

상반기

2024 사이버 위협 동향 보고서



과학기술정보통신부



KISA 한국인터넷진흥원

CONTENTS

상반기

2024 사이버 위협 동향 보고시



Part. 1 사이버 위협 동향

- 1 침해사고 신고 현황 04
- 2 사이버 위협 분석 07
- 3 사이버 위협 전망 13



Part. 2 전문가 컬럼

- 1 KISA 이태승 연구위원 :
'24.8.14 시행 정보통신망법의 주요 개정내용과 의의 18'
- 2 법무법인(유한) 태평양 윤주호 변호사 :
가상자산 이용자 보호법, 사업자가 고려하여야 할 사항 25
- 3 프라이빗테크놀로지 김영랑 대표 :
핵심 기술 융합과 실증 사례를 통해 살펴보는 제로 트러스트 전략 33
- 4 한남대학교 이만희 교수 :
SW 공급망 보안 가이드라인(1.0) 소개 및 발전 방향 44
- 5 S2W TALON :
랜섬웨어 그룹의 주요 동향 및 위험도 평가 62
- 6 AWS 신은수 보안기술총괄 :
안전한 클라우드 서비스 이용을 통한 정보유출 방지 75
- 7 네슨코리아 김동춘 실장 :
생성형 AI를 활용한 보안업무 혁신 84

Insights

상반기

2024년 사이버 위협 동향 보고서

Trend /

2024 상반기 사이버 위협 동향

01. 침해사고 신고 현황
02. 사이버 위협 분석
03. 사이버 위협 전망

Part. 1

01

침해사고 신고 현황

● 침해사고 신고 통계

과학기술정보통신부(한국인터넷진흥원)는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의 3(침해사고 신고 등)에 따라 민간분야의 정보통신서비스 제공자로부터 침해사고 신고를 받고 있다. 연도별 침해사고 신고 통계를 살펴보면 2022년 1,142건에서 2023년 1,277건으로 전년대비 약 12% 증가하였으며, 2022년부터 2024년 상반기까지 반기별 침해사고 신고 현황을 살펴보면 2022년 상반기 473건/ 하반기 669건이며, 2023년 상반기 664건/ 하반기 613건의 침해사고 신고가 있었다. 2024년 상반기 침해사고 신고 건수는 899건으로 전년 상반기 대비 35% 증가했는데, 이는 웹쉘(Web shell) 및 악성 URL 삽입(504건), DDoS 공격(153건) 등이 크게 증가했기 때문으로 보인다.

[표 1-1] 침해사고 신고 현황

[단위 : 건수]

구 분	2022년		2023년		2024년
	상반기	하반기	상반기	하반기	상반기
건수	473	669	664	613	899
합계	1,142		1,277		899

Trend | 사이버 위협 동향

● 유형별 침해사고 신고 통계

민간분야 침해사고는 DDoS 공격, 악성코드 감염, 서버 해킹 및 기타유형(정보유출, 스팸 문자 및 메일 발송 등) 유형으로 구분해 신고를 받고 있다. 2023년에는 DDoS 공격이 전년대비 약 2배로 급격히 증가했다. 전체 유형 중에서 서버해킹이 45.7%로 가장 높았고, 악성코드 감염이 23.5%, DDoS 공격이 16.7%, 기타 14.2% 순으로 나타났다.

2024년 상반기 유형별 침해사고 신고 통계를 살펴보면 서버 해킹이 전년 상반기 대비 58% 증가한 504건으로 가장 많은데, 이는 중소기업 등 상대적으로 보안관리가 취약한 기업들을 대상으로 홈페이지 웹 취약점을 악용한 웹쉘 공격 등이 증가한 것으로 보인다. 그 다음으로는 DDoS 공격이 153건으로 전년 상반기 대비 23% 증가한 것으로 확인되었다.

2022년부터 2024년 상반기까지 반기별 침해사고 신고 현황을 살펴보면 서버해킹이 2022년 상반기 275건/ 하반기 310건, 2023년 상반기 320건/ 하반기 263건, 2024년 상반기 504건으로 가장 많은 신고를 받은 것으로 나타났다. 그 다음으로는 DDoS 공격 신고가 2022년 상반기 48건/ 하반기 74건, 2023년 상반기 124건/ 하반기 89건, 2024년 상반기 153건으로 많았으며, 다음으로 악성코드 감염 신고가 2022년 상반기 125건/ 하반기 222건, 2023년 상반기 156건/ 하반기 144건, 2024년 상반기 106건 였다.

기타 유형별 침해사고 신고는 2022년 상반기 25건/ 하반기 63건, 2023년 상반기에는 64건/ 하반기 117건, 2024년 상반기 136건의 신고된 것으로 나타났다.

표 1-2 유형별 침해사고 신고 현황

[단위 : 건수]

구 분	연 도	2022 (상반기)		2022 (하반기)		2023 (상반기)		2023 (하반기)		2024 (상반기)	
		비율									
침해	DDoS 공격	48	10.1%	74	11.1%	124	18.7%	89	14.5%	153	17.0%
	악성코드	125	26.4%	222	33.2%	156	23.5%	144	23.5%	106	11.8%
	(랜섬웨어)	(118)	(24.9%)	(207)	(30.9%)	(134)	(20.2%)	(124)	(20.2%)	(92)	(10.2%)
사고	서버 해킹	275	58.1%	310	46.3%	320	48.2%	263	42.9%	504	56.1%
	기타	25	5.3%	63	9.4%	64	9.6%	117	19.1%	136	15.1%
합 계		473		669		664		613		899	

침해사고 신고 유형 중 악성코드 감염 통계를 살펴보면 악성코드 감염의 약 90% 이상을 랜섬웨어 신고가 차지하고 있다. 2024년 상반기 랜섬웨어 침해사고 현황을 살펴보면 92건으로 전년 상반기 대비 31% 감소한 것으로 나타나, 랜섬웨어로 인한 피해기업의 신고 건수가 2022년 이후로 감소 추세를 보이는 것으로 확인되었다. 다만, 랜섬웨어 침해사고 건수 중 제조업이 차지하는 비중은 2023년 상반기 41.8%에서 2024년

Trend | 사이버 위협 동향

상반기 47.8%로 증가한 것으로 나타났다. 다음으로 규모별 랜섬웨어 침해사고 통계를 살펴보면 중견기업은 전년 상반기 대비 12% 증가한 19건으로 나타났으며, 중소기업은 67건으로 전년 상반기 대비 39% 감소하였으나, 랜섬웨어 침해사고 건수 중 중소기업과 중견기업의 비중은 전체의 93.5%에 해당하는 것으로 나타났다.

랜섬웨어 침해사고 신고 기관(업)의 백업 여부 현황을 살펴보면 전체 백업률은 2022년 상반기 44.1%/ 하반기 40.1%, 2023년 상반기 47%/ 하반기 70.2%, 2024년 상반기 69.6%로 백업비중이 증가하고 있었고 그 중 2022년 상반기 23.1%/ 하반기 20.5%, 2023년 상반기 42.9%/ 하반기 35.6%, 2024년 상반기 40.6%가 백업까지 감염된 것으로 파악되었다.

● 업종별 침해사고 신고 통계

2024년 상반기 업종별 침해사고 신고 통계를 살펴보면 도매 및 소매업이 전년 상반기 대비 32.6% 증가한 126건으로 가장 많이 증가한 것으로 나타났으며, 업종별 침해사고 신고 비중을 살펴보면 정보통신업이 33.6%인 302건으로 가장 많이 신고한 것으로 나타났다. 이는 웹호스팅 등 IT 관련업체를 대상으로 한 침해사고가 증가하고 있으며, 도매 및 소매, 제조업에서는 보안 관리가 취약한 경우가 많아 침해사고 건수 중 차지하고 있는 비중이 높은 것으로 파악되었다. 2022년부터 2024년 상반기까지 반기별 침해사고 신고 현황을 살펴보면 정보통신업에서 2022년 상반기 201건/ 하반기 208건, 2023년 상반기 250건/ 하반기 192건, 2024년 상반기 302건으로 가장 많은 신고를 받았고, 제조업이 2022년 상반기 80건/ 하반기 165건, 2023년 상반기 130건/ 하반기 115건, 2024년 상반기 147건으로 그 다음으로 많았다. 도매 및 소매업이 2022년 상반기 60건/ 하반기 96건, 2023년 상반기 95건/ 하반기 89건, 2024년 상반기 126건이었으며, 협회 및 단체 등이 2022년 상반기 30건/ 하반기 40건, 2023년 상반기 39건/ 하반기 34건, 2024년 상반기 47건인 것으로 나타났다.

