정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

사이버공격을 통한 산업기술 유출 현황과 전망

김 종 완*, 이 재 균**, 장 항 배***

요 약

사이버 공간은 제4차 산업혁명의 진전과 5세대 이동통신(5G) 시대의 도래로 초연결사회의 핵심요소로 등장하였다. 하지만 이러한 사이버공간 활용성의 증대와 함께 취약성도 증대하고 있어 사이버상의 산업기술 유출 역시 증가할 전망이다. 실제로 국내외에서 중소기업, 대기업을 막론하고 다양한 사이버공격을 통한 산업기술 유출 사례가 속속 보고되고 있다. 특히, 과거 No Tech상의 사이버공격에서 APT, 다크웹, 클라우드 서비스 등 High Tech를 이용하는 고도화된 사이버공격으로 진화하고 있다. 이는 기업의 영업비밀 유출 노하우 손실, 일자리와 경쟁우위 손실 등 경제력 손실과 평판 하락에 큰 영향을 미친다. 이에 본 논문에서는 국내외 사이버공격을 통한 산업기술 유출사고의 영향력을 산정하고 이에 대한 시사점을 서술 한다.

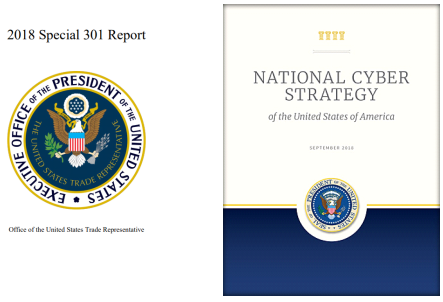
Ⅰ. 서 론

제4차 산업혁명의 진전과 5세대 이동통신(5G) 시대의 도래로 사이버공간은 초연결사회(hyper-connected society)의 핵심요소로 등장하였으며, 다양한 기술견인과 함께 그 활용성도 높아지고 있다. 그러나 사이버공간의 활용성과 함께 그 취약성도 같이 증대하고 있어 사이버상의 해외 기술유출도 더욱 증가할 것으로 예상되어, 주요 유출 대상이 글로벌 경쟁우위의 첨단기술임을 감안할 때 기존의 산업스파이 활동보다 훨씬 더 큰 위험과 피해를 줄 것이 예상된다.

美 무역대표부(USTR)는 미·중간 무역 전쟁이 격화되는 가운데, “2018년 스페셜 301조 보고서”을 통해 중국에 의한 사이버 해킹을 통한 미국 기업의 전산망 무단침입과 탈취가 계속되거나 증가하고 있다고 밝혔으며[1], 美 연방수사국(FBI)도 방첩 차원에서 중국의 기술 절도 약 1,000여 건을 조사하고 있는 등 미국과 중국의 기술 전쟁에 美 사법 기관까지 동원되어 전방위로 진행되고 있다고 블룸버그 등 외신이 보도하기도 했다.

이에 미국은 2018.9월 최근 증가하는 사이버상의 안보위협과 기업정보 탈취 등에 대응한 사이버보안을 강화를 위하여 ‘미국 사이버보안 전략(National Cyber Strategy)’을 발표했고, EU와 영국·독일·일본 등의 주요국가도 사이버상의 국가안보와 경제·산업정보 탈취 등에 대비한 적극적인 전략과 대책을 마련하고 있는 추세이다[2].

이러한 사례로 비추어봤을 때 사이버공격이 산업기술 유출 등 금전적 목적으로 트렌드가 바뀌었고, 국가의 지원을 받는 전문 해커조직이 정교한 공격을 감행하고 있는 상황을 반영한다면 국내 사이버상의 산업기술유출 환경은 보안에 취약한 것으로 볼 수 있다. 또한 해외 경쟁국 및 기업은 사회공학적 기법을 이용한 APT 공격으로 국내 기업의 국가핵심기술 등을 지



〔그림 1〕 스페셜 301조 보고서와 중국의 기술 및 National Cyber Strategy 2018

* 중앙대학교 융합보안학과 (대학원생, winstreet@cau.ac.kr)
** 중앙대학교 산업보안학과 (교수, ilsan61@cau.ac.kr)
*** 중앙대학교 산업보안학과 (교수, hbchang@cau.ac.kr)

속적으로 유출하고 있을 가능성이 농후한 바, 정보기관의 경제방첩 활동을 사이버분야로 확대·개척하여 국가차원에서 사이버상의 해외 기술유출에 대한 적극적인 대응이 필요하다. 이에 본 논문에서는 국·내외 사이버 기술 유출 사례를 소개하고 이러한 사고의 영향과 시사점을 도출하여, 이를 통해 사이버상의 경제방첩 방향과 전략을 모색해보려 한다.

