차세대 보안의 방향성과 핵심 기술 요소

김미희 이글루코퍼레이션 보안분석팀 팀장

1. 머리말

AI, 클라우드, 블록체인, 양자 컴퓨팅 등 차세대 기술의 발전은 디지털 환경을 변화시키며 새로운 비즈니스 기회를 제공하고 있다. 소프트웨어 기반 생태계의 발전과 기술융합으로 산업 간 경계가 모호해지면서 혁신적인 비즈니스 모델이 등장하고, 더 나은 고객 경험과 운영 효율성을 극대화할 기회가 창출되고 있는 것이다. 그러나 이러한 변화 속에서 사이버 보안은 새로운 위협에 직면하며 변화의 기로에 놓여 있다.

산업 간 연계로 인해 디지털 생태계의 복잡성(Complexity)이 높아지고 가시성(Visibility)은 낮아지면서, 디지털 환경은 새로운 공격 벡터로 인한 보안 위협에 노출되고 있다. 차세대 기술이 폭발적인 생태계 발전의 촉매제가 되는 동시에 고도화된 사이버 공격에 악용되면서, 사이버 공격 역시 새로운 전환점을 맞이하고 있다.

디지털 발전의 게임 체인저인 AI는 LLM(거대언어 모델, Large Language Model)과 생성형 AI를 기반으로 AI 시대의 황금기를 이끌고 있다. 대용량 언어 데이터를 학습해 결과를 제공하는 생성형 AI는 오픈 AI(OpenAI)의 Chat-GPT를 필두로 구글(Google)의 제미니(Gemini), 바이두(Baidu)의 어니봇(Ernie Bot), 재스퍼(Jasper)의 재스퍼(Jasper), 딥마인드(Deepmind)의 스패로우(Sparrow) 등 다양한 서비스를 바탕으로, 인간과 같이 창작이 가능한 새로운 경험을 제공하고 있다.

그러나 사이버 공격자들 또한 사회공학적 기법, 사기, 신규 취약점 발굴, 공격도구 자동 생성 등을 위한 악성 LLM 기반 서비스인 FraudGPT, WormGPT, BlackHatGPT, XXXGPT, WolfGPT 등을 앞 다퉈 공개하고 있다[1]. 이러한 AI의 무기화로 사이버 공격 기술이 보편화되면서 진입장벽이 낮아지고, 기존 사이버 보안 체계는 무력화되고 있다. 따라서 지능화(Intelligence)된 사이버 공격에 대응하기 위해 새로운 보안 전략이 필요해지고 있다.

이에 새로운 사이버 보안 방향성을 확립하고 핵심기술을 개발해, 지능화된 사이버 공격에 효과적으로 대응하기 위한 전략이 논의되고 있다. 차세대 보안은 단순한 방어를 넘어, 위협을 예측하고 선제적으로 대응하는 접근 방식을 요구한다. 안전한 디지털 환경을 구축하는 데 핵심적인 역할을 수행하기 위해선, 다양한 관점을 반영해 사이버 보안 위협 요인을 식별하고 대응할 수 있는, 다양한 기술 요소에 대한 고찰이 필요하다. 이에 따라 이번 원고에선, 차세대 보안을 위한 사이버 보안 패러다임을 분석하고, 이를 대응하기 위한 차세대 보안의 방향성과 핵심 기술 요소에 대해 살펴보고자 한다.

2. 차세대 보안 전략 및 핵심기술 요소

2.1 사이버 보안의 한계와 공격 패러다임의 변화

급변하는 사이버 보안 위협에 대응하기 위해선, 먼저 사이버 공격에 영향을 미치는 요인을 철저히 분석해야 한다. 사이버 공격은 공격을 수행하는 공격 주체, 공격으로 피해가 발생하는 공격 대상, 공격 기술이라는 3가지 요소로 구성되며, 이들 요소는 환경적 요인과 공격 목적에 따라 다음 <표 1>과 같이 분류할 수 있다.