표 1-3 업종별 침해사고 신고 현황

[단위 : 건수]

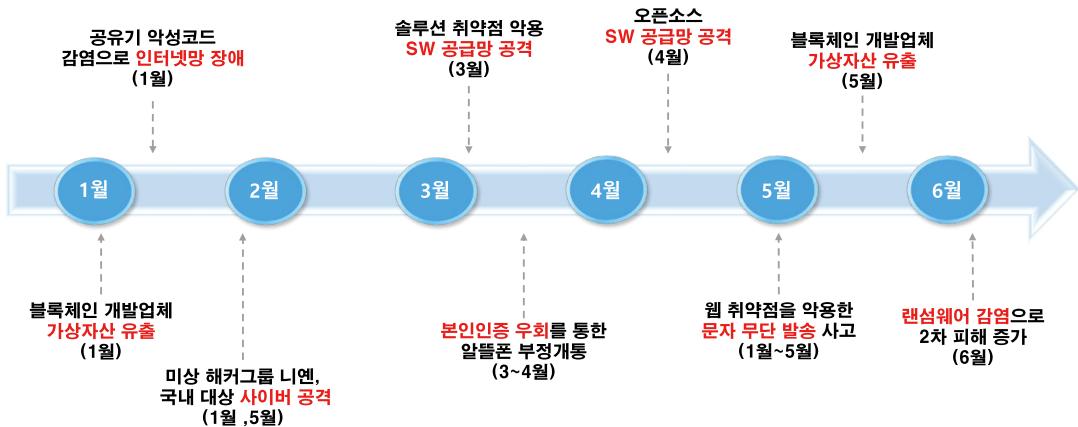
구 분	연 도	2022 (상반기)		2022 (하반기)		2023 (상반기)		2023 (하반기)		2024 (상반기)	
		비율		비율		비율		비율		비율	
정보통신업	201	42.5%		208	31.1%	250	37.7%	192	31.3%	302	33.6%
제조업	80	16.9%		165	24.7%	130	19.6%	115	18.8%	147	16.4%
도매 및 소매업	60	12.7%		96	14.4%	95	14.3%	89	14.5%	126	14.0%
협회 및 단체, 수리 및 기타 개인 서비스업	30	6.3%		40	5.9%	39	5.9%	34	5.5%	47	5.2%
기타	102	21.6%		160	23.9%	150	22.6%	183	29.9%	277	31.0%
합 계	473			669		664		613		899	

Trend | 사이버 위협 동향

Part. 1

02

사이버 위협 분석



[그림 1-1] 2024년 상반기 월별 주요 침해사고 이슈 동향

● 취약한 계정관리와 피싱메일을 통한 무차별적인 가상자산탈취공격

올해도 연초부터 국내 가상자산사업자가 침해사고를 당해 가상자산을 탈취당하는 사건이 발생했다. 그 중 대표적인 사례는 암호화폐 간 크로스 체인 플랫폼 운영 기업의 가상자산 침해사고다. 이는 국내 가상자산 침해사고 관련 사례 중 가장 큰 금액인 약 8,150만 달러(약 1,055억 원) 상당의 규모이며, 한국인터넷진흥원과 경찰청은 해당 사고를 공조하여 수사 중에 있다.

이외에도 동일 공격자의 여부는 알 수 없으나 코인 개발, 발급·운영 등 블록체인서비스 기업을 대상으로 가상자산 유출 피해 사례가 지속적으로 확인되고 있는데, 공격자는 정부기관이나 협력업체 등을 위장한 스피어 피싱을 통해 관리자 PC, 운영 서버 등을 원격제어하는 방법으로 악성코드에 감염시키고 가상자산 지갑파일 및 개인 키, 토큰 발행권한 등을 탈취하여 가상자산을 유출하였다. 이렇게 가상자산탈취 공격이 증가하고 있는 이유는 비트코인 등 가산자산 가치가 상승 등이 주요 요인으로 상반기 국내 침해사고는 전년대비 증가(4건 → 5건)했으며, 글로벌 블록체인 분석업체인 TRM Labs 조사에서도 2024년 상반기 가상자산 피해액은 전년도(약 9,000억 원) 대비 2배 증가한 약 1조 9천억 원으로 조사되었다.

Trend | 사이버 위협 동향

따라서, 기업의 보안관리자는 이와 같은 침해사고를 방지하기 위해 중요 정보를 다루는 직원들의 PC는 인터넷 접속을 최소화하거나 필요한 접속만 허용하는 등의 강화된 보안조치를 취할 필요가 있다. 또한 일부 단말장치 등이 악성코드에 감염되더라도 공격자가 중요 시스템까지 침투하지 못하도록 보안 시스템을 강화해야 하며, 자산관리 PC나 거래 운영 시스템 등 중요 자산에 대해서는 평소와 다른 비정상 행위(업무 시간 이외 접속, 대량의 네트워크 트래픽 발생, 해외 접속 등)를 상시 모니터링하는 체계를 도입할 필요가 있다. 이외에도 업무 특성상 원격제어 솔루션을 사용하는 기업이라면 다중 인증 체계 도입 및 계정 관리를 철저히 하고, 수시로 로그인 이력을 관리하여 비정상 접속 여부를 확인·관리해야 한다. 또한 조금이라도 피해가 의심될 경우 자체없이 한국인터넷진흥원에 신고하여 전문가 지원을 받아 피해가 확산되기 전에 차단할 수 있도록 사이버 침해대응 체계를 구축하고 반복적인 훈련을 통해 숙달할 필요가 있다.

더불어 침해사고 분석에서 사고 원인 확인과 사고 재발을 방지하기 위해 공격자의 침투경로를 확인하는 단계가 매우 중요하다. 그러나 보안 전문인력 확보나 예산 투자가 어려운 중소기업 등은 사내 자산관리 체계가 미흡하여 피해 자산 식별을 하지 못하는 경우가 발생하며, 시스템 로그도 제대로 저장되어 있지 않아 사고 원인 분석에 어려움을 겪는 경우가 많다. 따라서 기업에서는 내부 IT자산을 현행화하여 관리하는 보안정책을 운영하고, 중앙서버구축 등을 통해 중요 시스템의 로그는 별도로 보안 관리하는 것이 중요하다.

● 인터넷 접속 장애를 유발한 취약한 공유기 악성코드 감염 사고

올해 1월 초 지역 인터넷케이블사업자의 서비스 구역에 알 수 없는 원인으로 주말 동안 약 4시간 가량 가입자 인터넷의 접속장애가 발생했다. 이에 한국인터넷진흥원은 피해 사업자와 함께 서비스 장애 현장에 방문하여 비정상 트래픽을 유발한 가입자 공유기가 사고 원인이었음을 빠르게 밝혀내고 문제가 발생한 공유기의 신속한 교체를 통해 피해 확산을 조기에 차단했다. 이렇듯 인터넷 공유기나 NAS(Network Attached Storage) 등 IoT 기기는 미라이(Mirai) 봇 감염으로 인한 서비스 장애나 해킹 경유지 등으로 악용될 수 있으므로 기기 제조사는 개발단계에서부터 보안 내재화 개발과 판매 이후에는 지속적인 보안 패치 관리에도 관심을 가져야 하며, 사용자도 IoT 보안 인증제품 등 보안이 우수한 IoT 기기를 구매하고 활용하는 방안에 관심을 기울여야 한다.

Trend | 사이버 위협 동향

● 미상 해커그룹 니엔, 과시 목적의 취약한 국내 홈페이지 해킹 공격 지속

미상의 해커그룹 니엔은 작년에 이어 올해 상반기에도 보안에 투자가 어려운 영세한 비영리 기관이나 교육기관 등의 홈페이지를 해킹하고 내부 정보 등을 탈취하여 텔레그램을 통해 공개하는 등 자신들의 공격 실력을 과시하는 행위를 지속적으로 이어왔다.

표 1-4 한국인터넷진흥원(KISA) 침해사고신고 내 서버 해킹 건수

[단위 : 건수]

구 분	2022년		2023년		2024년
	상반기	하반기	상반기	하반기	상반기
건수	275	310	320	263	504
합계	585		583		504

이에 대비하기 위해 기업의 보안 담당자는 평소에도 인터넷에 노출된 자산의 원격접근 설정 및 계정 관리뿐만 아니라 정기적으로 취약점 점검, 보안패치를 철저히 적용해야한다. 특히 보안 패치 적용을 소홀히 할 경우 개인정보 유출, 랜섬웨어 감염, 업무 마비, 이용자 피해로 인한 고객신뢰 상실 및 경제적 손실 등의 심각한 피해가 발생할 수 있으므로 각별한 주의와 관심이 등 심각한 피해가 발생할 수 있으므로 각별한 주의가 필요하다.

위의 대응이 어려운 영세 중소기업들은 한국인터넷진흥원-보호나라(boho.or.kr)의 ▲내 서버 돌보미 ▲보안 취약점 점검 ▲ 중소기업 홈페이지 보안 강화 등 무료 정보보호 지원 서비스를 신청하여 침해사고 사전 예방을 지원받는 것이 무엇보다 중요하다.

● 중국 IT기업으로 위장한 정부지원 해킹조직의 실체

사이버 범죄를 사업 모델로 하는 단체가 계속 등장하고 있다. 2015년 이탈리아 ‘해킹팀’과 2021년 이스라엘 ‘NSO그룹’에 이어 올해는 중국의 ‘아이순(i-Soon)’이 등장했다. 아이순은 중국 쓰촨성 청두시에 기반을 둔 단체이며, 실제 쓰촨 안순(四川安洵信息技术有限公司, Sichuan Anxun Information Technology Company Limited)이라는 이름으로도 사업을 해 왔다. 이렇게 주도 면밀했던 ‘아이순’은 익명의 온라인 유저가 2024년 1월 15일, I-SOON@proton.me라는 이메일 주소를 등록하고 2월 16일, 이 이메일 계정으로 마케팅 자료, 기술 문서, 채팅 내용 등이 포함된 190MB 분량의 데이터가 깃허브에 업로드되며 세상에 공개됐다. 아직까지 내부 문건이 왜 공개되었는지 알 수 없으나 불만을 품은 내부자의 소행으로 추정되고 있으며 이를 통해 그 간 추정만 해오던 중국 정부 주도하에 조직적인 활동을 하고 있는 사이버 범죄단체의 실체가 드러났다.

