유출 행위자에 중점을 두었다. 논문 구성은 2장에서 군 내부자에 의한 군사기밀 유출 사례를 분석하고 3장에서 군에서의 정보유출 방지 현황을 살펴본다. 4장에서는 군 내부자 행위 기반으로 정보유출 방지 방안을 제안하며, 5장에서 결론을 맺는다.

2. 군 내부자에 의한 군사기밀 유출 사례 분석

다음 <표 1>은 최근 10년간 군 내부자에 의한 군사기밀 유출 사례[1-5]를 보여준다. 유출 사례를 살펴보면, 일반 기업이나 기관에서 발생하는 내부정보 유출 방식과 다른 양상임을 알 수 있다.

우선, 군사기밀 유출은 대부분의 군 간부에 의해서 발생한다는 점이다. 군 업무 특성상 군사기밀을 취급하기 위해서는 비밀취급 인가를 받아야 한다. 보안업무규정[6]에는 국가 안전보장과 국가이익 측면에서 누설될 경우에 위험 수준에 따라 1급, 2급, 3급 비밀로 구분하고 있다. 또한, 각 비밀을 생산하고 접근하기 위해서는 비밀등급별 비밀취급 인가를 받아야 한다. 대부분 간부들이 비밀취급 인가를 갖고 있는 이유가 전력증강, 방위산업, 적 정보 등과 같은 주요 군사기밀을 다루며, 영관급 장교는 보다 중요한 정보를 취급한다. 그래서 주요 내부정보를 유출하는 군 내부자는 간부(장교)가 대부분이다.

둘째, 유출 대상인 군사기밀은 대부분 전력증강이나 방위산업과 관련된 자료들이며, 군수업체로 제공된다. 방위산업의 규모는 수천억에서 수 조원까지 되는 사업이 대부분이기 때문에 군수업체에서는 사업 입찰에서 낙찰받기 위해서 사전에 관련 정보가 필요하다. 그래서 사업 관련 군사기밀을 획득하기 위해서 담당업무를 수행하는 군 내부자를 포섭하려고 한다. 내부자를 포섭할 때는 내부

<표 1> 군 내부자에 의한 군사기밀 유출 사례[1-5]

일자	내부자	내용	수단	목적
2018.6월	현역장교	직무상 비밀인 무인정찰기 대대창설과 관련한 수용시설 공사 사항 등이 포함된 국방 분야 사업계획서 등을 작성하여 변호사와 검사 등에게 전달	문서	취업
2017.12월	현역간부	타국에 파견된 정보원들의 신상정보를 동일 국가 정보원에게 전달	모바일(촬영)	금전적 이득
2017.2월	현역간부	전직 정보사 공작팀장이 정보사 후배를 통해 북한뿐 아니라 주변국의 군사, 외교, 경제 등 관련 정보와 외국에 활동하는 정보원 정보를 일본 무관하게 전달	모바일(촬영)	금전적 이득
2016.11월	현역장교	군 시설, 무기체계 위치 등이 담긴 군사 기밀문서 수십 건을 모바일 메신저로 연인관계인 정보담당 경찰관에게 전송	모바일(촬영)	공유
2016.7월	군무원 (예비역 장교)	3급 군사기밀인 합동무기체계목록서를 가방에 넣어 빼낸 다음 스캔하여 USB 담아 군수 에이전트 업체에 전달	스캔/USB	금전적 이득
2016.5월	현역장교	북한의 잠수함발사탄도미사일(SLBM) 수중 시출시험에 관한 정보를 지인인 통신매체 기자에게 누설	발설	공유
2014.7월	현역 장교	외국 방위산업체에 국지공역감시체계, 비행실습용 훈련기 구매계획 등 3급 군사기밀을 수십 건을 빼돌려 외국계 군수업체에게 전달	복사/사진	금전적 이득
2013.11월	예비역 장교	차기 군단 정찰용 무인항공기(UAV) 사업, 한국형공격헬기(KAH) 사업, 대형공격헬기(AH-X) 사업 등 3급 군사기밀을 몰래 빼내 미국 군수업체에 전달	복사	입찰
2013.5월	예비역 장교	예비역 장교가 해상초계기(S-3급) 작전운용성능을 후배가 직접 자필로 작성한 서류 1장을 군수업체에 전달	서류	취업
2011.3월	현역 장교	공군의 시기별 주요 무기 구입과 전력증강 계획을 담은 '합동무기체계기획서' 등 군의 방위력개선 사업과 관련한 군사기밀 2,3급 문서 10여건 유출	복사	금전적 이득

* 본 자료는 법원 판례와 인터넷 자료를 발췌하여 요약 정리한 내용임.