Ⅱ. 선행연구

2.1. 사이버 공간과 산업기술 유출

사이버 공간은 정보기술 인프라의 상호의존적 네트워크를 의미하며 인터넷, 통신 네트워크, 컴퓨터 시스템 및 임베디드 프로세서와 컨트롤러를 포함한다[3].

산업기술 유출은 사이버 공간에서 경제적 또는 산업적 영업비밀이나 소유권 정보를 소유자의 허가 없이 빼돌리거나 숨기는 기만취득 행위를 말한다[4].

2.2. 사이버범죄

사이버 범죄는 4가지 특징을 가지고 있는데, 실제공간에서 발생하는 물리적 범죄와 다르게 가해자와 피해자가 대면하거나 물리적 접촉의 가능성이 거의 없다는 것이다. 또한 사이버 공간은 시간과 공간의 제약이 없어서 사이버 범죄도 시공의 제약을 받지 않는다. 사이버 범죄는 해킹과 악성코드 등을 사용할 수 있는 일정 수준 이상의 컴퓨터 관련 지식을 필요로 하며 전문성 때문에 사이버범죄는 화이트칼라 범죄(White-Collar Crime)로 분류된다. 마지막으로 사이버 범죄는 비대면 상태에서 범죄가 일어나기 때문에 상대의 존재를 의식하지 않게 되며 공격자의 죄책감이 희박해지고, 공격이 대담해지는 경향이 있다.

Ⅲ. 국내 사이버기술 유출 사례

3.1. 국내 중소기업 사이버기술 유출 실태

2018년 중소벤처기업부의 '중소기업 기술보호 실태조사' 분석 결과, 중소기업은 기술을 유출하기 위한 해킹과 악성코드의 유포 및 경유지로 이용되며 사이버 공격에 취약한 것으로 드러났다. 이는 중소기업의 예산과 전문인력 부족으로 인한 자발적 정보보호 실천 활동이 미흡한 것으로 풀이된다[5].

〔표 1〕 중소기업 기술유출 피해 현황〔5〕

구 분	피해 경험율(%)	총 피해 금액(억 원)
2017년	3.8	1,022
2016년	3.5	1,097
2015년	3.3	902

3.2. 국내 중소기업 산업기술 유출 사례

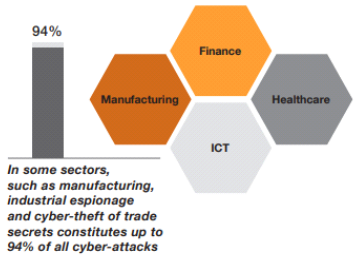
소프트웨어 개발 중소기업인 C사는 미래의 기술 먹거리와 해당 소프트웨어 시장의 동향을 파악하기 위해 국내·외 경쟁업체들의 시스템을 분석한 결과, 특정 경쟁업체의 시스템이 C사가 개발한 시스템과 유사한 형태를 보이고 있다는 것을 확인하였다. 이는 경쟁업체 직원이 C사의 기술을 유출하기 위해 중국인 해커를 고용하여 메일을 통한 악성코드를 감염시키는 방식을 통해 오랜 기간 동안의 해킹 공격으로 C사의 기술을 유출한 사실이 드러났고, C사의 소스코드를 무단으로 사용해왔던 것으로 수사 결과 파악되었다.

매출 200억의 Y중공업은 홈페이지 해킹을 통한 피해를 입은 후 보안에 더욱 신경썼고, 주요 임직원들에게는 유료 보안 소프트웨어를, 일반 직원들에게는 무료 보안 소프트웨어를 설치하게 하였다. 무료 소프트웨어의 이용자가 많고 보안 소프트웨어의 패치가 잦다는 점을 이용한 공격자는 소프트웨어 서버를 해킹하여 관리자 권한을 얻고 추후의 보안패치 시 보안을 위한소프트웨어로 위장된 악성코드를 심은 결과 Y중공업의 일반 사원 PC가 악성코드에 감염되었고, 이로 인해 많은 영업 기밀들이 유출되었다[6].