● 금융대출사기 등으로 악용되는 알뜰폰 부정개통 사고

상반기에는 기존 이동통신사보다 저렴한 요금제를 제공하는 여러 알뜰폰 사업자의 비대면 개통과정에서 부정개통이 이뤄지는 사고가 있었다. 이에 과기정통부와 한국인터넷진흥원은 3월부터 전담반을 구성·운영하여 온라인으로 휴대폰 개통이 가능한 모든 알뜰폰 사업자를 대상으로 본인확인 우회 취약점에 대한 점검을 전면적으로 실시해 조치했다. 그리고 향후 사업자 보안강화를 위한 정보보호관리체계(Information Security Management System) 인증과 정보보호최고책임자(CISO) 지정 의무화 등이 포함된 종합대책을 5월 발표했다.

기업들은 자사의 서비스에 대해 자체적인 취약점 점검을 상시 수행하고, 외부 보안전문가 등을 포함한 제3자의 객관적인 보안 수준 평가를 받아 부족한 점을 보완하여 이러한 사고 발생을 미리 방지할 수 있도록 노력하여야 한다. 정보보호 전문인력이나 예산이 부족한 중소기업은 이를 위해 한국인터넷진흥원-보호나라(boho.or.kr)에서 제공하는 무료 취약점 점검이나 SW 보안 약점 진단 서비스 등을 활용할 수 있다.

● 주요 기업 내부에 침투를 위한 오픈소스 SW 공급망 해킹 위협

〈 SW 공급망 공격 사례 〉

- 공격대상 : XZ Utils(리눅스 및 윈도 5.0 이상에서 실행, 데이터 압축/해제 시 사용하는 라이브러리)
- 공격장소 : 깃허브(GitHub, 전세계 9,000만명 이상 개발자 참여, 공개SW 저장·교류·관리 지원)
- 공격방법 : 'Jia Tan'이 2022년 2월부터 XZ 리포지토리에 기여하는 등의 방법으로 원 개발자인 Lasse Collin과 신뢰를 쌓은 후 XZ Utils에 악성코드를 삽입
- 코드발견 : 올해 2월 마이크로소프트의 개발자(안드레스 프런드)가 리눅스 유ти리티에 삽입된 악성코드 발견, 발견 당시 악성코드가 포함된 버전은 널리 배포되지 않은 상태

올해 발생한 XZ Utils 사고는 전세계적으로 큰 피해가 발생 우려가 있었던 SW 공급망 공격사례다. XZ Utils은 깃허브에서 관리되는 오픈소스 프로젝트로 리눅스 운영체제에서 기본적으로 제공하는 소프트웨어이다. 해당 프로젝트는 원 개발자인 Lasse Collin이 혼자 유지해 왔는데, 2021년 1월 처음 깃허브 계정을 생성한 'Jia Tan'이 2022년 2월부터 XZ 리포지토리에 기여하는 등 개발자와 신뢰를 쌓은 후 XZ Utils에 악성코드를 삽입하였다. 해당 악성 XZ-Utils 패키지는 공식적으로 배포되기 전에 마이크로소프트 개발자에게 우연히 악용될 수 있다는 사실이 발견되어 사전에 조치함으로써 큰 피해로 확산되지 않을 수 있었다.

SW 공급망 공격은 정상적이고 안전한 소프트웨어 프로그램일 것이라는 신뢰를 악용하기에 탐지가 쉽지 않다. 기업 보안 담당자들은 이런 신뢰에 기반한 비정상 행위를 판단하려는 노력과 함께 올해 5월 정부에서 발표한

Trend | 사이버 위협 동향

'소프트웨어 공급망 보안 가이드라인'을 잘 활용하여 SBOM(SW Bill of Materials) 기반 SW 공급망 보안 관리체계 도입 등을 통해 SW 공급망 공격에 대비할 필요가 있다.

● 스미싱, 투자 유도 사기 등 서민경제를 위협하는 스팸문자 급증

피싱의 사고 유형은 공격에 악용되는 매체에 따라 스미싱(문자메시지), 메신저 피싱(메신저), 이메일 피싱(이메일), 보이스 피싱(전화), 큐싱(QR코드) 등으로 나뉜다. 특히, 스미싱은 사람을 속이는 행위를 수행하기 위해 당시의 사회적 환경과 흐름을 발빠르게 반영한다. 2020년~2021년 코로나19 대유행 기간에는 백신 접종 및 재난 지원금 지원, 택배 관련 유형 스미싱 메시지가 많았던 반면에 지난해 12월부터는 금융 정보 사칭 유형이 급증하고 있다.

최근 6월에는 KISA와 펀테크 기업을 사칭한 스미싱 유포 정황도 탐지됐다. 공격자들은 'KISA와 함께하는 이벤트'라는 제목의 문자 메시지를 통해 피싱 페이지로 연결되는 URL을 발송하고, 피해자 이름, 전화번호, 주민등록번호 등의 개인정보를 입력하도록 유도하였다.

이러한 스미싱이 급증한 것에는 다양한 원인이 있는 것으로 보고 있다. 우선 아직도 스미싱을 통해 많은 정보를 불법적으로 확보할 수 있어서 불법적 발송이 시도되고 있다는 것과 함께 이에 대응하여 스팸 간편신고 기능('23.3월), 스미싱 확인서비스 기능개선('23.10월) 등 휴대폰의 신고 기능이 강화됨으로써 신고 접수가 자연스럽게 늘어났을 것으로 보고 있다. 또한 2020년 이후 문자메시지 발송사업자 크게 증가('24.6월 기준, 1,174개)하여 문자발송 기반이 확대된 것 외에도 국내 대량문자서비스에 대한 스팸차단 및 규제를 회피하기 위해 해외 서비스를 이용한 스팸발송도 지속적으로 증가하고 있는 것도 원인 중 하나로 보고 있다. 또한 웹페이지 취약점을 악용하여 해당 서버에 저장된 개인정보를 확보한 목표를 대상으로 대량문자 발송을 할 수 있었던 것도 관련된 원인으로 볼 수 있을 것 같다. 특히 올 6월에 집중된 대량 스팸 문자발송 유형으로 부고류의 금전탈취 목적의 스미싱이나 사행성 게임 유도가 많았으며 일부 침해사고에 의한 경우도 확인되었다.

문자발송시스템에 침입하기 위해 자주 악용되는 공격 기법으로는 ▲파일 업로드 페이지에서 파일 확장자 미검증 등 취약점을 이용해 공격자가 웹셀(백도어 악성코드)을 서버에 업로드하고 실행하는 방식, ▲SQL 인젝션 취약점을 악용한 비정상 질의 공격 방식 ▲추측 가능하거나 쉬운 관리자 계정을 비밀번호 대입공격으로 획득하는 방식 등이 있다.

문자발송시스템을 개발하거나 운영하는 기업은 이러한 공격에 대비하기 위해 ▲관리자 페이지 및 계정 관리 강화 ▲파일 업로드 기능 보안 강화 ▲웹 로그 주기적 점검 및 백업 ▲주기적인 악성 파일 점검 및 제거를 수행해야 한다. 또한 서비스 이용자는 ▲문자 메시지 내 확인되지 않은 URL 링크 클릭을 주의하고, 백신이나 통신사 스팸 예방 앱을 설치해 보안을 강화하며 의심스러운 URL의 악성여부를 실시간 확인할 수 있는 'KISA 보호나라 스미싱 서비스'를 이용하는 것도 좋은 해결책이 될 수 있다.

Trend | 사이버 위협 동향

● 랜섬웨어 공격은 기본, 피해 기업 자료를 공개하는 2차 피해 증가

상반기 랜섬웨어 공격 신고는 전년 대비 약 31% 감소하였으나, 6월 들어 점차 피해가 증가하고 있다. 특히 공격자들은 보다 효과적인 금전 협박을 위해 랜섬웨어 감염 시 대기업 등 원청까지 피해가 확대되는 중소·중견 규모의 제조기업을 주요 대상으로 삼았으며, 협상 결렬 시 다크웹을 통해 피해 기업의 내부 자료를 공개하는 이중 협박을 여전히 즐겨하고 있는 것으로 분석되었다. 한국인터넷진흥원은 증가하는 랜섬웨어 사고의 피해확산을 방지하기 위해 6월 말 한국인터넷진흥원–보호나라(boho.or.kr) 누리집을 통해 기업의 외부 시스템 접속 및 계정, 백업 관리 강화 등의 내용이 포함된 보안 공지를 진행하였으며 랜섬웨어 공격은 하반기에도 계속 될 것으로 보여 랜섬웨어 공격의 주요 대상이 되고 있는 중소·중견 기업의 보안 담당자는 주요 시스템의 예방 점검과 오프라인 백업, 모니터링 강화 등 주의가 필요하다.

또한 대기업 등 원청기업은 협력회사와 랜섬웨어 보안 대응 전략을 함께 검토하여 보안 투자 유도 및 침해대응 모의훈련을 함께 진행하는 등 보다 적극적으로 협력하는 지속가능경영(Sustainability Management) 활동의 강화가 필요한 시점이라고 생각된다.

지금까지 상반기 발생했던 국내 주요 사이버 위협 동향에 대해 발생 원인과 대응책을 살펴봤다. 상반기 특히 주목해야 할 시사점은 그동안 기업을 대상으로 금전탈취 목적의 사이버 공격이 알뜰폰 부정 개통, 문자발송 대행사의 문자무단발송 등을 악용한 금융사기, 투자사기를 통해 일반 국민을 대상으로 서민 경제를 위협하고, 국민 생활 일상의 불편을 초래하는 수준까지 확대됐다는 점이다.

