4차 산업혁명과 보안

4차 산업혁명 시대, “새로운 기술과 익숙한 위협”

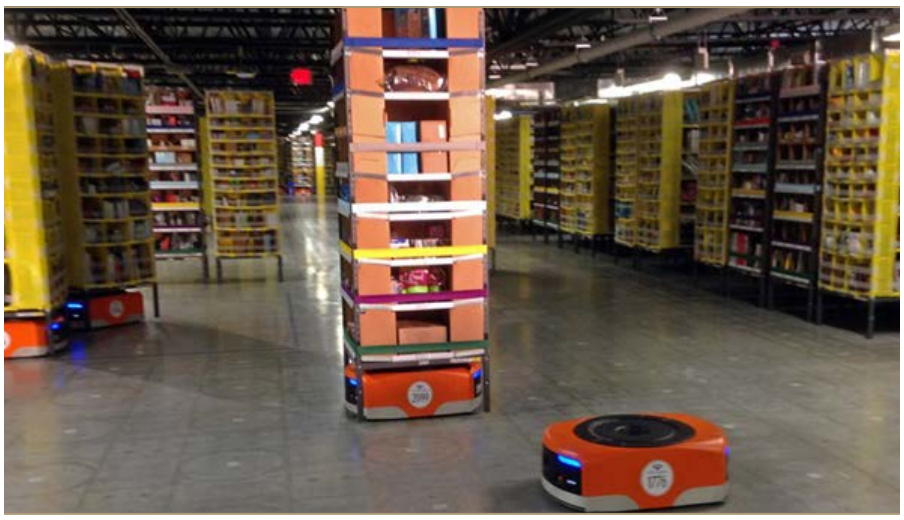
4차 산업혁명의 시대가 도래했다. 이 시대는 단순 기술의 발전으로 인한 공장 자동화, 제조 생산성만 의미하는 것이 아니다. 산업간 경계가 무너지고 사물과 사물, 사물과 사람, 사람과 공간 등 모든 것들이 연결되면서 새로운 가치가 창출되는 시대이다. 또한 이로 인해 사회 전반의 걸쳐 혁신적인 변화를 겪게 될 것이다. 그러나 4차 산업혁명이 제시하는 청사진의 이면에는 간과해서는 안될 위험이 존재한다.

이 글에서는 4차 산업혁명을 이끄는 주요 기술과 함께 고려해야 하는 보안에 대해 살펴본다.

새벽 1시.

축구장 46개 크기의 북미 최대 물류센터인 아마존 듀폰트(Dupont)시 창고 2층에서 들리는 소리는 ‘삐삐’하는 기계음뿐이다. 사람의 목소리는 들리지 않고 모습도 보이지 않는다. 1천여대의 로봇 키바(Kiva)만이 쉴 새 없이 움직이며 물건을 창고로 옮기고 있다. 1층에서는 6톤의 물건까지 들어 올릴 수 있는 대형 로봇 로보스토(Robo-Stow)가 물류창고에 도착한 물건을 2층 재고 창고로 올리는 일을 반복한다. 키바는 착실한 노동자처럼 줄을 맞춰 대기하고 있다가 자기 차례가 오면 파레트 위에 짐을 싣고 창고로 가서 놓여야 할 위치에 물건을 놓는다. 1천만개의 상품, 초당 50건의 주문, 하루 300만개를 배송하는 이 로봇들에게 지시를 내리는 것도 사람이 아닌 인공지능이다.

아마존의 로봇 1대는 인간 4명에 해당하는 일을 해낼 수 있다고 한다. 아마존은 2015년에 3만대였던 키바의 숫자를 2016년에는 4만5천대로 50% 늘렸다. 키바가 나른 물건을 포장 직전에 확인하는 일만 하는 1천여명의 인간 직원 수는 로봇만큼 늘지 않았다. 똑똑한 기계들이 그들만의 언어로 대화하며 뛰어난 일처리를 하는 상황은 아마존 창고뿐만 아니라 인간 사회 전반을 뒤흔들 기미를 보이고 있다. 이 변화를 우리는 '4차 산업혁명'이라고 부른다.