자와 근무경험이 많거나 친분이 두터운 지인을 중개자로 활용하는 것이 특징이다.

셋째, 유출수단은 스마트폰을 이용한 전송[7]과 복사나 재편집한 서류를 제공하는 방식을 활용한다. 군은 업무용 인트라넷과 인터넷을 물리적으로 분리하여 사용하고 있으며, 인터넷을 이용한 데이터 전송은 까다로운 절차를 걸쳐야 하기 때문에 네트워크를 통한 정보유출은 거의 불가능하다. 그래서 유출대상 내용을 스마트폰으로 촬영하여 메신저로 전공하거나 내용을 기억하고 있다가 발설하는 경우가 많다. 또한, 기억한 내용을 외부로 가서 문서로 재 작성하여 제공하는 경우도 있다.

마지막으로 정보 유출의 목적은 대부분 금전적 이득이나 재취업과 연관되어 있다. 군은 군 지휘구조 특성상 계급정년이 존재한다. 계급정년은 동일 계급에서 일정기간 동안 진급하지 못하면 퇴직하는 제도이다[8]. 예를 들면, 대위에서 소령으로 진급을 하지 못하면, 43세에 전역해야 하며, 소령, 중령, 대령은 다음 계급으로 진급하지 못하면 각각 45세, 53세와 55세에 전역해야 한다. 55세 이전에 전역할 경우에는 생활자금 마련이나 재취업이 절박할 수 있다. 그래서 조기 전역자들이 군수업체를 비롯한 외부 기업에서 재취업 목적으로 군사기밀을 요구한다거나 정보제공 대가로 금전적

유혹에 자유롭지 못한 이유가 여기에 있다.

2018년 국회 법제사법위원회에서 국방부 검찰단과 육/해/공군 법무실로 받은 자료에 의하면, 지난 5년간 군사기밀 보호법 위반 혐의로 33명이 입건되고 27명이 기소되었다고 밝힌 바 있다[9]. 이러한 위험을 무릎 쓰고 군사기밀을 유출하는 원인으로 다른 민간기관에 비해 빠른 계급정년을 손꼽는 것이다.

3. 군의 내부정보 유출 방지 대책 현황

3.1 기술/물리적 보안 대책

국방부는 군 업무용 인트라넷과 정보 검색용 인터넷을 물리적으로 분리하여 운영하고 있다. 군 업무용 PC를 통해서 작업한 내용이 외부로 전송되지 못하도록 별도의 업무망을 운영한다. 인터넷도 정보 검색용으로 사용되며, 외부로 메일이나 P2P 접속을 엄격하게 통제하고 있다.

2013년에는 스마트폰에 보안앱을 설치하여 청사 내에서는 안드로이드폰은 문자 송/수신과 통화만 가능하고 아이폰은 문자 수신과 통화만 가능하게 하였다[10]. 하지만 문자나 통화를 하는 과정에 군사기밀이 노출될 가능성이 높기 때문에 현재는 국방부와 합동참모본부 건물 내에는 스마트폰를 소지할 수 없게 하였다.

출력물의 외부 반출을 예방하고 담당자를 확인하기 위하여 워터마크를 적용하여 출력물에 출력자의 정보를 표시하게 하며, 출력물의 출처를 확인할 수 있도록 하였다. 하지만 출력물에 대한 통제와 관리가 제대로 되지 않기 때문에 다른 사람이나 외부인에게 쉽게 노출될 수 있다.

인터넷망에는 데이터 유출 방지 시스템(DLP)을 설치하여 외부로 전송되는 모든 데이터를 점검할 수 있도록 하였다. 또한, 접속자, 접속시간, 작업내용을 확인할 수 있도록 로그 관리 프로그램도 운영하고 있다.

업무용 PC나 인터넷용 PC에 이동형 저장장치의 접속을 금지하고 있다. 비인가 이동형 저장장치의 사용뿐만 아니라 인가된 저장장치라도 임의적으로 PC에 연결시키지 못하도록 규정하고 있으면 접속하더라도 인식하지 못하도록 하였다. 이동형 저장장치를 사용하기 위해서는 사전에 사용 허가를 승인받아야 한다.

