2023년 1차

# 사이버보안 대연합 보고서

CONTENTS

## 탐지·공유 분과

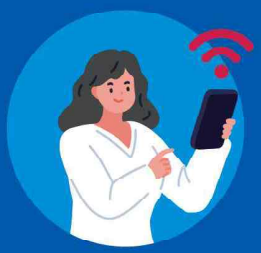


## 대응·역량 분과



## 정책·제도 분과






KISA 한국인터넷진흥원 kisia 한국정보보호산업협회

# 사이버보안 대연합 보고서

2023년 10월 20일 발행

발행인 이 원 태

발행처 KISA 한국인터넷진흥원
전라남도 나주시 진흥길 9 한국인터넷진흥원

2023년 1차

# 사이버보안 대연합 보고서

## 탐지·공유 분과

1. 2023년 6월 글로벌 해킹그룹 동향 분석 [장영준 수석, NSHC]
2. 한국 내 대북분야 종사자 겨냥 BitB 공격 동향 분석 [문종현 이사(센터장), 지니언스 시큐리티 센터(GSC)]

# 2023년 6월 글로벌 해킹그룹 동향 분석

장영준 수석, NSHC, cyj@nshc.net

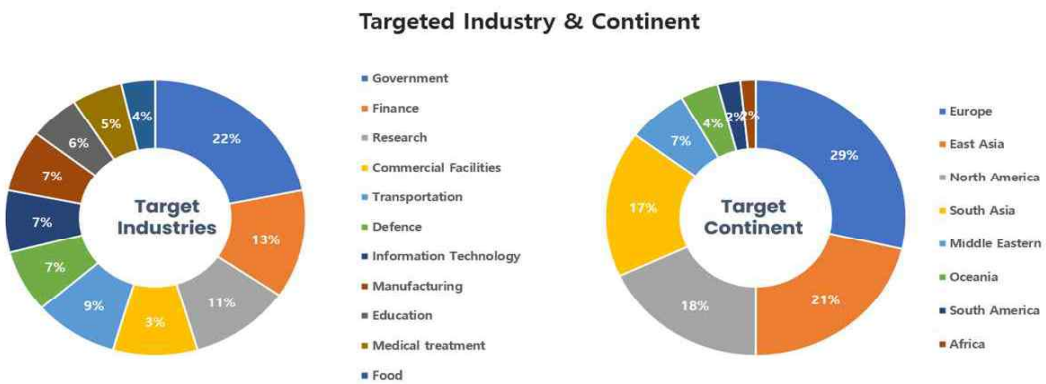
## 1. 개요

2023년 5월 21일에서 2023년 6월 20일까지 NSHC ThreatRecon팀에서 수집한 데이터와 정보를 바탕으로 분석한 해킹 그룹(Threat Actor Group)들의 활동을 요약 정리한 내용이다. 이번 6월에는 총 32개의 해킹 그룹들의 활동이 확인되었으며, SectorA 그룹이 41%로 가장 많았으며, SectorJ 그룹의 활동이 그 뒤를 이었다.

[그림 1] 2023년 6월에 확인된 해킹 그룹별 활동 통계


이번 6월에 발견된 해킹 그룹들의 해킹 활동은 정부기관과 금융 분야에 종사하는 관계자 또는 시스템들을 대상으로 가장 많은 공격을 수행했으며, 지역별로는 유럽(Europe)과 동아시아(East Asia)에 위치한 국가들을 대상으로 한 해킹 활동이 가장 많은 것으로 확인된다.

[그림 2] 2023년 6월 공격 대상이 된 산업 분야와 국가 통계



## 2. 해킹그룹별 활동 특징

### 1) SectorA 그룹 활동 특징

**SectorA 그룹**들 중 이번 6월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorA01, SectorA02, SectorA05, SectorA06, SectorA07 그룹이다.

**SectorA01 그룹**은 한국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 한국에서 사용하는 웹 보안 프로그램과 기업 자산 관리 프로그램의 원격 코드 실행(Remote Code Execution) 취약점을 사용하여, 공격 대상 시스템에서 악성코드를 다운로드 및 실행했다.

**SectorA02 그룹**은 한국, 호주, 캄보디아, 미국, 영국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 윈도우 바로가기(LNK) 파일 형식의 악성코드를 사용했으며, 북한인권 영화 상영회 협조 요청 문서로 위장하여 공격 대상이 악성코드를 실행하도록 유도했다.

**SectorA05 그룹**은 한국, 벨기에, 미국, 중국, 일본, 우크라이나, 영국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 북한 인권 단체와 관련된 주제로 위장한 피싱(Phishing) 메일에 윈도우 도움말 (CHM, Compiled HTML Help) 파일 형식의 악성코드가 존재하는 압축파일을 첨부하여 공격 대상에게 전달했으며, 최종적으로 시스템의 다양한 정보를 유출하는 악성코드를 사용했다.

**SectorA06 그룹**은 아랍에미리트, 호주, 이스라엘, 스위스, 인도네시아, 인도, 미국, 루마니아, 중국, 일본, 싱가포르, 미국, 이탈리아에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 맥OS(macOS) 사용자를 대상으로 PDF 뷰어(PDF Viewer)로 위장한 악성코드를 사용했으며, 공격 대상을 속이기 위해 마이크로소프트 애저(Microsoft Azure)의 보호된 문서로 위장한 미끼 문서를 사용했다.

**SectorA07 그룹**은 한국, 이스라엘에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 감정평가 협조 안내문으로 위장한 윈도우 바로가기(LNK) 형식의 악성코드를 ZIP 파일 형식으로 압축 후 배포했으며, 최종적으로 시스템 정보를 수집하는 비주얼 베이직 스크립트(Visual Basic Script)와 배치(Batch) 스크립트 파일을 사용했다.

현재까지 계속 지속되는 SectorA 해킹 그룹들은 한국과 관련된 정치, 외교 활동 등 정부 활동과 관련된 고급 정보를 수집하기 위한 목적을 가지며 전 세계를 대상으로 한 금전적인 재화의 확보를 위한 해킹 활동을 병행하고 있다. 이들의 해킹 목적은 장기간에 걸쳐 지속되고 있으며, 이러한 전략적 해킹 목적으로 당분간 변화 없이 지속적으로 진행될 것으로 판단된다.

### 2) SectorB 그룹 활동 특징

**SectorB 그룹**들 중 이번 6월에는 총 5개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorB22, SectorB38, SectorB50, SectorB73, SectorB75 그룹이다.

**SectorB22 그룹**은 라트비아, 타이완, 미얀마, 일본, 터키, 에스토니아, 그리스, 영국, 미국, 핀란드, 독일, 노르웨이에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 및 기관, 통신 산업 등의 다양한 조직을 대상으로 스피어 피싱(Spear Phishing) 이메일을 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 시스템에서 시스템 정보 수집, 명령 실행, 파일 삭제 등의 악성 행위를 수행하였다.

**SectorB38 그룹**은 미국, 이탈리아, 캐나다, 인도, 오스트레일리아, 싱가포르, 프랑스, 독일, 영국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 정부 및 기관, 외교부, 금융 등의 다양한 조직을 대상으로 스피어 피싱 이메일을 배포하여 공격 활동을 하였으며, 공격 대상 시스템에서 다운로더(Downloader) 기능의 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

**SectorB50 그룹**은 아랍에미리트, 미국, 독일에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 설문조사 문서로 위장한 압축 파일을 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 시스템에서 공격자의 명령에 따른 악의적인 행위를 수행하게 된다.

**SectorB73 그룹**은 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 중요 인프라 제공업체를 대상으로 공격 활동을 하였으며, 다양한 오픈 소스(Open Source) 도구 및 시스템 명령을 활용하여 정보 탈취 행위를 하였다.

**SectorB75 그룹**은 라트비아, 파키스탄, 중국, 독일, 홍콩, 미국에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 바라쿠다 이메일 시큐리티 게이트웨이 어플라이언스(Barracuda Email Security Gateway Appliance) 장비에서 발생한 취약점(CVE-2023-2868)을 악용하여 공격 활동을 하였으며, 공격 대상 시스템에서 정보 탈취 행위를 하였다.

현재까지 지속되는 SectorB 해킹 그룹들의 해킹 활동 목적은 전 세계를 대상으로 각국 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 것으로 분석된다.

### 3) SectorC 그룹 활동 특징

**SectorC 그룹**들 중 이번 6월 총 6개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorC01, SectorC04, SectorC05, SectorC08, SectorC13, SectorC14 그룹이다.

**SectorC01 그룹**의 활동은 우크라이나에서 발견되었다. 해당 그룹은 웹 메일 소프트웨어의 취약점을 악용하여 웹 메일 서버의 정보를 탈취했으며, 송수신 메일 주소를 변조하거나, 사용자 주소록을 훔쳐 2차 공격을 위한 발판을 마련했다.

**SectorC04 그룹**은 마이크로소프트 인증서로 서명된 정상적인 EXE 파일을 DLL 사이드 로딩(Side-Loading) 기법에 사용하여 악성코드를 실행시켰으며, 최종적으로 추가 악성코드를 다운로드 및 실행할 수 있는 다운로더(Downloader) 기능의 악성코드를 사용했다.

**SectorC05 그룹**의 활동은 우크라이나에서 발견되었다. 해당 그룹은 다단계 인증(MFA)이 없는 VPN 계정을 악용하였으며, 시스템 파괴 목적을 가진 배치(Batch) 스크립트 형식의 악성코드를 사용하여 시스템 내에 파일들을 삭제했다.

**SectorC08 그룹**의 활동은 미국, 러시아, 아랍에미리트, 우크라이나, 폴란드, 한국에서 발견되었다. 해당 그룹은 망 분리(Air Gap)가 된 시스템에 도달하기 위해 이동식 매체를 이용하여 측면 이동(Lateral Movement)을 시도했으며, 공격 대상 조직의 시스템에 윈도우 바로가기(LNK) 형식의 악성코드를 생성하여 공격 대상이 실행하도록 유도하는 방식을 사용했다.

**SectorC13 그룹**의 활동은 미국, 러시아에서 발견되었다. 해당 그룹은 포격에 대한 대피행동요령에 대한 내용으로 위장한 MS 워드(Word) 악성코드를 사용했으며, 공격 대상이 MS 워드(Word) 악성코드를 실행할 경우 템플릿 인젝션(Template Injection) 기법을 통해 악의적인 코드가 포함된 MS 워드(Word) 템플릿(Template)을 다운로드 및 실행한다.

**SectorC14 그룹**의 활동은 우크라이나에서 발견되었다. 해당 그룹은 포털 사이트(Portal Site)로 위장한 피싱 사이트(Phishing Site) 링크를 포함 한 PDF 파일을 첨부한 메일을 사용했으며, 포털 사이트(Portal Site) 보안 경고 내용으로 공격 대상이 PDF 파일을 실행하도록 유도했다.

현재까지 지속되는 SectorC 해킹 그룹들의 해킹 활동은 인접한 국가를 포함한 전 세계를 대상으로 각 국가들의 정부 기관의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

### 4) SectorD 그룹 활동 특징

**SectorD 그룹**들 중 이번 6월 총 2개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorD01, SectorD15 그룹이다.

**SectorD01 그룹**의 활동은 이스라엘, 오스트레일리아에서 발견되었다. 해당 그룹은 VPN 취약점에 노출된 서버를 대상으로 웹쉘(WebShell)을 사용하였으며, 최종적으로 머니버드 랜섬웨어(Moneybird Ransomware)를 배포했다.

**SectorD15 그룹**의 활동은 사우디아라비아, 이스라엘, 영국에서 발견되었다. 해당 그룹은 운송 및 물류 관련 웹 사이트를 대상으로 워터링 홀(Watering hole) 공격을 시도했으며, 웹 페이지에 삽입된 자바스크립트(JavaScript) 형식의 악성코드는 사이트 방문자의 운영체제 언어, IP 주소, 화면 해상도 정보 등을 수집했다.

SectorD 해킹 그룹들은 주로 정치적인 경쟁 관계에 있는 국가들을 대상으로 해킹 활동을 수행하였으며, 최근의 SectorD 해킹 그룹들의 해킹 활동 목적은 정부에 반대하는 인물 또는 국가들의 정치, 외교 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 분석된다.

### 5) SectorE 그룹 활동 특징

**SectorE 그룹**들 중 이번 6월에는 총 4개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorE01, SectorE02, SectorE04, SectorE05 그룹이다.

**SectorE01 그룹**은 영국, 네팔에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 VPN 소프트웨어로 위장한 악성코드를 배포하여 공격 활동을 하였으며, 최종적으로 다운로더(Downloader) 기능의 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

**SectorE02 그룹**은 미국, 파키스탄에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 채팅 앱, VPN 앱으로 위장한 안드로이드(Android) 악성코드를 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 단말기에서 연락처, 위치 정보 등의 민감한 정보를 탈취하였다.

**SectorE04 그룹**은 파키스탄, 덴마크에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 급여 인상 목록 문서 및 손상된 시스템(Compromised Systems) 목록으로 위장한 MS 엑셀(Excel) 문서를 배포하여 공격 활동을 하였으며, 최종적으로 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

**SectorE05 그룹**은 파키스탄에서 이들의 해킹 활동이 발견되었다. 해당 그룹은 개발 프로젝트 평가로 위장한 윈도우 도움말 파일을 배포하여 공격 활동을 하였으며, 최종적으로 악성코드를 설치하여 추후 공격을 위한 발판을 마련하였다.

현재까지 지속되는 SectorE 해킹 그룹들의 해킹 활동 목적은 인접한 파키스탄 정부와 관련된 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다. 그러나 최근에는 중국을 포함한 극동 아시아와 다른 지역으로 확대되고 있는 점으로 미루어, 정치, 외교 및 기술 관련 고급 정보들을 획득하기 위한 활동의 비중도 커지고 있는 것으로 분석된다.

### 6) SectorF 그룹 활동 특징

**SectorF 그룹**들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorF01 그룹이다.

**SectorF01 그룹**은 베트남, 체코에서 이들의 해킹 활동에 발견되었다. 해당 그룹은 금융 부문을 대상으로 악성코드를 배포하여 공격 활동을 하였으며, 최종적으로 공격 대상 시스템에서 시스템 정보 탈취, 파일 다운로드 및 업로드, 프로세스 인젝션(Process Injection) 등의 악성 행위를 수행하였다.

현재까지 SectorF 해킹 그룹은 이들을 지원하는 정부와 인접한 국가들의 정치, 외교 및 군사 활동과 같은 고급 정보를 수집하기 위한 목적과, 자국의 경제 발전을 위한 첨단 기술 관련 고급 정보 탈취를 위한 목적을 갖는 것으로 분석된다.

### 7) SectorH 그룹 활동 특징

**SectorH 그룹**들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorH03 그룹이다.

**SectorH03 그룹**은 파키스탄, 인도, 중국, 홍콩에서 이들의 활동이 발견되었다. 해당 그룹은 국방 제품 수출 문서 및 보안 조치 문서로 위장한 문서를 배포하여 공격 활동을 하였으며, 최종적으로 크림슨RAT(CrimsonRAT) 악성코드를 설치하여 정보 탈취 행위를 하였다.

SectorH 해킹 그룹의 해킹 활동은 사이버 범죄 목적의 해킹과 정부 지원 목적의 해킹 활동을 병행한다. 특히, 인접한 인도와 여러 가지 외교적 마찰이 계속되고 있어, 목적에 따라 인도 정부 기관의 군사 및 정치 관련 고급 정보들을 탈취하기 위한 활동들을 향후에도 지속적으로 수행할 것으로 분석된다.

### 8) SectorS 그룹 활동 특징

**SectorS 그룹**들 중 이번 6월에는 총 1개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorS01 그룹이다.

**SectorS01 그룹**은 캐나다, 콜롬비아, 브라질, 한국, 프랑스, 홍콩, 스페인에서 이들의 활동이 발견되었다. 해당 그룹은 엠바고(Embargo) 요청으로 위장한 어도비(Adobe) PDF 문서를 배포하여 공격 활동을 하였으며, 정보 탈취 행위를 하였다.

현재까지 지속되는 SectorS 해킹 그룹의 해킹 활동 목적은 인접한 남미 지역의 국가들에서 정치, 외교 및 군사 활동 등 정부 활동 관련 고급 정보를 수집하기 위한 목적으로 해킹 활동을 수행하는 것으로 분석된다.

### 9) Cyber Crime 그룹 활동 특징

온라인 가상 공간에서 활동하는 사이버 범죄 그룹은 이번 6월에는 총 7개 해킹 그룹의 활동이 발견되었으며, 이들은 SectorJ04, SectorJ09, SectorJ20, SectorJ27, SectorJ39, SectorJ110, SectorJ118 그룹이다.

이들은 다른 정부 지원 해킹 그룹들과 다르게 현실 세계에서 금전적인 이윤을 확보할 수 있는 재화적 가치가 있는 온라인 정보들을 탈취하거나, 직접적으로 특정 기업 및 조직들을 해킹 한 후 내부 네트워크에 랜섬웨어(Ransomware)를 유포하거나, 중요 산업 기밀을 탈취한 후 이를 빌미로 금전적 대가를 요구하는 협박 활동 등을 수행한다.

**SectorJ04 그룹**의 활동은 미국, 영국, 인도, 이탈리아, 캐나다, 아일랜드, 싱가포르에서 발견되었다. 해당 그룹은 MOVEit Transfer 취약점(CVE-2023-35708, CVE-2023-34362)에 노출된 시스템을 대상으로 클롭 랜섬웨어(Cl0p Ransomware)를 배포했다.

**SectorJ09 그룹**은 웹 사이트에 난독화 된 스키밍(Skimming) 스크립트를 삽입하여, 결제 페이지에서 사용자명, 주소, 메일, 전화번호와 신용카드 지불 정보 등을 수집하는 기존의 해킹 방식을 유지하고 있다.

**SectorJ20 그룹**의 활동은 영국에서 발견되었다. 해당 그룹은 여권 사진으로 위장한 윈도우 바로가기(LNK) 파일 형식의 악성코드를 사용했으며, 실행 시 난독화 된 배치(Batch) 스크립트 형식의 명령줄을 통해 추가 악성코드를 다운로드 및 실행한다.

**SectorJ27그룹**의 활동은 러시아, 중국, 오스트리아, 폴란드, 싱가포르, 몰도바, 독일, 아르헨티나, 불가리아, 터키, 미국, 남아프리카, 이탈리아, 벨라루스, 대만, 말레이시아, 알제리, 캐나다, 그루지야, 우크라이나, 스위스에서 발견되었다. 해당 그룹은 국제 운송 기업을 사칭한 피싱 메일에 MS 워드(Word) 악성코드를 첨부했으며, 최종적으로 원격 제어 기능을 가진 악성코드를 시스템에 설치하여 시스템 정보 수집 및 명령 및 제어를 시도했다.

**SectorJ39 그룹**의 활동은 러시아, 체코, 미국, 우크라이나, 오스트레일리아에서 발견되었다. 해당 그룹은 검색 결과 최상단에 광고를 게시하는 구글애즈(Google Ads)를 악용하여 피싱 사이트(Phishing Site) 접속을 유도했으며, 최종적으로 시스템 권한 탈취 및 명령 제어를 할 수 있는 악성코드를 사용했다.

**SectorJ110 그룹**의 활동은 우크라이나, 스페인에서 발견되었다. 해당 그룹은 내부에 청구서로 위장한 자바스크립트(JavaScript) 파일 형식의 악성코드가 존재하는 압축파일을 첨부하여 피싱 메일(Phishing Mail)을 배포했으며, 최종적으로 추가 악성코드를 다운로드 및 실행할 수 있는 기능을 가진 악성코드를 사용했다.

**SectorJ118 그룹**의 활동은 미국, 캐나다, 리투아니아에서 발견되었다. 해당 그룹은 불법 콘텐츠(Illegal Content)를 호스팅하는 웹 사이트를 악성코드 배포에 악용했으며, 최종적으로 사용한 크롬 브라우저 확장프로그램(Chrome Browser Extension) 악성코드는 브라우저 검색 정보 같은 민감한 정보를 수집하고, 임의의 광고를 브라우저에 삽입하는 기능을 가지고 있다.

# 한국 내 대북분야 종사자 겨냥 BitB 공격 동향 분석

문종현 이사(센터장), 지니언스 시큐리티 센터(GSC), chmun@genians.com

## 주요 요약(Executive Summary)


- 미국 내 국제비정부단체 링크 (LiNK)의 탈북민 활동 지원금 프로그램 사칭 공격
- 단체에서 운영하는 페이스북 내용을 그대로 모방해 정교한 피싱 사이트 개설
- 'Browser In The Browser(BitB)' 공격 기술을 적용해 대북활동 전문가 현혹
- 평소 쉽게 접할 수 있는 'Single Sign-On (SSO)' 서비스로 위장해 접근
- 거점 서버의 흐름을 추적한 결과, 북한 배후 해킹 그룹 APT37 인프라 연결 발견


## 1. 개요(Overview)

### 1) 국제 북한인권단체를 사칭한 위협 식별 (Threat Hunting)

지난 7월 24일 지니언스 시큐리티 센터(이하 GSC)는 북한 연계 해킹그룹의 소행으로 분류된 새로운 공격 징후를 포착했다. GSC는 이번 위협이 국내외 대북 전문가의 일상생활 감시와 개인 정보 탈취에 목적을 둔 사이버 첩보전 일환으로 보고 있다.

공격자는 국제 비정부단체인 '링크[LiNK : Liberty in North Korea]'에서 실제로 진행 중인 '체인지메이커 활동 지원금 프로그램' 모집 내용을 교묘히 사칭했다. 해당 단체는 북한 인권 개선과 탈북 지원 활동 등으로 알려져 있다.

해당 프로그램은 북한 출신 활동가를 대상으로 하고 있으며, 실제 지원 기한은 7월 26일로 공격이 확인된 24일 기준 약 2일의 여유가 있었다. 총 금액은 600만원으로 매달 50만원씩 12개월간 활동 지원금을 제공하게 된다. 나름 촉박한 신청 기한을 감안한다면 공격 대상자를 현혹하는데 충분한 요소로 볼 수 있다.