[그림 1] 아마존 물류센터와 로봇 키바 *출처: Brandon Bailey/AP

'4차 산업혁명'이란 용어는 2011년 하노버 박람회에서 독일이 발표한 'Industire 4.0'에서 유래되었다. 이는 독일이 갑작스럽게 새로운 개념을 들고 나온 것은 아니었다. 경제 부흥을 위해 2006년 메르켈 독일 총리의 주도 하에 준비해 온 '하이테크 2020'계획의 일부로서 ICT 융합과 IoT(Internet of Things)/IoS(Internet of Services) 연구개발, 2010년 CPS(Cyber Physical System) 연구 성과를 바탕으로 2011년에 'Industrie 4.0'이란 이름의 미래 프로젝트로 발족시킨 것이다. 독일이 Industrie 4.0을 내세우면서 구조적 변화를 꾀한 핵심 영역은 인더스트리(Industry)라는 용어 그대로 산업 일선인 제조 공장이었고 지멘스 암베르크 공장이 대표적인 사례로 손꼽혀 왔다. 현재 암베르크 공장의 자동화율은 75%를 넘고 7초마다 1개씩 제품이 출고되며 전 세계 공급 물량의 1/3을 담당하고 있다. 놀라운 것은 약 1천여 종의 제품을 연간 1천2백만개나 생산하는 이 공장의 불량률이 0.0011%(백 만개 당 1개)라는 사실이다. 공장의 디지털화 이후 과거와 비교해 보면 불량률은 400배 이상 향상되었고, 약 30%의 에너지 절감, 25% 비용 감소, 시장 출시 기간은 50% 절감이라는 효과를 보았다. 권터 크롭쉬 지멘스코리아 디지털팩토리 사업본부 대표는 "스마트공장으로 바뀐 뒤 생산성이 9배 늘었다. 10년 전과 비교했을 때 기계나 인력을 변경한 게 없는데 이런 성과를 냈다"고 말한다.



[그림 2] 지멘스 암베르크 공장 *출처: Brandon Bailey/AP

지멘스 암베르크 공장을 스마트팩토리로 만든 대표적 기술은 공장 안에 설치한 수만 개의 센서와 거기서 수집된 일 평균 5천만 건에 달하는 빅데이터의 활용이다. 제품과 설비마다 부착된 바코드를 통해 가동 상태와 불량품을 감지하고 분석 결과를 통해 기계의 가동과 정지 시점, 에너지 소비를 낮추기 위한 최적 공정을 초 단위로 예측해서 운영 시스템에 적용한다. 실세계의 상태가 센서를 통해 디지털 정보로 변환되어 사이버

시스템으로 모사(模寫)되고 그 데이터를 분석해서 최적의 결과를 위해 조정한 값을 물리적인 시스템으로 다시 반영하는 순환 체계, 이것이 곧 스마트팩토리와 4차 산업혁명의 핵심 요소인 CPS(Cyber Physical System)이다. 암베르크 공장에는 실상 4차 산업혁명의 중추적인 기술들이 모두 녹아 들어 있다. 이제 그 기술들에 대한 각론으로 들어가 보자.

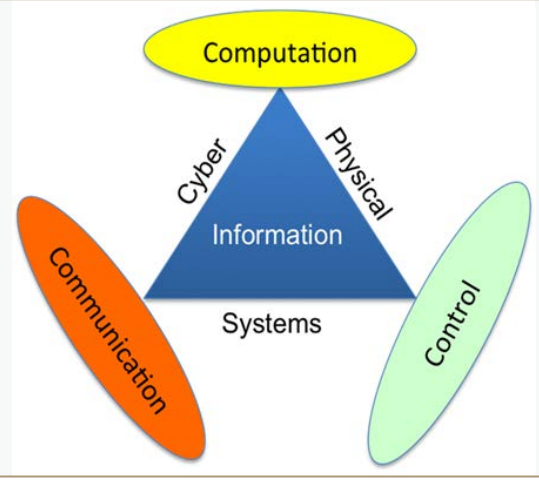
사이버물리시스템(Cyber Physical System, CPS)