Ⅳ. 해외 산업기술 유출 사례

4.1. 해외 산업기술 유출 실태

사이버공격을 통한 산업기술유출에 가장 큰 영향을 받는 부문은 제조, ICT, 금융, 헬스케어이며, 특히 제조분야에서는 산업기술 유출이 모든 사이버 공격의 94%를 차지할 정도로 산업 기술유출에 대한 피해가 증가하고 있다. 2018년 유럽국제정치경제센터(ECIPE)는 사이버 기술유출로 인해 유럽 내에서 600억 유로의 피



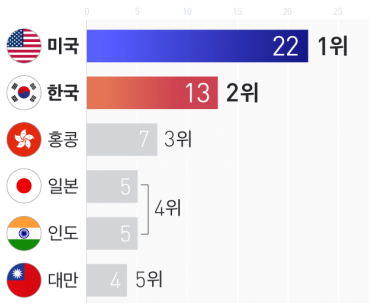
〔그림 2〕 제조분야에서의 산업기술 유출 피해〔7〕

해와 289,000개의 일자리를 손실 가능성을 예상하였으며, 이로 인해 유럽의 경제 성장률에 피해를 미칠 수 있다고 밝혔다[7].

특히 지능형지속위협(Advanced Persistent Threat, APT)의 피해사례가 증가하고 있는데, APT는 특정한 피싱 공격을 통해 여러 직원의 E-Mail 주소로 악성코드를 발송하여 컴퓨터 점유가 끝나면 수 시간 내에 기업 전체를 초토화시킬 수 있는 위력을 보여준다. 시만텍, 한국인터넷진흥원(KISA)에 따르면, 2016~2018년 APT 공격 발생 국가는 미국, 일본, 중국, 한국 등 기술이 발달된 경제 선진국에 집중된 경향을 보인다고 한다[8].

4.2. 중국에 의한 산업기술 유출 사례

중국은 APT10을 필두로 하여 관리형 IT 서비스 제공업체 활용을 통해 엔지니어링, 통신 및 항공우주 기술 등을 대상으로 하는 해킹작업을 미국을 포함한 전 세계를 대상으로 진행하고 있다. KeyBoy, TEMP.Periscope(APT40) 등의 APT 또한 서구 지역을 중심으로 공학과 해양산업 등의 학술 연구소와 기업 등을 대상으로 스파잉을 시도하며 현재도 그 빈도는 증가 추세이다.



〔그림 3〕 '16~'19 중국 해킹조직 주요 공격 대상〔9〕

중국에 의한 사이버기술 유출 사례는 주요 사례만 아래에 표기하였다.

〔표 2〕 중국에 의한 사이버 기술 유출 주요 사례

공격자	사 례
APT 10	- 메뉴패스팀으로도 불리는 APT10은 중국의 해커집단으로 2006년부터 관리형 IT 서비스 제공업체 활용을 통하여 미국, 유럽 및 일본 등 전세계의 항공 우주 및 통신 기업과 건설과 엔지니어링 기업, 정부기관을 노림 - 2014년 미국, 브라질, 프랑스를 비롯한 12개국에서 안보기밀, 영업비밀, 지식재산권 등을 유출시키기 위해 해킹을 저지른 혐의로 APT10 소속 중국인 해커 2명이 기소됨 - 이들은 IBM, HP 등 민간 기업들을 비롯하여 미국의 해군과 항공우주국(NASA) 제트추진연구소, 미국 에너지부 등의 정부 기관 전산망을 공격한 것으로 파악됨
APT 20	- 중국의 APT20은 2017년부터 미국, 영국, 프랑스 등 전 세계 항공, 건설, 에너지, 의료, 운송 등 다양한 산업에 스파이 공격을 진행 - APT20은 제이보스(JBoss)의 특정 취약한 버전이 운영되는 서버 등의 취약점을 통해 피해자의 네트워크에 진입하거나 스피어 피싱 메일, 공급망 공격, 휴대용 미디어 장비를 감염시켜 공격하는 방식을 사용 - APT20은 2025년까지 중국의 경제 부흥을 위한'메이드인 차이나 2025(Made in China 2025)'나 '일대일로'와 같은 대규모 사업을 돕기 위해 여러 산업 기밀을 세계 곳곳에서 스파잉하는 활동을 함

4.3. 기타 국가에 의한 산업기술 유출 사례

기타 국가에 의한 주요 산업기술 유출 사례는 다음과 같다.