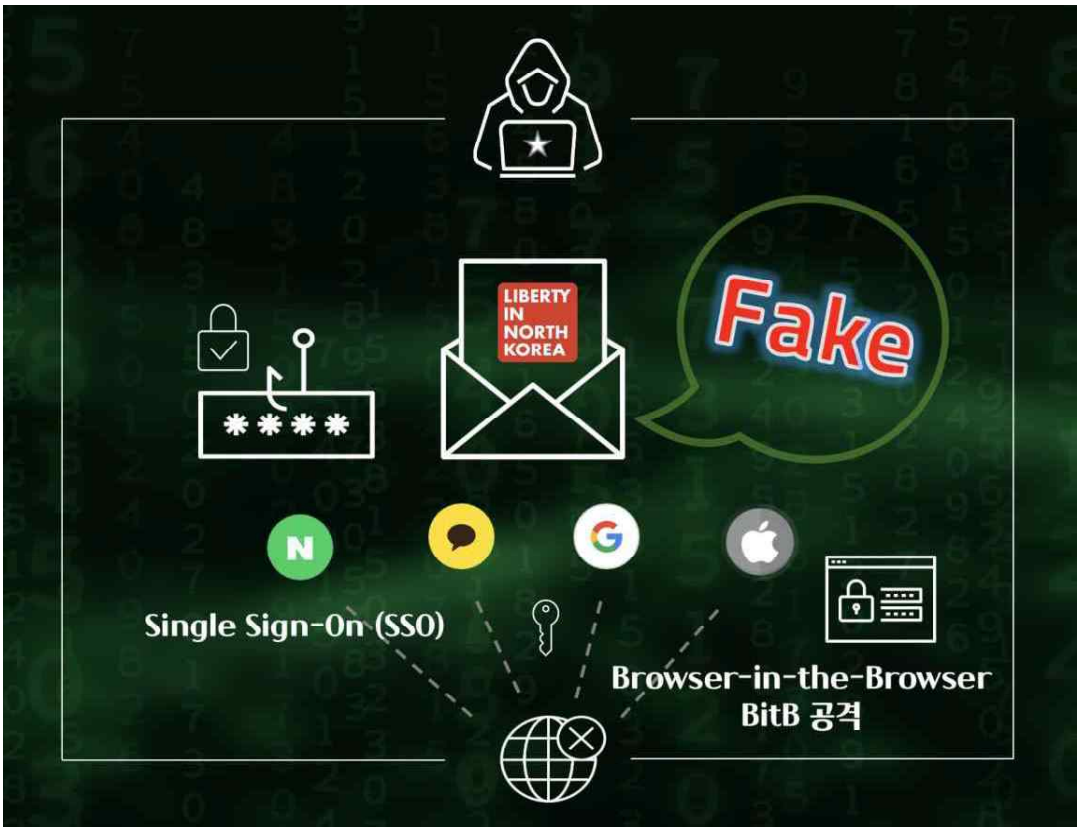
안내 포스터에 담긴 구체적 모집 대상을 살펴보면, ▶인권 옹호 및 인식 개선 활동 ▶북한 사람 중심의 콘텐츠 제작 및 배포 ▶탈북인 정착 지원 및 역량 강화 ▶기타 북한 사람들을 위한 활동 등 주로 북한 출신 활동 내용이 담겨 있다. 따라서 해당 위협은 탈북민이나 유관 단체가 주요 타깃에 해당될 수 있다.

### 2) 피싱 공격 흐름 (Phishing Attack Flow)

본격적인 공격은 이메일 내 상세 내용을 보려면 별도의 홈페이지 주소를 참고하라는 식으로 계정 해킹을 유인하는데, 실제 해당 프로그램에서 배포한 내용을 그대로 모방했다. 만약, 해당 내용에 속아 공격자가 직접 개설한 가짜 사이트로 연결되면, 피싱 공격이 진행된다.

마치 탈북민의 북한인권 활동 지원 프로그램처럼 조작된 피싱 이메일로 공격이 수행된다. 이메일 본문에 삽입된 가짜 홈페이지 주소에 접근할 경우 계정 탈취 목적의 피싱 사이트가 나타난다. 이때 입력된 이메일 주소와 비밀번호가 공격자에게 유출되는 과정을 거친다.

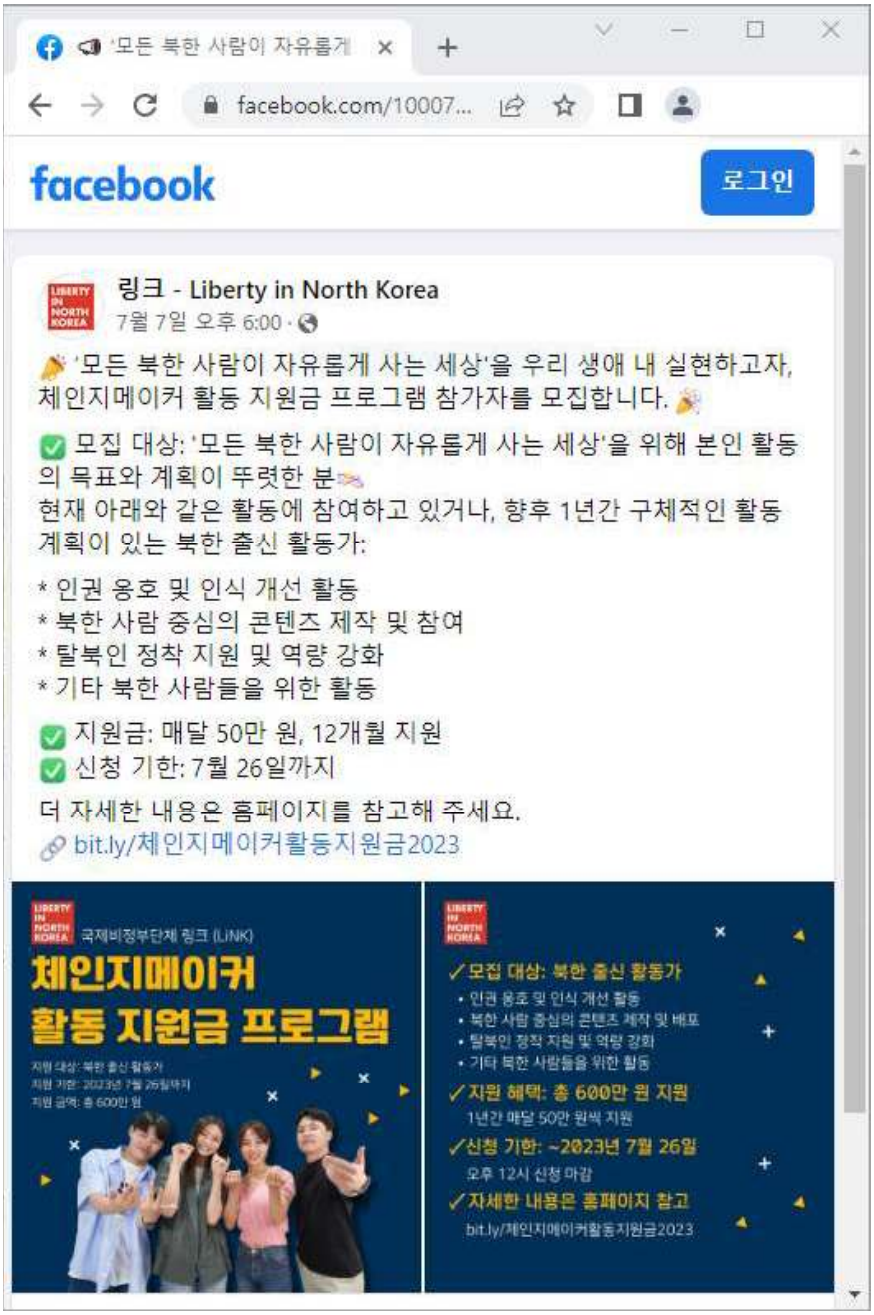
[그림 1] 피싱 공격 간략 흐름도



### 3) 공격 전술 및 기술, 절차 (TTPs) & BitB 공격

현존하는 미국의 북한인권 단체와 공식적으로 알려진 탈북민 활동지원 프로그램을 사칭해 시기적절한 맞춤형 전술 공격을 사용했다. 공격자는 해당 단체가 운영하는 페이스북 내용을 모방해 사용했으며, 북한 출신 활동가를 겨냥해 이메일 피싱 공격에 활용했다.

[그림 2] 링크(LiNK) 단체 공식 페이스북 안내문 화면




공격자는 다수의 탈북민 및 대북단체를 상대로 해당 공격을 수행했다. 특히, 일반적으로 많이 쓰이는 SSO(Single Sign-On) 단일 인증 방식을 공격에 접목했다.[1)]

공격 거점으로 사용할 피싱용 도메인과 웹 서버를 직접 구축했고, 'Browser In The Browser(BitB)' 공격 기술을 사용했다.[2)]

합법적인 웹 브라우저와 주소로 보이게 위장하는 것이 피싱 공격 성공의 가장 중요한 요소인 점을 감안한다면, 허위로 조작된 피싱 사이트가 공식 URL 주소처럼 보이게 만드는 것은 핵심적인 공격 절차 중 하나이다.

BitB 공격 기술은 웹 브라우저 내부에 인증 용도로 조작된 또 다른 팝업 창을 추가로 보여주는 피싱 수법이다. 이때 보인 웹 브라우저 화면과 URL 내용은 신뢰 가능한 공식 주소처럼 보이게 디자인이 가능하다. 따라서 겉으로 보이는 URL 주소만 믿고 비밀번호를 입력할 경우 해킹 피해를 입게 된다.

GSC는 본 피싱 공격이 BitB 공격 기술을 절묘하게 사용한 점에 주목했다. 이번 보고서 사례처럼 외관상 보여지는 URL 주소의 진위여부를 판단하는데 보다 세심한 주의와 관심이 필요한 이유이다. 육안상 인지된 주소만을 믿고 접근해 함부로 개인정보를 입력할 경우 예기치 못한 위협에 노출될 가능성이 높다.

BitB 공격을 감지하는 방법 중 하나는 팝업 로그인 창을 웹 브라우저 가장자리로 드래그(이동)하는 것이다. 팝업 창이 브라우저 화면 밖으로 벗어날 수 없다면 그것은 독립된 실제 창이 아니다.

더불어 본인이 사용하는 웹 브라우저의 유저 인터페이스(UI)와 일관된 디자인과 화면 모드를 유지하고 있느냐 비교하는 것이다. 웹 브라우저의 버튼이나 아이콘 등 구성 디자인 요소에 차이점이 없는지 면밀히 비교해 보는 것이다.

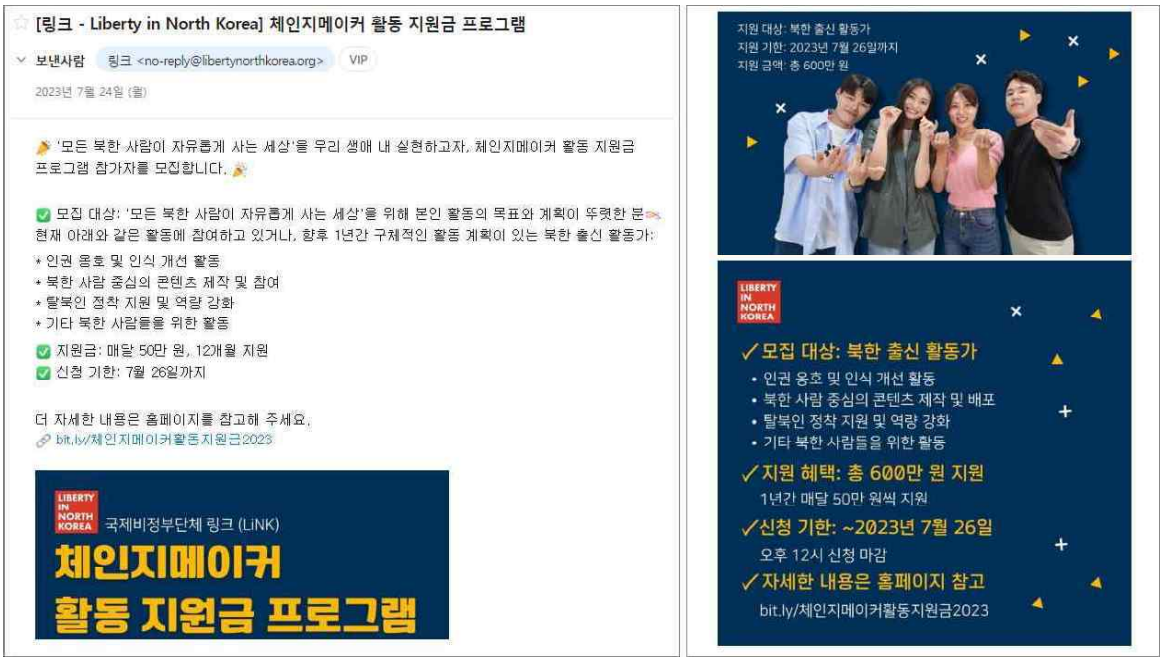
1) https://aws.amazon.com/ko/what-is/sso/
2) https://mrd0x.com/browser-in-the-browser-phishing-attack/

# 2. 공격 시나리오 (Attack Scenario)

## 1) 초기 접근 단계-피싱 (Initial Access-Phishing)

실제 공격에 사용된 이메일은 정교하게 제작된 것을 알 수 있다. 본문 내용 하단에 이미지로 포스터가 세로로 길게 포함된 형태이다. 이미지 바로 상단 영역에 피싱 공격용 링크가 'bit.ly' 단축 URL 주소처럼 삽입되어 있다.

[그림 3] 실제 공격에 사용된 이메일 화면




먼저 공격 발신지 주소와 피싱 거점이 동일하게 사용되었다. 이메일 보낸 이 주소는 마치 응답 없는 발송 전용 주소처럼 보이도록 'no-reply@libertynorthkorea[.]org' 주소가 사용됐는데, 공격에 따라 'info' 아이디가 사용되기도 한다.

피싱 사이트로 연결된 도메인 역시 'libertynorthkorea[.]org' 주소가 사용됐는데, 실제 정상 사이트 주소와 비교해 보면 조금 다른 것을 알 수 있다. 정상 사이트의 경우 도메인 중간에 [in] 단어가 포함된 'libertyinnorthkorea[.]org' 주소이다. 따라서 얼핏 보기에 가짜 사이트에 현혹된 가능성이 매우 높은 편에 속한다.

## 2) 피싱 메일 분석 (Phishing Email Analysis)

공격자는 'titan[.]email' 〈(구)flockmail[.]com〉 이메일 플랫폼 서비스를 악용해 피싱 공격을 수행한다. 이 서비스를 활용한 공격은 북한 연계 해킹 조직이 종종 사용하고 있다.[3)]

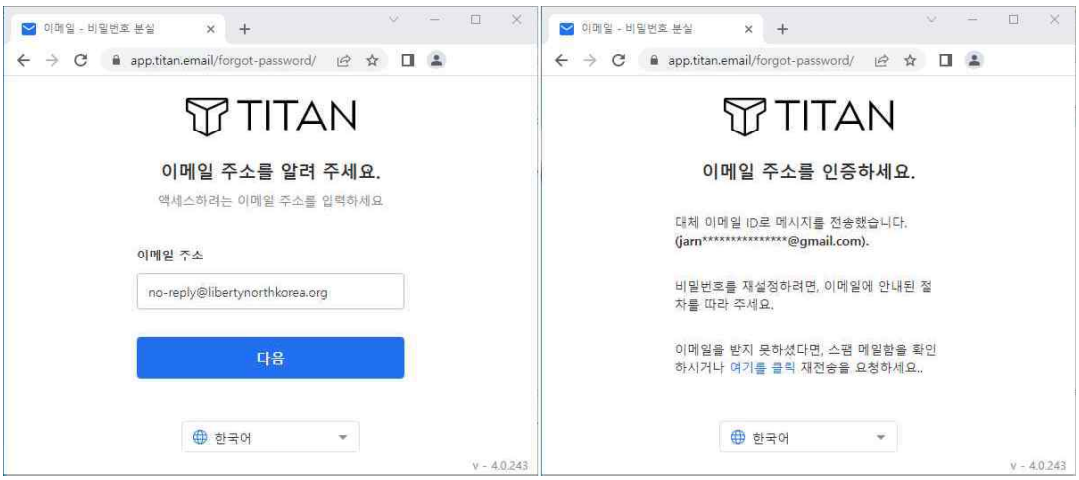
3) https://titan.email/about/

참고로 타이탄 이메일 서비스는 인도 출생 '바빈 투라키아(Bhavin Turakhia)'가 설립한 회사로, 위키디피아에 따르면, 인도에서 순자산이 많은 사람으로 선정된 바 있다. 이 인물은 인도의 온라인 교육 및 경쟁 프로그래밍 플랫폼인 코드쉐프(CodeChef) 설립에 참여한 것으로 알려져 있다.[4)]

흥미롭게도 코드쉐프는 국제 소프트웨어 프로그래밍 경진대회로 북한 김일성 종합대, 김책공대 학생들이 지난 2013년부터 경연에 참가해 수차례 우승을 차지한 것으로 알려져 있다.[5)]

현재 해킹 공격에 쓰이는 해외 이메일 플랫폼 서비스와 북한 학생들이 수년간 참여한 국제 프로그래밍 경연 대회의 연관성을 단순 우연으로 볼지는 앞으로 보다 심도 있게 관찰할 필요가 있다.[6)]

**[그림 4] 타이탄 이메일에 등록된 대체 메일 주소 화면**




앞서 공격에 사용된 발신지 'no-reply@libertynorthkorea.org' 메일 주소를 타이탄 서비스로 조회해 보면, 'jarn**********@gmail.com' 지메일을 대체 주소로 사용한 것을 알 수 있다. 자세히 보면, 영문 알파벳 R과 N을 소문자로 연이어 사용한 전형적 패턴을 볼 수 있는데, 보통 m 문자처럼 보이기 위한 수법이다.

이메일 내부 하단 위치에 수신 여부 등을 체크하기 위해 웹 비콘(Web Beacon) 이미지 기능이 숨겨져 있는데, 이때 사용된 도메인 주소는 'help.naver.com[.]de' 이다.

4) https://en.wikipedia.org/wiki/Bhavin_Turakhia
5) http://monthly.chosun.com/client/mdaily/daily_view.asp?idx=2122&Newsnumb=2017112122
6) https://www.hankyung.com/opinion/article/2023070719441

[그림 5] 이메일 내부에 숨겨져 있는 비콘 코드 화면

```
=3D"_blank" style=3D"color: rgb(0, 123, 217); cursor:
pointer; text-decorat=
ion: none; border: 0px; outline: none; list-style: none;
margin: 0px; text-=
align: inherit; padding: 0px; box-sizing: border-box;
touch-action: manipul=
ation; background-color: rgba(0, 0, 0, 0); display:
inline; font-family: in=
herit;">bit.
ly/=EC=B2=B4=EC=9D=B8=EC=A7=80=EB=A9=94=EC=9D=B4=EC=BB=A4=
=ED=99=9C=EB=8F=99=EC=A7=80=EC=9B=90=EA=B8=882023</a></spa
n></div><div styl=
e=3D"text-align: left;"><br></div></div></div>

</div>
<img src=3D"https://libertynorthkorea.
org/assets/media/           /35837970=
3_316934690663613_4979253201212185035_n.jpg"
width=3D"450px" height=3D"450p=
x">
<img src=3D"https://libertynorthkorea.
org/assets/media/           /35806292=
4_316934693996946_7643035514259184264_n.jpg"
width=3D"450px" height=3D"450p=
x">
</div><img src=3D'https://help.naver.com.de
/asset/media/   /background.jpg?=
```

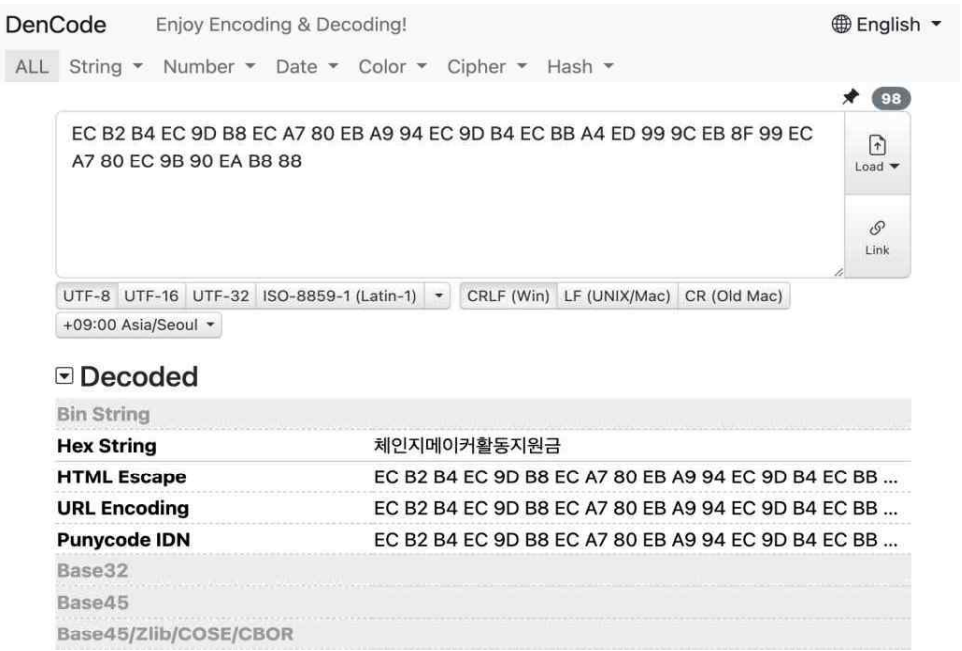
웹 비콘 상단에 위치한 피싱 링크(bit.ly/체인지메이커활동지원금2023) 주소는 한글 표기가 포함되어 있고, UTF-8 데이터가 포함되어 있다. 해당 코드는 DenCode 사이트에서 한글로 쉽게 변환이 가능하다.[7)]

[표 1] 피싱 링크로 사용된 데이터 화면

| |
|---|
| EC B2 B4 EC 9D B8 EC A7 80 EB A9 94 EC 9D B4 EC BB A4 ED 99 9C EB 8F 99 EC A7 80 EC 9B 90 EA B8 88 |

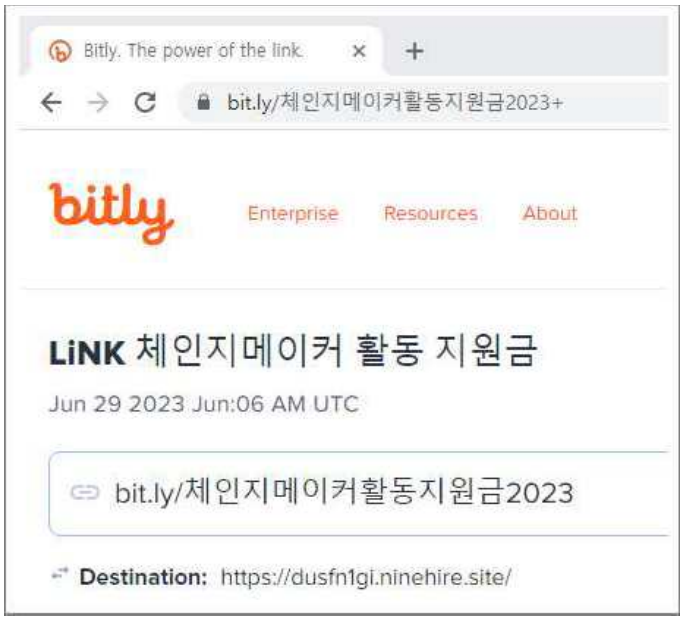
7) https://dencode.com/

[그림 6] DenCode 서비스로 변환된 한글 문자열 화면



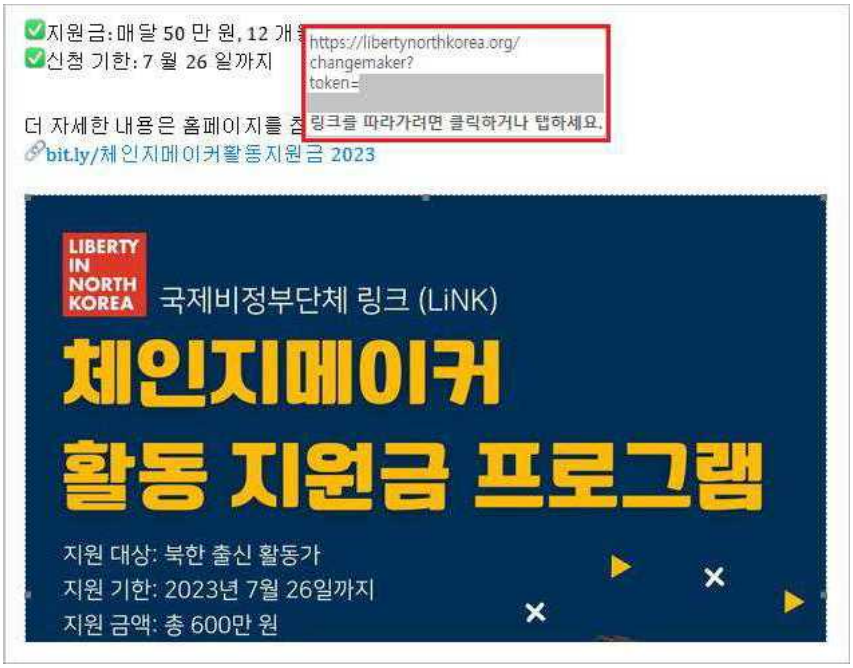

외관상 보여지는 Bitly 단축 URL 서비스의 최종 연결 주소는 6월 29일에 등록됐으며, (dusfn1gi.ninehire[.]site) 정상 LiNK 체인지메이커 활동 지원금 서비스로 연결된 것을 확인할 수 있다.

