2021-3호

AI TREND WATCH

2021. 2. 15.

인공지능: 사이버보안 패러다임의 전환

디지털경제연구실 김민진 전문연구원

KISDI 정보통신정책연구원
KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

인공지능: 사이버보안 패러다임의 전환

KISDI

디지털경제연구실 김민진 전문연구원

개 요

◈ **세계적으로 사이버 보안에 대한 중요도가 높아지는 가운데, 사이버 보안에서의 인공지능 기술이 주목받기 시작**

▶ 세계 각국은 사이버 보안 국가 전략을 수립하고 사이버 공격에 대응 하려는 노력을하고 있으며, 이에 우리 정부도 2019년 국가 사이버 안보계획을 수립하고 사이버 보안을 강화할 것을 발표

▶ 점차 고도화되는 사이버 공격에 대응하기 위해 인공지능 기술을 접목한 사이버 보안 적용 사례가 발견되고 있는 바, 사이버 보안에서의 인공지능의 역할이 주요해질 전망

◈ **본 고에서는 사이버 보안 정책, 개념, 시장 규모를 간단히 살펴보고 인공지능 기술이 사이버 보안에 미치는 영향을 조망한 후, 인공지능 보안 시장에서 수요 측면의 성장 잠재력이 높은 영역과 주요 공급 기업을 알아보고자 함**

주요 내용

1. 국내외 사이버 보안 정책

◈ **세계 각국은 증가하는 사이버안보 위협에 대응하기 위해 사이버 보안 국가전략을 수립하고 전략의 효과적 이행을 위한 전담기구 설치, 예산배정 등 추진기반 확충(국가 사이버 안보 기본계획, 2019)**

▶ 해외 주요국의 사이버 보안 국가전략 추진 현황

- (미국) 국가 사이버 전략 발표('18. 9), 국가 최상위 사이버보안 연구개발 전략계획 발표('19. 12)
- (영국) 국가 사이버 보안 전략 발표('16. 11), '20년까지 사이버 보안에 대한 예산을 2배 확대할 계획 발표(총 19억 파운드, 2.8조 원 규모)
- (중국) 국가 정보보호사고 응급 대응계획 발표('17. 6)

▶ 국내 사이버 보안 국가전략

- 사이버 안보 환경 변화, 안보 위협의 증대에 따라 관계부처 합동으로 국가 사이버 안보 기본계획을 발표('19. 9)

[참고] 국가 사이버 안보 기본계획('19~'22, '19. 9. 3. 확정) 주요내용

▶ (비전) 자유롭고 안전한 사이버 공간을 구현하여 국가 안보와 경제발전을 뒷받침하고 국제 평화에 기여

▶ (목표) ❶ 국가 주요 기능의 안정적 수행
❷ 사이버 공격에 빈틈 없는 대응
❸ 튼튼한 사이버 안보 기반 구축

▶ (전략과제) ① 국가 핵심 인프라 안전성 제고
② 사이버 공격 대응역량 고도화
③ 신뢰와 협력 기반 거버넌스 정립
④ 사이버 보안 산업 성장 기반 구축
⑤ 사이버 보안 문화 정착
⑥ 사이버 안보 국제협력 선도

자료: 관계부처 합동(2019. 9. 3.).

2. 사이버 보안의 개념과 시장 성장

◈ **사이버 보안은 악의적 로그인과 코드로부터 자산을 보호하는 활동을 말하며, 디지털 전환 확대와 함께 사이버 보안 시장 규모도 커질 전망**

▶ 사이버 보안은 컴퓨터·서버·모바일 기기·전자 시스템·네트워크(차량, 스마트홈, 공유기)·데이터에 대한 악의적인 전자적 공격[1]으로부터 보호하는 전반적인 활동을 뜻함