이 밖에도 접근제어 프로그램을 설치하여 운영하거나 암호통신 기술을 적용하고 있다.

3.2 군 내부정보 보안 대책의 한계

우선, 국방부와 합동참모본부는 건물 내로 스마트폰 반입을 불허하고 있지만, 육/해/공군본부는 아직까지 스마트폰을 등록하고 내부 반입을 허가하고 있다. 심지어는 예비역을 포함한 외부인도 건물 내부로 출입할 때, 스마트폰 반출 현황 기록부에 기재만 하면 사무실로 반입이 가능하다. 여전히 스마트폰에 의한 군 내부정보 유출 경로를 제공하고 있는 셈이다.

둘째, <표 1>에서 보는 바와 같이 군 내부자에 의한 정보유출 중에 내부자가 직접 문서나 복사본을 외부로 반출하는 경로도 있다. 군인이나 군무원이 부대 내로 출입할 때, 엑스레이 검사 장비 등을 이용하여 소지품을 검색하지만, 문서 내에 포함된 내용까지 검색하지는 못한다. 최근에는 보안복사용지를 이용하여 서류를 갖고 게이트를 통과할 때 경고음을 발생시키는 시스템[11]도 있지만, 모든 문서를 보안복사용지로 출력과 복사할 수 없는 한계점이 있다.

셋째, 군 내부자가 군사기밀을 기억하고 있다가 외부에서 발설하는 경우에는 탐지할 수 있는 방법이 없다. 군사기밀 내용을 처음부터 끝까지 몇 차례를 나눠서 기억하고 외부에서 편집하여 타인에게 제공하는 것을 탐지한다는 것은 거의 불가능하다. 그래서 정보유출 대상인 군사기밀이 아닌 정보유출 당사자인 내부자의 의심스런 행위를 감시하고 유출 행위를 탐지하는 연구가 활발히 진행되고 있다.

마지막으로 군 내부자가 비밀취급 인가만 있다

면 동일 비밀등급 이하의 군사기밀에 접근이 가능하다. 즉 본인의 업무와 연관성이 없다고 하더라도 비밀취급 인가증만 있다면 동일 부서 내에 있는 군사기밀의 접근이 가능하다. 심지어는 타부서의 군사기밀도 비밀열람기록부에 기록만 하면 비밀 열람이 가능하다.

4. 군 내부자 행위 기반의 정보유출 방지 대책

3장의 최근 군사기밀 유출 사례 분석 결과에서 알 수 있듯이 군 내부자에 의한 정보유출 경로는 정보통신망보다는 군 내부자의 출력물 무단 반출, 스마트폰을 이용한 모바일 전송, 그리고 기억 후 발설 방법을 활용하고 있다. 즉, 정보통신망을 활용할 경우에는 보안 시스템으로 인해 유출 흔적이 남아 발각될 위험이 크다는 것을 알고 있기 때문에 다른 방법을 선택하는 것이다. 그래서 유출 대상인 군사기밀을 감시 대상으로 한 방지 대책은 실효성이 부족할 수밖에 없다. 앞서 언급한 바와 같이 군사기밀을 감시하는 것보다 정보유출 담당자인 군 내부자의 행위를 감시하는 방안이 더 효율적이라고 판단된다. 본 논문에서는 정보유출 객체인 군사기밀(주요정보)이 아닌 정보유출 주체인 내부자에 의한 정보유출 행위를 예방하고 감시하며, 탐지하는 방안을 제시하고자 한다.

4.1 정보유출 행위 예방 대책

정보유출 행위 예방은 군 내부자에게 군사기밀을 유출할 수 있는 요인을 제거하는 것이다. 예방대책은 군 내부자가 외부인으로부터 군사기밀 유출에 대한 청탁을 받더라도 군사기밀을 유출하지 못하도록 사전에 유출 의도나 시도를 차단하는 것을 목적으로 한다.

업무 목적상 불가피하게 스마트폰을 건물 내로 반입하더라도 사무실 내로 반입하지 않도록 사무실별 보관함을 설치하는 것이다. 즉, 스마트폰을 이용하여 군사기밀을 촬영하여 전송하는 것을 사전에 차단하는 것이다. 아울러 군사기밀 열람이나 작업을 수행한 후 일정시간 동안 스마트폰을 사용하지 못하도록 한다. 이는 스마트폰용 전용 보안 앱을 통해서 비밀작업 이후에 사용시간을 설정하도록 한다. 그리고 비밀 작업용 PC의 사용 기록이나 열람 시간과 보안 앱을 통해서 스마트폰 사용(송신) 기록을 상호 대조함으로써 위반 여부를 확인할 수 있다는 것을 공지한다.