[그림 7] 실제 정상 단축 URL 주소 화면



하지만 단축 URL 내부 링크는 피싱 서버 'libertynorthkorea[.]org' 주소로 연결돼 있으며, 토큰 인자 값이 없을 경우에는 공식 사이트로 전환시켜 분석을 회피한다.

[그림 8] 해킹 이메일에 쓰인 단축 URL 주소 화면

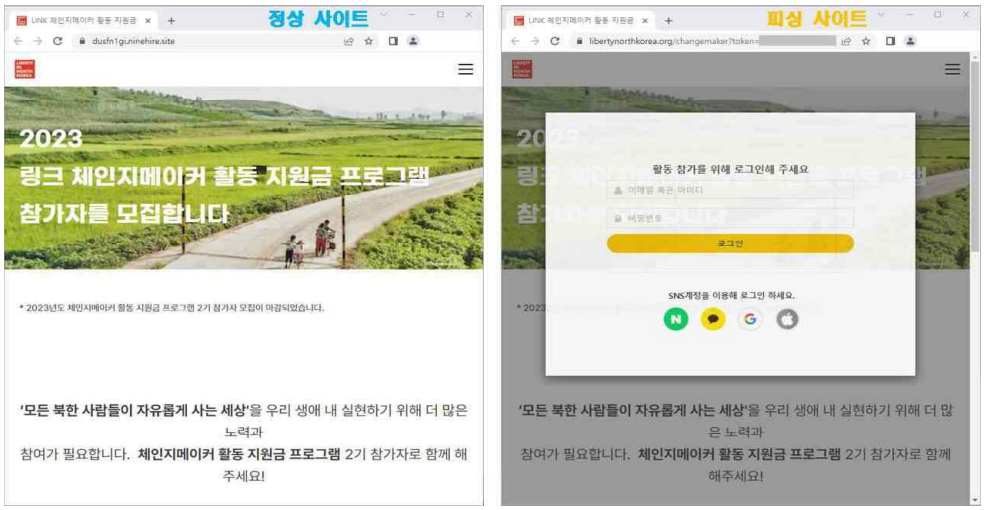


# 3. 피싱 위협 분석 (Phishing Threat Analysis)

## 1) 정교한 유사 웹 사이트 구축

피해 대상자가 'libertynorthkorea[.]org' 주소를 클릭해 접근하면, 정교하게 디자인된 가짜 웹 사이트가 나타난다. 정상 사이트와 피싱용으로 제작된 가짜 사이트를 비교해 보면 로그인 창 팝업 여부가 다른 점을 볼 수 있다.

[그림 9] 정상 사이트(좌)와 피싱 사이트(우) 비교 화면




피싱 사이트는 원래 정상 웹 사이트(dusfn1gi.ninehire[.]site)의 내용을 그대로 보여주도록 아이프레임을 구성했다. 여기서 눈에 띄는 점은 아이프레임 아이디 값이 조선뉴스(chosunnews)라는 점이며, 웹 페이지 종속 스타일 시트(Cascading Style Sheet) 파일도 'chosun.css' 파일명을 사용했다. GSC는 해당 피싱 사이트를 조사하는 과정 중에 공격자가 조선일보(chosun[.]com) 웹 사이트의 폰트 설정 및 'style.css' 값을 일부 활용한 점을 확인했다.

[표 2] 피싱 사이트의 아이프레임 코드 화면

```
〈iframe id="chosunnews" src="https://dusfn1gi.ninehire.site/"
style="width:100%;height:100%;border-width:0px;"
scrolling="no"〉〈/iframe〉
```

### 2) BitB 피싱 공격 기술

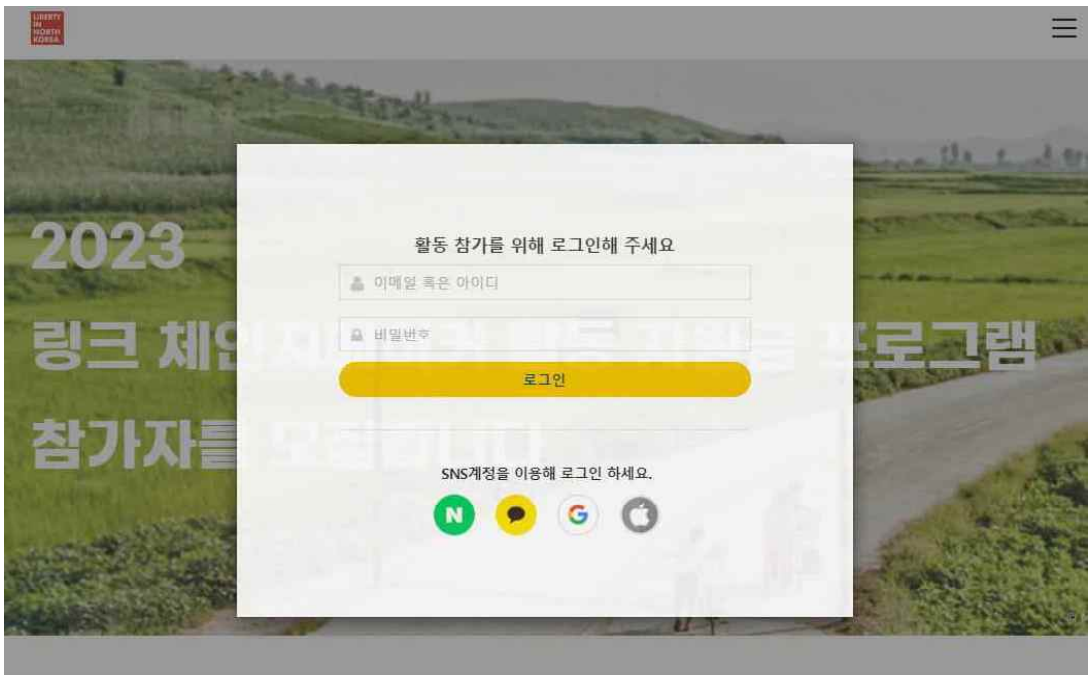
피싱 공격용 웹 사이트는 공식 Liberty in North Korea (libertyinnorthkorea[.]org) 도메인 주소와 유사하게 만든 점이 특징이다.

[표 3] 공식 사이트와 피싱 사이트 도메인 비교

| | | |
|---|---|---|
| 정상 도메인 | libertyinnorthkorea[.]org | dusfn1gi.ninehire[.]site |
| 피싱 도메인 | libertynorthkorea[.]org | - |

조작된 사이트로 연결되면 '활동 참가를 위해 로그인해 주세요' 타이틀을 가진 팝업 창이 나타난다. 자체 이메일 로그인 유도 화면과 'SNS계정을 이용해 로그인 하세요'라는 내용의 SSO(Single Sign-On) 단일 인증 방식 아이콘을 보여준다.

[그림 10] 피싱 사이트 접근 시 보여지는 팝업 창 화면



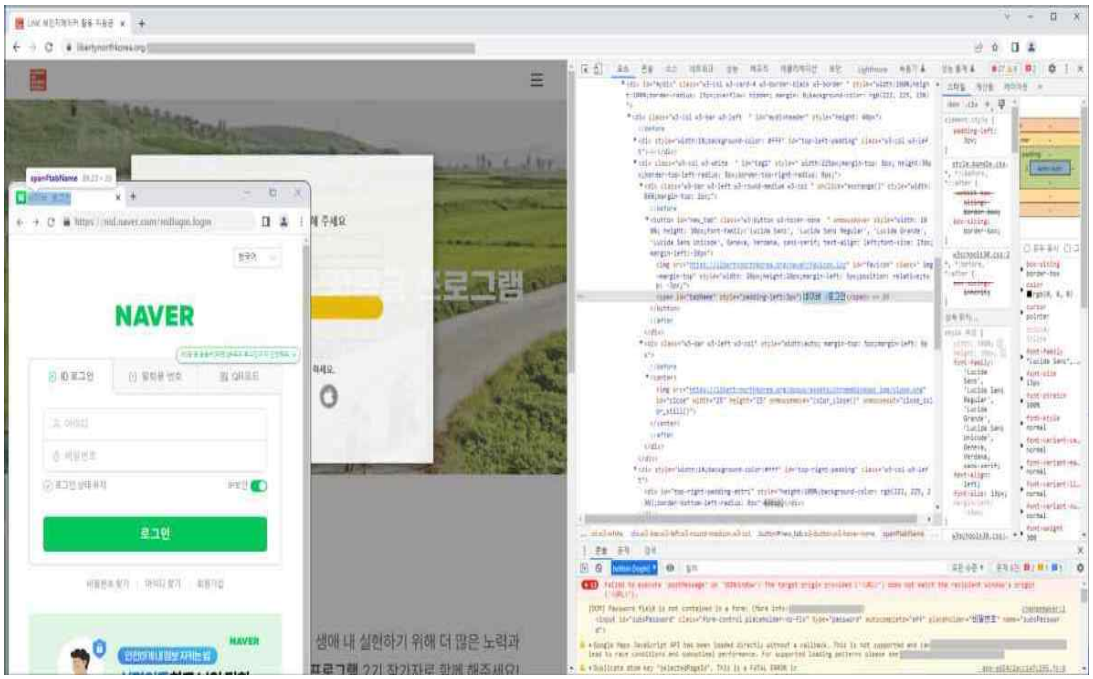

이메일 혹은 아이디와 비밀번호 수동 입력을 통한 직접적 로그인 계정 탈취 방식을 사용할 뿐만 아니라, ▶네이버 ▶카카오 ▶구글 ▶애플 등의 계정이 선택적으로 유출될 수 있는 방식이다.

SSO 통합적 단일 인증 방식은 번거로운 별도의 가입절차가 없어 편의상 많이 쓰이고 있다. 평소 접해 보지 못한 생소한 웹 사이트에 신규로 가입하거나 로그인하는 것은 보안상 매우 조심스러운 부분이다. 일반적으로 악성 의심 사이트를 구별하는데 있어, 절차상 가장 우선시되는 점은 웹 브라우저상 접속 주소일 것이다. 주소창에 보이는 인터넷 URL 경로가 내가 기존에 잘 알고 있던 도메인이라면 충분히 신뢰하고 로그인을 진행할 것이다.

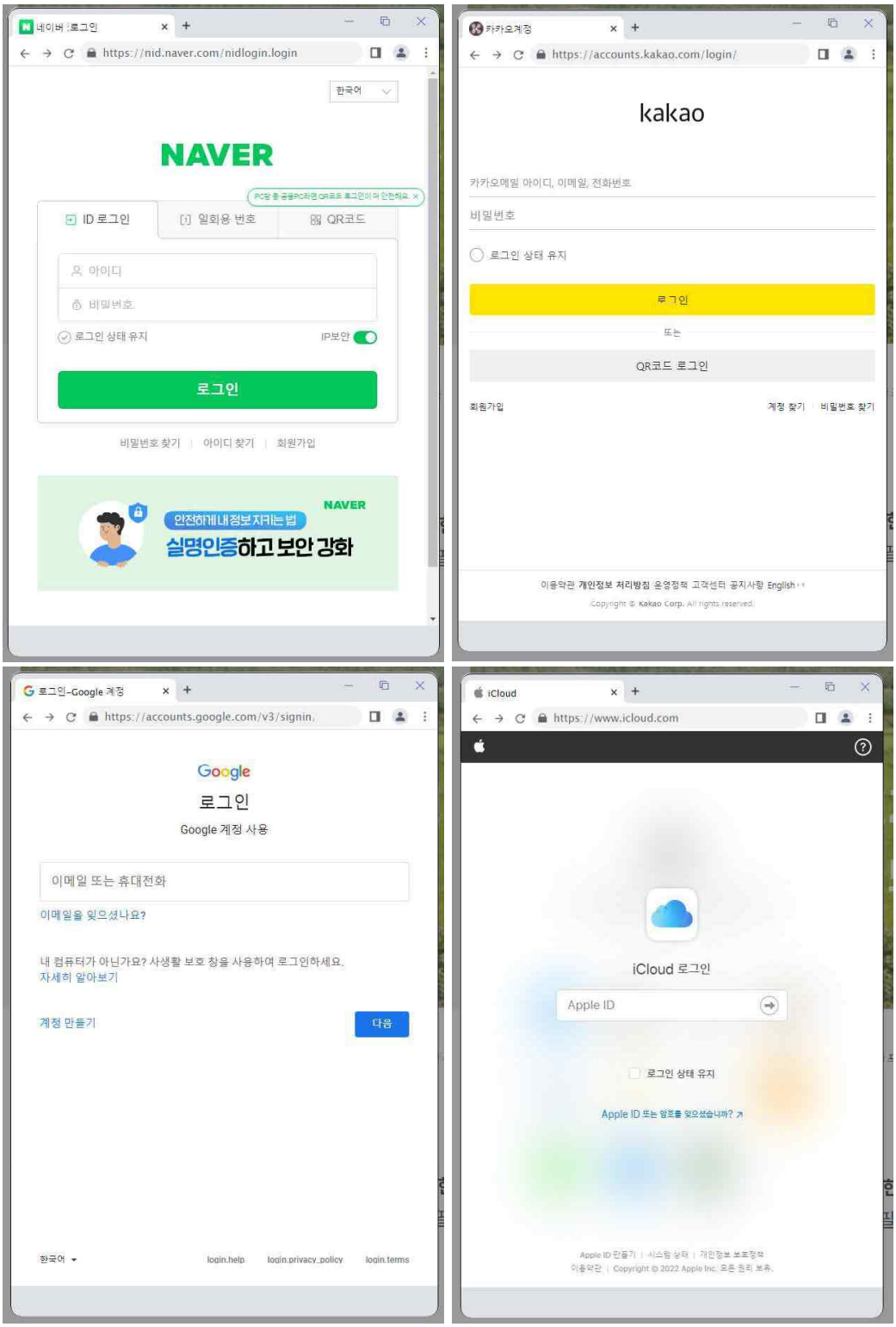
더구나 앞서 설명한 'Browser In The Browser(BitB)' 공격 기술을 사전에 숙지하지 못했다면, 이러한 공격에 쉽게 노출될 수 있다. 쉽게 말해, 웹 브라우저 내부에 또 다른 가짜 웹 브라우저 화면을 디자인해 띄우는 절묘한 속임수 기법이다. 공식 URL 주소가 포함된 팝업 창을 띄우는 것이기 때문에 주소창에 입력된 도메인 자체를 공격자가 얼마든지 임의로 설정할 수 있다.

공격자는 팝업 창의 스타일과 클래스, 아이콘, 이미지 연결 등을 디자인해 마치 포털 사의 공식 로그인 서비스처럼 화면을 만들었다. 더불어 국내외 기업의 계정 정보 탈취가 가능하도록 다양한 로그인 팝업 창을 제작해 두었다.

**[그림 11] 가짜 로그인 팝업 창과 내부 코드 화면**



[표 4] BitB 기법의 피싱용 팝업 창 화면 비교




상기 서비스별 가짜 팝업 창을 살펴보면, 나름 실제 서비스처럼 보이도록 정교하게 모방했다. BitB 공격의 가장 치명적 위협 요소는 바로 정상 URL 주소가 보인다는 점이다.

각 팝업 로그인 창에 삽입된 URL 주소를 하나씩 추출해 비교해 보면, 실제 공식 회사의 도메인 사이트가 포함된 것을 알 수 있다. 단순히 영어 알파벳을 유사하게 만든 전형적인 웹 피싱 기법과 다르게 정상 인터넷 주소가 보이도록 조작한 것이 핵심이다.

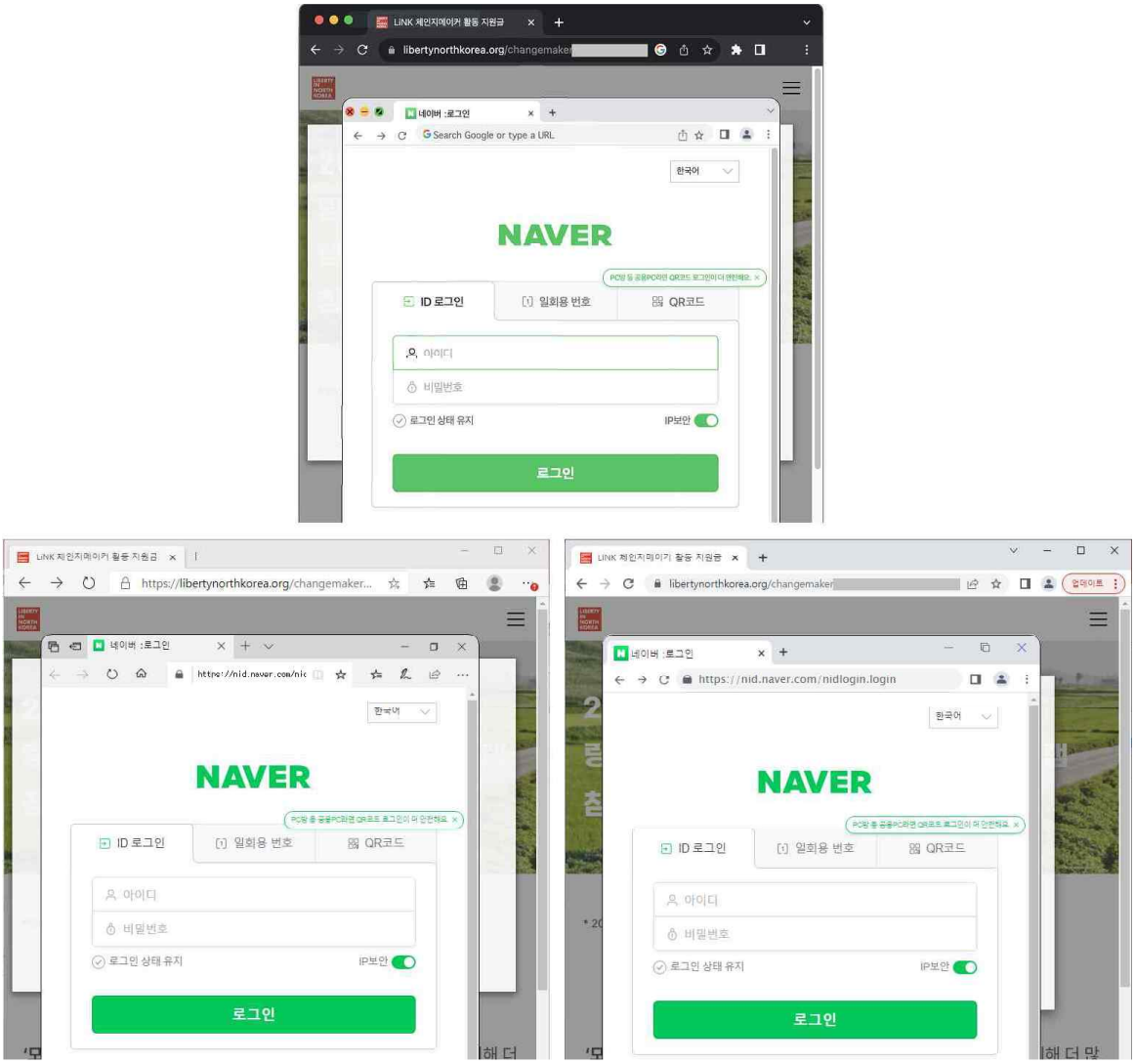
[그림 12] BitB 피싱 로그인 창 화면의 디자인된 URL 주소 화면


물론, 여기에도 허점은 존재한다. 구글 피싱 사이트의 경우 주소 가장 끝단의 슬래시(/) 부분 영역 일부가 잘려 보이는 현상이 목격된다. 그리고 BitB 주소 창 영역의 페이지 공유 및 탭 북마크 추가 아이콘이 보이지 않을 수 있다.