<표 1> 사이버 보안 트렌드 및 영향도 분석

구분	공격원인	상세설명
환경 요인	SW 생태계 확산	• 오픈소스(OSS) 보편화로 머신러닝, AI, 블록체인, 클라우드 등 높은 수준의 시드기술이 확산돼 다양한 산업 생태계의 SDx(Software Defined Everything) 촉발 • CI/CD, MSA(Micro Service Architecture), DevOps를 통해 생산성과 효율성 향상
	차세대 기술 기반의 공격 고도화	• Chat-GPT, 제미니, 어니봇, 재스퍼, 스패로우 등 생성형 AI기술 보편화 • FraudGPT, WormGPT, BlackHatGPT, XXXGPT, WolfGPT 등 악성 LLM기반 HaaS(Hacking as a Service) 성행 • LanChain등 LLM기반 애플리케이션 취약점 악용 증가
공격 요인	금전적 목적 공격 강화	• 직접적 피해: 국가 지원의 사이버 공격그룹 및 서비스형 랜섬웨어 공격그룹에 의한 공격으로 랜섬웨어나 암호화폐 거래소 해킹 확산 • 간접적 피해: 정보 유출 및 서비스 운영 중단, 고객 신뢰 및 충성도 하락으로 인한 기업 이미지 훼손
	정치적 목적의 공격 강화	• 기술 발전에 따른 국제 안보 환경이 변화함에 따라 국가안보에 영향을 미칠 수 있는 외교·안보·국방·통일 등의 분야에서 사이버 공격 증가 • 국제사회 간의 갈등으로 인한 패권전쟁이 초국가적 위협요인으로 작용하면서 사이버 안보와 보안에도 영향

공격자가 목표한 공격 목적을 달성하려면, 공격 대상의 취약점을 발견하고 이를 이용할 수 있는 공격기법, 기술, 도구를 마련해야 한다. 과거엔 개인적 호기심이나 과시를 위한 공격이 많았다면, 최근엔 정치적·금전적 목적의 공격이 주를 이루고 있다.

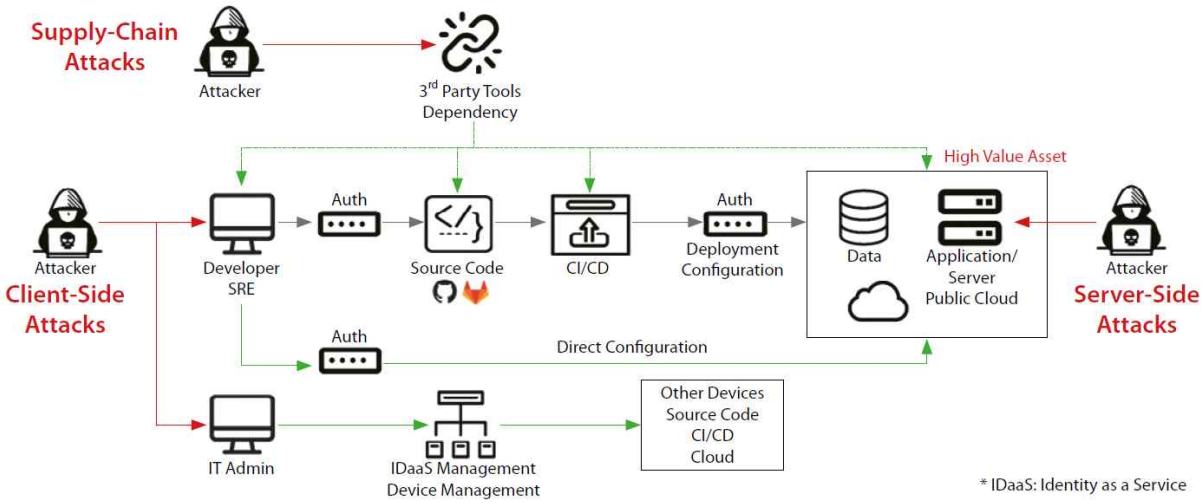
금전적 목적을 충족하기 위해 가장 효과적인 방법은 암호화폐를 탈취하는 것이다. 대표적 공격 방법 중 하나가 랜섬웨어 유포나 암호화폐 거래소처럼 직간접적으로 암호화폐와 관련된 플랫폼을 공격하는 것이다. 미국 블록체인 분석기업인 체이널리시스(Chainalysis)에 따르면, 2023년 북한은 20개 암호화폐 업체를 해킹해 10억 달러 이상의 자산을 탈취했으며, 이는 최근 8년 동안 가장 높은 수치다[2].