또 다른 예방 대책으로는 사업추진 확정이나 예정인 전력증강 사업과 방위산업, 군 발주 대형 프로젝트 등과 관련된 기업과 동 기업에 취업한 예비역 장교들의 현황을 공지한다. 단, 개인정보보호법에 위반되지 않도록 기업에서 제공한 직원 현황을 참고한다. 방위산업체가 예비역 간부들을 상근이나 비상근으로 채용하면, 국방부가 요구할 시에 명단을 제공할 수 있도록 협정을 체결하는 방법도 있다. 아울러 현황은 별도로 대외비 수준으로 관리하며 사업관련 관계자들에게 제한적으로 제공될 수 있도록 한다. 국방부의 군수사업은 대규모의 예산이 투입되기 때문에 국/내외 군수업체에서 유리한 입장에서 입찰하기 위해 현역장교들을 통해서 관련 정보를 입수하고자 한다. 이러한 기업의 관계자나 예비역 장교들과의 의심스런 접촉을 피하기 위해서 사업 관련 기업의 관계자와 예비역 장교들의 현황을 유지한다면 예방 차원에서 사업 실무자에게 도움이 될 것으로 보인다.

4.2 군 내부자 행위 감시 대책

군 내부자는 비밀작업을 수행할 때 비밀생산용 PC를 이용한다. 이때 비밀작업과 관련된 군사기밀을 참고할 수 있다. 군사기밀은 대부분 전자문서 형태로 저장되어 있으며, 별도의 비밀합동보관소에서 보관하고 있다[12]. 군 내부자가 군사기밀을 참고할 때 전자문서를 비밀생산용 PC에서 열람하게 된다. 이러한 행위들을 감시할 수 있는 시스템을 설치해야 한다.

군 내부자가 최근에 비밀작업용 PC을 언제 사용하였고 얼마동안 사용하였는지, 군사기밀이 저장된 이동형 저장매체에 얼마나 자주 접근하였는

지, 그리고 접근한 군사기밀 내용의 가치가 얼마나 중요한지 등의 지표를 갖고 내부자의 활동을 감시할 수 있는 보안 시스템을 설치해야 한다. 즉, 접근시간과 사용시간, 군사기밀에 접근한 빈도수 그리고 자산의 가치를 감시 지표로 활용하여 군사기밀에 대한 내부자의 활동 수준을 정량적으로 평가해야 한다. 이러한 보안 시스템은 실시간으로 내부자 행위에 대한 평가가 이루어질 수는 없지만, 로그파일을 통해서 평가결과가 산출되어 이상행위로 식별되면 향후 비밀작업 시에 주 감시대상으로 선정할 수 있다[14].

최근에는 인공지능 기술을 활용한 사용자 행위 패턴 인식 기술을 활용하여 사용자의 이상 행위를 탐지하고 예측하는 보안기술이 개발되고 있다[13]. 인공지능 기술의 딥 러닝과 신경망 알고리즘을 활용하면 사용자의 패턴을 학습하여 사용자의 정상적인 행위 범위를 정의하고 사용자 행위의 이상여부를 감지할 수 있다. 군의 군사보안시행세칙에는 비밀작업 절차가 수록되어 있기 때문에 이러한 절차에 벗어나는 행위는 이상행위로 간주할 수 있다. 또한, 개인마다 고유의 업무수행 행위 패턴을 갖고 있기 때문에 이러한 패턴을 이탈하는 경우도 이상행위로 간주할 수 있다. 인공지능을 활용한 사용자 행위 패턴 인식 및 예측 기술을 정보유출 탐지 시스템에 적용한다면 군 내부자가 비밀작업 절차와 개인의 고유 업무 패턴에 맞게 작업을 수행하고 있는지 실시간으로 감시할 수 있다.