아울러 화면을 다크 모드로 설정해 사용하는 등 이용자 환경의 개별 조건에 따라 사전에 의심해 볼 만한 여지가 충분히 존재하거나 발견해 낼 수도 있다. 이외에 창 테두리나 모서리 화면이 사용 중인 웹 브라우저와 상이하거나 어눌하게 표시된 점도 확인할 수 있다.

이처럼 얼핏 보기에 실제 사이트로 혼동할 수 있다는 점에서 각별한 주의가 필요한 부분이다. 그리고 공격자는 macOS Chrome, MS Edge, Google Chrome 등 웹 브라우저 종류에 따라 나름 맞춤형 디자인을 적용했다.

[그림 13] OS 및 웹 브라우저별 비교 화면




BitB 공격 여부를 가장 쉽고 정확하게 확인하는 방법은 팝업 창이 현재 사용 중인 웹 브라우저 영역 밖으로 이동이 가능한지를 보는 것이다. BitB 피싱의 경우 팝업 창 자체가 단순히 별도의 웹 브라우저처럼 디자인으로 위장된 것이지 완전히 독립된 상태가 아니다. 따라서 기존 웹 브라우저 내에서만 이동이 가능한 고유한 특성을 활용한 방안이 있다.

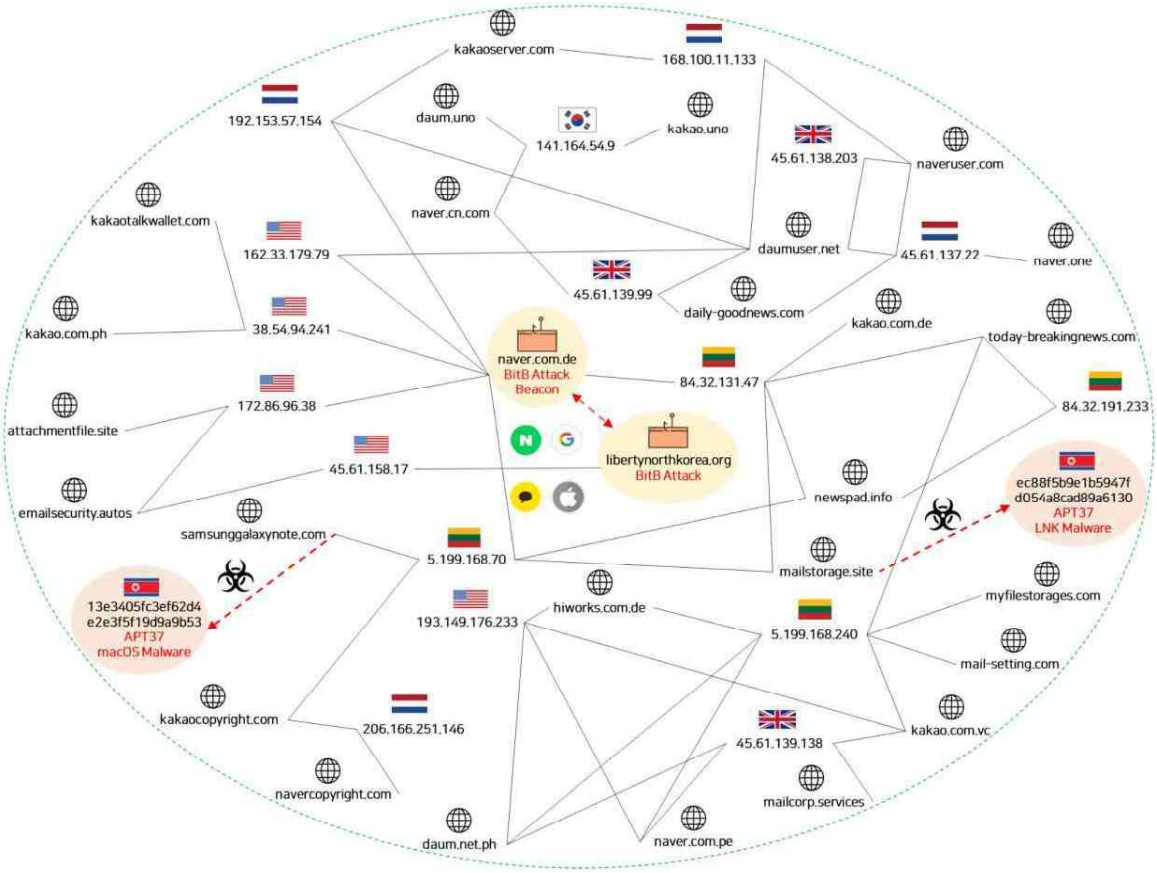
# 4. 위협 인프라 유사도 (Similarity)

## 1) BitB 피싱과 APT37 공격 거점의 연결 고리

GSC는 BitB 공격에 활용된 위협 지표를 조사하는 과정에서 APT37 공격 인프라와 연결된 고리를 찾았다.

이번 BitB 피싱 공격에 활용된 'libertynorthkorea[.]org' 도메인은 분석 시점 당시 미국 아이피 '45.61.158[.]17' 주소로 연결되었으며, 'ru.emailsecurity[.]autos' 도메인도 동일한 아이피가 사용되었다. 서브 도메인 중 'protect.emailsecurity[.]autos' 주소가 존재하며, '172.86.96[.]38' 주소로 연결된다.

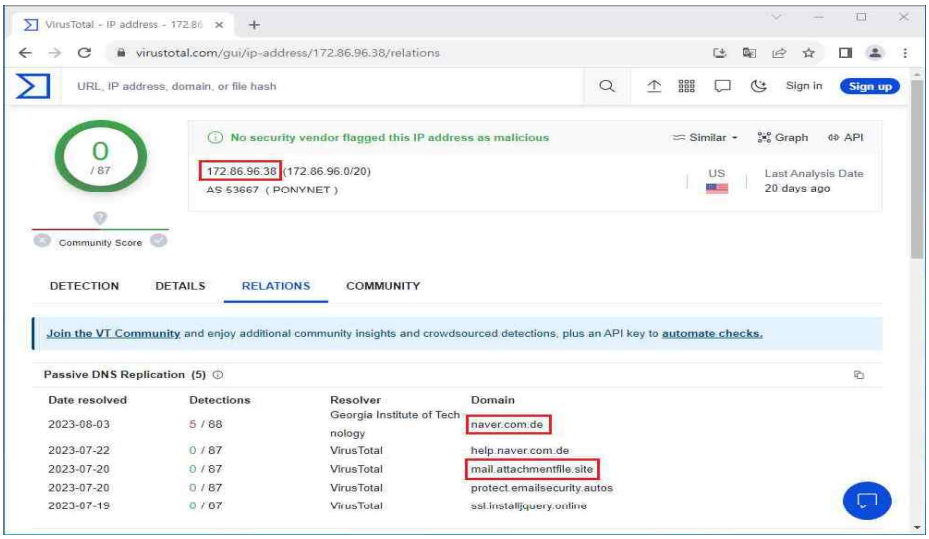
[그림 14] BitB 공격 도메인과 APT37 공격 연관성 화면




'172.86.96[.]38' 아이피에 연결됐던 Passive DNS 이력을 조회해 보면, 마치 국내 포털사처럼 위장된 'naver.com[.]de' 도메인이 사용된 기록을 확인할 수 있다. 참고로 여기서 언급된 Passive DNS란, 특정 (악성) 도메인이 DNS 쿼리를 통해 IP Lookup된 휘발성 히스토리를 누적해 기록해 둔 것으로, 특정 기간 동안 이뤄지는 네트워크 위협 활동을 조사하는데 의미 있는 위협 인텔리전스 정보로 활용된다.

이렇게 확인된 'naver.com[.]de' 도메인의 경우, 앞서 설명된 해킹메일 본문 내 숨겨진 비콘 도메인과 동일한 것을 볼 수 있다. 단순 우연으로 위협 인프라가 오버랩 된 것이 아니라, 계획적으로 활용됐을 가능성이 높은 이유이다.

[그림 15] 바이러스 토탈 '172.86.96.38' 관계 결과 화면




'naver.com[.]de' 도메인은 '84.32.131[.]47' 리투아니아 소재의 아이피로 할당된 바 있는데, 해당 인프라는 다수의 위협 지표로 사용되었다. 특히, 국내 언론사 웹 사이트처럼 위장한 'newspad[.]info' 도메인의 서브 주소가 대표이다.

'5.199.168[.]70' 아이피 주소의 경우 ▶samsunggalaxynote[.]com 스마트폰 사칭 주소를 포함해 ▶attachment.mailstorage[.]site ▶today-breakingnews[.]com 도메인과도 연결된 바 있고, 기존 APT37 그룹이 사용한 곳이다.

[표 5] 언론사 도메인으로 위장한 침해지표 비교 화면

| 언론사명 | (Sub) Domain 주소 | | IP 주소 (국가코드) |
|---|---|---|---|
| 뉴데일리 | 공식 | newdaily.co[.]kr | [생략] |
| | 피싱 | newdaily.newspad[.]info | 84.32.131[.]47 (LT)<br>5.199.168[.]70 (LT) |
| 조선일보 | 공식 | chosun[.]com | [생략] |
| | 피싱 | chosun.newspad[.]info | 84.32.131[.]47 (LT)<br>5.199.168[.]70 (LT) |
| 국민일보 | 공식 | kmib.co[.]kr | [생략] |
| | 피싱 | kmib.newspad[.]info | 84.32.131[.]47 (LT)<br>5.199.168[.]70 (LT) |

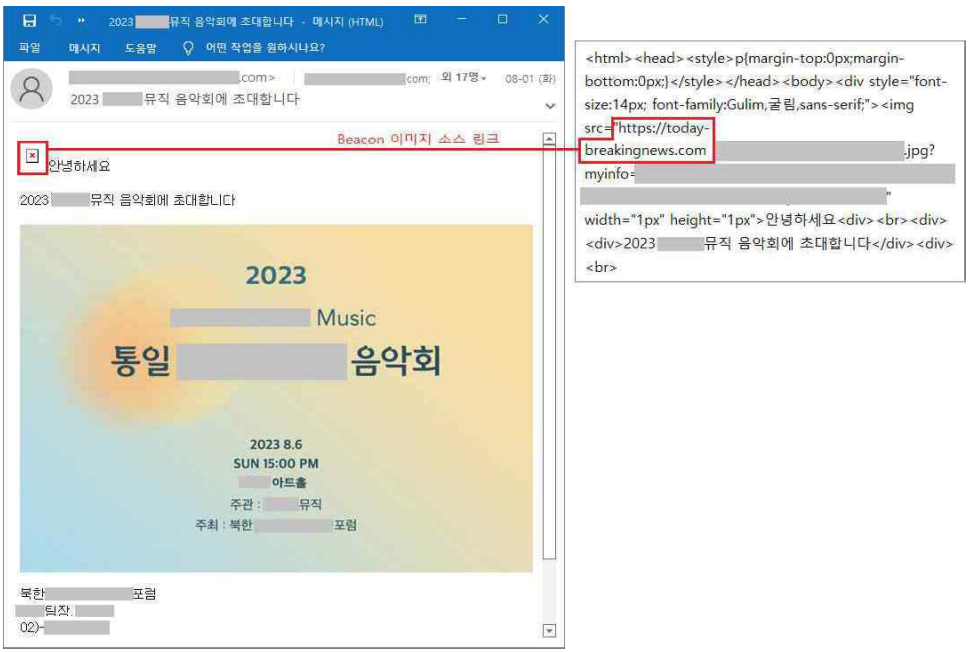
| 언론사명 | (Sub) Domain 주소 | | IP 주소 (국가코드) |
|---|---|---|---|
| 연합뉴스 | 공식 | yonhapnews.co[.]kr | [생략] |
| | 피싱 | yonhap.newspad[.]info | 84.32.131[.]47 (LT)<br>5.199.168[.]70 (LT) |
| 세계일보 | 공식 | segye[.]com | [생략] |
| | 피싱 | segye.newspad[.]info | 84.32.131[.]47 (LT)<br>5.199.168[.]70 (LT) |
| 전자신문 | 공식 | etnews[.]com | [생략] |
| | 피싱 | etnews.newspad[.]info | 84.32.131[.]47 (LT)<br>- |
| 중앙일보 | 공식 | joongang.co[.]kr | [생략] |
| | 피싱 | joongang.newspad[.]info | 84.32.191[.]233 (LT)<br>- |
| 동아일보 | 공식 | donga[.]com | [생략] |
| | 피싱 | donga.newspad[.]info | 84.32.191[.]233 (LT)<br>- |

### 2) 통일 음악회 사칭 APT37 공격 유사 사례

2023년 8월 1일, 대북분야 종사자 및 탈북민 약 18명 상대로 통일 관련 음악회 초대로 사칭한 피싱 공격이 수행된다. 해당 이메일에는 악성 링크나 첨부 파일이 존재하지 않는다.

그러나 이메일 내부에 비콘용 호스트(today-breakingnews[.]com) 주소가 숨겨져 있어 수신자들이 해당 메일을 열람하는지 원격지에서 정찰하게 된다.

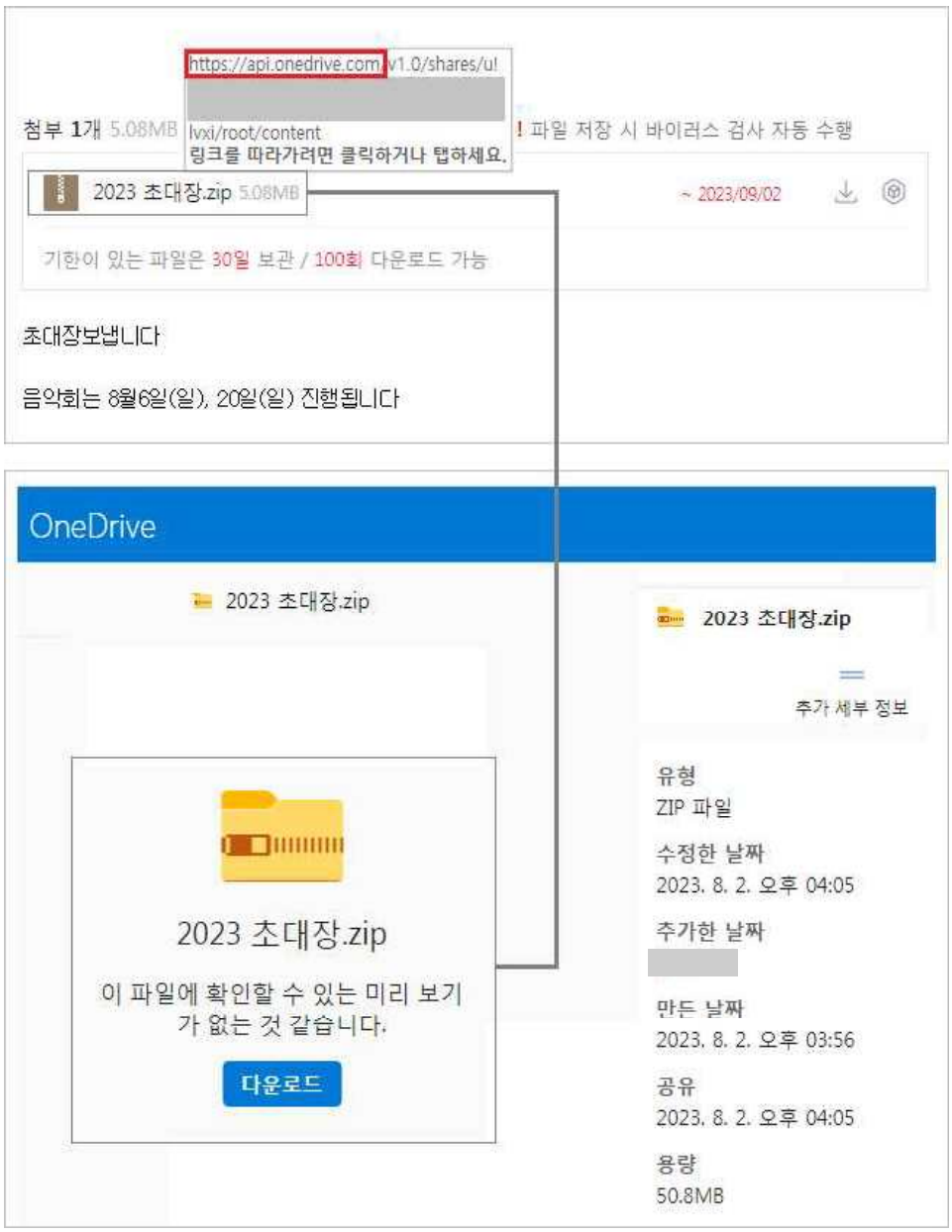
[그림 16] 통일 관련 음악회로 사칭해 현혹 중인 메일의 비콘 코드 화면



해당 이메일 수신자 중 음악회 초대에 현혹돼 추가 문의나 회신 등 반응을 보인 인물에게는 두번째 메일을 보내며, 악성 파일 링크를 삽입하게 된다.

마치 정식 초대장을 보내주는 것처럼 가장한 두번째 메일에는 '2023 초대장.zip' 첨부 파일이 원드라이브(OneDrive) 클라우드로 연결된 상태로 전송된다.

[그림 17] 음악회 초대장으로 위장한 해킹 이메일 화면




다운로드 된 압축 파일 내부에는 '2023 초대장.pdf.lnk' 이름의 바로가기 유형의 악성 파일이 포함되어 있다. LNK 악성 코드가 작동되면 내부에 포함된 Powershell 명령 등이 작동한다.

그 다음 공격자가 지정한 또 다른 원드라이브 클라우드 경로에서 마치 PDF 문서처럼 위장한 'homoa.pdf' 파일이 호출되는데, 이것은 암호화된 ROKRAT 변종 악성 파일로 메모리상에 파일리스 기반으로 작동하여 컴퓨터 정보를 피클라우드(pCloud)로 유출하게 된다.

본 사례에서 식별된 'today-breakingnews[.]com' 도메인은 BitB 피싱 공격의 비콘으로 쓰인 'naver.com[.]de' 도메인과 연결되는 '84.32.131[.]47' 아이피 주소 등과 정확히 연결된다.

선별한 몇 가지 케이스만 비교해 봐도, 전형적인 APT37 공격과 BitB 피싱이 직간접적으로 연결되고 있다는 것을 관찰할 수 있다.

# 5. 결론 및 대응방법 (Conclusion)

## 1) 실제 공식 행사 프로그램 사칭한 BitB 공격 등장

본 보고서는 실제 국내 특정인을 겨냥한 BitB 공격으로 평소 보안에 많은 관심과 경각심이 높은 이용자라도 정교한 피싱 공격에 현혹돼 노출될 가능성이 높은 유형으로 보다 각별한 주의가 필요하다.

거듭 강조하지만, BitB 공격 기술은 외관상 정상 URL 주소로 접속된 웹 브라우저 상태로 오인할 수 있기에 이곳에 기술된 내용뿐만 아니라, 앞으로 발생 가능한 유사 사례에 대한 적극적인 대비가 요구된다.

APT 공격이 날이 갈수록 지능화·고도화·다양화되고 있다. 국가배후 위협 행위자들은 거점 인프라 구축에 많은 자원과 비용을 투자하고 있어, 악성여부 판단 및 분석이 점차 어려워지는 추세이다.

## 2) BitB 피싱 공격 대응 방안

앞서 기술한 바와 같이, BitB 공격은 현재 이용 중인 웹 브라우저 화면상에 새로운 웹 브라우저 팝업화면처럼 정교하게 디자인한 새 창 화면을 띄우고, 이용자 로그인 정보를 입력하게 유도하는 절묘한 피싱 수법이다.

이때 보여지는 팝업창의 URL 주소는 공격자가 구성한 디자인으로 실제 공식 URL 주소를 임의로 삽입할 수 있기 때문에 육안상 정상 웹 사이트 주소와 동일하게 보여진다.

따라서 URL 주소만으로 진위여부를 판단하기 어렵다. 하지만, BitB 공격의 특성 상 새로 팝업 된 화면은 현재 이용 중인 웹 브라우저의 영역 밖으로 이동이 불가능하다. 그러므로, 로그인 정보 입력 창이 나타날 경우 우선 URL 주소의 정상 여부를 파악 후 웹 브라우저가 독립적으로 자유롭게 웹 브라우저 영역 밖으로 이동이 가능한지 따져보는 것만으로 BitB 피싱 피해를 최소화할 수 있다.