▶ 디지털 전환의 확대에 따라 사이버 보안 시장도 성장할 것으로 전망

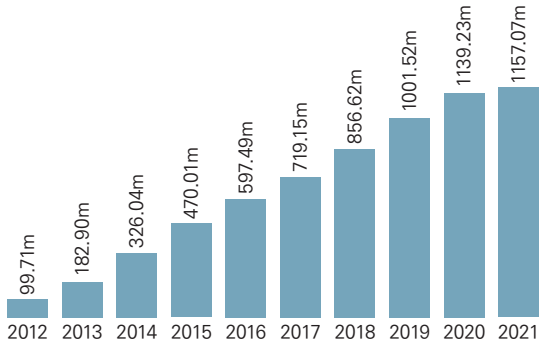
– 인공지능, 빅데이터, 클라우드 등으로 대표되는 디지털 전환은 사이버 공격 대상의 증가를 야기하여, 궁극적으로 사이버 보안의 중요성이 더욱 부각될 것

• 세계적으로 탐지된 총 악성코드는 '12~'20년 간 연평균 33.4% 증가했으며, '20년에만 1억3771만 개의 새로운 악성코드가 발견(AV-TEST, 2021)

• 글로벌 보안 소프트웨어 시장은 연평균 12.1% 성장하여 '19년에는 432억 달러 규모(Gartner)

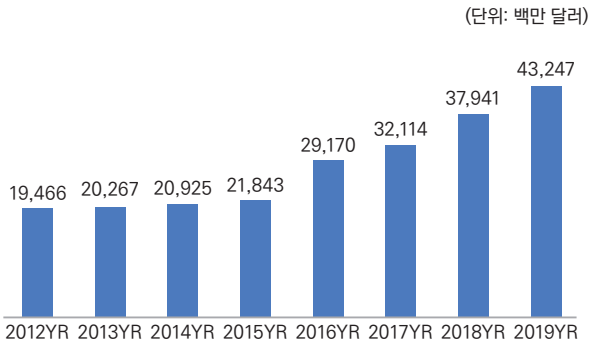
1) 악의적인 전자적 공격(사이버 공격): 디도스(Distributed Denial of Service: 동시다발적 좀비PC화로 트래픽 과부하), APT(Advanced Persistent Threat: 악성코드 클릭 유도, 내부통신망 접속권한 탈취), 파밍(인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동), 스미싱(문자메시지를 이용한 피싱) 등(한국판 뉴딜 실무지원단, 2021)

[그림 1] 탐지된 총 악성코드 수



자료: AV-TEST 홈페이지

[그림 2] 글로벌 보안 소프트웨어 시장



자료: Gartner(2012-2019); 재구성

3. 사이버 보안에서의 인공지능 기술의 영향

◈ **(사이버 보안에서의 인공지능) 사이버 보안에서 인공지능은 기술의 가치가 증가할 것**

▶ 인공지능은 사이버 공격에 대해 정확하면서도 선제적으로 위협을 탐지하고 예측하며, 빠르게 대응할 수 있도록 할 것(WEF, 2020)

- (사이버 공격 탐지 및 대응 효율화) 인공지능은 잠재적인 사이버 공격을 자율적으로 식별하거나 대응하여 비용과 시간을 절약하는 데에 기여할 것
  - Capgemini Research Institute(2019)[2]에 따르면 인공지능은 사이버 보안 체계 중 특히 위험 탐지 영역에서의 활용이 두드러지며, 응답자의 69%가 인공지능이 공격 탐지에 더 높은 정확성을 가질 것이라고 응답
  - Capgemini Research Institute(2019)에 따르면 응답자의 64%, 74%가 각각 인공지능이 사이버 공격을 탐지하고 및 대응하는 데에 소요되는 비용과 시간을 절약한다고 응답
- 인공지능은 사이버 공격의 예측, 탐지, 대응의 모든 보안 단계에 적용 가능(백악관 과학기술정책처, 2019)

◈ **(사이버 공격에서의 인공지능) 인공지능 보안의 발전에는 인공지능에 의한 사이버 공격의 진화가 중요한 요인**

▶ 인공지능과 사이버 공격의 접목은 공격 범위와 횟수를 증가시키거나 공격 정확성을 제고하고 우회 공격을 가능케할 수 있음(WEF, 2020)