그런데 북한이 그 1년 전인 2022년 15개 암호화폐 업체를 해킹해 탈취한 금액은 17억 달러에 이른다. 즉, 약 40%의 감소세를 보인 것인데, 암호화폐 업체의 보안 수준이 향상돼 탈취 금액에도 영향이 있는 것으로 볼 수 있으나, 암호화폐 특성상 가격변동이 빈번하게 발생하기에 범죄자금에도 편차가 발생하고 있는 것으로도 해석할 수 있다. 특히, 암호화폐의 편차가 심하면 추가적인 사이버 공격의 발생 빈도가 증가하는 것으로 미루어 볼 때, 불법 자금의 차이를 해소하기

위해 새로운 공격 경로를 모색하는 것을 알 수 있다[3].

이러한 상황에서, 국가 지원형 사이버 공격 그룹들은 정치적 목적을 달성하기 위한 사이버 공격을 병행하고 있다. 국내의 경우, 지정학적 조건과 정치·경제적인 이슈가 맞물려 중국, 러시아, 북한 등에 의한 사이버 공격이 빈번하게 발생하고 있다. 2014년부터 발생한 방산 관련 대기업 해킹[4] 및 한국수력원자력 해킹을 통한 자료유출 사고[5], 2016년 대우조선해양 해킹 사고[6], 2021년 KAI(한국항공우주산업, Korea Aerospace Industries) 해킹 사고[7] 등이 국가 주도 사이버 공격으로 인한 피해 사례들이다.

최근엔 국내 소프트웨어 공급망을 이용한 공격 사례가 증가하고 있다. [그림 1]과 같이 소프트웨어 생태계에서 공급망 공격의 공격벡터는 크게 세 가지로 구분될 수 있다. 소프트웨어 개발 업체에 개발자로 위장 취업하거나 개발자를 타깃으로 공격하는 클라이언트 기반 공격(Client-Side Attacks), 소프트웨어 업데이트 서버 등을 공격하는 서버 기반 공격(Server-Side Attacks), 소프트웨어 구성요소 공격(Supply-Chain Attack)이다.



[그림 1] 소프트웨어 기반 생태계의 공급망 공격벡터

이러한 공격들은 방산, 첨단기술, 외교, 안보 등의 분야에서 정보를 절취하기 위한 목적으로 해킹 메일이나 제로데이 취약점을 이용해 이뤄진다. 이 외에도, 인증서 탈취 및 소스코드 내 백도어 삽입 등을 통한 공격도 시행되고 있다. 해당 공격들은 조직이나 기관을 직접 공격하는 것보다 더 효율적이며, 공급망 공격 특성상 중앙 집중형 구조로 인해 피해가 폭발적으로 증가할 수 있기 때문에 빈번하게 사용되고 있다.

이처럼 최근 사이버 공격은 기존 보안 체계를 무력화하고 공급망 공격을 통해 대규모 타깃 공격을 감행할 수 있는 수준으로 확대되고 있다. 이에 따라 지능화된 사이버 공격을 고려한 대응 전략과 차세대 기술활용 방안이 절실히 필요하다.