# 6. 침해 지표 (Indicator of Compromise)

## 1) 주요 MD5 Hash

- ec88f5b9e1b5947fd054a8cad89a6130
- 13e3405fc3ef62d4e2e3f5f19d9a9b53
- 51a82ce016de1c5d9c6e815b7d6d91b3

## 2) 연관된 명령제어(C2) 호스트 서버

- libertynorthkorea[.]org
- naver.com[.]de
- kakao.com[.]de
- hiworks.com[.]de
- samsunggalaxynote[.]com
- today-breakingnews[.]com
- daily-goodnews[.]com
- newspad[.]info
- attachmentfile[.]site
- mailstorage[.]site
- myfilestorages[.]com
- naveruser[.]com
- daumuser[.]net
- naver[.]one
- daum[.]uno
- kakao[.]uno
- kakaoserver[.]com
- kakaotalkwallet[.]com
- kakaocopyright[.]com
- navercopyright[.]com
- emailsecurity[.]autos
- daum.net[.]ph
- kakao.com[.]ph
- naver.com[.]pe
- mailcorp[.]services

- kakao.com[.]vc
- mail-setting[.]com
- naver.cn[.]com
- 141.164.54[.]9
- 38.54.94[.]241
- 84.32.131[.]47
- 84.32.191[.]233
- 5.199.168[.]70
- 5.199.168[.]240
- 45.61.137[.]22
- 45.61.138[.]203
- 45.61.139[.]99
- 45.61.139[.]138
- 45.61.158[.]17
- 162.33.179[.]79
- 168.100.11[.]133
- 172.86.96[.]38
- 192.153.57[.]154
- 193.149.176[.]233
- 206.166.251[.]146

# 7. 공격 지표 (Indicator of Attack)

## 1) MITRE ATT&CK[8] Matrix - APT37[9] Group Descriptions

[표 6] MITRE ATT&CK, Tactics and Techniques

| Tactic | Technique | Description |
|---|---|---|
| Reconnaissance | T1598.002[10] | Phishing for Information: Spearphishing Attachment |
| | T1598.003[11] | Phishing for Information: Spearphishing Link |
| Resource Development | T1585.002[12] | Establish Accounts: Email Accounts |
| | T1585.003[13] | Establish Accounts: Cloud Accounts |
| Initial Access | T1566.002[14] | Phishing: Spearphishing Link |
| | T1566.003[15] | Phishing: Spearphishing via Service |

# 8. 참고 자료 (Reference)

[표 7] 참고 자료

| 연번 | 제목 | 출처 |
|---|---|---|
| 1 | [Genians] 한국내 macOS 이용자를 노린 APT37 공격 등장 | https://www.genians.co.kr/blog/threat_intelligence_report_macos |
| 2 | [Genians] 북한인권단체를 사칭한 APT37 공격 사례 | https://www.genians.co.kr/blog/threat_intelligence_report_apt37 |
| 3 | [mrd0x] Browser In The Browser (BITB) Attack | https://mrd0x.com/browser-in-the-browser-phishing-attack/ |
| 4 | [zscaler] Fake Sites Stealing Steam Credentials | https://www.zscaler.com/blogs/security-research/fake-sites-stealing-steam-credentials |

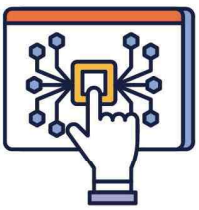
8) https://attack.mitre.org/
9) https://attack.mitre.org/groups/G0067/
10) https://attack.mitre.org/techniques/T1598/002/
11) https://attack.mitre.org/techniques/T1598/003/
12) https://attack.mitre.org/techniques/T1585/002/
13) https://attack.mitre.org/techniques/T1585/003/
14) https://attack.mitre.org/techniques/T1566/002/
15) https://attack.mitre.org/techniques/T1566/003/

2023년 1차

# 사이버보안 대연합 보고서

## 대응·역량 분과

1. 금융권의 챗GPT 서비스 활용을 위한 방안 [전진환 CISO, 신한DS]
2. 게임회사에서 AI 서비스 도입하기 [김동춘 실장, 넥슨]
3. 생성형AI 유통분야 보안대응 방안 [손주욱 CISO, 신세계디에프]



# 금융권의 챗GPT 서비스 활용을 위한 방안

전진환 CISO, 신한DS, germanus74@gmail.com

## 1. 개요

2022년 11월, OpenAI사가 GPT-3.5를 근간으로 출시한 생성형 인공지능(AI) 서비스인 챗GPT가 일반에 공개된 이후 많은 이용자가 기존의 적용 방식과 다르게 인공지능을 접목한 사례들을 경험하면서 놀라움을 금치 못했다.

기존 산·학·연에서는 주로 AI에 방대한 데이터를 효과적으로 학습시키고, 최적의 결과를 예측하기 위해 좀 더 정확도를 높이는 방법이 무엇인지 탐구해 왔다. 또한 자동학습을 통해 사람이 인지한 수준과 동일하게 현상을 판단할 수 있도록 반복 학습이 이루어져, 유사한 상황과 패턴이 발생할 때 기존과 같은 결과를 도출할 수 있도록 검증해 왔다.

반면 챗GPT는 기존 방식과는 사뭇 다르게 이용자가 앞서 질문한 내용과 현재 질문의 내용에 대해 전반적인 맥락과 의미를 이해하고, 이용자가 마치 다른 사람과 대화하는 것처럼 편안하고, 자연스러운 피드백을 제공한다는 특징이 있다.

챗GPT와 같은 대규모 언어 모델(LLM : Large Language Model)을 탑재한 AI 챗봇은 개발자가 손쉽게 프로그래밍 하도록 지원하고, 연구자가 논문의 전반적인 틀을 구성할 수 있도록 자동화하는 등 IT, 교육, 의료, 법률의 다양한 분야에서 전문가가 수행해 온 창조적인 활동들을 사람과 유사하게 처리할 수 있는 능력을 갖추었다는 데 그 의미를 가진다.

## 2. 생성형 AI 서비스 시장의 성장

챗GPT에 대한 이용자들의 관심, 이용량과 활용범위가 급격히 증가함에 따라, 글로벌 IT 회사인 마이크로소프트(MS)사는 빙 검색과 챗GPT를 결합한 빙챗(BingChat), 구글(Google)은 바드(Bard)를 출시하였고, 국내에서는 네이버(NAVER)가 하이퍼클로바를 공개하면서 생성형 AI 서비스 시장에 도전장을 내밀었다.

향후 LLM을 이용한 생성형 AI 서비스는 비즈니스와 각 산업에 밀접한 상관관계를 가지게 될 것이고, 기업의 서비스 운영을 위해 필수적으로 접목하는 활동들이 지금보다 많아질 것으로 예측된다.

기본적으로 챗GPT는 API 인증방식을 적용하는데, HTTP Header 정보에 API Key를 세팅하여 인증받을 수 있다. 기업용은 계정을 생성하면 API Key를 자동으로 발급하고, 여러 개(n)의 Key가 발급될 수 있도록 지원하고 있다. 또한 발급된 API Key는 기업에서 자체적으로 관리할 수 있도록 하고 있다. 챗GPT의 이용과금은 GPT 3.5 Turbo

기준 1,000토큰[16] (약 750단어)당 0.002달러 (약2.6원)로 API 호출 시 요청 및 응답 메시지 기준 1건당 약 1원으로 책정되어 있다. 특히, 계정관리를 통해 개인별 사용량을 제한하고, 요금을 관리할 수 있도록 서비스의 제어가 가능하다.

## 3. 생성형 AI 서비스의 활용

### 1) 생성형 AI 서비스의 활용 분야

챗GPT를 포함한 LLM 방식의 생성형 AI 서비스는 다음과 같이 다양한 영역에서 그 활용도가 높아질 것으로 예상된다.

먼저, 조직 내 지식베이스를 생성하기 쉬워 내부정보의 축적 및 검색, 활용이 가능하도록 구축할 수 있다. 또한, 문서를 생성하고, 서식화 등 특정 주제를 기반으로 글쓰기, 논문작성 등이 가능함에 따라 업무 보고서 작성 및 기획문서의 초안을 마련하는 데 유용하게 사용될 수 있다.

추가로 여러 가지 언어의 한계를 넘어설 수 있어서 해외의 보안기술과 관련된 최신 트렌드를 통번역 하여 문서화하는데 사용될 수도 있다. 특히, IT 측면에서는 프로그램 개발자를 위한 개발 코드의 작성과 개발된 소스 코드의 검증 및 수정을 자동화할 수 있어 개발 업무의 완성도를 높이고, 개발 시간과 공수를 축소할 수 있다는 장점이 있다.

[표 1] **생성형 AI 서비스 활용 예시**

| 활용 분야 | 내용 |
|---|---|
| 지식 관리 | 조직 내부 지식베이스(KMS) 생성, 검색 및 활용 |
| 문서 생성 | 보고서 작성, 문서 통번역, 기획안 작성 |
| 프로그래밍 | 개발 코드 작성, 소스 코드 오류 검증 및 수정 |
| 데이터 분석 | 대용량 데이터의 분석, 분류, 판별 |
| 보안 위협 탐지 | 이상징후 탐지, 이용자 행위 분석 등 위협 식별 |
| 교육 훈련 | 학습자료 생성 및 질의응답 시스템 구축 |

### 2) 생성형 AI 서비스 활용 통한 보안 강화

더욱이 정보보호 분야에서는 사내 이상징후 탐지, 로그 분석, 보안정책 검토 등을 수행하여 보안 위협을 식별하고, 식별된 위협을 자동으로 대응할 수 있도록 활용할 수 있다. 먼저, 사내 이상징후 탐지의 경우 네트워크 트래픽에서 특정 IP 주소나 포트에서 의심스러운 트래픽이 발생할 때 이를 이상징후로 판단하고 실무자에게 경고를 보낼 수 있다.

16) 토큰(token) : 챗GPT가 인식하는 요청/응답에 대한 글자 단위

이용자의 행위에 대한 로그 분석은 특정 이용자 계정이 로그인 시도에 실패한 횟수가 급증하는 경우 이러한 로그 데이터를 분석하여 패턴을 식별하여 오·남용을 분석할 수 있다. 또한, 보안솔루션에 적용된 보안정책이 잘못 적용되어 공격자가 시스템에 침입할 수 있는 경로가 열려 있는 경우 이를 식별하고 차단하는 등의 사전 대응이 가능하다.

[표 2] **보안 활동 내 생성형 AI 활용**

| 보안 활동 적용 | 내용 |
|---|---|
| 이상징후 탐지 | 특정 IP 주소나 포트에서 의심스러운 트래픽 탐지 |
| 이용자 로그 분석 | 특정 이용자의 로그 분석으로 오·남용 행위 탐지 |
| 보안정책 검토 | 보안솔루션의 보안정책 정합성 검토 |

### 3) 보안 분야 내 생성형 AI 활용 관련 문제점

챗GPT가 여러 산업에서 비즈니스 성공에 유용함을 제공할 수 있을 것이라는 긍정적 예측과는 달리, 아직까지 보안 부문에서는 그 특성으로 인해 적용 및 활성화까지는 많은 시간이 소요될 것으로 보인다.

일례로, 통상 회사에서 보안 취약점을 진단할 때 챗GPT가 특정 서비스의 설정 파일을 점검하거나, 소스 코드에 대한 분석 능력을 학습할 수 있어서 사람에 의한 점검자 기반의 모의해킹보다 점검의 효과성과 취약점을 찾아내는 시간적 측면에서 속도가 빠르고, 일관된 결과를 도출해 낼 것처럼 보인다.

그러나 챗GPT를 학습시킬 때 보안 취약점 관련 데이터가 부족하거나 최신 트랜드가 누락될 경우, 취약점으로 볼 수 없는 내용을 취약점으로 도출하는 부정확성을 보였다.

또한, 국내 법령과 관련하여 정보보호담당자와 점검자들이 진단 시 중요하게 생각하는 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)나 개인정보(개인정보, 개인(신용)정보, 고객번호 등), 민감정보(생체인식정보, 건강정보 등)들을 단순 데이터로 인식하여 진단 결과에서 중요정보 유출 문제를 빠뜨리는 부족함도 보였다. 이 경우 점검자에 의한 수동 진단이 추가로 필요하고, 도출된 취약점 확인하기 위해 전문가 판단이 수반될 수밖에 없어 취약점 진단의 자동화는 어렵다고 볼 수 있다.

### 4) 보안 분야 내 생성형 AI 활용 관련 개선 노력

이를 개선하기 위해 최신 보안 위협과 관련된 방대한 CVE[17] 정보를 학습데이터로 제작하여, 충분한 시간 동안 자동학습(Machine Learning)을 시켜야만 기존보다 좀 더 정교한 진단모델을 생성하고, 사람에 의해 진단한 결과와 유사하게 결과를 도출할 수 있었다.

17) CVE: Common Vulnerabilities and Exposures의 약자로, 공개적으로 알려진 컴퓨터 보안 결함을 가리키는 고유 표기임

[표 3] 보안 취약점 진단시 점검자-챗GPT 상호비교

| 취약점 진단 | 점검자 | 챗GPT |
|---|---|---|
| 진단 결과 | 분석 정확도가 높음 | 점검자의 추가 검증 필요 |
| 주요 정보 식별 | 식별 | 학습된 일부 정보만 식별 |

특히, 생성형 AI 서비스 모델을 악용하면 사이버 공격 개시가 가능하였고, 이를 위한 악성 콘텐츠의 개발 및 생성이 손쉬워진다는 문제도 있다. 가령, 2023년 아크로니스의 사이버 위협 리포트에서 확인할 수 있듯이 AI 모델을 활용한 내부망 악성 소프트웨어를 개발하여 재현한 결과를 봐도 생성형 AI 모델링이 가진 보안 위협을 충분히 설명할 수 있다. 특히, 회사 내부정보를 학습데이터로 입력하면 영업기밀이 부지불식간에 유출되거나, 잘못된 결과를 오·남용함으로써 편향된 의사결정을 내릴 수도 있다.

양날의 검과 같은 특성을 가진 챗GPT의 안전한 활용과 이용자의 인식 제고를 위해 생성형 AI 서비스에 대한 다양한 산업별 보안 기준이 사업자에게 제공되어야만 한다. 이러한 문제점을 방지하기 위해 국가정보원 등에서는 2023년 6월 "챗GPT 등 생성형 AI 활용 보안 가이드라인"[18]을 일반에 배포하여 보안 수칙을 제정하도록 하고, 안전한 활용을 위해 노력하고 있다.

## 4. 금융권의 생성형 AI 서비스 활용방안

### 1) 금융권의 생성형 AI 서비스 관련 제약 사항

금융권도 여러 산업 분야와 유사하게 업무시스템에 챗GPT와 같은 생성형 AI 서비스를 접목한 후 고객 친화적인 금융상품 및 서비스 개발을 위해 API에 연동할 것인지, 자체 개발을 할 것인지에 대해 많은 의견이 분분하다.

다만, 금융권은 전자금융감독규정 제15조(해킹 등 방지대책) 제1항 제3호에 따라 망분리 규정을 엄격하게 적용하고 있어 챗GPT 연동이 쉽지는 않다. 규정을 자세히 살펴보면, 내부 통신망과 연결된 내부 업무용 시스템의 경우 인터넷(무선통신망 포함) 등 외부 통신망과 분리·차단 및 접속 금지되어야 하고, 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우[19]이거나 업무상 필수적으로 외부 기관과 연결해야 하는 경우로 한정하여 금융감독원장의 확인을 받는 경우 망분리 적용을 예외로 할 수 있기 때문이다.

즉, 챗GPT 등과 같이 외부망에 있는 생성형 AI 서비스를 활용하기 위해서는 이용자가 고객의 개인(신용)정보와 회사의 기밀정보를 처리하지 않아야 하고, 연구·개발 등 이외의 목적으로 사용할 수 없도록 기술적 조치를 적용한 경우로만 챗GPT 이용을 제한하도록 하고 있기 때문이다.

18) 국가사이버안보센터, "챗GPT 등 생성형 AI 활용 보안 가이드라인", 2023.06.
19) 단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 시행한 후 금융감독원장이 정한 망분리 대체 정보보호 통제를 적용한 경우로 제한한다.

### 2) 금융권의 생성형 AI 서비스 활용방안

그럼에도 불구하고 챗GPT 서비스 연동을 위해 다음의 여러 방안을 고려해 볼 수 있다.

먼저, 챗GPT 서비스(외부망)와 내부 인터넷망 사이를 직접 연동하거나, 내부망 내 챗GPT 시스템 별도 구축하는 방법이 있다. 또한, 챗GPT 서비스(외부망)와 내부 인터넷망 사이의 통신을 통제하는 방식으로 연결해 볼 수 있다. 지금까지는 내·외부망을 연동하되 모니터링을 통해 이용자의 데이터를 분석하고, 질의를 차단하는 방식이 가장 합리적인 방안으로 볼 수 있다.

앞서 언급한 첫 번째 방안은 내부 인터넷망과 챗GPT API를 직접 연동하여 사용하는 가장 손쉽게 처리하는 방법이나 서비스 이용자의 이상 행위를 통제할 수 없고, 연구·개발 목적으로 그 이용을 한정할 수 없으므로 전자감독규정 등의 현행 법령을 위반할 가능성이 높다. 또한, 외부에 연동되어 있어서 사이버 공격에 노출될 가능성이 있어 보안 위협이 증가하게 되므로 해당 연계 방안의 적용은 거의 불가능에 가깝다.

두 번째, 내부망에 챗GPT 서비스를 직접 구축하는 방안은 방화벽으로 외부망으로 분리·차단하여 보안 위협으로부터 내부정보를 가장 효과적으로 보호할 수 있고, 안전하게 이용·운영될 수 있는 방식이다. 다만, 생성형 AI의 가장 큰 장점인 다양한 패턴과 추세에 관한 학습이 불가능하고, 성능 향상을 위해 막대한 구축 비용을 부담해야 한다는 문제가 있다. 특히, 주기적으로 신규 정보의 업데이트와 데이터 검증을 통한 현행화를 위해 AI 관련 기술 및 지식을 가진 전문가의 확보가 선행되어야 한다는 점도 불리하게 작용한다.

세 번째, 내부망과 챗GPT 서비스 통신 간 모니터링을 통한 연동방안은 금융권에서 가장 적용될 가능성이 높아 보이는 방식이다. 이는 내부망과 외부망 사이에 프록시 시스템을 구축한 뒤 적정 이용자의 인증관리와 접근제어를 통해 통제함으로써 이용을 가능케 한 방식이다. 대부분 산업 분야에서 이 방식을 적절하게 활용할 것으로 보이며, 챗GPT 이용의 보안성 확보를 위해 데이터 트랜잭션이 발생할 때마다 자연어에 대한 모니터링 및 분석이 필수적으로 적용되어야 하는 방식이다.

[표 4] **내부망-챗GPT 간 연계방식**

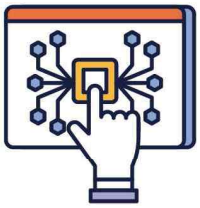
| 연계 방식 | 내용 | 비고 |
|---|---|---|
| 직접 연결 | 내부 인터넷망과 챗GPT 서비스 직접 연결 | 법 위반 가능성 |
| 내부 구축 | 내부망에 챗GPT 서비스 별도 구축 | 비용, 정보갱신 제한 |
| 망연계 통제 | 내부망과 챗GPT 서비스 통신 간 모니터링 | 보안성 확보 가능 |

앞서 설명한 망연계 통제 방식으로 챗GPT 서비스 이용을 고려한다면, 중요정보 및 개인정보의 유출을 차단하기 위해 자연어의 통제, 보안솔루션의 적용 등 몇 가지 요소를 추가로 고려해야만 한다. 챗GPT에서 채팅 방식의 질의로 인해 생성되는 요청과 응답에 이용된 자연어를 분석한 뒤 오·남용이 발생하면 차단할 수 있도록 기술적 통제가 이루어져야 한다.

기업의 내부 기밀이나 중요정보들이 외부로 유출되지 않도록 이용자들이 사용하는 구문과 자연어의 단어 또는 문자열, 문장을 분석함으로써 형태소로 분리하고 규칙을 만들어 차단·처리하는 등의 관리활동이 병행되어야 한다. 이를 위해 라이브러리를 통해 이용이 제한된 단어나 금칙어를 등록하고, 분석된 단어들의 필터링 및 모니터링을 지속해서 수행해야 한다. 또한 숫자로 질의 된 경우 정규식을 도입하여 검증 후 필터링하고, 요청 메시지에 대해 해당 길이를 제한하는 방식을 적용해야 할 것이다. 추가로 생성된 모든 대화내용은 향후 추적관리를 위해 암호화한 후 별도 저장·관리될 필요가 있다.

다음으로 챗GPT API에 요청과 응답 시 악성코드 탐지 및 외부 공격을 차단하기 위해 보안솔루션도 필수적으로 운영해야만 한다. 이를 위해 데이터 송·수신 간 공격자가 해독할 수 없도록 SSL-VA을 적용하여 데이터를 암·복호화하고, 방화벽을 통한 외부 IP의 접근제한과 서비스 포트를 최소화해야 한다. 또한, 이용자 질의로 개인정보 및 중요정보 등이 유출되지 않도록 데이터 유출 차단을 위한 개인정보의 패턴, 주요 키워드 허용 여부 등이 포함된 이용자의 접속 로그를 주기적으로 모니터링 및 분석, 대응해야 한다.

마지막으로 앞서 제시된 방안 이외에 추가로 다양한 합법적인 방안이 제안될 수 있고, 금융권의 경우 여전히 금융감독원의 비조치의견 요청을 통해 유권해석을 받아야 하는 법적 검증 과정이 남아있음을 유념해야 한다. 우리가 챗GPT 서비스의 안전한 활용을 위해서는 반드시 사내 기밀정보, 고객정보 등을 업무 목적 이외에 사용하지 않고, 공식 플러그인 사용을 통해 관리함으로써 오·남용을 축소 및 보안 위협의 발생 가능성을 사전 통제해야만 한다. 또한 모든 임직원의 인지제고는 생성형 AI 서비스의 보안성을 확보하는 데 매우 중요한 요소이다.



# 게임회사에서 AI 서비스 도입하기

김동춘 실장, 넥슨, happydal@nexon.co.kr

## 1. 게임회사에서 AI

게임 산업은 웹, 소프트웨어 개발부터 2D, 3D의 아트영역에 이르기까지 폭넓은 업무영역을 가지고 있다. 더불어 게임 서비스가 실제 구동 되는 시스템, 어플리케이션 등과 같은 일반적인 IT영역과 게임운영을 위한 사업기획, 사업운영, 고객 응대까지 다양한 범위를 가지고 있다.

업무영역 다양성으로 AI 서비스를 도입 활용하고자 하는 범위 또한 다양하다.

사업영역 전반에서 일반적인 언어모델을 활용하여 문서 번역, 문서 초안 작성, 대화형 검색, 챗봇 등을 사용할 수 있다. 게임영역의 특성을 반영하여 게임에서 수집되는 데이터를 기반으로 유저 맞춤형 추천시스템, 해킹 툴을 사용하는 비정상 유저의 식별, 비정상 결제 식별 등에 활용되기도 한다. 게임 내에서 수집되는 채팅 내용, 게임 스크린샷을 AI 모델을 이용하여 비정상 유저를 식별하는 등 다양한 범위에서 활용 되고 있다.

보안 영역에서는 시스템, 서비스, DB 등 원시로그에서 비정상을 탐지하거나 보안관제 이벤트의 정확도 향상, 보안이벤트 자동대응 및 자동응답 메시지 생성 등 다양한 범위에 사용되고 있다.

## 2. 생산형 AI 활용사례

게임 산업에서 AI가 활용되는 다양한 사례 중 아래와 같이 주요 사례를 살펴 볼 수 있다.

AI만을 사용하거나 하나의 단독 모델만으로 구현되는 사례는 드물며, 기존 시스템과 결합하여 사용하는 사례가 대부분이다. 아래는 이해를 돕기 위해 크게 두 가지 분류로 구분하였다.