4차 산업혁명 기술이 실현되는 모든 장(場)은 CPS라고 볼 수 있다. CPS가 공장에 구현되면 스마트 팩토리, 사람이 사는 집으로 옮겨가면 스마트 홈, 의료시설에 대입하면 스마트 헬스케어, 국가 행정에 도입이 된다면 스마트 거버먼트가 된다. 어떤 경우든 공통적인 구조는 현실의 상태를 디지털 데이터로 전환하여 처리한다는 데 있다. 일단 디지털 데이터로 변환되면 분석할 수 있고 그 결과 더 나은 의사결정과 제어가 가능해지기 때문이다.

CPS의 흔한 예는 많은 사람들이 손목에 찬 장비에 구현되어 있다. 핏비트(Fitbit)라는 스마트워치는 심장박동과 신체의 움직임을 일정 주기로 체크한 후 블루투스를 통해 데이터를 스마트폰에 저장한다. 스마트폰 소프트웨어는 그 데이터를 분석해서 사용자가 하루 활동을 통해 칼로리를 얼마나 소모했는지 목표 체중에 다다르려면 얼마나 더 걸어야 하는지 알려줄 뿐더러 수면 상태가 어떤 패턴인지 심장박동수가 정상이 아니라서 진료를 받을 필요가 있는 건 아닌지 알려 준다. 스마트워치뿐만 아니라 스마트폰을 쓰더라도 내장된 진동 센서를 통해 소유자의 실세계 활동 상황을 사이버세계에 데이터로 저장시키는 일이 가능하다.

필자는 산업공학 전공으로 FA(Factory Automation)와 CAM(Computer Aided Manufacturing)등을 교과목으로 배웠다. 직장 생활 초기(1991년경)에는 자동차 회사 생산기술 본부에서 생산라인을 설계하고 시공하는 업무에 관여했었다. 그때도 조립 라인은 80% 이상 로봇이 설치되어 있었고 각종 장비의 운영 상태는 통신으로 전달되어 중앙 관제실에서 모니터링 했다.

그렇다면 과거의 FA와 지금의 스마트팩토리는 무엇이 다른 것인가? 가장 큰 차이는 중앙 관제실에서 명령을 내리는 주체가 누구인지에 대한 것이다. 예전의 로봇은 작동하기 전에 모든 작업 절차와 움직임을 미리 프로그래밍 해 놓아야만 했다. 장비의 계측 결과는 관리시스템에 나타나지만 임계치에 이르면 경고등이 켜져서 그 후론 사람이 움직여서 조치를 하는 게 일반적이었다. 지금은 그런 일까지도 컴퓨터가 한다. 오늘날 로봇의 움직임은 사전 프로그래밍도 가능하지만 로봇이 스스로 학습해서 필요한 작업 동작을 습득하는 일이 가능해졌다. 계측기의 측정값에 따른 상황은 컴퓨터가 판단해 수행주체(actuator)에게 명령을 전달해서 자동으로 조정한다. 즉, 전체 시스템의 통제권을 사람이 갖느냐 컴퓨터가 갖느냐가 3차와 4차 산업혁명을 가르는 것이다.



[그림 3] CPS(Cyber Physical System)의 핵심 기능

인공지능(Artificial Intelligence, AI)

앞서 언급한 지멘스 암베르그 공장에는 센서가 수 만개 설치되어 있고 그를 통해 수집되는 데이터가 하루 5천만건이다. CPS의 두뇌 역할을 컴퓨터가 맡게 된 것은 당연한 일인지 모른다. 사람이라면 결코 하루에 5천만건의 데이터 양을 처리할 수 없거니와 24시간 실시간 대응이란 물리적으로 불가능하기 때문이다. 한편으로는 컴퓨터로 처리할 수 있게 하기 위해 디지털 데이터를 만들어낸 것이기도 하다.