〔표 3〕 기타 국가에 의한 산업기술 유출 주요 사례

공격자	사 례
APT 28	- APT28 소속의 러시아 스파이 7명은 화학무기 감시기구, 도핑감시기구, 원자력 관련 기업 등 전세계에 대한 사이버 해킹을 감행하였음 - 이들은 미국의 원자력 기업인 웨스팅하우스에 침투하여 원자력 기술을 빼내려 했으며, 더 나아가 정부기관, 기업, 심지어 미국의 민주당 등 정당 정보에 대한 침투도 시도
북한	- 북한의 라자루스 그룹은 김정은 암살을 소재로한 영화인 '더 인터뷰'의 상영을 막으려 소니픽쳐스를 해킹하여 내부망 공격뿐만 아니라 임

	직원의 정보, 급여 등의 개인정보는 물론 제작 기술, 영화 유출 등 다양한 문서를 유출함 - 이에 미국은 북한 국적 해커 박진혁과 그가 속한 '조선 엑스포' 합영회사를 독자 제재 명단에 올리고 기소하여 북한 정부가 지원한 사이버 범죄와 관련한 첫 정식 기소가 됨

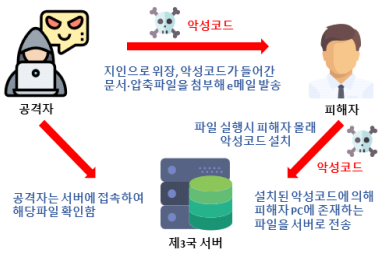
Ⅴ. 사이버공격을 통한 산업기술 유출의 방법

5.1. No Tech, "Social engineering"

기존의 No Tech의 의미는 기술이 적용되지 않은 물체로 연필, 포스트잇 등을 예로 들 수 있다. 산업기술 유출에서의 No Tech란, 기술을 사용하지 않고 사람의 마음(心), 권력 및 지위 등을 이용하여 상대를 속여서 기술을 유출하는 것을 의미한다.

No Tech에서의 산업기술 유출 방법으로는 우선 스피어피싱(Spear Phishing)이 있다. 스피어피싱은 지인 사칭, 흥미로운 정보 안내 등의 스팸메일을 통해 상대방의 PC에 접근하여 악성코드를 설치 후 Service Account를 탈취하는 방식으로 상대방의 기술정보를 훔치는 방식이다.

다음으로는 합작·투자자 설립의 방법이 있다. 중국은 해외 기업이 중국에서 사업을 하기 위한 단계(합작·투자 강요 등)를 법률로 제정하여 해외 기업의 지적재산권 및 독점 정보를 얻는 방식을 사용한다.



〔그림 4〕 스피어피싱 개요

회사명	중국 파트너	연도	분야	투자액
퀄컴	구이저우 성	2016	고성능 서버칩	2억8000만
AMD	THATIC	2016	서버칩	2억9300만
VM웨어	수곤인포메이션	2016	클라우드컴퓨팅가상 현실화 소프트웨어	5000만
휴렛팩커드엔터프라이즈	칭화홀딩스유니스플렌더그룹	2016	네트워크 서버	45억
마이크로소프트	C.E.T.C 그룹	2015	소프트웨어	4000만
웨스턴디지털	칭화홀딩스유니스플렌더그룹	2016	데이터센터 스토리지	3억
시스코 시스템스	인스퍼그룹	2016	네트워크 시스템	1억
인텔	스프레드트럼/ RDA마이크로일렉트로닉스	2014	스마트폰 칩	15억

〔그림 5〕 미국 기업 중국 제휴·합작사 설립 현황〔10〕

5.2. Low Tech

기존의 Low Tech는 낮은 단계의 기술이 적용된 기계로 MP3플레이어, 라이트 등 단순한 기능을 가진 것을 뜻한다. 사이버 기술유출에서의 Low Tech란, 상대방의 암호를 얻을 수 있는 프로그램을 설치하는 등 기존의 낮은 단계의 기술을 이용하여 기술을 유출하는 것이다.

Low Tech에서의 사이버기술 유출 방법으로는 우선 스크린샷(Screen Shot)이 있다. 스크린샷(Screen Shot) 방법은 화면해킹 방법으로 상대방의 화면을 그대로 가져와서 상대방의 아이디 및 비밀번호를 취득하는 방법이다.

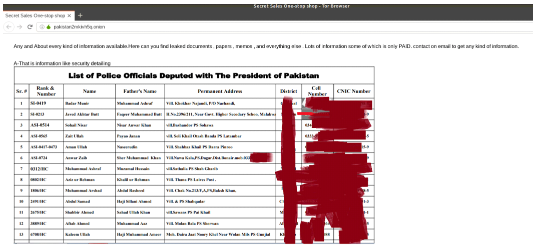
그리고 키 로깅(Key Logging) 방법이 있다. 키 로깅은 상대방이 타이핑하는 문자를 그대로 로깅하여 가져오는 방법으로, 실시간으로 비밀번호를 취득할 수 있다.