### 1) 대규모 언어 모델 사용

**① 문서 번역 서비스**

- 각 기 다른 언어로 작성된 텍스트, 문서 이미지를 사용자가 원하는 언어로 변환
- 사람이 1차 번역 작성한 문서를 좀 더 자연스러운 타언어로 변환
- 예시
  - 사용자는 ChatGPT, Bing Chat 등을 사용하여 국문 메일, 계약서 등을 일문, 영문으로 번역하거나 상황에

적합한 단어, 문장으로 수정

**② 메일, 워드, PPT 등 문서 초안 작성**

- 사용자가 몇 가지 조건을 제시하여 메일, 문서의 초안을 작성
- 사용자가 소유하고 있는 문서, 메일, 메신저 기록을 학습하여 문서 초안을 작성
- 예시
  - 사용자는 ChatGPT, Bing Chat 등에 몇 가지 간단한 조건을 입력하여 초안 작성
  - 사용자는 MS Copilot을 사용하여 자신이 소유하거나 접근 가능한 데이터와 메신저 대화 내용 등을 학습하여 사용자가 원하는 문서 초안 작성

**③ 대화형 검색 서비스 및 챗봇**

- 사용자의 요구사항을 대화형으로 질의하고 이에 적합한 데이터를 응답
- 예시
  - Azure AI로 회사 내부 인트라넷, Jira, Confluence, Git 등에서 저장 관리되는 회사 내부 데이터를 참조하여 임직원의 요청에 적합한 데이터 제공
  - 회사 내부 데이터와 인터넷에 공개 된 데이터를 혼합하여 임직원 또는 외부 이용자가 질의사항에 적합한 응답을 챗봇 형태로 제공

**④ 프로그래밍**

- 게임, 웹 등 프로그래밍 영역에서 새로운 코드 생성, 수정, 버그 수정 등
- 예시
  - 사용자는 ChatGPT에 소스코드를 업로드하여 버그 수정 또는 코드 최적화
  - 사용자는 ChatGPT, Github Copilot 등과 에디터를 연동하여 주석 등 간단한 요구사항을 입력하여 최종 코드 결과물 생성

**⑤ IT보안**

- 각종 보안, 서비스 로그에서 언어모델 기반 해킹, 장애 등 비정상 탐지
- SOAR 이벤트 처리 이력을 학습하여 해킹 자동 대응 및 자동응답
- 해킹, 피싱 등 악성 메일을 자동생성하여 내부 교육에 사용
- 예시
  - DB Query, Web Query를 언어모델로 학습하여 비정상 요청 탐지
  - 로그 유형을 언어모델로 학습하여 평소 유입이 없는 장애로그 자동 식별
  - 보안관제이벤트 처리 이력을 학습하여 SOAR 기반 자동응답, 가이드 제공
  - ChatGPT, Bing Chat 등으로 정교한 피싱메일 제작하여 내부 모의훈련에 사용

### 2) 수치 또는 이미지 모델 사용

**① 이미지 생성**

- 사용자의 몇 가지 요구사항을 텍스트로 입력하여 결과 이미지 생성
- 사용자가 스케치 단계의 이미지로 최종 결과물 이미지 생성
- 사용자가 제작한 이미지를 요구사항에 맞춰 리터칭하여 최종 결과물 생성
- 예시
  - Midjourney에 사용자가 몇 가지 조건을 입력하여 원하는 이미지 생성
  - Adobe Firefly를 이용하여 사용자는 요구사항을 텍스트로 입력하여 이미지를 합성하거나 리터칭하여 결과물 생성
  - Bing Image creator에 몇 가지 조건을 텍스트로 입력하여 이미지 생성

**② IT 보안**

- 각종 보안, 서비스 로그에서 수치 기반 해킹, 장애 등 비정상 탐지
- 임직원의 평소 행위를 학습하여 내부자 해킹, 어뷰징 등 탐지
- 예시
  - 각 서비스별 평소 로그량, 형태를 시계열 수치기반으로 학습하여 비정상 탐지
  - 외부 서비스 노출되는 웹페이지, 서비스 이미지를 학습하여 내부시스템 노출탐지
  - 임직원의 데이터 사용, 반출입현황 수치를 학습하여 내부정보 유출 탐지

**③ 게임보안**

- 게임 내에서 수집되는 수치데이터, 이미지를 학습하여 게임해킹툴, 게임 매크로 등을 사용하는 비정상 유저 식별
- 게임 내 재화의 흐름을 학습하여 게임 내 비정상 구매, 판매 등 경제활동 탐지
- 게임 내 유저의 대화에서 비속어, 욕설 등 탐지

## 3. 생산형 AI 서비스 구현 방식

사업의 목적, 데이터 민감도 등에 따라 생산형 AI 서비스 구현 방식이 결정된다.

인프라, 학습데이터, 모델 등 전 영역을 자체 구축하는 방식과 일부 영역 또는 전체 영역 모두를 외부 서비스를 활용하는 방식으로 구분된다.

### 1) 자체구축

생산형 AI 운영인프라, 학습모델, 학습데이터 등 모든 영역을 자체적으로 구축하여 제공 작성된 텍스트, 문서 이미지를 사용자가 원하는 언어로 변환

**① 주요 장점**

- 학습/질의 데이터를 단독으로 관리하여 손쉬운 데이터 통제 가능
- 학습 데이터의 범위지정 및 사전 필터링으로 결과 신뢰도 향상
- 학습 모델 및 학습 범위를 지정할 수 있어 사업 목표에 최적화 된 결과 도출
- 개인정보 등 민감정보를 사전에 통제하거나 저장 위치를 지정할 수 있음

**② 주요 단점**

- 생산형 AI의 구축, 운영 능력 및 AI관련 전문 인력 필요
- 사업 규모에 따라 대규모 인프라 필요

### 2) 외부 서비스 사용

생산형 AI의 전체영역 또는 일부를 외부 서비스를 이용하는 방식으로 주요 예시는 아래와 같다.

[표 1] **학습데이터 기준 서비스 예시**

| 구분 | 학습데이터 | 서비스 예 |
|---|---|---|
| 학습된 모델 | 서비스 제공사 | OpenAI, MS Azure, Bing Chat, Github Copilot 등 |
| 자체 학습 | 자체 데이터 | OpenAI, MS Copilot, AWS Bedrock, GCP Vertex AI등 |

예를 들어 회사 내부에 번역, 사내 지식검색, 프로그래밍, 비정상탐지 서비스를 구축한다면 아래와 같이 정의할 수 있다.

[표 2] **사업목적 기준 서비스 예시**

| 구분 | 모델학습 | 참조데이터 | 서비스 예 |
|---|---|---|---|
| 번역 | 불필요 | 불필요 | OpenAI, Bing Chat 등 |
| 지식검색 | 불필요 | 회사 데이터 | openAI, Azure Copilot 등 |
| 프로그래밍/이미지생성 | 불필요 | 불필요 | Github Copilot, Adobe Firefly 등 |
| 문서작성 | 필요 | 회사 데이터 | O365 Copilot 등 |
| 비정상탐지 | 필요 | 회사 데이터 | AWS, GCP 등 내부서비스 |

**① 주요 장점**

- 인프라, 데이터 없이 즉시 사용 가능
- 운영기술, 전문 운영인력, AI 대한 지식 불필요

**② 주요 단점**

- 학습원천데이터, 학습모델이 불명확하여 결과 데이터의 추가 검증 필요
- 학습원천데이터가 불명확한 경우 산출물에 대한 상업적 활용이 어려울 수 있음

- 내부 데이터를 학습 또는 참조데이터로 활용하는 경우 철저한 보안통제 필요
- 질의/학습에 이용 된 데이터가 서비스 제공사에 의해 2차 활용 될 수 있음
- 일부 분야에서 사업 목적에 부합된 결과물 도출이 힘들 수 있음

## 4. 생산형 AI 서비스를 SaaS처럼 생각하기

실제로 생산형 AI서비스를 내부에 도입하는 경우 일반적인 SaaS 서비스와 동일한 관점으로 접근하면 기본적인 위험을 식별하고 통제할 수 있다. 특히 내부 데이터의 유출 관점에서는 일반적인 SaaS 서비스 도입과 유사한 것을 확인할 수 있다.

### 1) 위험 식별

1차 사업목적을 식별하고 그에 필요한 조건을 식별하여 적절한 통제기준을 마련한다. 이는 각 사 마다 사업의 목적과 범위, 내부규정, 취급 데이터에 따라 달라질 수 있으며 아래는 주요 항목의 예시이다.

- 생산형 AI 서비스의 사업 목적은 무엇인가
- 생산형 AI 서비스에 사용되는 데이터는 무엇인가
- 내부 데이터인 경우 적절한 통제와 모니터링 수단으로 관리가능한가

### 2) 보호 조치

생산형 AI 서비스 사용 시 질의 내용, 자체학습을 위한 데이터는 회사 내부 데이터로 민감도 높을 수 있으며, 만약 개인정보를 사용하는 경우 개인정보등급에 따라 개인정보처리시스템에 부합하는 기술적, 관리적 보호 조치가 필요하다.

- 회사 내부 데이터 사용 시 저장 위치 지정 및 통제 가능한가
- 회사 내부 데이터로 모델을 학습하는 경우 별도로 모델이 관리되는가
- 질의/학습 데이터는 타 이용사와 별도로 구분되어 관리되는가
- 개인정보 등의 민감정보가 저장되는 경우 지역지정이 가능한가
- 서비스로 전송 된 모든 데이터는 접근통제 및 이력관리가 가능한가
- 사업자간 NDA 체결로 회사 데이터를 보호받을 수 있는가
  - MS, AWS, GCP, OpenaAI 등 각 사 마다 NDA 체결형식, 보장범위 등이 다르며, 일반적인 계약서 상 NDA 체결이 아닌 홈페이지 약관 등으로 처리되고 있어 각 사 환경에서 이를 수용가능한 지 철저한 검토가 필요함

[그림 1] MS Bing Chat Enterprise 약관 예시

Microsoft를 데이터 컨트롤러로

Bing Chat Enterprise는 Microsoft가 데이터 컨트롤러인 연결된 서비스입니다. 사용자의 프롬프트는 엔터프라이즈 서비스에 도달하기 위해 organization Microsoft 365 테넌트 경계를 Bing Chat 그대로 둡니다. 그러나 이 데이터는 전송 중에 암호화되며 Microsoft는 편의성을 위해 짧은 캐싱 기간을 초과하여 이 데이터를 보존하지 않습니다. 브라우저가 닫혀 있으면 채팅 토픽이 다시 설정되거나 세션 사간이 초과되면 Microsoft는 모든 프롬프트와 응답을 삭제합니다.

채팅 응답을 제공하기 위해 Enterprise는 Bing Chat 처리에 글로벌 데이터 센터를 사용하고 미국 데이터를 처리할 수 있습니다. 선택 사항인 Bing 지원 연결된 환경은 Microsoft의 EUDB(EU 데이터 경계) 약정에 속하지 않습니다. 자세한 정보: 모든 EU 데이터 경계 서비스에 적용되는 자속적인 데이터 전송. 또한 회사 데이터가 지리적 또는 테넌트 경계 내에 남아 있어야 할 수 있는 EAS(기업 구독 계약) 또는 CASA(캠퍼스 및 학교 계약)의 조건에 속하지 않습니다.

미리 알림으로 엔터프라이즈 Bing Chat 는 테넌트 경계 내에서 조직 데이터에 액세스할 수 없으며 채팅 대화는 기본 모델을 학습시키는 데 저장되거나 사용되지 않습니다.

데이터가 테넌트 또는 지리적 경계 내에 있어야 한다는 엄격한 요구 사항이 있는 조직은 생성 AI 서비스를 제공하기 위해 Microsoft 365 Copilot 또는 Azure Open AI를 고려해야 합니다. Bing Chat 엔터프라이즈는 소비자 지향적 생성 AI 서비스를 사용하는 것보다 조직을 위한 보다 안전한 대안으로 고안되었습니다.

자세한 내용은 Microsoft 365 Data Residency 및 Microsoft 개인정보처리방침을 참조하세요.

## 5. 생산형 AI 서비스가 일반 SaaS와 다른점

ChatGPT, Bing Chat 등 AI 서비스는 일반적으로 SaaS와 유사하게 보안을 고려해야 한다. 다만 생산형 AI 서비스 특성 상 할루시네이션과 질의, 학습으로 입력 된 내부 데이터의 관리를 추가로 고려해야 한다.

### 1) 학습 데이터의 적절성

대규모 언어 모델, 이미지 모델 등을 사용할 때 원천 학습데이터의 검토가 필요하다.

- AI 서비스에서 참조하는 원천 데이터가 신뢰할 수 있는 데이터인가
- 사용자 질의를 요청에 부합하게 해석하고 신뢰된 결과를 응답하였는가
- AI 서비스에 참조하는 원천코드, 이미지가 적절한가
- 원천코드/이미지의 라이선스, 오픈소스 유형 등이 적절한가
- 원천코드의 악성코드 등의 해킹 위험성은 없는가

### 2) 데이터 기반 권한 설정 강화

회사 내부 데이터를 학습하는 경우 데이터 접근권한 관리가 더욱 강화 되어야 한다.

- 원천 데이터를 접근권한에 기반하여 학습하여야 함
- 원천 데이터를 학습 대상과 비학습 대상으로 구분하여 관리하여야 함
- 원천 데이터에서 개인정보, 기밀정보를 철저히 구분, 필터링하여 관리하여야 함
- 원천 데이터의 접근권한이 부실 한 경우 AI서비스가 유출경로가 될 수 있음
- 사용자가 AI에 질의한 요청의 민감도를 구분하고 관리하여야 함

• AI 서비스에서 생산된 데이터가 Cloud에 저장되는 경우 외부유출을 통제해야함

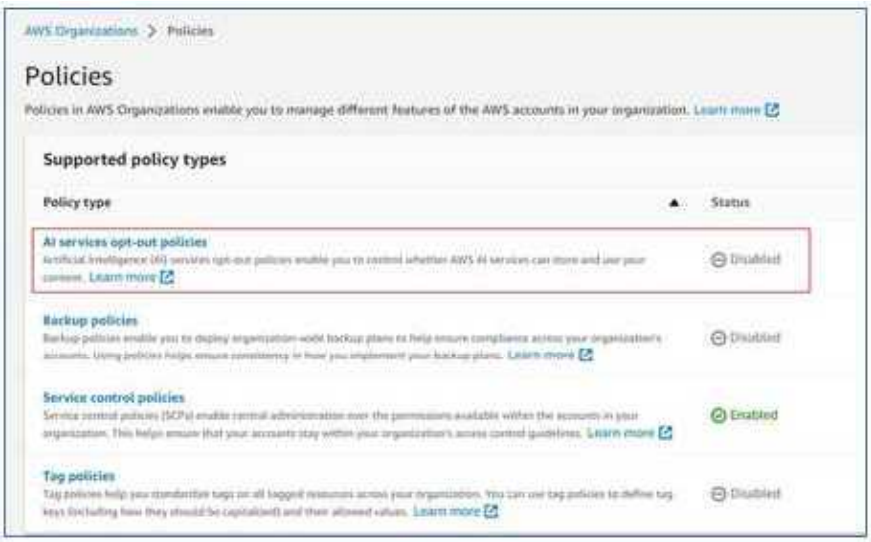
[그림 2] Adobe Admin Console의 데이터 공유제한 예시


### 3) 서비스 제공자의 데이터 2차 활용

OpenAI, MS, AWS, GCP, Adobe 등 다양한 AI 서비스에 사용되는 데이터의 2차 활용 범위를 지정하여야 한다.

• 사용자 질의 데이터, 내부 학습데이터 모두 2차 활용되지 않도록 설정 하여야함
  – 특히 회사의 중요정보를 학습하는 경우 제공사에서 2차 활용되지 않도록 설정
• 특히 NDA 또는 약관을 검토하여 데이터가 2차 활용되지 않음을 필히 확인

[그림 3] AWS opt-out 설정 예시



[그림 4] Adobe의 2차 활용 제한 조항 예시

> *Note: Adobe will not include enterprise user content (including Firefly inputs and outputs) in datasets used to train Firefly models. This does not apply to use of Firefly as part of any feedback or improvement programs in which the customer/user has the ability to control to use of their content for training.*

## 6. 남아있는 과제

생산형 AI서비스를 실제 현장에 도입하는 경우 아직도 많은 과제가 잔존해 있다.

다양한 업체에서 GPT 또는 다양한 모델을 조합하거나 학습하는 원천데이터를 변경하여 새로운 생산형 AI 서비스를 런칭하고 있다. 하지만 생산형 AI 서비스가 참조하는 원천데이터가 무엇이며 어떤 모델의 조합을 사용하고 있는지 명확하지 않다.

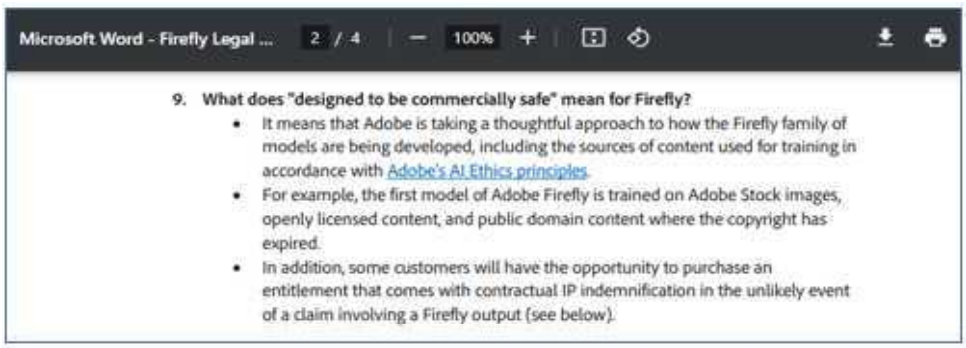
이에 따라 외부의 생산형 AI서비스를 사용하는 경우 아래와 같은 문제가 잔존하게 된다.

### 1) 산출물의 적정성 및 라이선스

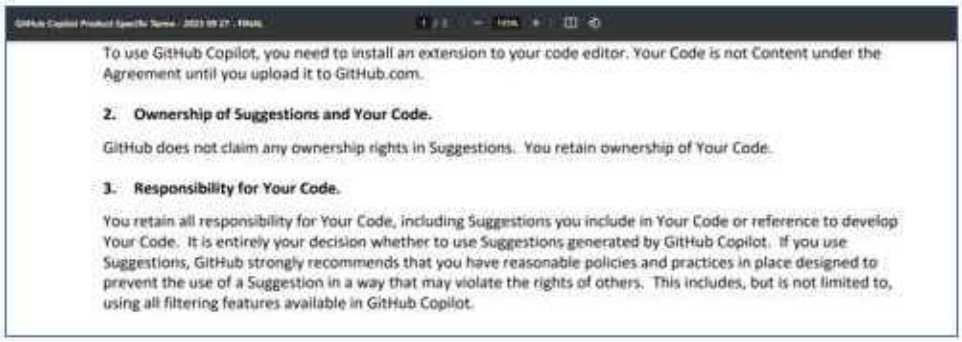
학습한 원천데이터의 신뢰도, 상업적라이선스 등의 범위를 명확히 확인하여야 한다.

- 생산형 AI 결과물의 도출방식을 명확하게 설명할 수 있는가
  - 예시 : 증명 된 원천데이터 사용유무, 개인정보 등과 같은 민감정보 포함 유무 등
- 생산형 AI의 결과를 상업적 용도로 사용할 수 있는가
  - 예시 : 문서 인용부, 이미지, 프로그램 소스코드 등을 상업적으로 사용할 수 있는가
- 원천데이터가 2차 가공 시 상업적으로 활용할 수 있는 범위에 포함되는가
  - 예시 : Adobe Firefly는 원천데이터가 모두 Adobe 소유로 상업적 사용 가능
- 생산형 AI에서 생산 된 결과물의 중복 가능성을 검증할 수 있는가

[그림 5] Adobe firefly 상업적 활용 예시



[그림 6] Github Copilot의 소유권 명시 예시



To use GitHub Copilot, you need to install an extension to your code editor. Your Code is not Content under the Agreement until you upload it to GitHub.com.

**2. Ownership of Suggestions and Your Code.**

GitHub does not claim any ownership rights in Suggestions. You retain ownership of Your Code.

**3. Responsibility for Your Code.**

You retain all responsibility for Your Code, including Suggestions you include in Your Code or reference to develop Your Code. It is entirely your decision whether to use Suggestions generated by GitHub Copilot. If you use Suggestions, GitHub strongly recommends that you have reasonable policies and practices in place designed to prevent the use of a Suggestion in a way that may violate the rights of others. This includes, but is not limited to, using all filtering features available in GitHub Copilot.

### 2) 서비스 사업자에게 관리 위임

SaaS서비스에서 가지고 있는 모든 위험을 그대로 가지고 있다.

- 사용자의 질의데이터가 안전하게 별도 보관되는가
- 사용자가 업로드한 학습원천 데이터가 안전하게 별도 관리되는가
- 사용자의 모든 데이터는 접근통제, 로깅, 암호화 등을 제공하는가
- NDA 또는 약관은 위험을 충분히 감소할 수 있으며 변경이 없는가
- 개인정보 등의 민감데이터를 식별하고 별도 분리 보관할 수 있는가

### 3) 지속적으로 생산되는 외부 서비스

새로운 생산형 AI서비스가 지속적으로 생겨나고 있어 보안관리자 입장에서 이를 신속히 인지하고 선제 대응하는 것은 매우 어렵다.

- ChatGPT, Bing 과 같은 유사 서비스 생성을 인지할 수 있는가
- 신규 생산형 AI 서비스로 회사 데이터 이동을 탐지할 수 있는가
- 신규 생산형 AI 서비스를 네트워크, 엔드포인트 등에서 통제할 수 있는가

기존 업무에 생산형 AI 서비스 접목은 다양한 분야에서 이루어 지고 있다. 단순 검색부터 프로그래밍, 이미지 생성, 보안에 이르기까지 범위가 매우 다양하다.

외부 생산형 AI 서비스 사용 시에도 인프라, 원천데이터, 모델 등 모든 영역을 위임하여 사용 또는 원천데이터는 내부데이터를 사용하거나 인프라만을 사용하는 등 방식도 다양하다.

따라서 생산형 AI 서비스 도입 시에는 사업상 사용의 목적과 범위를 명확히 하고 그에 따라 생산형 AI 서비스의 종류와 사용 범위를 검토해야 한다.

# 생성형AI 유통분야 보안대응 방안

손주욱 CISO, 신세계디에프, ksjw1@shinsegae.com

## 1. 개요

최근 ChatGPT, bard, 하이퍼클로바 등 생성형 AI 기술이 빠르게 진화하고 있다. 특히 ChatGPT의 경우 베타 버전 출시 2개월만에 MAU가 1억 명을 넘어설 정도로 히트하였는데 세계적으로 가장 성공한 서비스로 평가받는 인스타그램 30주, 틱톡 9주 보다 빠른 역대 최고 성적이다. 생성형 AI는 텍스트, 이미지, 음성 등 다양한 형태의 창의적인 콘텐츠를 생성할 수 있는 기술로, 유통 분야에서도 다양한 방식으로 활용될 수 있다.