2.2 지능화된 사이버 공격 대응전략 및 핵심 기술요소

클라우드, ICS/OT, IoT/IIoT 등 인프라 복잡성이 증대되면서 부적절한 보안 아키텍처 구성이나 설

정으로 인한 보안 이슈가 늘어나고 있다. 이에 따라 유기적인 보안 체계가 필요해지고 있으며, AI, 블록체인, 디지털 트윈, 양자 암호 등 차세대 기술을 접목해 사이버 보안 문제를 해결하려는 노력이 지속되고 있다.

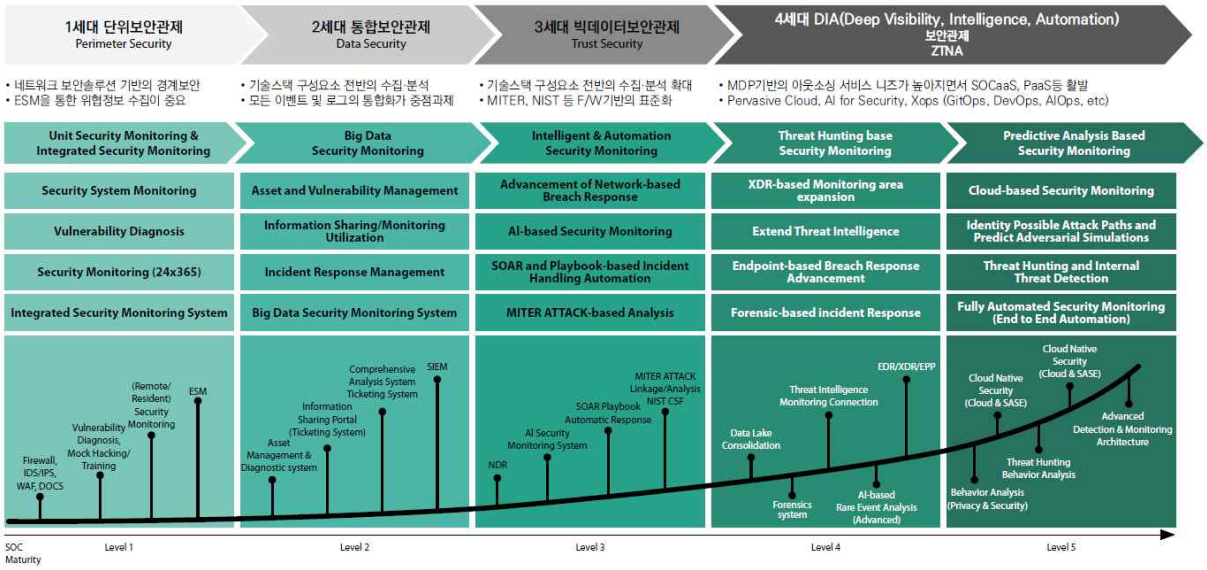
복잡한 인프라 보안을 강화하기 위해선 사이버 보안 위협의 패러다임을 반영한 체계적인 보안 체계를 수립하는 것이 중요하다. FedRAMP, FIPS 140-2, NIST SP 800시리즈 등 다양한 보안 프레임워크가 존재하지만, NIST(미국 국립표준기술연구소, National Institute of Standards and Technology)에서 발표한 CSF(Cybersecurity Framework)가 가장 널리 사용되고 있다. 최근 발표된 CSF 2.0은 다양한 규모 조직과 기업의 기술 스택, 소프트웨어 생산자를 포함한 다양한 공급망 위험 관리의 중요성을 반영하고 있다. 이를 잘 보여주는 것이 CSF 1.0에서 제시한 식별(Identify), 예방(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)라는 5가지 프레임워크 코어에, 거버넌스(Governance)라는 요소를 추가해 발표한 점이다. 이는 공급망 보안 위협 및 보안의 가시성을 확보하기 위한 효율적인 보안 관리 방안을 통해, 적절한 보안 수준을 제공하기 위한 목적이라고 할 수 있다[8].