제어의 중추 역할을 하는 컴퓨터 시스템을 흔히 통칭해서 인공지능이라 말하는데, 스마트 팩토리에서 이용되는 인공지능의 기능은 계획과 스케줄링 수립, 프로세스와 자원 배분의 최적화, 로보틱스가 해당된다. 인공지능의 범주는 매우 다양하고 이론의 역사도 컴퓨터 하드웨어와 맞먹을 정도로 오래되었다. 사람의 언어를 문자로 바꾸거나 문자를 언어로 바꾸는 기술, 세계의 여러 언어를 상호 번역을 해 주는 자연어 처리, 사물 인식, 특정 분야의 지식을 축적해서 의견을 제시하는 전문가 시스템(예: IBM 왓슨) 등이 모두 인공지능의 영역에 속한다.

1956년 마빈 민스키, 존 매카시, 클로드 새넌 등이 참석한 다트머스 컨퍼런스에서 인공지능의 개념이 탄생되었다고 알려져 있다. 그러나 대중이 인공지능이란 용어를 자주 접하게 된 것은 몇 년 되지 않은 듯싶다. 인공지능 홍보에 혁혁한 공을 세운 것은 2017년 이세돌 9단과 바둑을 둬서 4:1로 이긴 인공지능 알파고일 것이다. 덤으로 우리는 딥러닝이라는 용어까지 익숙하게 되었는데, 인공지능을 부흥시켰고 4차 산업혁명의 중추로 자리잡게 된 인공지능의 핵심 기술이 바로 딥러닝이기도 하다.

기존 컴퓨터의 한계는 인간보다 훨씬 많은 정보를 기억할 수 있고 훨씬 빠른 속도로 계산을 해낼 수 있지만 일하는 방법(Algorithm)을 인간이 일일이 가르쳐야 한다는데 있었다. 이 문제를 개선하기 위해 컴퓨터로 하여금 스스로 일을 처리하기 위한 알고리즘을 학습시키는 방법이 고안되었는데 그것을 머신러닝(Machine Learning)이라고 한다. '알고리즘을 찾아내는 알고리즘'인 셈이다. 머신러닝의 갈래도 지도 학습, 비지도 학습, 강화 학습 등 여러 유형이 있지만 공통적으로 필요한 자원이 바로 데이터이다. 머신러닝은 본질적으로는 반복적인 데이터 분석과 무수한 시행착오를 통해 최적값을 찾아가는 과정이기 때문이다.

인공지능의 역사가 오래 되었음에도 불구하고 뚜렷한 성과가 나기 시작한 시기는 데이터가 폭발적으로 증가하는 시기와 맞물린다는 점에 주목할 필요가 있다. 2016년에 알파고(후속 버전과 구분을 위해 '알파고리'라고 부른다)는 인간을 이겨 회자되었지만 17개월 뒤 후속 버전인 알파고제로는 바둑 이론에 대한 아무런 사전 정보 없이 강화 학습을 한 지 3일만에 '알파고리'를 능가하는 수준이 되었다고 한다.

바둑을 두지 않아 알파고와 같은 인공지능이 낯설다면 지금 스마트폰을 켜고 아이폰은 '시리야'를, 안드로이드라면 '오케이 구글'을 불러 보자. 당신은 인간의 언어로 어떤 요구를 할 수 있고, 컴퓨터인 스마트폰은 적절한 답변을 하려고 할 것이다. 단순한 그 대화가 가능하기까지 엄청난 머신러닝과 인공지능 기술의 발전이 필

요했다는 점을 기억할 필요가 있다.