이에 과학기술정보통신부(한국인터넷진흥원)는 올해 8월 14일부터 시행되는 침해사고 신고 시기 및 사고 후속조치 강화 등의 내용이 포함된 개정된 정보통신망법을 통해 증가하는 기업 침해사고를 보다 적극적으로 대응하여 피해확산을 차단 할 예정이며, 한국인터넷진흥원은 증가하는 디지털 민생범죄에 적극 대응하고 선제적으로 예방하기 위해 지난 5월 16일 국민피해대응단(보이스피싱대응팀, 스미싱대응팀, 디지털위협분석팀) 신설을 골자로 조직개편을 단행하고 검·경 수사기관 및 금융, 통신사 등 유관 기관들과 더욱 유기적으로 협력하여 기업과 국문 경제의 피해 및 일상생활의 불편을 최소화 할 수 있도록 노력하고 있다.

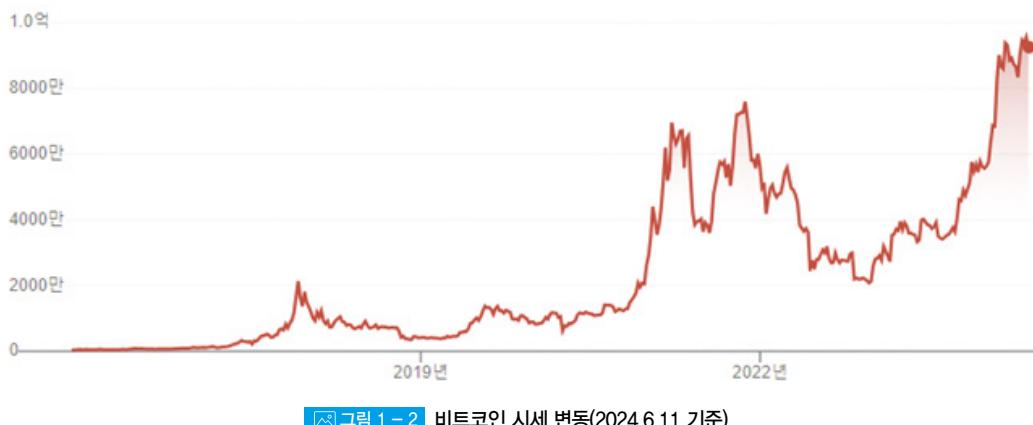
Part. 1

03

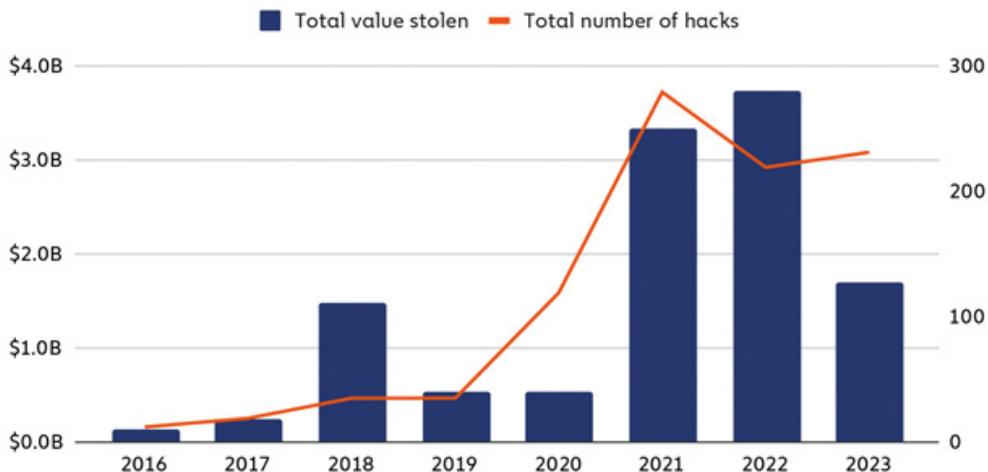
사이버 위협 전망

● 코인가치 상승에 따른 거래소 및 개인 대상 가상자산 탈취공격 지속

가상자산에 대한 해킹 공격은 가상자산의 시세와 관련된다고 볼 수 있다. 비트코인 시세 그래프와 가상자산 피해 규모를 비교해 보면 대체적으로 상당한 상관관계를 나타내고 있음을 볼 수 있다.



Trend | 사이버 위협 동향



▣ 그림 1 – 3 2016년~2023년 해킹으로 인한 피해 규모(출처: 체이널리시스, 2024.1.24)

2023년 부진했던 비트코인이 2024년에 활황세를 보이면서 역대 최고점을 찍고 있다. 이로인해 올해 가상자산 해킹이 2023년에 비해 증가할 것으로 예측된다. 지난해 하반기부터 올해 상반기까지 국내에서도 가상자산사업자에 대한 해킹이 여러 건 발생했다. 다만 국내 가상화폐와 원화 간 거래를 지원하는 대형 가상자산거래소의 경우 2021년 이후 해킹을 통한 가상자산 유출이 발생하지 않았다는 점이 눈에 띄는데 이는 사고 이후 거래소들이 보안 강화에 투자해온 결과로 볼 수 있다.

상반기에는 이런 대형 거래소보다는 상대적으로 보안이 약한 일반 가상자산사업자에 대한 사이버 공격이 집중된 만큼 하반기에도 유사한 경향이 계속될 것으로 보인다. 이러한 흐름은 하반기에도 계속될 것으로 보인다. 특히, 블록체인 브릿지나 DeFi(탈중앙화 금융) 등 대량의 가상자산거래 서비스 사업자는 전세계 해커의 공격 대상이 될 수 있으므로 항상 보안에 유의해야 한다.

비트코인 시세에 즉각 영향을 받는 것은 사업자보다 오히려 이용자에 대한 사이버위협이다. 이용자는 가상자산 보호를 위해 자신의 개인키 관리를 안전하게 하는 것이 무엇보다 중요하다. 그러므로 가상자산거래소를 이용하는 개인이라면 무엇보다 보안에 철저한 거래소를 선택하고 거래 시 소유기반 2차인증 등 개인보안 설정을 강화하여 사용하는 것이 중요하며 누구에게도 개인키 관련 정보를 알려주지 않고, 개인 키가 유출되지 않도록 유의해야 한다.

● 기업의 내부 보안 강화를 우회하기 위한 SW 공급망 공격 지속

기업 중요 자산을 공격하기 위해서는 기업 내부에 침투해 악성코드를 설치하는 최초 침투가 중요하다. 중요 자산을 많이 보유한 기업일수록 각종 보안솔루션으로 중무장한 요즘, SW 공급망은 기업 내부로 침투할 수 있는 효율적이고 효과적인 '약한 고리'다. SW 공급망 공격이 지속, 확대되는 이유다.



▣ 그림 1-4 유명오픈소스저장소(깃허브, PyPI, NPM)

공개 소프트웨어를 쓰지 않는 개발사가 거의 없을 정도로 공개 소프트웨어는 광범위하게 이용된다. 대부분의 공개 소프트웨어가 깃허브나 PyPI, NPM(Node Package Manager) 같은 공용 저장소에서 개발·관리되고 있어서 공개 소프트웨어와 공용 저장소는 밀접한 관계에 있다. 상반기에는 공용 저장소와 공개 소프트웨어를 공격해 광범위한 개발 결과물에 악성코드를 심으려는 시도가 있었다. 사용자는 많지만 공개 소프트웨어에 대한 기여자나 공용 저장소의 관리자는 적다는 특성을 악용한 것이다.

하반기에도 이러한 시도가 계속될 것으로 보인다. 이미 깃허브에는 수많은 악성 프로젝트를 통해 악성코드가 올라가 있다는 보도가 종종 나온다. 공용 저장소 및 공개 소프트웨어를 사용하는 기업과 개발자는 이러한 점에 유의해야 한다.



▣ 그림 1-5 최근 제로데이 취약점 공격에 악용되는 VPN 관련 솔루션

상반기 이반티(ivanti)의 가상사설망(VPN) 솔루션에서 심각한 제로데이 취약점이 발견돼 CISA를 비롯해 이를 사용하는 조직이 피해를 당했다. 이반티 VPN은 2021년에 세계적으로 사이버 침해를 당했던 펄스시큐어를 이반티가 인수해 만든 것으로 2021년 흐름이 되풀이되는 양상이다.

VPN은 외부 인터넷에서 기업 내부로 들어가는 지름길을 열어주므로, VPN에 보안 취약점이 있으면 기업에 치명적일 수밖에 없다. 일반적으로 보안제품은 다른 SW나 기기를 관리하기 위해 관리자 권한 같은 특수 권한을 갖고 있어서 보안제품에 취약점이 발생하면 대형 보안사고로 이어지기 쉽다. 이 점은 역으로 공격자들이 보안제품을 공급망 공격의 주요 표적으로 삼기 좋은 이유가 되기도 한다.

Trend | 사이버 위협 동향

보안제품 이외에도 네트워크 관리 SW, 자산 관리 SW 등 기업 주요 자산을 관리하는 소프트웨어는 공급망 공격의 표적이 되기 쉬우므로, 개발사(또는 공급사)와 운영사 모두 제품 보안 관리에 더욱 유의해야 한다.

● 파리 하계 올림픽, 미 대선 이슈 등을 악용한 피싱 공격 지속

2024년은 선거의 해다. 우리나라 총선(4월)을 비롯해 대만 총통 선거(1월), 인도 총선(4월), 유럽의회 선거(6월), 영국 총선(7월), 미국 대선(11월) 등 세계적으로 굵직한 선거가 진행되고 있다. 선거(특히 대통령 선거)가 있을 때는 선거 시스템 자체에 타격을 가하거나 특정인을 당선시키거나 떨어뜨리기 위한 사이버공격 뿐만 아니라 사람들이 선거와 정치·사회적 사안에 관심이 쏠리는 것을 틈타서 돈벌이로 악용하기 위한 피싱 공격이 기승을 부리기도 한다.