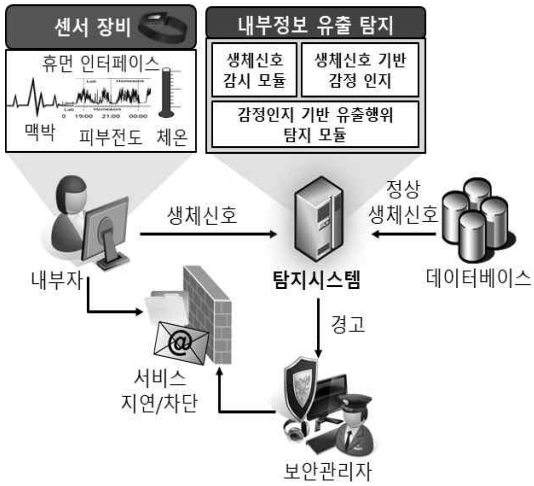
4.3 내부자의 이상행위 탐지 대책

기존의 내부정보 유출 방지·차단 시스템은 정보통신망을 통해서 외부로 유출되는 데이터를 대상으로 하기 때문에 그 이외 수단으로 유출하는 것을 차단하는 것은 한계가 있다. 특히, 군 내부자에 의한 정보유출 경로는 본인이 직접 유출하는 것이 대부분이기 때문에 기존의 내부정보 유출방지 시스템이 갖고 있는 보안 취약점을 보완할 필요가 있다. 그래서 탐지대상을 유출 대상인 군사기밀이 아닌 유출 당사자인 군 내부자로 변경하고 탐지기법도 시스템에서의 행위기반이나 규칙기반이 아닌 내부자의 감정변화를 기반으로 한 탐지방안이 보다 효율적일 것이다.

최근에 생체신호를 이용한 보안시스템 개발이 활발하게 진행되고 있으나, 생체신호 변화를 통해서 사용자의 이상행위를 탐지를 하는 보안기술 분야는 걸음마 단계이다. 생체신호를 이용한 사용자의 이상행위 탐지 기술의 원리는 다음과 같다.

우선, 인간은 평소와 다르게 행동하거나 생각할 경우에 감정변화가 일어나는데 그 중에서 긴장, 불안, 초조 등의 감정요소에서 변화가 크게 발생한다. 만약 군 내부자가 외부로부터 청탁을 받아 군사기밀을 유출하려고 계획한다면, 그 시점부터 감정변화가 발생하여 심리적 변화를 알아차릴 수 있다. 이러한 변화는 사람이 갖고 있는 고유한 생체신호의 변화를 통해서 측정할 수 있다. 생체신호는 사람이 긴장하거나 운동을 하거나 불안에 떨면 다양한 형태의 신체반응에 대한 결과로 나타나는 신호를 의미하며, 이러한 신호를 측정하여 사람의 감정 상태를 추론할 수 있다.

엄정호의 '내부정보 유출 탐지를 위한 새로운 접근론: 감정인지 기술의 사용으로[15]' 에서는 처음으로 생체신호를 이용하여 내부자의 이상행위 탐지의 가능성을 보여주었다. 다음 그림은 생체신호를 이용한 내부정보 유출 탐지 시스템의 프레임워크를 보여준다.



(그림 1) 생체신호를 이용한 정보유출 탐지 시스템의 프레임워크[15]

위 시스템의 대상자는 전력증강이나 방위산업, 적 전력정보 등 중요한 정보를 다루고 있는 영관급 장교 이상이며, 이들의 정상적인 생체신호는 사전에 수집하여 데이터베이스에 저장시킨다. 내부자가 비밀작업을 수행할 때, 팔찌형 생체신호 수집 센서를 손목에 착용하면 시스템이 작동하여 비밀작업 동안 생체신호를 지속적으로 수집한다. 만약에 군사기밀 유출 청탁을 받고 비밀내용을 암기하려고 하거나 다른 종이에 적을 때에는 불안, 초조, 긴장과 같은 감정변화가 발생하여 생체신호도 변화하기 시작한다. 이럴 경우에 1차 경고 메시지를 전송하고 그럼에도 불구하고 지속적으로 작업을 진행한다면 서비스를 중단시킨다.

위와 같은 보안 시스템이 군에 도입되면, 군 내부자의 정보유출 시도를 탐지할 수 있어서 기존의 보안 장비보다 효과적일 것으로 판단된다.

5. 결 론

군 정보 유출은 해킹이나 외부자 침입으로 인한 유출보다는 내부자에 의한 군사기밀 유출이 보다 심각하다. 특히, 방위전력 사업이나 적 전력 현황 자료 등과 같은 군사기밀을 담당하는 내부자가 유출하는 정보는 국방안보뿐만 아니라 국가안보에도 막대한 위험을 초래할 수 있다.