빅데이터(Big data)

인공지능의 학습 방법 중 딥러닝에서 절대적으로 필요한 것은 대량의 데이터이다. 학습과 검증을 위한 데이터가 많으면 많을수록 딥러닝을 통해 도출된 알고리즘의 정확도는 높아진다. 1942년에 나온 인공신경망(Artificial Neural Network) 이론에 토대를 둔 딥러닝은 2006년 제프리 힌튼 교수가 획기적인 성능 개선을 가능하게 한 방법론을 찾은 뒤 재도약할 기회가 생겼다. 하지만 결정적인 원인은 빅데이터와 GPU(Graphic Processing Unit)라는 하드웨어의 등장이 시기적절하게 맞았기에 활짝 꽃을 피울 수 있었다. 물론 빅데이터는 그 자체로도 충분한 활용 가치가 있다. 다만 4차 산업혁명의 맥락으로 볼 때는 인공지능이 중심이 되는 CPS에서 대량의 데이터가 혈액과 같은 역할을 한다는 점을 강조하고 싶은 것이다.

빅데이터를 활용하든 안 하든 지금 인류가 만들어내는 디지털 데이터 양은 어마어마하다. 전 세계에서 가장 책이 많은 도서관이 미국 의회도서관이고, 여기에는 약 3200만권의 책이 있다고 한다. 500페이지 책 1권을 바이트로 환산하면 약 500MB정도이고 미국 의회도서관의 책들을 바이트로 환산하면 32TB밖에 되지 않는다. 그런데 하루에 새로 만들어지는 데이터 양은 약 2.5엑사바이트, 책으로 환산하면 25억권 분량이 생산되고 있다는 것이다(출처: IDC&EMC 2011년 'Digital Universe Study'보고서).

빅데이터는 대개 처음부터 설계에 의해 만들어진 데이터라기보다 주어진 데이터가 축적된 사후에 목적을 부여해서 분석하는 과정이 더 많기 때문에 흔히 3V나 4V란 용어로 특징을 요약한다. 4V로 표현할 때 V는 Volume(축적되는 데이터 크기가 매우 크다), Velocity(매우 빠른 속도로 데이터가 생성된다), Variety(데이터 유형이 정형화되어 있지 않다), Veracity(통계분석을 위한 모수가 커짐으로써 더 정확한 결론을 유도할 수 있다)를 뜻한다. 빅데이터의 활용 사례는 구글에 검색된 '독감' 키워드 분석을 통한 미국 내 독감의 전파 경로 파악 성과도 있고, 아마존에서 책을 사면 관심 제품을 추천하는 방식도 이면에는 빅데이터 분석이 쓰이고 있다. 국내 사례로는 제빵 업체 P사가 특정 날씨에 잘 팔리는 빵의 상관도를 분석해서 날씨에 맞춰 많이 팔릴 만한 빵을 공급한다는 기사를 볼 수 있다.

사물인터넷(Internet of Things 또는 Internet of Everything)

4차 산업혁명의 기본적인 장(場)은 CPS이고, CPS는 물리적 세상의 데이터를 디지털화해서 가상 영역으로 불러들인 후 컴퓨터(인공지능)를 통해 분석해서 다른 목적에 이용하거나 다시 물리적 장치로 피드백하는 체계라는 점을 지금까지 설명했다. CPS의 핵심은 데이터이다. 데이터를 통해 인공지능이 학습하고 데이터를 통해 분석하고 통제를 하며 데이터를 전송하기 위해 통신이 존재하는 것이다. 4차 산업혁명의 시대에는 더 이상 공장, 집, 사무실 등 특정 공간이 큰 의미가 없다. 네트워크로 연결된 모든 세상이 CPS의 영역이 되기 때문이다.