▣그림 1-6 프랑스 파리 하계 올림픽과 미국 대선 이슈

특히 11월에 치러질 미국 대선은 전 세계적인 관심사여서, 미국 대선 때마다 나타난 피싱 공격이 이번에도 세계 곳곳에서 나타날 것으로 보인다. 특히 생성형 AI의 발전으로 특정 후보를 사칭한 선거 캠페인이 벌어질 가능성도 있다. 국민의 올바른 판단을 저해한다는 면에서 사이버 위협이 민주주의 근간을 위협하는 상황이 될 수도 있다.

7월~8월, 열리는 파리 올림픽 역시 사이버 위협 동향에 영향을 미칠 것으로 예상된다. 올림픽의 근간이 되는 IT 시스템에 대한 공격이나 올림픽을 주제로 한 피싱 역시 상당히 많아질 것으로 예측된다.

상반기

2024년 사이비 위협 동향 보고서

Insights /

전문가 칼럼

-
- 01/ KISA 이태승 연구위원 :
‘24.8.14 시행 정보통신망법의 주요 개정내용과 의의’
 - 02/ 법무법인(유한) 태평양 윤주호 변호사 :
가상자산 이용자 보호법, 사업자가 고려하여야 할 사항
 - 03/ 프라이빗테크놀로지 김영랑 대표 :
핵심 기술 융합과 실증 사례를 통해 살펴보는 제로 트러스트 전략
 - 04/ 한남대학교 이만희 교수 :
SW 공급망 보안 가이드라인(1.0) 소개 및 발전 방향
 - 05/ S2W TALON :
랜섬웨어 그룹의 주요 동향 및 위험도 평가
 - 06/ AWS 신은수 보안기술총괄 :
안전한 클라우드 서비스 이용을 통한 정보유출 방지
 - 07/ 넥슨코리아 김동춘 실장 :
생성형 AI를 활용한 보안업무 혁신

Part. 2

01

‘24.8.14 시행 정보통신망법의 주요 개정내용과 의의

– 침해사고 신고제도 실효성 및 침해사고 후속조치 강화 –

KISA 이태승 연구위원

2024년 8월 14일 시행 예정인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(약칭 : 정보통신망법)」은 작년에 국회 발의 및 입법 절차를 거쳐 2024년 2월 13일 개정·공포되었으며, 정보통신망법 시행령도 정보통신망법의 시행일에 맞춰 개정·시행될 예정이다.

본 글은¹⁾ 8월에 시행되는 정보통신망법과 시행령의 주요 개정내용인 침해사고 신고제도 실효성 및 침해사고 후속조치 강화에 관한 사항을 소개하고([표 2-1] 참조), 시행에 맞춰 대비할 사항 및 이번 개정·시행의 의의를 살펴본다.

■ 표 2-1 주요 개정내용

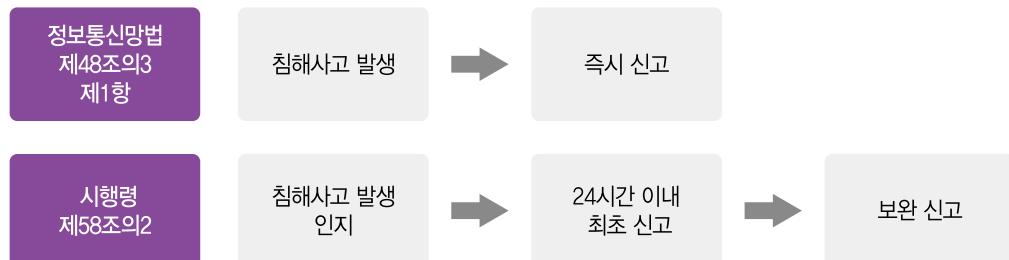
개정 정보통신망법	개정 시행령(입법예고안)
제48조의3(침해사고의 신고 등) <ul style="list-style-type: none"> (신설) 침해사고 신고의 시기·방법·절차를 시행령에서 정함 	(신설) 제58조의2(침해사고 신고의 신기, 방법 및 절차 등) <ul style="list-style-type: none"> 침해사고의 발생을 알게 된 때부터 24시간 이내 신고 서면, 전화, 인터넷 홈페이지 등의 신고 방법 최초·보완 신고절차
제48조의4(침해사고의 원인분석 등) <ul style="list-style-type: none"> (개정) 침해사고 조치 '권고' → '이행 명령' (신설) 이행 점검 (신설) 시정 명령 (신설) 이행 점검 방법·절차를 시행령에서 정함 	(신설) 제58조의3(침해사고 후속 조치의 이행여부 점검 방법 및 절차) <ul style="list-style-type: none"> 이행 점검 前 점검 계획 통지
제76조(과태료) <ul style="list-style-type: none"> (개정) 침해사고 신고의무 미이행 과태료 상향 – 1천만원 이하 → 3천만원 이하 (신설) 침해사고 조치 시정 명령 미이행 과태료 – 3천만원 이하 	제76조(과태료) <ul style="list-style-type: none"> (개정) [별표 9] 과태료의 부과기준 개정

1) 본 글은 저자의 주관적인 견해가 포함된 기고문으로 저자가 소속된 한국인터넷진흥원의 공식 견해가 아님을 알려드립니다. 그리고 법령에 대한 정확한 해석은 소관 부처에 문의하시기 바랍니다.

● 주요 개정내용

1 침해사고 신고제도 실효성 강화

이번 주요 개정내용 중 하나는 침해사고 신고 실효성 제고를 위한 침해사고 신고기준 명확화이다. 개정 전·후 조문을 비교하면, 침해사고 신고 시기·방법·절차의 필요한 사항을 시행령에서 정하도록 정보통신망법 제48조의3제4항이 신설되었으며, 이에 기반하여 시행령 제58조의2가 신설되었다. [그림 2-1]은 시행령 제58조의2의 침해사고 신고 시기·절차를 정보통신망법 제48조의3제1항에 기반하여 설명하고 있다.



[▣ 그림 2-1] 침해사고 신고 시기·절차

① 신고시기 명확화 : '알게된 때부터 24시간 이내'

이번 개정을 통해, [표2-2]의 밑줄로 표시된 조문과 같이 시행령에서 침해사고 신고시기가 명확하게 규정되었다.

[▣ 표 2-2] 침해사고 신고시기 관련 조문

개정 정보통신망법	개정 시행령(입법예고안)
<p>제48조의3(침해사고의 신고 등) ① 정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학 기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다.</p> <p>② ~ ③ < 생략 ></p> <p>④ 제1항에 따른 신고의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.</p>	<p>제58조의2(침해사고 신고의 시기, 방법 및 절차 등) ① 정보통신서비스 제공자가 법 제48조의3제1항에 따라 침해사고 신고를 하려는 경우 침해사고의 발생을 알게 된 때부터 24시간 이내에 다음 각 호의 사항을 과학기술정보통신부장관 또는 인터넷진흥원에 신고하여야 한다.</p> <p>< 이하 생략 ></p>

Insights | 전문가 칼럼

시행령의 조문을 세부적으로 살펴보면, '침해사고의 발생을 알게 된 때부터'는 침해사고 신고의무 발생시점을 명확히 나타내고 있다. 또한, '알게 된 때부터 24시간 이내'는 신고의무 준수기한을 명확히 설명하고 있으며, '어떤 일이 행하여지는 바로 그때'라는 뜻을 가진 '즉시'를 '24시간 이내'로 명확히 하였다.

참고로, 국내외 침해사고 관련 관련법의 신고 시기·방법·절차는 [표 3-3]과 같다. 개인정보보호법은 개인정보가 유출등이 되었음을 알게되었을 때부터 72시간에 신고하도록 규정하고 있으며, 미국의 연방정보보안현대화법(FISMA)에 기반한 관리예산처(OMB)의 메모랜드 M-15-01은 연방기관에게 침해사고가 침해사고 대응조직(CSIRT) 등에 도달 한 후 1시간 이내에 최초 신고를 하도록 규정하고 있다. 또한, 유럽연합의 사이버보안지침(NIS2)의 제23조는 중대한 침해사고를 알게된 때부터 24시간 이내에 최초 신고를 하도록 규정하고 있다.

또한, 이번에 시행되는 정보통신망법의 제76조는 침해사고 신고제도의 실효성 강화를 위해 침해사고 신고 미이행시 과태료를 1천만원 이하에서 3천만원 이하로 상향하여 규정하였다(정보통신망법 제76조제1항제6호의6 참조).

■ 표 2 - 3 | 국내외 관련법의 침해사고 신고 시기·방법·절차

국가	법령	신고시기	신고방법	신고절차
한국	정보통신망법 및 시행령	침해사고의 발생을 알게 된 때부터 24시간 이내 최초신고	서면, 전자우편, 전화, 인터넷 홈페이지 등	최초 및 보완신고
	개인정보 보호법 및 시행령	개인정보 유출을 알게 된 때부터 72시간 이내에 신고	서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법	최초 및 보완신고
미국	연방정보보안현대화법(FISMA)에 기반한 관리예산처(OMB) 메모랜드 M-15-01	침해사고 발견·탐지 이후 1시간 이내 신고	전자우편, 인터넷 홈페이지 등	-
유럽연합(EU)	사이버보안지침(NIS2)	중대한 침해사고를 알게된 때부터 24시간 이내 자체 없이 신고	-	최초 신고 (사고인지 24시간 이내) 보완 신고 (사고인지 72시간 이내) 중간 신고 (침해사고 접수기관 요청시) 최종 신고 (보완 신고 1개월 이내)

② 신고방법 다양화 : 서면, 전자우편, 전화, 홈페이지 등

이번에 신설되는 정보통신망법 시행령 제58조의제2항은 서면, 전자우편, 전화, 인터넷 홈페이지 등의 다양한 침해사고 신고방법을 명시함으로써 침해사고를 알게되었을 때는 언제, 어디서나 신속하게 침해사고를 신고할 수 있도록 편리성을 높였다. 참고로, 개인정보 보호법 시행령 제40조(개인정보 유출 등의 신고)는 개인정보 유출 신고방법을 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법으로 규정하고 있다.