최근 군사기밀 유출사례 분석 결과를 볼 때, 군 내부자에 의한 정보유출 경로는 정보통신망보다는 내부자 본인이 직접 출력/복사본을 반출하며, 스마트폰으로 촬영한 후에 메신저로 전송하거나 군사기밀 내용을 기억한 후에 외부에서 문건으로 재작성하여 넘겨주는 경우가 많다. 이러한 내부정보 유출 경로를 차단하기 위해서는 기존의 정보유출 방지 시스템으로는 효과적이지 못하다. 그래서 유출 대상인 군사기밀이 아닌 유출 주체자인 군 내부자를 대상으로 한 방지 대책을 내부자 행위 중심으로 제안하였다.

우선 군 내부자가 유출 의도를 갖지 않도록 스마트폰 관리 방안과 내부정보 유출을 청탁하는 군수업체 관계자와 예비역 장교 현황을 유지함으로써 사전 모의를 하지 못하도록 하였다. 둘째는 내부자의 행위를 감시하기 위해서 내부자의 활동 수준 평가 시스템과 사용자 이상행위 감지 시스템 설치를 제안하였다. 마지막으로 내부정보 유출을 시도하는 군 내부자의 이상행위에서 오는 감정변화 즉, 불안, 초조, 긴장 등과 같은 감정요소를 생체신호를 이용하여 탐지하는 보안 시스템 개발 및 운영을 제안하였다.

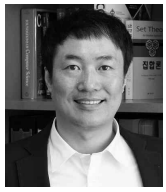
현재의 내부정보 보안 시스템으로 군 내부자에 의한 내부정보 유출을 100% 감시하고 탐지하는 것은 쉽지 않다. 하지만, 내부정보 유출 의도나 시도를 사전에 차단할 수 있는 예방 대책과 감시 대책을 마련함으로써 군 내부자에 의한 내부정보 유출을 최소화할 수 있는 방책이라고 판단된다.

참고문헌

[1] https://mn.kbs.co.kr/news/view.do?ncd=4363049 (검색일: 2020.1.16.)
[2] https://news.chosun.com/site/data/html_dir/2019/10/01/2019100101012.html (검색일: 2019.12.16.)
[3] https://casenote.kr/ (검색일: 2019.12.15.)
[4] http://www.ilyosisa.co.kr/news/articleView.html?idxno=146563 (검색일: 2019.12.15.)
[5] http://m.ilyo.co.kr/?ac=article_view&entry_id=204677 (검색일: 2019.12.15.)
[6] “보안업무규정” 대통령령 제30352호, 국가정보원, 2020.
[7] 이수인, “군사기밀보호법 위반행위의 실태와 대응 방안”, 동국대학교 석사학위논문, 2015.
[8] “군인사법”, 법률 제16928호, 국방부, 2020.
[9] http://www.the-news.co.kr/news/articleView.html?idxno=8502 (검색일: 2020.1.20.)
[10] 김종철, “산업보안 관점에서 경찰 내부정보 유출방지 연구”, 중앙대학교 석사학위논문, 2018.
[11] 장경준, “방위산업기술 자료의 외부 반출 시

보호 방안", 한국정보보호학회지, 제28권 제6호, pp.50~55, 2018.
[12] "보안업무규정 시행규칙", 대통령훈령 제341호, 2015.
[13] 방성혁, 배석현, 박현규, 전명중, 김제민, 박영택, "순환신경망 기반의 사용자 의도 예측 모델", 정보과학회논문지, 제45권 제4호, pp.360~369, 2018.
[14] 엄정호, "SFI 분석 기법을 이용한 내부자 활동 수준의 정량적 평가", 보안공학연구논문지, 제10권 제2호, pp.113~122, 2013.
[15] Jung ho Eom et al, "New Approach for Detecting Leakage of Internal Information; Using Emotional Recognition Technology", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS, Vol.9 No.11, pp.4662~4679, 2015.

[저 자 소 개]



엄 정 호 (Jung-ho Eom)
1994년 2월 공군사관학교 항공공학과 학사
2003년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사
2008년 2월 성균관대학교 컴퓨터공학과 박사
2011년 3월~현재 대전대학교 군사학과 교수
email : eomhun@gmail.com

김 남 욱 (Nam-Uk Kim)
2009년 2월 성균관대학교 컴퓨터공학과 학사
2012년 2월 성균관대학교 컴퓨터공학과 석사
2012년 3월~현재 성균관대학교 컴퓨터공학과 박사과정 재학
email : nukim8275@gmail.com