5.3. High Tech

기존의 High Tech는 고도한 기술이 적용된 과학기술의 집약체로, 컴퓨터, 스마트폰 등 현재도 계속 발전하고 있는 기술이다. 사이버 기술유출에서의 High Tech란, 상대방의 취약점을 파악하여 내부에서부터 공격하거나(From In) 외부로부터 직접 타격(From Out)하는 방법 등으로 이루어진다.

High Tech에서의 사이버 기술유출 방법은 APT(Advanced Persistent Threat) 공격이 있다. APT는 지능형 지속위협의 뜻으로 대부분의 사이버 범죄자와 달리 APT 공격자는 더 긴 시간에 걸쳐 공격의 목표를 달성하며, 네트워크에서 이들을 제거하려는 시도에도 빠르게 적응하여 네트워크 권한을 상실했을 때에도 같은 피해자를 계속 표적으로 삼는 방법이다.

다음으로는 클라우드 서비스(Cloud Service)에서의 기술유출이 있다. 클라우드 서비스는 조직이 데이터, 애플리케이션, 워크로드를 사용, 저장 및 공유하는 방식을 지속적으로 변화시키며 분산처리에 따른 보안 적용의 어려움과 보안책임 공유의 문제에서 취약점을 가지고 있다. 또한, 다크웹을 통한 방식이 있다. 다크웹은 위조서류 제작, 위조신분증 제작, 매춘, 인신매매, 기술



〔그림 6〕 다크웹을 통한 기술정보 유출과 거래 사례(추정)

거래 등을 암호화폐를 보상으로 익명성의 뒤로 숨어 현재도 활발하게 범죄가 일어나고 있는 곳이다.

Ⅵ. 결 론

6.1. 사이버공격을 통한 산업기술 유출 사고 영향

영업비밀의 유출 및 탈취에 따른 사이버범죄의 비용 산정은 가장 중요한 요소이나, 영업비밀 유출로 인한 손실(악영향)을 수치화하기에는 매우 어렵다. 기업의 이해관계자들은 사이버공간에서의 영업비밀 유출은 직접적 영향력은 10%정도이며 나머지 90%는 노하우 손실, 일자리와 경쟁우위 손실 등의 장기적인 간접적 영향에서 차지한다고 주장한다. 또한 기업 내 사이버공격에 따른 위기관리는 5천만~2억 유로의 비용이 소요되며 사이버공간에서의 영업비밀 유출 및 탈취로 경제적 손실과 평판 하락이 가장 큰 악영향으로 뽑힌다. 즉, 기업 내 정보 및 데이터의 손질은 이직률의 증가와 나아가 기업의 파산까지 야기할 수 있다.

기업에게는 또한 영업기회, 판매기회 손실, 생산력 저하, 시장우위 선점 위조 등을 포함한 기회비용(Opportunity costs)을 부과한다. 더하여 기밀의 강제공개에 따라 고객관계, 계약 손실 및 영업명 가치 하락 등 기업의 평판이 하락(Reputational damage)하게 되는 영향이 있다. 덧붙여 사이버기술 유출에 따른 영업비밀 노출은 R&D의 실효성 저하와 경쟁우위 손실을 야기함에 따라 혁신성이 저하(Negative impacts on innovation)되며 사이버기술 유출이 증가할 경우 유출 위험에 따라 기업의 혁신 투자 정도가 감소할 수 있다. 마지막으로, 사이버안보 소프트웨어에 대한 전세계 지출을 포함하며 사이버안보 보험료에 대한 비용도 포함한 보안 비용 강화(Increased costs for security)를 일으킨다.

6.2. 산업기술 유출사고의 영향과 대책 시사점

민감한 산업정보와 무역비밀 등과 같은 기술정보가 디지털화 되면서 핵심인력 불법채용, 적대적 M&A, 비인가된 이동저장장치로의 자료전송 등과 같이 기존의 한정된 방법을 넘어 다양한 사이버기술들을 악용하여 새로운 형태의 기술유출(탈취)사고가 발생하고 있다. 이를 해결하기 위해서 공개된 사이버기술 유출사고에 관한 단편적인 사례를 고려해 볼 때, 보호대상(기술정보)의 가치는 동일하나 보호대상 환경과 형태(사이버공간에서 디지털화된 기술정보)가 변화함에 따라 새로운 기술유출 사고현황에 대한 인식과 심각성을 공유할 필요가 있다.