- (공격 속도 증가 및 범위 확대) 공격 자동화로 전문 지식의 도움이 없이도 사이버 공격을 고속화 하거나 공격의 범위를 확장시킬 수 있음

2) 소비재, 소매, 은행, 보험, 자동차, 유틸리티 및 통신을 포함한 7개 산업의 고위 임원 850명 대상

- (정확성 향상) 딥러닝 분석을 활용하여 보다 정교한 공격 가능
- (스텔스 공격 시도) 탐지 및 제어를 피하기 위해 인공지능을 악용하여 은밀히 공격(보안관제 우회를 위한 악성코드가 진화하는 다양한 공격이 이미 실행 가능한 것으로 나타남)

[참고] 인공지능을 활용한 사이버 공격 가능성 시연 사례

◈ **정찰과 침투 단계를 자동화한 사이버 공격**

▶ 보안 전문 기업인 제로폭스(Zerofox)는 트위터를 이용해 악성링크 클릭 유도를 시연(2016)

- 인공지능을 활용해 공격 대상의 선호도를 조사하여 공격 대상이 링크를 클릭할만한 짧은 댓글을 달도록 함
- 해커가 200개의 댓글을 작성하는 동안 인공지능은 819개의 댓글을 작성했고, 해커는 잠재적으로 49명을 감염시킨 반면 인공지능은 275명을 감염시킴