현재 한국인터넷진흥원은 전자우편, 전화, 인터넷 홈페이지 등의 방법*으로 침해사고 신고를 받고 있다.

* 전자우편(certgen@krcert.or.kr), 전화(☎118), 보호나라 홈페이지(boho.or.kr, krcert.or.kr)

③ 최초·보완 신고 절차 마련

이번에 신설되는 정보통신망법 시행령 제58조의2제1항은 최초 신고와 보완 신고의 구분을 통해 침해사고 발생 인지시 파악된 침해사고 정보를 중심으로 신속히 신고를 하도록 규정하고 있다. 참고로, 우리나라의 개인정보보호법 시행령 제39조제2항은 개인정보 유출 신고를 최초 신고와 추가로 확인된 내용에 대한 보안 신고로 구분하고 있으며, 유럽연합의 사이버보안지침(NIS2)의 제23조는 중대한 침해사고를 알게된 때부터 24시간 이내에 최초 신고, 침해사고를 알게된 때부터 72시간이내에 보완 신고, 침해사고 신고 접수기관 요청시 중간 신고, 보완 신고 후 1개월 이내에 최종 신고를 하도록 규정하고 있다([표 2-3] 참조).

2 침해사고 후속조치 강화

이번에 시행되는 정보통신망법은 과기정통부에게 침해사고 조치 이행 명령, 이행 점검, 시정 명령에 관한 권한을 부여함으로써 침해사고 후속조치를 강화하였다. [그림 2-2]는 정보통신망법 개정 전·후의 침해사고 후속조치를 비교·설명하고 있다.

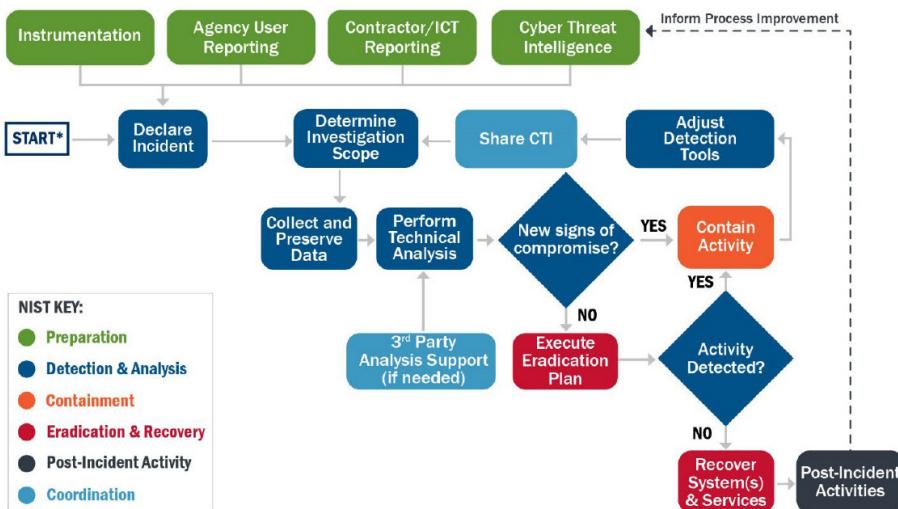
또한, 침해사고 조치 시정 명령에 대한 미이행시 3천만원 이하의 과태료를 부과하도록 정보통신망법 제76조 제1항제6호의7을 신설하였다.

Insights | 전문가 칼럼



▣ 그림 2-2 개정 전·후 침해사고 후속조치 비교

이번에 강화된 침해사고 후속조치(Post-Incident Activities)는 침해사고 재발 방지를 위해 필요한 단계로([그림 2-3] 참조), 미국의 경우, 美 사이버보안청(CISA)이 2021년 11월에 발표한 침해사고 대응 절차의 후속조치 단계는 CISA에게 연방기관의 침해사고 대응 결과를 확인할 것을 요구하고 있으며, 연방기관에게는 침해사고 대응 결과보고서 제출을 비롯하여 CISA의 자료제출 및 침해사고 조치 요구를 이행할 것을 요구하고 있다.



▣ 그림 2-3 美 CISA의 침해사고 대응 절차

● 법령에 시행에 맞춰 대비할 사항

정보통신망법의 적용 대상자인 정보통신서비스 제공자는 이번 정보통신망법과 시행령의 개정·시행에 맞춰, 앞서 설명한 주요 개정사항이 반영된 침해사고 신고 및 대응체계를 갖출 필요가 있다.

1 ‘24시간 이내’ 침해사고 신고체계 마련

주요 개정사항인 “침해사고의 발생을 알게 된 때부터 24시간 이내에 신고”에 부합하도록 침해사고 신고체계를 마련 또는 개선할 필요가 있다. 특히, 침해사고 신고는 과태료가 부과되는 의무사항이므로 「침해사고 발생 시점」, 「침해사고 발생 인지 시점」, 「침해사고 신고 시점」을 구분하여 관리하고 증빙을 남길 필요가 있다.

또한, 법령에 부합한 침해사고 신고체계를 지속성있게 관리하기 위한 방안으로 침해사고 대응 성과지표인 침해사고 발생부터 탐지까지의 평균 시간(MTTD, Mean Time to Detect), 침해사고 탐지 후 식별까지의 평균 시간(MTTI, Mean Time to Identify) 등을 침해사고 신고체계에 도입할 필요가 있다.

[표 2-4]은 해킹에 따른 개인정보 유출이 발생한 경우를 사례로 하여 신고 대응을 설명하고 있다.

■ 표 2-4 해킹에 따른 개인정보 유출 발생 시 대응 방법

신고 대상 및 시점	신고 방법	법적 근거
• 침해사고(해킹사고) 발생 인지 후 ‘24시간 이내’ 신고	• 전화(☎118) • 보호나라 홈페이지(boho.or.kr, krcert.or.kr)	정보통신망법 제48조의3
• 개인정보 유출 발생 인지 후 ‘72시간’ 이내 신고	• 전화(☎118) • 개인정보 포털(www.privacy.go.kr) 등	개인정보보호법 제34조

2 침해사고 신고 중요성에 대한 인식 제고

사이버의 특성상 침해사고를 조기에 대응하지 않을 경우 침해사고의 피해가 확산될 수가 있으므로 침해사고 신고의 중요성에 대한 인식을 제고하는 노력이 필요하며, 이와 함께 조직의 이미지 실추 우려 등의 이유로 침해사고 신고를 기피하는 인식을 바꾸기 위한 노력도 병행할 필요가 있다. 특히, 최근 사이버동향은 사이버보안 침해사고(cybersecurity incident)가 해당 기업에만 국한되지 않고, 다른 기업과 특히 고객의 알 권리와도 관련된 사항임을 강조하고 있다. 일례로, 美 증권거래위원회(SEC)는 상장사 투자에 영향을 미치는 침해사고(Material Cybersecurity Incident*)에 대해 4일 이내 신고 및 이를 공시하는 제도를 '23.12월 시행하였으며, 올해 제정 예정인 유럽연합의 사이버복원력법(Cyber Resilience Act)은 디지털제품에서 발생한 사이버보안 사고는 조직 내외로 영향을 미칠 수 있으므로 디지털제품 제조사에게 24시간 이내 규제당국 신고와 함께 사고의 영향을 받는 디지털제품 소비자에게도 통지하도록 규정하고 있다.

* 언론에 보도된 침해사고, 규제당국에 신고한 침해사고, 기업의 이미지 손상을 야기한 침해사고 등

③ ISMS-P 등에 기반한 침해사고 대응체계 마련

침해사고 신고 및 후속조치에 관한 주요 개정내용은 침해사고 대응 절차의 시작과 마지막 단계로([그림 2-3] 참고), 침해사고 대응체계 전반에 대한 관리가 요구되므로, 정보보호 및 개인정보보호 관리체계(ISMS-P) 등의 도입은 이를 위한 방안이 될 수 있다. ISMS-P는 이번 주요 개정사항을 포함하여 침해사고 예방과 대응 전반을 관리할 수 있는 보안대책 요구사항을 포함하고 있어, 이를 기반으로 조직의 침해사고 예방·대응을 체계적으로 관리하고 개선할 수 있다.

● 이번 개정·시행의 의의

'24.8.14일에 시행되는 정보통신망법과 시행령은 신속한 침해사고 대응 및 재발방지 강화를 위해 침해사고 신고제도와 후속조치의 실용성을 강화했으며, 우리나라 뿐만 아니라 미국과 유럽연합의 침해사고 관련 법령 등에도 부합하도록 개선한 측면이 있다. 따라서 이번 시행되는 정보통신망법과 시행령의 주요 개정사항은 우리나라의 사이버보안을 강화하는데 기여할 것으로 판단된다.

Part. 2

02

가상자산 이용자 보호법, 사업자가 고려하여야 할 사항

법무법인(유한) 태평양 윤주호 변호사

● 가상자산 관련 입법 동향

가상자산 및 가상자산 사업자에 대한 규제체계를 어떻게 할 것인지에 대한 구체적인 방향성을 정하기 이전에 가상자산과 관련된 자금세탁 위험 등을 해소하기 위한 목적에서 2020. 3. 24. 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」이 개정되어 개상자산에 관한 자금세탁 방지를 위한 조항들이 신설됐다.