보안 체계를 구체화할 수 있는 프레임워크가 준비됐다면, 다음으로는 다양한 보안이슈를 식별하고, 이에 대응할 수 있는 조직과 기술을 접목한 환경을 구성해야 한다. 지능화된 사이버 공격에 대응하기 위해선, 클라우드, 네트워크, 애플리케이션, 엔드포인트 등 인프라를 구성하는 기술 스택에서 발생하는 대량의 이벤트나 경보를 수집하고 분석해 보안 위협을 식별하고 예측할 수 있어야 한다. 여기엔 빅데이터 분석, AI 등 차세대 기술이 필수적이다. 현재 연구자들은 악성코드, 인포스틸러(Infostealer), 다크웹(DarkWeb)/딥웹(DeepWeb) 등의 위협 정보를 수집하고 특징을 추출해 AI 기반 핵심 대응 기술을 개발하고 있다.

기존 보안체계는 SOC(보안관제, Security Operation Center)를 통해 운영됐다. 이는 인프라 보호를 위해 구성된 다양한 이기종 보안솔루션을 모니터링하기 위한 조직과 기술을 집약한 것이다. 지금껏 SOC는 외부망과 내부망의 보안 경계(Security Perimeter)에서 발생하는 위협을 식별했으나, 공급망 공격이나 APT, 파일리스(Fileless), LotL(Living of the Land) 등의 공격이 증가하면서 시그니처(Signature), IoC와 같은 단순 탐지 메커니즘이 한계를 보이고 있다. 이 때문에 공격자의 전략과 전술을 기반으로 공격 과정을 분석하는 TTP(Tactic, Technique, Procedure) 기반 방어체계를 구축하는 것이 중요하다.

[그림 2]는 지능화된 사이버 보안 위협에 대응하기 위한 SOC 발전현황을 보여준다. SOC는 이제 다양한 로그를 수집하고 분석할 수 있도록 위협 인텔리전스(Threat Intelligence)를 활용하고, 대량의 데이터를 자동 분석해 발견되지 않은 보안 위협을 식별(Deep Visibility)해야 한다. 결국 대량의 데이터 속에서 위협 정보를 탐지하기 위해선, 더 많은 데이터를 활용해 위협을 분석할 수 있도록 AI와 자동화(Automation) 기술이 필수적으로 요구되는 것이다.

한편, 차세대 기술을 바탕으로, 디지털 환경에서 발생하는 다양한 사이버 공격을 탐지하고 대응하는 MDR(Managed Detection Response)이 클라우드와 결합하며, 사이버 보안의 아웃소싱화가 용이해지고 있다. 이를 통해 서비스형 보안(CSaaS, Cybersecurity as a Service)이 본격화 되고 있는 것이다. SOCaaS(SOC as a Service), PaaS(Penetration as s Service), SWGaaS(Secure Web Gateway



[그림 2] 사이버 보안위협에 따른 SOC 발전현황

as a Service), DLPaaS(Data Loss Prevention as a Service) 등 다양한 서비스형 보안 모델은 조직의 보안 요구에 맞춰 위협 헌팅(Threat Hunting), 능동적 방어(Active Defense), 디셉션(Deception) 등 다양한 보안 기능을 유연하게 제공하고 있다. 이는 비용 절감 효과와 함께, 전문적인 보안 관리를 지원할 수 있게 한다.

사이버 보안 위협에 대응하기 위한 체계·환경 구축이외에도, 개인정보 및 민감 정보를 보호하기 위한 기술도 연구되고 있다. 동형 암호(Fully Homomorphic Encryption) 및 연합 학습(Federated Learning), 영지식 증명(Zero-knowledge proofs), 합성 데이터(Synthetic Data) 등의 PET(개인정보 보호 강화 기술, Privacy Enhancing Technology)를 통해 개인정보 최소화 및 익명화를 실시하는 것이다. 이는 적대적 AI 활용 등으로 인한 정보 유출 등에 대응하는 방안으로 꼽힌다.