▶ 조지메이슨 대학 교수 씬 팔카(Sean Palka)는 메일보안시스템(SEG)을 우회하는 악성 공격 기법 공개

- 인공지능에 활용되는 기계학습을 활용해 SEG의 사이버 보안 패턴을 스스로 학습하도록 함

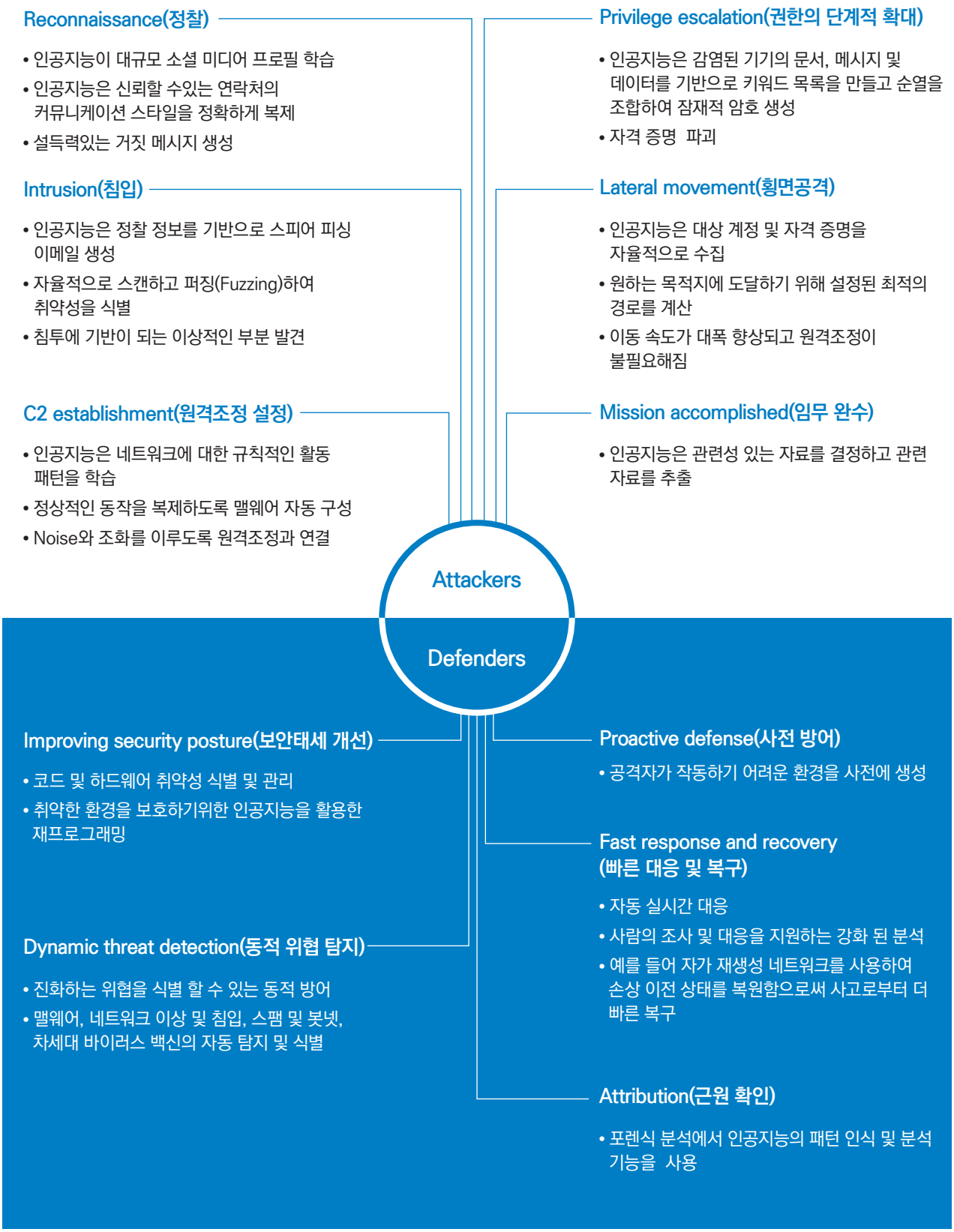
◈ **사이버 공격의 잠입과 확산 단계에서의 인공지능 활용**

▶ IBM은 잠입에서 공격까지의 과정을 쉽게 하기 위한 인공지능 악성코드 딥락커(DeepLocker)를 공개(2018)

- 공격 대상자가 화상앱을 사용했을 때 인공지능 기반 영상기술을 활용해 공격 대상자 여부를 확인한 후 공격 대상자로 판단될 경우 랜섬웨어 공격

자료: The Science Times(2020. 5. 11.).

[그림 3] 인공지능 공격자-방어자 균형



자료: WEF(2020)

4. 인공지능 보안 시장과 주요 Player 동향

◈ **인공지능 기반 보안 솔루션에 대한 수요가 증가하면서 인공지능 보안 시장의 빠른 성장이 전망되며, 사이버 보안 업체의 인공지능을 활용한 솔루션 개발이 활발히 이루어지고 있음**

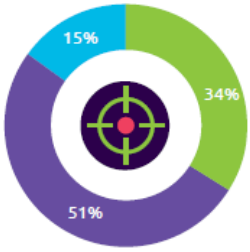
▶ (시장 전망) 사이버 보안에서의 인공지능의 비중이 커질 것으로 전망되며, 이에 따라 인공지능 보안 시장은 꾸준히 성장할 전망

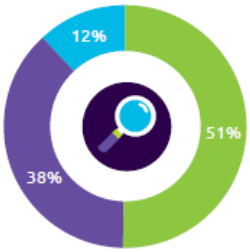
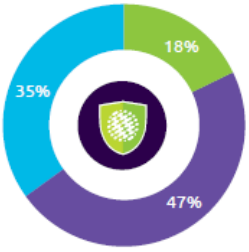
- 사이버 보안에서 인공지능의 가치는 2027년까지 460억 달러에 이를 것으로 예상(WEF, 2020)
  - 사이버 보안 특허 출원에서도 인공지능/머신러닝이 전체의 49%를 차지(WIPRO, 2020)

▶ (수요) 사이버 보안에 인공지능 기술을 적용하려는 경향이 확인됨

- 기업은 사이버 보안에서 인공지능의 필요성을 인식하고 있음
  - 설문 대상 기업의 69%는 사이버 공격에 대응하기 위해 인공지능이 필요하다고 응답(Capgemini Research Institute, 2019)
  - 설문에 응답한 기업의 55%가 인공지능/머신러닝을 사이버 보안에 적용할 계획이 있다고 밝힘(Cognilytica, 2018)
- 특히 사이버 공격 탐지 영역에서의 인공지능의 활용이 높고 시장 성장 가능성이 클 것
  - Capgemini Research Institute(2019)는 잠재력이 큰 인공지능 보안 영역으로 네트워크 리스크 스코어링, 탐지(침입, 사기, 악성코드), 행동 분석을 제시