그리고 그 이후 테라—루나 사태, 미국의 FTX 거래소 파산 사태 등 가상자산시장에서 발생한 일련의 사건들로 인하여 가상자산에 대한 투자자(이하 “이용자”)에게 막대한 피해가 발생하면서, 가상자산 이용자 보호와 불공정거래행위 규제 중심의 입법이 필요하다는 점에 관해 의견이 모아져 「가상자산 이용자 보호 등에 관한 법률」(이하 “이용자보호법”)이 2023. 7. 18. 제정되어, 2024. 7. 19부터 시행될 예정이다.

또한, 국회에서는 이용자보호법 시행 전까지 금융위원회에게 가상자산시장을 개설·운영하는 가상자산사업자가 가상자산의 발행과 유통과정에서 발생시키는 이해상충 문제를 해결하기 위한 용역 등을 진행하고, 이를 포함한 추가 입법 개선 방향을 마련해 국회에 제출하도록 하여, 향후 22대 국회에서는 가상자산에 관한 추가 법안 등이 입법화될 것으로 예상되고 있다.

본 칼럼에서는 올해 7월부터 시행되는 이용자보호법과 금융위원회가 입법예고 등을 한 이용자보호법의 하위 규정들을 중심으로 가상자산사업자가 준수해야 할 의무, 불공정거래행위, 금융위원회의 가상자산사업자에 대한 감독·검사권한 등을 살펴본다.

● 이용자보호법 및 하위규정안의 주요 규제 내용

1 가상자산 및 가상자산사업자의 정의

이용자보호법은 가상자산을 ‘경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표(그에 관한 일체의 권리를 포함한다)’라고 포괄적으로 정의를 하면서, 가상자산에 포함되지 아니하는 예외 사항들을 규정하고 있다. 이용자보호법에서 가상자산에 대한 정의 규정은 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」(이하 “특금법”)과 동일하지만, ‘한국은행이 발행하는 전자적 형태의 화폐 및 그와 관련된 서비스’를 가상자산에서 추가적으로 제외해 중앙은행 디지털화폐(CBDC)이 가상자산에 포함되지 아니하다는 점을 명확히 했고, CBDC가 조만간 발행될 가능성이 있다는 점을 추정케 하고 있다.

이와 함께 이용자보호법은 가상자산사업자를 ‘(i) 가상자산을 매도·매수(이하 “매매”라 한다)하는 행위, (ii) 가상자산을 다른 가상자산과 교환하는 행위, (iii) 가상자산을 이전하는 행위 중 대통령령으로 정하는 행위, (iv) 가상자산을 보관 또는 관리하는 행위, (v) 위 (i) 및 (ii)의 행위를 중개·알선하거나 대행하는 행위를 영업으로 하는 자’로 정의하고 있다.

한편, 이용자보호법 시행령안에서는 위 가상자산 이전의 범위에 “이용자의 요청에 따라 가상자산의 매매, 교환, 보관 또는 관리 등을 위해 하나의 가상자산주소에서 다른 가상자산주소로 가상자산을 전송하는 행위 등 가상자산을 이전하는 모든 행위”를 말한다고 규정하여, 이전의 범위를 광범위하게 정의하고 있는데, 이러한 규율은 현행 특금법과 동일하므로, 현재 가상자산사업자 범위가 이용자보호법 시행 이후에도 달라지지는 않을 것으로 전망된다.

한편, 금융규제당국에서는 가상자산의 보관업과 관련해 ‘사업자가 개인 암호키 등을 보관·저장하는 프로그램만 제공할 뿐 개인 암호키에 대한 독립적인 통제권을 가지지 않아 가상자산의 이전·보관·교환 등에 관여하지 않는 경우’에는 가상자산 보관업에 해당하지 않는다고 밝힌 바 있는데, 이러한 해석은 이용자보호법 이후에도 동일하게 적용될 것으로 판단된다.

2 이용자 자산의 보호를 위한 가상자산사업자의 의무

이용자보호법은 이용자 보호를 위해 가상자산사업자에게 (i) 고객 예치금의 예치·신탁 의무, (ii) 고객 가상자산과 동일종목·동일수량의 실질적 보관 의무, (iii) 해킹·전산장애 등 사고에 대비한 보험·공제 가입 또는 준비금 적립 의무, (iv) 가상자산 거래기록의 생성·보관 의무를 부과하고 있다.

a. 고객 예치금의 예치·신탁 의무

가상자산사업자는 이용자의 예치금을 고유재산과 분리해 은행 등 대통령령으로 정하는 공신력 있는 관리기관에 대통령령이 정하는 방법에 따라 예치 또는 신탁하여 관리하여야 하며, 가상자산사업자는 대통령령으로 정하는 경우 외에는 예치 또는 신탁한 예치금을 양도하거나 담보로 제공할 수 없다. 또한, 이렇게 관리기관에 예치된 예치금은 상계·압류(가압류 포함)의 대상이 되지 않도록 하여, 향후 가상자산사업자가 파산 등에 처하게 되었을

Insights | 전문가 칼럼

때에 가상자산사업자의 채권자가 이용자 예치금을 압류 등을 할 수 없도록 하여 이용자 보호를 충실히 하고 있다.

이용자보호법 시행령안에서는 은행 등 공신력 있는 관리기관으로 은행 및 특별법에 따른 은행으로 한정하고 있으며, 관리기관은 예치 받은 가상자산사업자의 예치금을 국채증권 또는 지방채증권의 매수, 금융기관이 지급을 보증한 채무증권의 매수 등의 방법으로만 사용하도록 하여 이용자 예치금을 보호하고 있다. 또한 이용자보호법 시행령안에서는 가상자산사업자가 사업의 전부 또는 일부를 양도하는 경우에 한하여 위 예치금을 다른 사업자에게 양도할 수 있도록 정하고 있을 뿐, 담보로 제공할 수 있는 사항을 정하지 않아, 가상자산사업자가 예치금을 담보로 운용할 수는 없는 것으로 생각된다.

b. 고객 예치 가상자산과의 분리보관의무 및 동일종류·동일수량 보관 의무

가상자산사업자는 자기 소유 가상자산과 이용자가 예치한 가상자산을 분리하여 보관하여야 하며, 이용자로부터 위탁 받은 종류와 수량의 가상자산을 실질적으로 보유하고 있어야 한다. 또한, 가상자산사업자는 콜드월렛 등을 통하여 일정 비율 이상의 가상자산을 인터넷과 분리하여 보관하여야 한다.

그리고 위 콜드월렛 보관 의무 비율에 관하여 시행령안에서는 가상자산의 경제적 가치(가상자산 종류별로 총 수량에 최근 1년간 1일 평균 원화환산액을 곱한 금액의 총합)의 100분의 70이상으로 정하고 있으나, 고시안에서는 이를 100분의 80으로 정하여, 가상자산사업자는 콜드월렛에 경제적 가치의 80%를 보관하여야 하며, 그 비율을 매월 관리하여야 한다. 금융규제당국은 위와 같이 예치 받은 가상자산 자체가 아니라 경제적 가치를 기준으로 콜드월렛 보관비율을 산정하도록 하여 이용자 보호에 충실할 뿐만 아니라, 가상자산사업자의 부담을 줄여 절충적인 입장을 취한 것으로 해석되고 있다.

한편, 이용자보호법에서는 가상자산사업자에게 동일종류, 동일수량의 가상자산을 실질적으로 보관하도록 하여, 그 해석에 따라 현재 가상자산사업자가 행하고 있는 스테이킹 서비스가 어려워질 수 있는바, 이에 대해서는 금융규제당국의 해석을 주목할 필요가 있다.

예를 들어, 현재 제공되는 스테이킹 서비스 중에서 가상자산 그 자체는 가상자산사업자가 보관을 하면서, 그 투표권을 위하여 스테이킹 하였을 때에 이를 이용자보호법 위반으로 해석할 것인지에 대해서는 논란의 여지가 있다고 보인다.

c. 해킹·전산장애 등 사고에 대비한 보험·공제 가입 또는 준비금 적립 의무

가상자산사업자는 해킹·전산장애 등에 따른 책임을 이행하기 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등의 조치를 하여야 한다. 한편, 가상자산사업자가 보험에 가입하거나 준비금을 적립하여야 하는 기준은 고시안에서 정하고 있는데, 보험의 경우에는 이용자 가상자산의 경제적 가치에서 콜드월렛에 보관하는 부분을 제외한 나머지 금액의 100분의 5에 해당하는 금액 또는 30억 원(실명확인계좌를 운영하지 않는 가상자산사업자는 5억 원) 중 큰 금액 이상을 보험금액으로 가입하여야 한다.

Insights | 전문가 칼럼

d. 가상자산 거래기록의 생성·보관 의무

가상자산사업자는 가상자산거래기록을 그 거래관계가 종료한 때부터 15년간 보존하여야 한다. 한편, 시행령안에서는 (i) 가상자산거래의 거래자 정보 및 거래대상 가상자산, (ii) 가상자산거래의 종류, 수량, 금액 및 거래 상대방에 관한 정보, (iii) 가상자산거래의 일시, 전자적 장치의 종류 및 전자적 장치를 식별할 수 있는 정보, (iv) 가상자산거래가 이루어지는 가상자산주소 등에 관한 기록을 가상자산거래기록이라고 규정하여, 가상자산주소 이외에 전자적 장치를 식별할 수 있는 정보(IP주소, 기기정보 등)도 보관을 하도록 하고 있으므로, 이 점에 주목할 필요가 있다.