사물인터넷은 이 데이터를 끌어 모으고 반응하는 일꾼

과 같다. 센서를 통해 수집하고 제어장치를 통해 중앙의 지시를 반영한다. 미쉐린타이어는 타이어에 센서를 부착해서 타이어가 마모되는 정도로 비용을 과금하는 새로운 서비스를 개시했다. 포드 자동차는 차량에 부착된 센서를 통해 운전자의 운전 패턴과 차량 성능 정보를 수집하고 있다. 사물인터넷은 전력공급관리, 물류 추적, 교통 상태 모니터링, 상수도 관리, 가로수 조명 관리, 쓰레기 처리까지 광범위한 목적으로 활용된다. 또 가정에서는 냉장고, 디지털 도어락, CCTV, 에어컨, TV 등에 스며 들었다. 비록 우리는 들을 수 없지만 인터넷을 통한 기계들의 대화는 사방에서 끊임없이 이어지고 있다. 이 부지런한 디지털 일꾼들이 모아온 데이터가 모여 빅데이터가 되고 인공지능을 성장시키는 재료가 되고 더 유용한 정보를 정련해 낼 데이터 광산이 된다.

4차 산업혁명시대의 보안 이슈

1. 사물인터넷 관련 보안 이슈

사물인터넷은 수많은 기기가 중앙시스템과 통신을 한다는 점에서 위험이 크다. 과거에는 중앙 시스템이라는 성으로 들어 갈 수 있는 길이 몇 개만 허용되었다면 IoT 시스템에서는 수백 개 수천 개의 작은 길이 생긴 셈이다. 이들 중 하나만 해킹을 해도 중앙에 접속할 방법이 생기는 것이고 사물인터넷 기기 다수를 점유하면 중앙시스템을 전복시킬 도구로 쓸 수 있을 것이다.

더 심각한 위협은 사물인터넷이 인간에 대한 공격 도구로 쓰일 수 있다는 점이다. 2018 평창올림픽 개막식 때 인텔이 하늘에 1200대의 드론을 띄워 드론쇼를 진행했다. 한 사람의 통제에 따라 군집 비행으로 멋진 쇼를 연출하기도 했지만, 만약 그 운용체계를 해킹해서 1200대의 드론을 운집한 군중을 향해 가미가제 특공대 같은 비행 무기로 쓴다면 상상만 해도 끔직한 사태가 일어날 것이다. 물론 이번 평창 동계올릭핌 개막식 드론쇼는 개막식 전 사전 녹화한 것이라 그럴 위험은 없었다.