〈표 1〉 사이버 보안 단계별 인공지능 활용 현황, 잠재력이 높은 영역 및 사례

<table>
<tr><th>활용 현황[주1)]</th><th colspan="2">잠재력이 높은 인공지능 보안 영역[주2)]의 개요 및 사례</th></tr>
<tr><td rowspan="3">예측
 
</td><td colspan="2">사용자/기계 행동 분석</td></tr>
<tr><td>개요</td><td>인간의 행동과 다른 특징을 보이는 행동을 식별하거나, 의심스러운 이용자 행동을 구별하여 사이버 공격을 탐지/차단</td></tr>
<tr><td>사례</td><td>ISFM(유럽 자율주행 셔틀 기업)
인공지능 기반 행동을 프로파일링하고 접근을 제어함으로써 자율주행 차량의 전자 제어 시스템을 해킹으로부터 보호</td></tr>
</table>

탐지 	침입 탐지	
	개요	높은 정확성을 바탕으로 한 자동화된 방식으로 사이버 공격을 실시간 신속하게 탐지, 분석, 방어
	사례	*Berkeley Labs* 사이버 보안 방법론과 머신러닝 알고리즘, 센서 기술을 결합하여 전력망 침입을 감지하는 보안 모니터링 및 분석 프레임워크 구축
	사기탐지	
	개요	머신러닝을 활용한 사기 위협 감지
	사례	*PayPal* 거래를 실시간으로 분석하는 딥러닝 시스템을 사용하여 사기율을 수익의 0.32%로 감소
	악성코드 탐지	
	개요	기존의 식별된 악성코드 특성을 사용하여 잠재적인 악성코드 예측
	사례	*Duke Energy, BP, Honeywell(석유 및 가스 기업)* 실시간 센서 데이터와 인공지능을 활용하여 다양한 침입을 감지
대응 	네트워크 리스크 스코어링	
	개요	데이터를 통해 정량적으로 위험을 등급화하며, 고위험순으로 위협의 우선순위를 지정하는 시간을 단축
	사례	*Verizon* 인공지능 기반 보안평가 프레임워크를 통해 기업이 위험을 식별하고 우선 순위를 지정하며, 즉각적인 보안 조치가 필요한 위험에 집중할 수 있도록 지원

주1) 인공지능 기술의 보안에의 활용 정도: High utilization Medium utilization Low utilization
주2) 잠재력이 큰 인공지능 보안 영역: 인공지능을 보안에 적용했을 때 복잡성이 낮고 혜택이 큰 영역
자료: Capgemini Research Institute(2019); 재구성.

▶ (공급) 사이버 보안 업체에서는 인공지능을 활용한 솔루션 개발이 이루어지고 있음

– 국내외 기존·신생 보안 소프트웨어 주요 기업들은 인공지능을 활용한 사이버 보안 솔루션 개발하거나 인공지능 기반 신생업체를 인수하여 인공지능 보안 솔루션 개발