## 2. 생성형 AI 유통분야 서비스 활용 범위

**첫번째**로 생성형 AI는 대량의 데이터 학습을 통해서 마케팅 활용이 가능하다. 상품의 이미지, 영상, 리뷰 등을 생성하여 소비자의 관심을 유도할 수 있다.

**두번째**로 고객 상담을 자동화하여 고객응대에 있어 적극적인 대응이 가능하다. 이를 통해 24/7 고객 지원을 제공하고 응답 시간을 단축시키는 등의 이점이 있다.

**세번째**로 상품추천 및 개인화 서비스가 가능하다. 소비자의 취향에 맞는 상품을 추천하거나 소비자의 구매 패턴을 분석하여 맞춤형 서비스를 제공할 수 있다.

**네번째**로 생성형 AI를 사용하여 수요 예측과 재고 관리를 최적화가 가능하다. 이를 통해 재고 비용을 절감하고 물류 프로세스를 최적화할 수 있다.

이와 같이 생성형 AI는 다양한 서비스를 유통분야에 활용이 가능하다.

# 3. 생성형 AI 유통분야 서비스 활용 사례

## 1) 유통분야 국내사례

- **A사**: 모바일 앱 내에 '쇼핑 AI' 서비스를 개발해 고객들에게 제공하고 있다. A사의 '쇼핑 AI'는 ChatGPT를 기반으로 개발된 대화형 고객 응대 서비스이며 ChatGPT의 기본 알고리즘에 쇼핑 고객에게 적합한 방송 정보와 리뷰, 상품 장단점 분석 등이 추가된 학습 모델을 적용하였고 고객들은 질문을 통해 A사에서 판매하는 상품 정보뿐만 아니라 날씨와 유행 등 일반적인 정보까지 모두 얻을 수 있다.
- **B사**: 광고 카피, 판촉행사 소개문 등 마케팅 문구 제작에 특화된 네이버의 생성형 AI 하이퍼클로바를 기본엔진으로 사용하고 있는 '루이스'를 업무에 정식 도입하여 광고카피 등에 활용하고 있다.
- **C사**: 네이버의 생성형 AI 기술을 활용해 사업 혁신에 나설 예정이다. 이용 고객의 편의성을 증대하고 고객 데이터의 효율적 활용을 통한 개인화 서비스 제공계획에 있다.
- **D사**: 생성형 AI를 통해 고객 맞춤형 마케팅, AI 기반 고객 상담 등의 서비스를 개발할 계획이다.

이처럼 유통업계에서는 자사의 경쟁력확보를 위해 생성형 AI도입을 신속하게 추진하고 있다.

## 2) 유통분야 해외사례

- **E사**: 생성형 AI인 베드록을 출시한 E사는 판매자를 대상으로 판매자들이 새로 등록하려는 상품의 주된 특징을 키워드 형태로 입력하면, 생성형 인공지능 도구가 상품명과 상품설명 등을 대신 작성해주는 서비스를 운영 중에 있다.
- **F사**: 회사 직원 5만명에게 생성형 AI비서를 제공 계획에 있다. 해당 투자를 통해 운영을 간소화하고 생산성을 향상하며 조직 전체의 의사결정을 개선할 수 있다. 따라서 더 가치가 있는 전략적 업무에 집중할 수 있다.
- **G사**: 이미지 해석 기능 갖춘 생성형 AI를 오픈소스로 공개하고 해당 서비스를 통해 쇼핑몰 이용 시 시각 장애인에게 정보를 지원하는데 향후 활용할 수 있도록 지원하고 있다.

## 4. 생성형 AI 내부 업무 활용 현황

**A사**는 생성형 AI의 리스크를 최소화하기 위해 생성형 AI의 사내 사용을 모두 차단하고 있다. A사는 생성형 AI를 사용함으로써 발생할 수 있는 여러 문제 즉, 회사의 기밀이나 개인정보유출 우려와 생성된 정보가 왜곡되어 오히려 검수 M/M가 더 발생할 수 있는 리스크를 통제하고 있다.

**B사**는 A사와 마찬가지로 생성형 AI의 사내 사용을 차단하고 있다. 다만, 필요시 담당임원 승인하에 사용 예외를 허용하여 생성형 AI가 필요한 사업부의 업무 효율성을 높이고 있다.

**C사**는 제한 없이 생성형 AI를 사내에서 사용하고 있다. 생성형 AI를 사용함으로써 발생할 수 있는 리스크보다 사용함으로써 얻을 수 있는 여러 이점을 더 높게 평가하여 C사는 생성형 AI를 통해 여러 업무를 검토하고 있다.

유통분야 각 사는 추구하고자 하는 방향성에 따라 여러 방식으로 운영을 하고 있으나 대부분 B사와 같은 방식으로 운영을 하고 있다. 하지만 잘 알려진 생성형 AI에 한해서 제한적으로 차단하고 있으며, 파생되어 잘 알려져 있지 않거나 신생 생성형 AI의 경우에 대해서는 사용 제한하기는 어려운 상황이다.

## 5. 생성형 AI 유통분야 도입 이점 및 리스크

### 1) 유통분야 생성형 AI 도입 이점

- **생산성 향상**: 상품 설명, 고객 상담, 마케팅 자료 생성, 다양한 언어로 번역 등의 업무 자동화로 인해 직원들은 더 전략적인 작업에 집중할 수 있다.
- **고객 서비스 향상**: 생성형 AI를 통해 빠르고 정확한 고객 서비스를 제공하며, 고객 만족도를 높일 수 있다.
- **비용 절감**: 자동화된 프로세스와 예측 분석을 통해 비용을 최적화할 수 있다.
- **마케팅 효율화**: 생성형 AI를 활용하여 개인화된 마케팅 전략을 구현하고 고객을 효과적으로 유치가 가능하다.

### 2) 유통분야 생성형 AI 리스크

- **개인정보 및 중요정보 노출**: 생성형 AI사용시 회사의 중요 정보 및 개인정보 유출 및 수집 가능성이 존재하여 소비자의 프라이버시 침해, 기업 이미지에 부정적인 영향을 끼칠 수 있다.
- **왜곡된 정보**: 생성형 AI로 생성된 실제와 구분하기 어려운 왜곡된 상품정보 정보로 인하여 소비자의 신뢰를 떨어뜨리고 기업 매출에 부정적인 영향을 미칠 수 있다.

# 6. 생성형 AI 보안 대응방안

## 1) 내부 사용자 측면

- **정책 지침 반영**: 생성형 AI 사용에 따른 정보유출 이슈에 대해서는 차단 정책으로 운영을 하고 있다고 하더라도 파생되어지는 생성형 AI들이 많기 때문에 내규에 사용하지 말아야 하는 범위를 특정하고 문제 발생시 해당 책임소재를 분명히 할 필요가 있다. 또한, 필요시 보안서약서 징구를 통해 사용자의 책임을 명시하는 방안으로도 보완이 필요하다.
- **상용서비스 이용**: 개인정보 및 중요정보가 외부로 노출이 되지 않는 상업용 서비스를 이용하거나, 사용자와 생성형 AI 서비스 간에 중계 및 모니터링 방식으로 주요정보 필터링 또는 사후 감시를 할 수 있는 서비스를 활용할 수 있다.

[그림 1] **모니터링 및 필터링 서비스 예시**


- **인식제고 활동**: 생성형 AI를 사용함으로써 발생할 수 있는 여러 사례들 중심으로 공지 및 교육을 통해, 인식제고 활동이 지속적으로 운영이 되도록 관리가 필요하다.

## 2) 서비스 측면

- **왜곡정보 현행화**: 학습데이터의 다양성 확보가 필요하며 왜곡을 최소화할 수 있는 기술 개발 및 검수 역량강화가 필요하다.

## 7. 결론

이처럼 AI 기술의 발전과 함께 유통 산업에서 AI의 활용은 더욱 확대될 것으로 전망되며 유통 기업의 경쟁력을 강화하고 고객에게 더 나은 경험을 제공하는 데 중요한 역할을 할 것이다. 따라서 급변하고 있는 시장상황에서 생성형 AI는 유통업계 경쟁력 확보를 위해 필요한 도구임에는 틀림이 없다. 다만, 정보유출, 왜곡, 신뢰도 문제 등이 선결되어야 활용도를 높일 수 있기 때문에 여러 리스크를 해결할 수 있도록 업계의 지속적인 관심과 투자 노력이 선행되어야 할 것이다.

2023년 1차

# 사이버보안 대연합 보고서

## 정책·제도 분과

1. 국내 정보보호산업 현황 분석

[사이버보안 대연합 정책·제도 분과]

# 국내 정보보호산업 현황 분석

사이버보안 대연합 정책·제도 분과

## 1. 개요

국내외 사이버보안(정보보안)* 산업의 현황과 주요 동향 분석을 통해 국내 보안 산업 활성화를 위한 정책 방향 제시

*「정보보호산업법」상 정보보호는 정보보안과 물리보안을 포괄하나, 사이버보안에 한하여 분석된 글로벌 자료와의 정합성을 위해 본 보고서의 분석 범위를 사이버보안 산업으로 한정

## 2. 국내외 사이버보안 산업 주요 동향

### 제로트러스트(Zero Trust)

'美 국가 사이버보안 행정명령(2021. 5)'으로 제로트러스트가 기반 기술로 채택되었으며, 민간의 관심과 시장 규모가 증가

*「IT 보안 의사결정자 71%가 제로트러스트 전환을 고려하고 있으며(IDG), 글로벌 SASE 시장은 '21년 12억 달러 → '26년 41억달러까지 성장할 것으로 예상(Markets&Markets)

### 공급망 보안

오픈소스 취약점으로 인한 위협이 증가하고 미국의 SBoM 관련 제도가 강화*되면서 보안 기업은 공급망 보안 포트폴리오 강화**

* 미연방기관에 SW 내장 제품을 납품할 경우 SBoM 제출을 의무화(2021. 5)

** 팔로알토네트웍스 : 자사 솔루션에 소프트웨어 구성 분석 기능 추가(2022. 3)
태니엄 : 오픈소스 SW의 구성을 분석하고 결함을 제거하는 '태니엄 SBoM' 출시(2022. 11)

### 클라우드

클라우드 전환에 따라 클라우드 호나경의 위협 탐지를 위한 보안 솔루션*과 함께, 구독형 보안 서비스(SECaaS)에 대한 수요 증가 전망

* CWPP : 클라우드 상 리소스(가상 머신, 컨테이너 등)의 가시성 확보, 취약점 탐지
CSPM : 컴플라이언스, 보안 정책에 기반하여 클라우드상의 위험을 지속적으로 모니터링

## 2. 국내외 산업 규모

### 국내 정보보호산업 규모

국내 주요 보안 기업들은 '22년에도 호실적*을 이어가고 있으며, '22년 정보보안산업 규모는 약 5.1조 원으로 예측(최근 3년간 연평균 성장률 13.1%)

* SK쉴더스 : 1~3분기 사이버보안 매출은 2,699억 원으로 전년 동기 대비 17.1% 증가
  안랩 : 1~3분기 매출액은 1,578억 원으로 전년 대비 12.7% 증가

※ 국내 SW산업 규모 : '22년 36.9조 원, 전년대비 6.6% 성장(소프트웨어정책연구소, '22.11)

[표 1] 국내 정보보안 시장 규모

| 구 분 | '18년 | '19년 | '20년 | '21년 | '22년(예측) |
|---|---|---|---|---|---|
| 매출액 | 3.1조 원 | 3.6조 원 | 3.9조 원 | 4.5조 원 | 5.1조 원 |
| 성장률 | 12.3% | 16.1% | 8.3% | 8.4% | 13.1% |

※ 출처 : 2022년 정보보호산업 실태조사(한국정보보호산업협회, '22. 9.)

### 해외 정보보호산업 규모

'22년 글로벌 사이버보안 시장은 전년 대비 약 7.2% 성장한 209조원(169.2B$) 규모로 예측되며, 최근 3년간 연평균 11.1% 성장

※ 글로벌 시장 규모는 향후 2년간 연평균 12% 성장해, '24년 약 262조 원(212.1B$) 규모로 예측(Gartner)

[표 2] 해외 정보보안 시장 규모

| 구 분 | '18년 | '19년 | '20년 | '21년 | '22년(예측) |
|---|---|---|---|---|---|
| 매출액 | 142조원 (115B$) | 156조원 (126.5B$) | 171조원 (138B$) | 195조원 (157.8B$) | 209조원 (169.2B$) |
| 성장률 | 13.5% | 10.0% | 9.1% | 14.3% | 7.2% |

※ 출처 : Worldwide Information Security & Risk management End-user Spending by Segment(Gartner)

글로벌 시장 분석 기관(Mckinsey & Company 등)은 시장 성장 동인으로 기업 표적의 사이버위협 증가, 제로트러스트·클라우드 보안 등 보안패러다임 전환, 규제 요건에 대한 준수 요구 등을 제시

### 글로벌 권역별 사이버보안 시장 규모

2022년 기준 세계 최대 보안시장은 미국으로 약 79조원의 규모이며, 절반에 가까운 시장 점유율을 유지하고 있으며, 유럽(약 43조원), 중국(약 17조원), 일본(약 12조원), 동남아(약 4.8조원), 중동(약 4.4조원) 순으로 사이버 보안 시장 점유 중

[표 3] 주요 권역별 사이버보안 시장 규모(2022년)

| 구 분 | 북미(미국,캐나다) | 유럽* | 아시아** | 중동·아프리카 | 중남미 |
|---|---|---|---|---|---|
| 규 모 | 약 86조원<br>(68.7B$) | 약 43조원<br>(34.5B$) | 약 41조원<br>(33.3B$) | 약 6.9조원<br>(5.5B$) | 약 4.6조원<br>(3.7B$) |
| 점유율 | 47% | 24% | 23% | 4% | 3% |

※ 출처 : STATISTA, * 유럽 : EU 27개국, 영국 ** 아시아 : 동아시아 5개국, 아세안(ASEAN) 10개국, 인도

### 글로벌 사이버보안 시장 내 국내 보안 시장 비중

글로벌 사이버보안 시장에서 국내 보안 시장의 비중은 '22년 기준 약 2.44% 수준으로 최근 3년간 완만하게 증가 중('20년 : 2.30% → '21년 : 2.33% → '22년 : 2.44%)

## 3. 국내 기업의 수출 현황

코로나19 지속기간 중 전 세계적으로 보안 수요가 급증하면서 동남아시아, 미국, 유럽 등 전역에서 수출 증가세를 보였으며, 지리적으로 가까운 이점이 있고 국내 시장 대비 큰 시장을 보유한 일본, 중국, 동남아시아에 편중

[표 4] 국내 정보보안기업의 권역별 수출액 및 비중

| 구 분 | 일 본 | 중 국 | 미 국 | 유 럽 | 기 타 | 합 계 |
|---|---|---|---|---|---|---|
| '20년 | 862억<br>(59.2%) | 243억<br>(16.7%) | 67억<br>(4.6%) | 7억<br>(0.5%) | 277억<br>(19%) | 1,456억<br>(100%) |
| '21년 | 642억<br>(42.1%) | 177억<br>(11.6%) | 197억<br>(12.9%) | 98억<br>(6.4%) | 412억<br>(27.0%) | 1,526억<br>(100%) |

일본 수출 비중은 전년 대비 17.1%p 감소*하였으나, 장기간 거래를 통해 구축된 신뢰를 기반으로 회복될 가능성이 있음

* 주요 일본 진출 기업인 윈스는 일본 최대 이통사(NTT 도코모) 대상의 IPS 장비 교체 물량이 축소되면서, 수출액이 '20년 151억원에서 '21년 69억원으로 감소

[표 5] 주요 권역별 국내 정보보호기업 진출 현황

| 국 가 | 기업 진출 현황 |
|---|---|
| 미 국 | 파수, 지니언스, SK쉴더스, 옥타코, 네이블커뮤니케이션즈 등 |
| 유 럽 | 한컴위드(영국), 센스톤(영국), 노르마(독일), 씨프로(영국) 등 |
| 중 국 | 이글루코퍼레이션, 파이오링크, 엘에스웨어 등 |
| 일 본 | 윈스, 시큐아이, 유니온커뮤니티, 한드림넷 등 |
| 동남아시아 | 워터월시스템즈(베트남), 파이오링크(베트남), 시큐레터(말레이시아) 등 |
| 중 동 | 시큐레터, 이지케어택, 한컴위드(사우디아라비아), 기원테크(오만) 등 |

**향후 정책 방향**

시장 성장 가능성, 시장 내 국내 기업의 경쟁력을 고려했을 때, 동남아·중동 권역 선점을 집중 지원*할 필요가 있으며, 국내 보안 기업·제품에 우호적이고 마케팅, 기술 지원이 가능한 현지 인력 확보**를 통해 지속가능한 수출 생태계 조성 필요

* 신흥 시장 선점을 위해 정부 간(G2G, G2B) 협력 강화, 기업 간 동반 진출 등 신뢰 기반 해외 진출 전략이 요구됨

** 국내 보안 기업과 해외 교육기관이 협력하여 현지 인력을 양성하고, 국내 기업 취업 연계 등 필요

## 4. 사이버보안에 대한 수요 및 투자 분석

### 공공기관

국내 정보보안 기업의 매출액에서 공공부문 매출액이 차지하는 비율은 약 41.1%로 가장 높음

- 공공부문 정보보호 수요 예보('22.11)에 따르면 '23년 공공부문 정보보안 제품·서비스 구매 예산(예정)은 5,662억원으로 전년 대비 2.2% 증가
- 보안 기업은 공공진출을 발판 삼아 민간에 진출하는 경향이 있으나, 기존 제도(CC인증 등)는 신규 기술과 스타트업 진입에 대해 폐쇄적인 구조

**향후 정책 방향**

정보보호제품 신속확인제 도입 등 지속적인 제도 개선을 통해 새로운 기술, 제품이 공공시장에 적시 도입되고 민간으로 확산될 수 있도록 유도

### 민간·금융

국내 정보보안 기업의 매출액에서 민간부문 매출액은 약 40.2%, 금융부문 매출액은 약 18.7% 차지

- 국내 대기업들은 제품의 성능, 글로벌 지사와의 호환성 측면에서 글로벌 사이버보안 기업*의 제품을 선호하며, 특히 네트워크 보안, 클라우드 보안, 엔드포인트 보안 및 통합보안 솔루션 부문에서 외국계 기업이 높은 성능을 기반으로 강세를 보임

  * 팔로알토네트웍스, 포티넷, 트렌드마이크로, 시스코, MS가 대표적이며, 5개 기업의 국내 보안 시장 매출액은 3~500억(기업 당), 총 점유율은 50% 이상으로 추정

- 금융업은 「전자금융거래법」에 따라 이용자 보호 조치를 수행 중으로 정보보호 공시 결과 정보보호 투자액, 투자 비중이 타 업종 대비 우수

  ※ 정보보호 투자액 : 금융 및 보험업(70억원) 〉 정보통신업(49억원) 〉 제조업(35억원)
  IT 대비 정보보호 투자 비중 : 금융 및 보험업(10.49%) 〉 제조업(9.74%) 〉 건설업(9.62%)

**향후 정책 방향**

국내 보안 기업의 기술 수준 제고를 통해 국산 비중을 높이고, '정보보호 공시제도'를 통해 민간 기업의 경쟁적 보안 투자 유도

## 5. 사이버보안 기업 분석

### 주요 동향(해외)

통합 보안 솔루션化 트렌드와 함께 글로벌 기업들은 활발한 M&A를 통해 기술력을 강화하고 규모의 확대에 나서는 추세

[표 6] '22년 글로벌 사이버보안 분야 주요 M&A 사례

| 인수 기업 | 인수 대상 | 강화 분야 | 시기 | 인수액 |
|---|---|---|---|---|
| 구글(미국) | 맨디언트(미국) | 클라우드 보안 | '22.3. | 54억불 |
| | 시엠플리파이(이스라엘) | 클라우드 보안 | '22.1. | 5억불 |
| IBM(미국) | 란도리(미국) | 공격 표면 관리* | '22.6. | 4억불 |
| 팔로알토네트웍스(미국) | 사이더시큐리티(이스라엘) | 애플리케이션 보안 | '22.11. | 3억불 |

* 공격 표면 관리(ASM, Attack Surface Management) : 공격자가 공격 대상의 내부 시스템에 접속하여 공격할 수 있는 노출된 경로에 대한 위협을 감지 및 식별하는 솔루션

## 주요 동향(국내)

국내에서도 사이버보안 분야 M&A 사례가 일부 존재하지만 글로벌 추세에 비해 M&A가 활성화되지 않은 상황

[표 7] '22년 국내 사이버보안 분야 주요 M&A 사례

| 인수 기업 | 인수 대상 | 강화 분야 | 시기 | 인수액 |
|---|---|---|---|---|
| 안랩 | 제이슨(한국) | AI보안 | '20.1. | 비공개 |
| | 나온웍스(한국) | OT보안 | '21.7. | 비공개 |
| LG전자 | 사이벨럼(이스라엘) | 자동차 보안 | '21.9. | 1,300억원 |
| 이글루코퍼레이션 | 파이오링크(한국) | 클라우드 보안 | '21.10. | 350억원 |

국내 정보보안 기업 중 매출액 1,000억 이상 기업이 3개에 불과하고, 84%가 매출액 100억 미만의 영세 기업으로 구성되어 있어 경쟁력이 부족한 상황

[표 8] 매출액 규모별 국내 정보보안 기업 현황

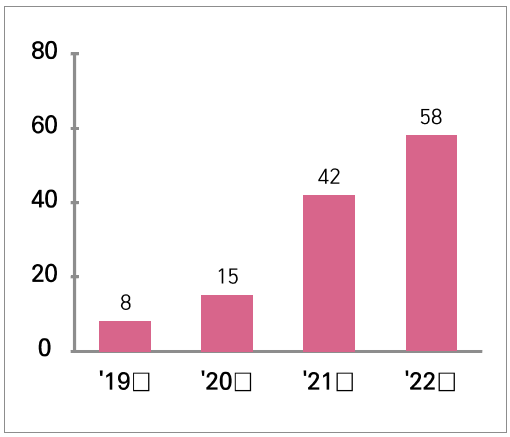
| 매출액 규모('21년 기준) | 기업 수(개) | 비중(%) | 주요 기업 |
|---|---|---|---|
| 1,000억 이상 | 3 | 0.4% | SK쉴더스, 안랩, 시큐아이 |
| 300억 이상 ~ 1,000억 미만 | 11 | 1.6% | 윈스, 이글루코퍼레이션, 파수 |
| 100억 이상 ~ 300억 미만 | 93 | 13.9% | 펜타시큐리티시스템, 지니언스, 지란지교시큐리티 |
| 100억 미만 | 562 | 84.0% | 스틸리언, 시큐레터 |
| **합 계** | **669** | **100.0%** | - |