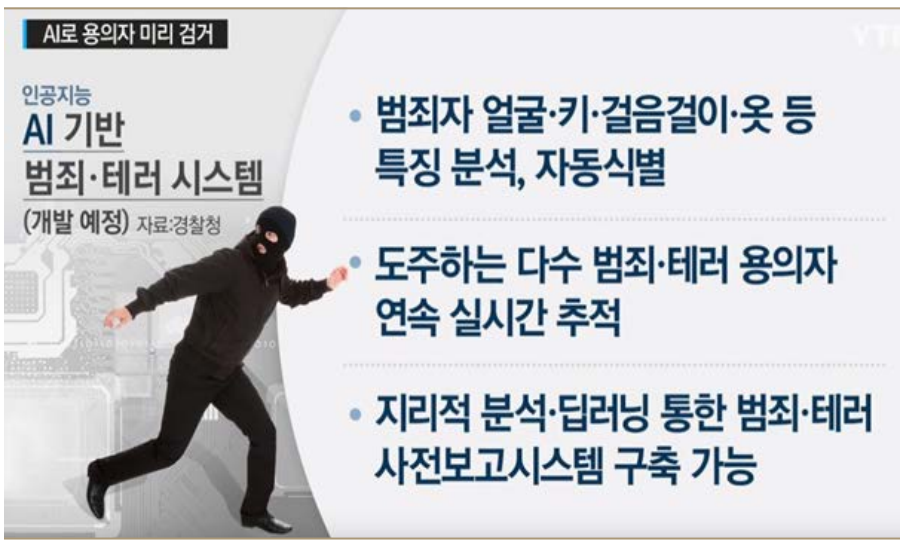
2. 빅데이터 관련 보안 이슈

빅데이터는 다양한 형식의 데이터를 대량으로 수집해서 의미 있는 분석 결과를 도출한다. 기존처럼 의도적으로 설계를 하는 경우도 적용될 수 있지만, 애초에 검색이나 분석 목적으로 설계하지 않은 날 것의 데이터들이라도 많은 양이 축적되면 특별한 정보를 끄집어 낼 수 있다고 보는 것이다. 빅데이터 시스템에서 대표적으로 거론되는 보안 이슈는 개인정보의 무단 이용이 발생할 위험이다. 우리나라 법 기준으로 개인정보란 단독 또는 다른 정보와 결합을 통해 살아있는 사람을 식별할 수 있는 정보라고 정의하고 있다. 빅데이터라는 창고에 입고되는 정보들은 개별적으로는 특정 개인을 식별할 수 없는 정보일 수 있다. 하지만 빅데이터 기술을 이용하여 여러 정보를 연관시켜 파악하면 특정 개인을 식별할 방법이 있을 수 있기 때문에 프라이버시 침해 위험 역시 높아질 수밖에 없다.

3. 인공지능 관련 보안 이슈

공상과학 소설이나 영화에서는 인공지능이 독자적인 사고를 하고 인간에게 반기를 들거나 나아가 인간을 지배하려고 하는 상황을 공포스럽게 묘사하곤 한다. 그러나 지금으로선 인공지능이 저절로 인간의 지배를 벗어날 위험보다는 인공지능을 특정 인간이 지배하게 되는 상황을 더 걱정해야 할 듯하다. 특히 인공지능이 신문기사를 쓴다거나 스마트팩토리처럼 제조 시스템을 통

제하거나 전문가시스템이 의료진단이나 법무적인 판단을 대신하는 상황이 되었을 때 인공지능의 의사결정에 편향을 일으키는 개입이 발생하면 치명적인 결과를 초래할 수 있다. 예를 들어, 인공지능이 멀쩡한 사람을 말기암환자라고 판정하거나 범죄자라고 판단하는 상황을 떠올려 보라.



[그림 4] 기반 범죄 · 테러 시스템 *출처: YTN

4. 4차 산업혁명 기술의 본질에 따른 위험

4차 산업혁명은 사물인터넷을 통한 빅데이터의 수집과 피드백, 빅데이터 분석을 통한 인공지능의 학습과 활용에 기반한 가상물리시스템에서 비롯된다고 요약할 수 있다. 정보를 수집하고 제어되는 디바이스들은 특정 공간의 제약을 벗어난 물리 세계에 퍼져 있고 이들을 연결시키는 것은 다양한 대역의 통신망이다. 4차 산업혁명의 보안 위협이 커지는 이유는 많은 단위의 연결성을 기반으로 하는 기술의 본질에서 비롯된다. 위협의 접점이 많으면 많을수록, 통제 범위가 넓으면 넓을수록, 운용되는 공간이 광범위할수록 위험은 통제하기 어렵기 마련이다. 자동차 부품에 장착된 센서가 중앙의 컴퓨터에 데이터를 보낼 수 있다면 악성코드가 담긴 데이터를 보내지 말란 법이 없지 않는가.

현재 대부분의 시스템 취약점 점검은 특정 장비나 소프트웨어를 대상으로 한다. 서버, DB, WAS, 보안장비 취약점은 대개 권고하는 보안 설정 값, 안전한 보안정책 적용 여부를 판단하고 네트워크 장비 역시 환경설정 사항을 분석하는데 그치곤 한다. 시스템이 연동되는 상황에서 취약점을 찾는 일은 모의해킹을 통해서도 수행 가능하지만 그 역시도 침투 가능성을 찾는데 치중되어 있어 전 영역의 위험 분석을 한다고 보기는 어렵다. 4차 산업혁명 기술과 관련한 위험 분석은 이렇듯 특정 자산에 대해서만 적용될 수도 없고 그렇게 한정해서도 안된다. 모든 대상이 필연적으로 연결되어 운영되는 상황을 고려하고 노드와 링크를 포함한 연결 구조 별로 분석 단위를 설정해서 위험분석을 해야할 것이다.