〈표 2〉 국내외 주요 인공지능 보안 서비스 제공 기업

구분	기업명	인공지능 보안 솔루션/활동
Gartner 선정 3년 연속 보안 소프트웨어 top 5 선정 기업	Symantec (미국)	• 시만텍 ICSP 뉴럴(인공지능 기반 산업제어시스템(ICS) 보호 솔루션, '18) – 인공지능을 이용해 USB기기에서 악성코드를 탐지, 대응함으로써 사물인터넷(IoT)환경을 겨냥한 공격을 차단 • SEP15(SymantecEndpointProtection,'19) – 보안상태평가, 적용, 학습, 권장사항을 자동으로 처리
	McAfee (미국)	• McAfee Investigator(인공지능과 머신러닝을 사용하여 데이터 수집 자동화, '17) – 위협 우선순위 지정 – 빠르고 철저한 악성코드 조사 • McAfeeEndpoint('17) – 딥러닝을 통한 보안 의사 결정 – 보안 프로그램 실행 전후 기계학습
	IBM (미국)	• X-포스 익스체인지(보안 위협 인텔리전스 플랫폼) – 전세계에서 매일 200억 건 이상 발생하는 각종 이벤트를 실시간으로 감시하고 위협을 탐지
국내 주요 기업	안랩 (한국)	– 인공지능 기반 보안 관제 스타트업인 제이슨의 지분 60% 인수('20) – 인공지능 기반 이상행위 분석 기술 접목으로 솔루션/서비스 고도화, 향후 인공지능 기반 클라우드 보안 관제 등으로 사업 및 기술 시너지 확대 목적
	이스트시큐리티 (한국)	• Threat Inside(딥러닝 기술이 적용된 신제품 악성코드 위협 대응 솔루션, '18) – 악성코드를 식별, 분류하고, 악성코드의 상세 정보와 유형에 맞는 대응 가이드 제공(정확성, 신속성 강화)
CBinsights 인공지능 100대 유니콘 기업	Obsidian Security(미국)	– 엔터프라이즈 ID를 보호하기 위해 머신러닝 기반 기술을 구축 – 인공지능을 적용하여 기업 하이브리드 클라우드 환경에서의 보안 지원
	SentinelOne (미국)	– 인공지능을 적용하여 온프레미스(On-premise) 및 클라우드 환경 모두에서 실시간으로 위협을 자동으로 제거
	Onfido(영국)	– 얼굴 생체 인식 기능이있는 인공지능 기반 기술을 제공하여 사용자의 정부 발급 신분증이 진짜인지 사기인지 평가
	Abnormal Security(미국)	– 인공지능 기반 위협 탐지 엔진이 사람, 관계 및 비즈니스 컨텍스트에 대한 다양한 데이터 세트를 분석하여 비정상적인 행동을 이해하고 공격을 차단 – 사용자에게 공격이 차단된 이유를 명확하게 설명하여 인공지능 판단에 대한 투명성 제공
	Dark Trace(영국)	– 인공지능 방어시스템, 네트워크 침입 탐지: 인공지능 기술을 활용해 사물인터넷(IoT) 보안 침해와 데이터 손실 등 각종 사이버 위험에 대비한 업무환경 조성 ※ 2017년 워너크라이(WannaCry) 랜섬웨어가 수백개 기관을 대상으로 이메일과 파일 등을 보내 클릭을 유도해 사이버 공격이 이뤄졌을 때 다크트레이스의 인공지능 방어시스템은 몇 초 만에 방어

인공지능 사이버 보안 주요 기업	Vade Secure (프랑스)	• 인공지능 기반 이메일 보안 솔루션 – 피싱 감지를 위한 supervised 머신러닝 – 스피어 피싱 감지를 위한 이상감지 및 자연어처리 – 인공지능 기반 자동화
	CrowdStrike (미국)	• Threat Graph(인공지능 기반 클라우드 보안 소프트웨어) – 인공지능 기반 소프트웨어가 학습을 통해보안이슈를 빠르게 구별, 최적화된 방법으로 대처하여 해킹 방어
	SparkCognition (미국)	• DeepArmor – 인공지능을 이용하여 악성코드의 형태를 지속적으로 학습하고 바이러스의 변이를 인지
	Vectra(미국)	• Cognito Detect(인공지능 사이버 보안 솔루션) – 상시 학습을 통한 위협 탐지 자동화 – 감지된 사고를 심층적이고 광범위하게 조사 – 네트워크 메타 데이터, 로그 및 클라우드 이벤트 실시간 데이터 수집/분석/저장

주1) Obsidian Security: (기업가치) 2700만 달러/ (펀딩 규모) 2,950만 달러(2019)
주2) SentinelOne: (기업가치) 30억 달러/ (펀딩 규모) 6억9,650만달러(2020)
주3) Onfido: (기업가치) 2억 달러/ (펀딩 규모) 2억1,610만 달러(2020)
주4) Abnormal Security: (기업가치) 5억 달러/ (펀딩 규모) 7,400만 달러(2019)
주5) DarkTrace: (기업가치) 16억 5천만 달러/ (펀딩 규모) 2억 3,230만 달러(2018)
주6) Crowd Strike: 2019년 대비 매출 2020년 91% 성장
자료: CBInsights, Gartner, 각 사 홈페이지 및 News Clipping; 재구성.