3. 맺음말

지금까지 사이버 보안 생태계의 보안 위협 패러다임, 그리고 이에 대응하기 위한 차세대 보안의 방향성과 핵심기술 요소에 대해 살펴봤다. 최근의 사이버 보안 체계는 지능화된 사이버 공격과 AI의 무기화로 인해, 보안 체계 무력화라는 한계에 도달했다. 그 극복을 위해선, 지능화된 사이버 위협 분석 기술을 활용해, 위협 인텔리전스를 기반으로 국가 주도형 사이버 공격과 사이버 범죄 행위에 대한 위협 프로파일링 및 위협 헌팅을 수행해야 할 필요가 있다. 이를 통해 잠재적인 보안 위협을 식별하는 것이 중요하다. 특히, AI, 블록체인, 메타버스 등 다양한 기술로 인해 공격표면(Attack Surface)이 증가함에 따라, 범용적 위협 분석을 위한 표준화된 기술 적용과 고도화된 기술이 필요하다.

지능화되고 자동화된 기술 고도화를 바탕으로 한, ZTA(Zero Trust Architecture) 기반 보안 체계를 적용하기 위해선 고성능 AI 기술과 시각화가 필요하다. 또한, 은닉 채널, 가상화폐 등의 범죄 정보 및 사이버 위협 정보를 수집하고 이를 도메인별 교차 분석해, 신종 사이버 범죄를 예측하고 추적하기 위한 기술 연구도 수반돼야 한다. 이를 위해 인프라를 구성하고 있는 자산을 식별

하고 위협을 파악해 우선순위에 따른 대응 전략을 모색하는 것이 중요하다.
결론적으로, 차세대 사이버 보안 체계 구축과 발전을 위해선, 지능화되고 자동화된 기술에 대한 지속적 연구와 적용이 필수다. 이를 통해, 좀 더 안전하고 신뢰할 수 있는 디지털 환경을 조성할 수 있을 것이다. 앞으로 이러한 노력이 사이버 보안의 새로운 기준을 세우고 더욱 효과적인 대응 전략을 마련하는 데 기여할 것으로 기대해 본다.

[참고문헌]

[1] Studying Underground Market for Large Language Models, Researchers Find OpenAI Models Power Malicious Services, Jan 19, 2024, techpolicy.press, https://www.techpolicy.press/studying-black-market-for-large-languagemodels-researchers-find-openai-models-power-malicious-services/
[2] The 2024 Crypto Crime Report, Chainalysis, FEBRUARY 2024, https://go.chainalysis.com/2024-crypto-crimereport-kr.html
[3] 진화하는 북한의 사이버 공격 현황과 대응, 2023.11.1., 국가안보전략연구원, https://www.inss.re.kr/publication/bbs/ib_view.do?nttId=41036988&bbsId=ib&page=1&searchCnd=0&searchWrd=
[4] 북한, 방산업체 등 대기업 계열사 해킹...군사기밀 노린 듯, 2016.6.13., 연합뉴스, https://yonhapnewstv.co.kr/news/MYH20160613008100038
[5] 한수원 해킹 악성코드의 작동 원리는?, 2014.12.20., 연합뉴스, https://news.kbs.co.kr/news/pc/view/view.do?ncd=2987836
[6] 대우조선해양 3번째 해킹당했다...정부 합동조사, 2021.10.29., SBS 뉴스, https://news.sbs.co.kr/news/endPage.do?news_id=N1006516108
[7] KAI도 원자력연 당했던 VPN 취약점으로 해킹 당했다, 2021.7.1., 보안뉴스, https://m.boannews.com/html/detail.html?idx=98762
[8] NIST CYBERSECURITY FRAMEWORK, https://www.nist.gov/cyberframework

※ 출처: TTA 저널 제214호