두 번째로, 서비스 중지, 디도스(DDos) 공격 등을 통해 사회적, 정치적인 혼란을 일으키기 위한 사이버공격(악의적인 취약점 공격, 악성코드 등)은 사이버 공간에서의 산업기술의 획득을 통하여 경제적인 편취를 목적으로 한 공격으로 변화되고 확대되고 있다. 기존 사이버공간 영역에 대한 경계선 침해행위에 대응할 수 있는 선(線) 중심의 보호대책(탐지) 수립이 적절하였으나, 사이버공간에 저장된 정보자체에 대한 탈취활동으로 변화됨에 따라 내용(面)중심의 보호대책 마련이 필요하다. 또한 공공영역, 민간영역 등의 공간중심의 보호대책보다 영역구분이 모호한 사이버공간도 함께 고려하여 금융정보, 개인정보, 의료정보 등의 내용중심의 보호대책 설계가 요구된다.

다음으로 소수집단에 의해 한정된 기업대상의 사이버기술 유출과 탈취사고 등이 국가적 차원의 조직화된 집단을 통해(중국, 러시아, 북한, 이란 등) 산업대상의 사이버기술 유출과 탈취로 확대되고 있다는 영향이 있다. 산업의 지속가능성 확보(국가경쟁력 강화)하기 위해서는 새로운 위험으로 부상되고 있는 사이버기술 유출사고에 선제적으로 대응하기 위해 국가적 차원의 거시적인 보호대책(중장기적인 보호대책 수립, 관련 법제도 개정 등)마련이 시급한 상태이다.

마지막으로, 물리 공간에서의 기술유출사고와 달리, 전자 공간에서의 기술유출사고는 기존의 물리 공간과 연계하여(Cyber Physical Space) 융·복합적인 위험형태로 발생하기 때문에 기존의 시스템 중심의 보안대책보다는 한계가 존재한다. 이러한 한계를 극복하기 위해 물리적 공간에서 산업의 고유자산(Unique Asset)을 활용한 업무흐름에 따라 다양한 형태의 위험발생가능하

기 때문에(No Tech + Low Tech + High Tech), 보호 대상 산업에 대한 이해를 바탕으로 예방보다는 예측 중심의 보안기술 개발과 균형감 있는 보안인재 양성이 필요할 것이다.

참 고 문 헌

[1] Office of the United States Trade Representative(USTR), “2018 Special 301 Report”, 2018

[2] White House, “National Cyber Strategy of the United States of America”, 2018

[3] 배덕현, “사이버공간의 정의와 특징-몇 가지 사례를 중심으로-”, 문화역사지리, 27(1), 129-143, 2015

[4] NCSC, “Foreign Economic Espionage in Cyberspace”, 2018

[5] 중소벤처기업부, “중소기업 기술보호 실태 조사”, 2018

[6] 한국산업기술보호협회, “중소기업 기술유출사례 및 대응방안 연구”, 2014

[7] European Commission, “Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber”, 2017

[8] 시만텍·한국인터넷진흥원, “최근 3년간 APT 공격 발생 국가 순위”, 2018

[9] KBS, “미국 다음 ‘한국’…중국 해커 ‘통신’ 집중 공격”, https://news.kbs.co.kr/news/view.do?ncd=4308463, 2019

[10] 이투데이, "중국에게서 지적재산권 보호하겠다는 트럼프…중국서 간·쓸개 다 내주는 퀄컴", https://www.etoday.co.kr/news/view/1524067, 2017

〈저 자 소 개〉

김 종 완 (Jongwan Kim)

2015년 2월 : 홍익대학교 영어교육과 졸업

2018년 9월~현재 : 중앙대학교 융합보안학과 석·박통합과정

<관심분야> 산업보안, 기술유출, 보안교육

이 재 균 (Jaekyun Lee)

2018년 : 중앙대학교 융합보안학과 박사

2018년~현재 : 중앙대학교 산업보안학과 산학협력중점교수

<관심분야> 산업보안, 산업보안 유관기관, 정책정보

장 항 배 (Hangbae Chang)

종신회원

2006년 : 연세대학교 정보시스템관리 박사

2014년~현재 : 중앙대학교 산업보안학과 정교수

<관심분야> 중소기업 정보보호, 정보 오남용 및 유출방지, 성과분석 체계