시 사 점

◈ **디지털 전환의 확대에 따라 사이버 보안은 중요한 이슈로 부각될 전망**

▶ 데이터 이동에 따른 개인정보 보호 필요성 증대, 5G 경쟁 본격화에 따른 사이버 공격 표면 증가, 안전하고 스마트한 재택 근무 환경 니즈 발생, 내부 보안 강화 등은 2021년 주목해야 할 사이버 보안 이슈(Palo Alto Networks, 2020)

◈ **아울러 점차 고도화되는 사이버 공격에 대응하는 데에 있어 인공지능 기술은 사이버 보안의 필수 요소가 될 것이며, 인공지능이 사이버 보안 패러다임을 주도하게 될 것**

▶ 인공지능 기술의 발전은 사이버 공격과 사이버 보안의 고도화에 기여할 것

– 인공지능 기술을 활용한 자동화, 분석 능력 고도화는 사이버 보안의 정확성과 대응 속도 향상에 기여할 것

- 반면, 인공지능을 활용한 사이버 공격의 고도화 역시 인공지능 보안 활성화를 촉진하게될 것

▶ 인공지능이 사이버 보안 시장을 주도하게 될 것으로 예상됨에 따라 국내외 사이버 보안 솔루션 공급 기업들은 관련 인공지능 보안 솔루션을 출시하거나, 인공지능 보안 스타트업을 인수하는 등의 행보를 나타냄

◈ **국내에서도 국가 사이버 안보 기본계획으로 사이버공격 대응역량 고도화를 위해 인공지능 기술의 적용을 과제로 제시하고 있는 바, 관련 기업들이 방어 도구를 개발할 수 있도록 지원하는 등 인공지능 산업 성장 기반 마련이 필요**

참고문헌

Andrew J. Lohn(2020. 12), A Primer for Policymakers on Machine Learning Cybersecurity

Capgemini Research Institute(2019), ReinventingCybersecurity withArtificial Intelligence.

CBinsights(2021), The Top 100 AI Startups Of 2020: Where Are They Now?.

Cognilytica(2018. 12), AI in cybersecurity.

Gartner(2012-2019); Market Share Analysis: Security Software, Worldwide.

Palo Alto Networks(2020. 12. 15),2021년에 주목해야 할 사이버 보안 주요 이슈.

The Science Times(2020. 5. 11.), 사이버 공방전에 활용되는 인공지능.

WEF(2020. 11), Future Series: Cybersecurity, emerging technology and systemic risk, INSIGHT REPORT.

wipro(2020), STATE OF CYBERSECURITY report 2020.

ZDNET(2019. 3. 26.), AI 사이버 보안, 이제 선택이 아닌 필수.

관계부처합동(2019. 9. 3.), 국가 사이버 안보 기본계획.

국경완·공병철(2019), 인공지능을 활용한 보안기술 개발 동향. IITP.

디지털데일리(2019. 4. 12.), 디지털전환 외치지만 과연 보안투자 따라가고 있나.

이스트소프트(2018. 10. 24.), 이스트 시큐리티 AI 악성코드 위협 대응 솔루션 쓰렛 인사이드 출시.

인공지능신문(2020. 1. 22.), 안랩, 인공지능 보안 역량 강화에 나섰다.

전혜수(2020. 6. 3.), 자동화와 인공지능: 사이버 보안의 새로운 시대를 개척하다, 인사이트 리포트, 삼성SDS.

한국판 뉴딜 실무지원단(2021. 1. 8.), K-New Deal Weekly.

AV-TEST 홈페이지(https://www.av-test.org), 최종접속일: 2021. 2. 3.

AWAKE 홈페이지(https://awakesecurity.com/glossary/ai-security/), 최종접속일: 2021. 2. 3.

KISDI AI TREND WATCH는 인공지능 관련 주요 이슈와 최신 동향 정보를 제공하는 온라인 정기간행물입니다.
KISDI AI전략센터 및 산학연 전문가들이 참여하여 매월 15일과 30일에 온라인으로 배포합니다.
본지에 게재된 내용은 본 연구원의 공식 견해와 다를 수 있습니다.
보고서와 관련된 문의는 김민진 전문연구원(minjinkim@kisdi.re.kr, 043-531-4356)으로 연락주시기 바랍니다.