새로운 보안트렌드에 부합하는 스타트업이 주목받으며 글로벌 사이버 보안 유니콘*이 급증하는 가운데 국내 보안 유니콘[20]은 전무

* '23년 1월 기준 총 58개사(미국 45개, 이스라엘 7개, 캐나다 3개, 중국 1개, 스위스 1개, 리투아니아 1개)

20) 유니콘(Unicorn) : 유니콘 기업은 기업 가치가 1조원(10억 달러) 이상이고 창업한 지 10년 이하인 비상장 스타트업 기업

[표 9] 사이버보안 유니콘 기업 수




[표 10] 주요 사이버보안 유니콘 기업

| 기업명 | 국가 | 사업 분야 | 기업 가치 |
|---|---|---|---|
| 싱크(Synk) | 미국 | 클라우드 보안 | 85억달러 |
| 레이스워크(Lacework) | 미국 | 클라우드 보안 | 83억달러 |
| 위즈(Wiz) | 이스라엘 | 클라우드 보안 | 60억달러 |
| 아크틱 울프(Arctic wolf) | 미국 | 위협 탐지·대응 | 43억달러 |
| 일루미오(Ilumio) | 미국 | 제로트러스트 | 27.5억달러 |

**향후 정책 방향**

기술가치평가 및 컨설팅 지원, IR대회 개최 등 M&A 수요 기업 간 네트워킹 지원으로 M&A 활성화 기반을 마련하고, 정부 주도의 사이버보안 펀드 조성을 통해 정보보호기업에 대한 투자 활성화 도모

## 6. 국내 지역별 분석

### 주요 현황

국내 사이버 침해사고의 73%가 서울 외 지역에서 발생하고 있으나, 정보보호 기업·인력 등 정보보호 인프라는 수도권에 편중*

* 국내 정보보안 기업의 73%, 인력의 67%가 서울에 편중(출처 : '22년 국내 정보보호산업 실태조사)

- 지역별 주력 산업 활성화를 위해 정보보안 내재화가 필수적으로 요구되면서 향후 지역의 정보보안 수요가 증가할 것으로 예측

[표 11] 권역별 국내 정보보안기업 수 및 특징

| 지 역 | 정보보안기업 수 | 정보보안기업 특징 |
|---|---|---|
| 수도권(서울, 경기, 인천) | 581개 | 서울, 경기 내 정보보안 기업 집중 |
| 강원 | 5개 | 디지털 헬스케어 관련 보안 수요 존재 |
| 충청권(대전, 충북, 충남, 세종) | 29개 | 스마트시티, 대학·연구기관 중심의 보안 수요 존재 |
| 전라권(광주, 전북, 전남, 제주) | 12개 | 광주 AI 집적 단지 조성에 따라 보안 수요 증가 예측 |
| 대구·경북 | 16개 | 메타버스, 인공지능 산업 육성 중 |
| 부산·울산·경남 | 26개 | 스마트시티, 블록체인, 핀테크 산업 육성 중 |

이에, 정부는 지역 균형 발전을 강조하며 지역의 혁신 성장 기반 강화*를 통한 양질의 일자리 창출, 지역 특성 극대화 등을 추진 중

* 세금 감면, 규제 완화를 통해 기업의 지방 투자·이전을 촉진하는 기회발전특구 정책 등

**향후 정책 방향**

지역에 특화된 보안 기업, 청년 인재를 양성하고 기회발전특구 등 타 정책과의 연계를 통한 지역 산업 육성과 지역별 보안 수요, 보안 기업 및 인력 규모, 지자체의 관련 정책 등 분석을 통한 맞춤형 정책 추진 필요

## 7. 사이버보안 인력 분석

### 주요 현황

사이버보안 영역의 확대와 중요성 증가에 따른 사이버 전문인력 수요 급증으로 전세계적인 인력 부족 현상이 지속되고 있으며, 미국·중국 등 주요국은 교육투자 확대, 사이버 대학·대학원 운영 등 전문인력 양성을 위한 노력 지속 중

- 국내는 향후 5년간('22~'26년)의 수요에 대응하는 신규 인력 공급(4만명), 재직자 역량 강화 교육(6만명) 등 약 10만명의 인력 양성 필요
- 산업계는 특히 보안 제품·서비스 개발을 위한 전문 인력 양성과 지역 인력 양성을 요청했으며, 융합 보안인력 수요 증가 예측

[표 12] **국내 분야별 공급 필요 인력 수**

| 신규 공급 필요 인력(4만명) | | | 재직자 역량 강화 교육(6만명) | | |
|---|---|---|---|---|---|
| 제품개발 (0.5만명) | 보안관리 (3만명) | 사고대응 (0.5만명) | 제품개발 (0.8만명) | 보안관리 (4.4만명) | 사고대응 (0.8만명) |

**향후 정책 방향**

인력 양성 사업과 산업계 연계성을 강화*하여 실전형 인재를 육성하고, 화이트해커·보안개발자 등 최고급 인력** 양성

* 시큐리티 아카데미 신설

** 화이트햇 스쿨, S-개발자 과정 신설

# 8. 부록

## 1) 2022년 정보보호산업 실태 조사 주요 통계

### 정보보호 매출액

'21년 매출액은 약 13조 8천억 원으로 전년대비 13.4% 증가하였고, 정보보안은 4조 5천억 원(16.0%↑), 물리보안은 9조 3천억 원(12.1%↑)

[표 13] 정보보호 매출액(단위 : 백만원)

| 구분 | 정보보안 | | 물리보안 | | 합계 | |
|---|---|---|---|---|---|---|
| | 매출액 | 성장률(%) | 매출액 | 성장률(%) | 매출액 | 성장률(%) |
| 2021 | 4,549,734 | +16.0 | 9,311,446 | +12.1 | 13,861,180 | +13.4 |
| 2020 | 3,921,387 | +8.4 | 8,302,865 | +9.8 | 12,224,252 | +9.3 |
| 2019 | 3,618,773 | +17.4 | 7,561,734 | +7.5 | 11,180,507 | +10.5 |

### 정보보호 수출액

'21년 수출액은 약 2조원으로 전년대비 8.5% 증가하였으며, 정보보안은 1천 5백억 원(4.8%↑), 물리보안은 1조 9천억 원(8.8%↑)

[표 14] 정보보호 수출액(단위 : 백만원)

| 구분 | 정보보안 | | 물리보안 | | 합계 | |
|---|---|---|---|---|---|---|
| | 매출액 | 성장률(%) | 매출액 | 성장률(%) | 매출액 | 성장률(%) |
| 2021 | 152,604 | +4.8 | 1,924,176 | +8.8 | 2,076,780 | +8.5 |
| 2020 | 145,592 | +18.6 | 1,767,931 | +6.7 | 1,913,523 | +7.5 |
| 2019 | 122,766 | +49.1 | 1,657,080 | +12.4 | 1,779,846 | +14.4 |

### 정보보호 기업

정보보호 기업은 총 1,517개로 보안내재화 수요 증가, 보안 제품·서비스의 수요 증대로 인해 소폭 증가(18.2%↑)

[표 15] 정보보호 기업 현황(단위 : 개)

| 구분 | 정보보안 | | 물리보안 | | 합계 | |
|---|---|---|---|---|---|---|
| | 매출액 | 성장률(%) | 매출액 | 성장률(%) | 매출액 | 성장률(%) |
| 2021 | 669 | +26.0 | 848 | +12.8 | 1,517 | +18.2 |
| 2020 | 531 | +12.3 | 752 | +21.1 | 1,283 | +17.3 |
| 2019 | 473 | +1.9 | 621 | +13.1 | 1,094 | +8.0 |

## 정보보호 인력

비대면 업무 확대 등 일반 기업들의 보안 수요 증가에 따라 정보보호 기업의 전체 종사자 수는 총 63,562명(16.2%↑)으로 증가

[표 16] 정보보호 인력 (단위 : 명)

| 구분 | 정보보안 | | 물리보안 | | 합계 | |
|---|---|---|---|---|---|---|
| | 매출액 | 성장률(%) | 매출액 | 성장률(%) | 매출액 | 성장률(%) |
| 2021 | 17,699 | +11.8 | 45,863 | +18.0 | 63,562 | +16.2 |
| 2020 | 15,832 | +18.3 | 38,874 | +18.2 | 54,706 | +18.2 |
| 2019 | 13,378 | +10.9 | 32,897 | +2.9 | 46,275 | +5.1 |

## 2) 국내외 주요기업 동향

### 국내 주요기업 동향

[표 17] 국내 주요기업 동향

| No. | 기업명 | 매출액[21] | 분야 | 제품·서비스 분야 | 최근 동향 |
|---|---|---|---|---|---|
| 1 | SK쉴더스 | -<br>(공시하지 않음) | 정보보안/<br>물리보안 | 네트워크 보안<br>엔드포인트 보안<br>클라우드 보안<br>보안용 카메라<br>물리보안 솔루션 등 | **(신기술개발)** AWS 전용 클라우드 보안 서비스 출시, 지능형 CCTV 기반 영상 모니터링 솔루션 고도화<br>**(사업영역)** MS와 빅테크 기반 미래 신성장사업 추진 MOU 및 '포스아이'와 OT 보안사업확대 MOU 체결 |
| 2 | 안랩 | 1,993억 | 정보보안 | 엔드포인트 보안<br>네트워크 보안<br>클라우드 보안<br>보안관제, 컨설팅 | **(신기술개발)** 모바일 금융 보안위협 통합관리 서비스 및 대형 제조장비 전용 보안솔루션 출시<br>**(사업영역)** '페스카로'와 자율주행/자율협력주행 분야 보안 사업 협력을 위한 MOU 체결 |
| 3 | 시큐아이 | 1,250억 | 정보보안 | 네트워크 보안<br>클라우드 보안<br>보안관제, 컨설팅 | **(신기술개발)** 고성능 침입방지시스템(IPS), AI 기반 보안위협분석 플랫폼, 취약점 분석 솔루션 출시<br>**(사업영역)** 기존 일본시장 전용 보안솔루션에서 융합보안 분야를 추가 출시하며 일본 IT 보안시장 확대 계획 |
| 4 | 이글루<br>코퍼레이션 | 906억 | 정보보안 | 보안 관제,<br>클라우드 보안<br>보안 컨설팅 | **(신기술개발)** 인공지능 기반 보안 오케이션 자동화 대응(SOAR) 기술 및 차세대 분석 엔진(SIEM) 개발<br>**(사업영역)** '21년 파이오링크를 인수하면서 클라우드 보안 사업 강화, OT보안 등 포트폴리오 다각화 |
| 5 | 윈스 | 904억 | 정보보안 | 네트워크 보안<br>엔드포인트 보안<br>클라우드 보안<br>보안관제, 컨설팅 | **(신기술개발)** AI·빅데이터를 활용한 보안관제 자동화 제품 개발하고 이를 기반으로 SaaS 서비스 출시 예정<br>**(사업영역)** 美크라우드스트라이크와 협력하여 MSP 사업 확대 및 부산 에코델타 스마트시티사업 보안 담당 |
| 6 | 한국정보<br>인증 | 556억 | 정보보안 | 인증/전자서명,<br>생체인식<br>보안시스템 | **(신기술개발)** SK쉴더스와 협업하여 제1금융권의 업무시스템에 모바일 양자OTP 서비스 적용<br>**(사업영역)** 가상자산 금융 서비스를 목표로 국내 블록체인 기업 '페어스퀘어랩'에 110억원 투자 유치 |
| 7 | 파이오링크 | 543억 | 정보보안 | 네트워크 보안<br>보안컨설팅,<br>네트워크보안 | **(신기술개발)** 오피스 보안관제 서비스 및 웹 애플리케이션 보안에 특화된 고성능 웹방화벽 출시<br>**(사업영역)** 3S소프트와 HCI 기반의 VDI, 디지털 워크스페이스 관련 사업에 협력하는 MOU 체결 |
| 8 | 이니텍 | 502억 | 정보보안/<br>물리보안 | 인증/전자서명,<br>데이터 암호화,<br>생체인식<br>보안시스템 | **(신기술개발)** 인증통합플랫폼 '이니허브'를 구독형 클라우드 인증 서비스로 확대<br>**(사업영역)** 모바일 신분증, 전자문서 플랫폼 및 결제 서비스, 타 산업분야의 다양한 플랫폼과의 연계 추진 |
| 9 | 파수 | 368억 | 정보보안 | 네트워크 보안<br>엔드포인트 보안<br>데이터 보안<br>클라우드 보안<br>보안컨설팅 등 | **(신기술개발)** AI 기반 비정형 데이터 내 개인정보검출·마스킹 솔루션 개발, 데이터 식별·분류 솔루션 확대<br>**(사업영역)** 클라우드 기반의 SaaS와 관리형 보안 서비스 영역 확대 계획 |
| 10 | 지니언스 | 314억 | 정보보안 | 네트워크 보안<br>엔드포인트 보안<br>클라우드 보안 | **(신기술개발)** EDR 솔루션에 랜섬웨어 기능 확대, 제로트러스트 보안 솔루션 출시<br>**(사업영역)** EDR 제품 중 최초로 국가정보원 보안적합성 검증제도 통과, 제로트러스트 기반 기술에 대한 특허 취득 |
| 11 | 이스트<br>소프트 | 288억 | 정보보안 | 엔드포인트 보안<br>네트워크 보안<br>데이터 보안 | **(신기술개발)** AI 버츄얼 휴먼 기술 개발, 알약 개방형 OS 및 알약 내 PC지키미 개방형 OS 출시<br>**(사업영역)** 주요 클라우드 사업자에 자사 구독형 보안 솔루션 연동 예정 |

## 글로벌 주요 기업 동향

[표 18] 글로벌 주요 기업 동향

| No. | 기업명[22] | 매출액[23] | 제품·서비스 분야 | 최근 동향 |
|---|---|---|---|---|
| 1 | Microsoft | 50,100백만불 | Microsoft Azure/ 클라우드 컴퓨팅 | MS '챗GPT 기능 추가 예정 애저 오픈AI 서비스' 출시(techm, 2023.1) |
| 2 | IBM | 14,110백만불 | IBM Osprey/ 양자 컴퓨팅 | IBM, 433 큐비트 양자 프로세서 공개(zdnet, 2022.11) |
| 3 | CISCO | 13,600백만불 | CISCO Webex Room/ 네트워크 장비 제조 | 시스코, 시스코 네트워킹 아카데미 통해 향후 10년간 'IT 인력 2,500만 양병' 발표(ciokorea, 2022.10) |
| 4 | Trellix | 2,000백만불 [24] | Trellix 플랫폼/ 확장탐지대응(XDR) | 심포니테크놀로지그룹(STG), 맥아피와 파이어아이 사업부 합쳐서 트렐릭스 탄생(보안뉴스, 2022.1) |
| 5 | Palo Alto Networks | 1,600백만불 | Prisma Cloud/ 클라우드 보안 | 팔로알토 네트웍스, AWS를 위한 관리형 차세대 방화벽 서비스 출시 (MiraKle Ahead, 2022.8) |
| 6 | Fortinet | 1,150백만불 | FortiGate/ 네트워크 보안 | 포티넷, 비정상 네트워크 행위 탐지 및 대응 'FortiNDR' 발표 (정보통신신문, 2022.9) |
| 7 | Check Point | 578백만불 | CloudGuard/ 클라우드 보안 | 체크포인트 소프트웨어, 차단 우선 접근방식 보안 제품군(Horizon) 출시 (NK경제, 2022.9) |
| 8 | Trend Micro | 408.43백만불 | Trend Micro One/ 확장탐지대응(XDR) | 트렌드 마이크로, 5G 특화망 보안 자회사 '시티원' 설립(2023.1) |
| 9 | CyberArk | 152.7백만불 | CyberArk PAM/ 권한접근관리(PAM) | 가트너, 2022 매직 쿼드런트 권한접근관리 분야 리더로 사이버아크 선정(newswire, 2022.7) |
| 10 | SentinelOne | 115.3백만불 | Singularity XDR/ 확장탐지대응(XDR) | 센티넬원, XDR 아이덴티티 확보 위해 아티보 네트웍스 인수 (보안뉴스, 2022.3) |

21) 2021년 매출액
22) 마켓앤마켓(MarketsandMarkets) 가트너 2022 매직 쿼드런트 사이버보안 분야 유망기업 상위 10개 선정
23) Trellix 제외 인베스팅닷컴(investing.com) 내 각 회사별 실적 페이지 참고
24) "맥아피 엔터프라이즈&파이어아이 통합..매출 2조 보안기업 탄생, 데이터넷, 2021.10.12

### 3) 주요 국내 진출 외국계 기업 현황

[표 19] 주요 국내 진출 외국계 기업 현황

| 세부 분야 | 외국계 기업 | 국내 총판(파트너사) | 지사 |
|---|---|---|---|
| 네트워크보안 | 시스코 | 아이넷뱅크, 영우디지털, 에스케이네트웍스, 신성씨앤에스 | O |
| | 라드웨어 | 오픈베이스, 시스원 | O |
| | 포어사이트 | 포어사이트 | O |
| | 주니퍼네트웍스 | 인성디지탈, 지에스엔시스템즈 | O |
| | 체크포인트 | 키미데이타 | O |
| | F5 | 오픈베이스 | O |
| | 아루바네트웍스 | 키미데이타, 엑스퍼넷 | O |
| | 에어로화이브 | 롯데정보통신, 한아IT | O |
| | Barracuda | 시큐와이드, 안랩 | |
| | 소포스 | 다우데이타, 소프트이즈 | O |
| | 인포블럭스 | 엑스퍼넷 | O |
| APT | 파이어아이 | KCC정보통신, 투씨에스지, 쿠퍼스시스템즈, 오픈베이스, 크로니아이티 | - |
| | 팔로알토네트웍스 | 코오롱베니트, 지에스엔시스템즈, 쿼리시스템즈, 쿠도커뮤니케이션, 안랩 | O |
| | 담발라 | 피플러스 | O |
| | 트렌드마이크로 | 시스원, 안랩 | O |
| | EMC | 에스씨지솔루션즈 | O |
| 백신 | 시만텍(노턴라이프락) | 한국정보기술안전 | O |
| | 카스퍼스키랩 | 한국카스퍼스키랩(kltec) | O |
| | 아비라 | 인섹시큐리티 | O |
| 정보유출방지 | 블루코트 | 동훈아이텍 | O |
| | 맥아피(인텔) | 비쥬얼데이타(솔루션), 시스원, 초록에스티 | O |
| 빅데이터분석 | Splunk | 엠오에스에이 | O |
| 통합보안솔루션 | IBM | 안랩, 코오롱베니트 | O |
| | 포티넷 | KCC정보통신, 이브레인테크, 한일네트웍스, 시스원, 오픈베이스, 안랩, 넷엔시큐, 쿼리시스템스, 한국정보기술안전 | O |
| 보안외장스트로리지 | DataLocker | 소프트와이드시큐리티 | O |
| DB암호화 | 보메트릭 | 롤텍 | O |
| 시스템 보안 솔루션 | 한국오라클 | 로이트지엠씨, 타임게이트 | O |
| 차세대 방화벽 | 포스포인트 | 유니포인트 | O |
| 통합보안관제 시스템 | Rapid7 | KCC정보통신, 시큐다임, 에버트러스트정보기술, 쿼리시스템스, 안랩 | O |
| 보안관리시스템 개발 | RSA | 오픈베이스, 안랩 | O |
| 네트워크 접근제어 | Pluse Secure | 지에스엔시스템즈 | O |

[표 20] 제품 품목별 동향

| 분류 | 제품 품목 | 동 향 | 주요 기업 | |
|---|---|---|---|---|
| | | | 국내 | 해외 |
| 정보 보안 | 네트워크 보안 | IoT·엣지컴퓨팅·5G 등 새로운 통신환경에 적합한 차세대 네트워크 보안 기술 확산 | 원스<br>시큐아이<br>안랩 | 시스코<br>VM웨어 |
| | 엔드포인트 보안 | 금융에서 산업 전반으로 EDR 수요 급증, 랜섬웨어 및 신·변종 악성코드 대응 솔루션 개발 | 안랩<br>이스트시큐리티<br>지니언스 | 시스코<br>트렌드마이크로 |
| | 플랫폼 보안·보안관리 | 개별 보안제품 도입감소, 플랫폼의 확장된 보안취약점 및 통합 보안 관리에 필요한 보안기술 등장 | SGA솔루션즈<br>이글루<br>SK쉴더스 | VM웨어<br>IBM<br>팔로알토 |
| | 콘텐츠·데이터 보안 | 콘텐츠데이터 암·복호화 및 스트리밍 등 실시간 데이터제공 서비스에 보안위협 식별에 AI 기술 연계 | 펜타시큐리티<br>지란지교<br>피앤피시큐어 | 시스코<br>팔로알토<br>탈레스 |
| | 클라우드 보안 | 비대면 서비스, 가상오피스 등 클라우드 기반 플랫폼 및 서비스 보안을 위한 기술개발 박차 | 시큐아이<br>안랩<br>이글루 | 트렌드마이크로<br>팔로알토 |
| 물리 보안 | 보안용 카메라 | AI, IoT 등을 카메라와 접목하여 지능형 감시환경 구축 | 이노뎁<br>인콘 | 하이크비전<br>샤오미 |
| | 보안용 저장장치 | 포맷(아날로그, 네트워크)에 상관없이 저장할 수 있는 펜타브리드 방식으로 변화 | 아이디스<br>한화테크윈 | 하이크비전<br>웨스턴디지털 |
| | 물리보안 솔루션 | 물리보안 솔루션에 ICT 기술, 정보보안을 접목하여 토탈 솔루션으로 제공 | SK쉴더스<br>에스원 | 하니웰인터내셔널<br>KNY엔터프라이즈 |
| | 출입통제 장비 | 카드를 제외하고 비접촉식 얼굴인식, 홍채인식 등으로 출입 통제 수단 다양화 | 마이즈<br>만사시스템 | 제네텍<br>FAAC |
| | 생체인식 보안시스템 | 얼굴, 지문 홍채 인식뿐만 아니라 정맥인식 및 음성·다중 인식으로 확대 | 슈프리마<br>유니온커뮤니티 | 메그비<br>이투 |

2023년 1차

# 사이버보안 대연합 보고서

탐지·공유 분과
대응·역량 분과
정책·제도 분과

KISA 한국인터넷진흥원 kisia 한국정보보호산업협회