5. 소프트웨어와 네트워크는 여전히 기본 요소

4차 산업혁명의 요소 기술은 새로운 컴퓨터, 새로운 운영체제를 필수로 하지 않는다. 네트워크 역시 기존과 같이 TCP/IP를 기반으로 하고 있다. 기존의 다양한 IT 기술을 연계하여 데이터를 집적시키고 그 데이터를 활용하여 컴퓨터를 더 지능적으로 운용하는 것이 4차 산업혁명 기술의 특징이다. 따라서 전통적인 시스템의 취약점과 위협, 그리고 대응 방법은 여전히 유효하다. 스마트홈의 웹캠이나 디지털도어락 해킹 시연에서도 공격에 활용된 취약점도 디폴트계정 사용, 암호화 되지 않은 패킷 전송 등 10년 전이나 20년 전이라도 존재했을 고전적인 약점들이다. 자율주행 자동차는 자동차에 설치된 운영시스템을 해킹하는 일도 가능하지만 '연결성'에 착안해서 자율주행차에 시스템 데이터를 업데이트하는 중앙 서버를 해킹하는 것이 더 효과적인 공격이 될 수 있고 그를 위한 APT 공격 전략 역시 오랜 기간 통

용될 것으로 보인다.

6. 인간이라는 취약점과 위협

4차 산업혁명이 진전될수록 인간의 지위는 높아지고 입지는 좁아지게 될 것이다. 지난 2016년 열린 다보스 포럼에서는 2020년까지 전 세계적으로 약 770만개의 일자리가 사라지고 대신 200만개의 일자리가 생길 것으로 예견했다. 여기에는 인간이 차지하고 있던 중간 계층의 의사결정과 업무 처리는 인공지능과 로봇이 담당하게 되고 인공지능을 넘어선 수준에서 기계를 통제하는데 필요한 일에 인간이 투입될 것이란 의미가 내포되어 있다. 기계가 지배하는 세상에서 더 상위 단계의 중요한 지위에 인간이 있다는 뜻이다. 그런데 고질적인 취약점이며 가장 통제하기 힘들고 예측 불허인 대상이 바로 인간 아닌가. 아무리 기술이 발달하고 산업혁명이 몇 차례 거듭된다 할지라도 200만년을 유지해 온 인간의 사고 체계와 심리적 특성이란 바뀌기 힘들다. 결정된 규정을 지키지 않고 절차를 무시하고 예외로 취급 받기를 원하며 보안보다는 자기가 편히 일하기를 선호하는 인간의 습성이 유지되는 한, 모든 보안은 결코 완벽하게 적용될 수가 없다. 4차 산업혁명 시대에 이르러 다수의 인간이 축출되고 한편으로는 소수의 인간이 더 큰 힘을 지니게 되는 상황에선 인간에 대한 위험관리가 익숙하면서도 궁극적인 과제로 남게 될 것이다.

글을 쓰다 보니, 제목 그대로 그럴듯한 4차산업혁명이란 주제로 시작했다가 익숙하고 뻔한 보안 이야기로 마무리된 감이 없지 않다. 그러나, 몇 번을 숙고해도 기술과 보안이 같은 궤적을 타지 않는다는 생각은 바뀌지 않았다. 결국 보안이란, 끊임없는 위협과 약점의 발생과 그에 대한 대처라는 반복의 과정일 뿐 특정한 기술, 특정한 취약점, 특정한 위협에 대한 절대적이고 확실한 대처방안이라는 정적인 상태로는 절대 고착되지 않는다. 보안을 고민하는 우리는 어떠한 혁명의 시대가 도래하든지 그저 계속 주시하고 생각하고 대비할 따름이다.