③ 불공정거래의 규제

이용자보호법은 「자본시장과 금융투자업에 관한 법률」(이하 “자본시장법”)과 유사하게 미공개 중요정보 이용행위, 시세조종 행위, 부정거래 행위 등을 불공정거래행위로 규정하고, 금융위원회가 ‘해당 불공정거래행위로 얻은 이익 또는 이로 회피한 손실액의 2배 상당 내지 40억원 이하의 과징금’을 부과할 수 있도록 정하고 있다.

이용자보호법에서 금지하고 있는 불공정거래행위는 가상자산 사업 관련자가 미공개중요정보를 이용하여 거래를 하는 행위, 가상자산의 매매에 관하여 매매가 성황을 이루고 있는 듯이 잘못 알게 하거나, 그 밖에 타인에게 그릇된 판단을 하게 할 목적으로 하는 통정매매, 부정한 수단, 계획 또는 기교를 사용하는 행위 등이 포함된다.

이외에도 가상자산사업자는 자기 또는 「금융회사의 지배구조에 관한 법률 시행령」 제3조 제1항의 특수관계인이 발행한 가상자산의 매매 그 밖의 거래를 하여서는 아니된다. 기준 특금법 및 그 시행령에서는 가상자산사업자나 상법 시행령 제34조 제4호 각 호에 따른 특수관계인이 발행한 가상자산의 매매·교환을 중개·알선하거나 대행하는 행위만을 금지하고 있었으나, 이용자보호법에 따라 향후 가상자산사업자는 특수관계인이 발행하는 가상자산에 대하여 매매 등을 할 수 없도록 정하고 있는바, 이러한 점을 고려하여야 한다.

한편, 이용자보호법에서는 가상자산사업자에게 이용자의 가상자산에 관한 입금 및 출금을 정당한 사유 없이 차단하여서는 아니된다고 정하고 있다. 사실 가상자산사업자는 약관에 따라 정당한 사유 없이 이용자의 가상자산에 대한 입금 및 출금 등을 차단하지 못 하도록 정하고 있었으나, 이용자보호법에서는 이를 법률상 의무로 정하고 있으며, 나아가 약관에 따라 인정되던 정당한 사유를 보다 엄격히 정하고 있는바, 입출금을 차단하는 약관 조항을 법률의 규정에 맞추어 개정할 필요가 있다.

또한, 가상자산사업자는 가상자산의 가격이나 거래량이 비정상적으로 변동하는 이상거래를 상시 감시하고 적절한 조치를 취하여야 한다. 이러한 이상거래 탐지의 경우에 이미 가상자산사업자들이 자체적으로 진행하고 있었으나, 이용자보호법에서 이상거래 탐지 의무를 명시하고 있으며, 이상거래의 범위에 관하여 시행령안에서 규정하고 있는바, 시행령안 및 현재 금융규제당국이 마련하고 있는 이상거래탐지 모범규준에 따라 이상거래 탐지 시스템을 추가 구축하는 등의 조치를 취하여야 한다.

Insights | 전문가 칼럼

위 불공정거래에 관한 규율 체계는 자본시장법에서의 규율 체계와 유사하고, 실제 가상자산 시장에서도 불공정거래행위가 벌어지고 있다는 점에서 위와 같은 규율 체계는 필요하다고 생각된다. 다만, 가상자산 사업에 있어서의 불공정거래에 관하여 규제가 시작되는 단계인 바, 아래 몇 가지 사항에 대해서는 추가적인 논의 및 입법 개선이 필요한 것으로 생각된다.

먼저, 자본시장법에서는 시장조성에 대한 규정을 두고 있으나, 이용자보호법에서는 시장조성에 관한 사항을 규정하고 있지 아니하여, 가상자산 시장에 있어서는 여전히 시장조성행위가 허용되지 않는 것으로 해석된다. 즉, 시장조성행위는 원칙적으로 불공정거래에 해당하지만 그에 대한 예외를 통해 시장조성행위가 허용되는데, 이용자보호법에서는 시장조성행위에 대한 예외 요건을 두고 있지 아니하여 가상자산 시장에 있어서는 시장조성행위가 허용되지 않는 것으로 해석된다. 하지만, 가상자산의 경우에도 상장된 지 얼마되지 않은 가상자산의 경우에는 시장조성행위가 필요할 수 있다는 점에서 이에 대한 재검토가 필요하다고 생각된다.

두번째로 현재 정당한 사유가 없는 경우 입출금이 금지된다는 조항과 관련하여 현행 이용자보호법의 입법 방향은 타당하다. 다만, 시행령안 제11조 제3항에서 가상자산사업자로 하여금 사전에 이용자에게 가상자산에 관한 입금 및 출금이 차단될 수 있음을 안내하도록 규정하고 있는데, 이 조항의 해석에 관하여 논란이 발생할 수 있다. 즉, 시행령안 제11조 제1항의 사유들을 보면, 가상자산사업자가 사전에 입출금이 차단되는 것을 이용자에게 알릴 수 없는 사유가 포함되어 있다. 예를 들어, 정보통신망 등의 개선 등의 사유로 네트워크의 이용이 불가능한 경우를 가정해 보면, 이러한 사유는 가상자산사업자가 통제할 수 없는 사유이기 때문에 사전에 이용자에게 이로 인한 입출금 차단을 공지할 수 없다. 따라서, 시행령안 제11조 제3항은 현행과 같이 약관 등을 통해 특정 사유가 발생하는 경우 입출금이 차단될 수 있다는 점을 알리면 족하다고 해석되어야 하고, 이를 넘어서서 입출금이 차단되는 모든 구체적인 사건을 사전에 이용자에게 통지하도록 하는 것은 부당하다고 생각된다. 따라서, 시행령안 제11조 제3항에 관한 합리적인 해석이 필요하다고 할 것이다.

4 금융위원회의 감독 및 검사권 등

가상자산사업자에 대한 감독 및 검사권은 금융위원회가 가지게 된다. 검사 결과 법 위반 사항이 발견될 경우 금융위원회는 시정명령, 경고, 주의, 영업정지 등 제재처분을 할 수 있으며, 시행령안 및 고시안에서는 검사 방법, 절차, 위반의 정도에 따른 조치 사항을 정하고 있다.

한편, 가상자산사업자에 대한 검사권은 시행령안을 통해 금융감독원장에게 위탁되어 있다. 이용자보호법에 따라 가상자산사업자에 대한 검사권이 금융감독원장에게 위탁됨에 따라 특금법에 따른 검사권한과 이용자보호법에 따른 검사권한이 금융정보분석원 및 금융감독원에 각기 나누어지게 되어, 양 기관의 협의가 중요한만큼 시행령안에서는 위 두 기관이 검사 등에 관하여 상호 통지를 하도록 규정을 하고 있다.

5 가상자산 관련 위원회의 설치

이용자보호법에 따라 금융위원회는 가상자산사업자에 대한 정책 및 제도에 관한 사항의 자문을 위하여 가상자산 관련 위원회를 설치·운영할 수 있다. 위원회의 구성 및 운영 등에 관하여 필요한 사항은 시행령안에서 정하고 있는데, 시행령안에 따르면, 가상자산사업자에 대한 정책 및 제도에 관한 사항을 자문하기 위한 가상자산위원회를 둘 수 있고, 그 위원은 15명 이내의 위원으로 구성되며, 위원장은 금융위원회 부위원장이 당연직으로 수행하게 된다.

6 한국은행의 자료제출 요구권

이용자보호법은 가상자산이 실물 금융에 영향을 미칠 수 있다고 보아, 한국은행에게 금융통화위원회가 가상자산 거래와 관련하여 통화신용정책의 수행, 금융안정 및 지급결제제도의 원활한 운영을 위하여 필요하다고 인정하는 경우에는 가상자산사업자에 대하여 자료제출을 요구할 수 있는 권한을 부여하고 있다.

7 집단소송

이용자보호법 발의 단계에서는 이용자보호법에 가상자산의 불공정거래행위로 인하여 다수인에게 피해가 발생한 경우 그 중의 1인 또는 수인(數人)이 대표당사자가 되어 손해배상청구소송(이하 “집단소송”)을 제기할 수 있도록 정하였으나, 이는 추후 국회 논의 과정에서 제외되었다. 다만, 가상자산의 경우에도 불특정다수 이용자의 손해가 발생할 가능성이 높으므로, 가상자산 이용자 보호에 관해서도 집단소송 제도가 도입될 가능성은 항상 열려 있다고 판단된다.

● 부대의견

앞서 살펴본 바와 같이 국회에서는 이용자 보호를 중심으로 한 1단계 법안(이용자보호법)에 대한 합의뿐만 아니라, 가상자산 발행, 공시 등 시장 질서 규제를 보완하는 2단계 입법을 준비하기 위한 의무를 부여하는 등 다양한 부대의견을 채택했다.

부대의견에 따라 금융위원회는 이후 (i) 스테이블 코인(증권형 토큰, 유틸리티 토큰 등을 포함)에 대한 규율체계를 확립하며, (ii) 사고 발생시 「전자금융거래법」과 유사한 입증책임 전환규정 및 (iii) 자기 또는 특수관계인이 발행한 가상자산의 거래제한 관련된 대통령령 제정을 위해 연구용역 등을 추진하고 개선방안을 검토하여 국회 정무위원회에 보고하여야 하며, 이에 따라 금융위원회는 지난 5월 관련 사항을 국회에 보고했다.

금융위원회에서 국회에 보고한 내용으로는 이해관계가 크고 구조적 분리가 용이한 보관·관리업의 가상자산 거래소로부터의 분리, 통합공시시스템을 통한 공시 관련 규제 도입 등이 포함된 것으로 알려져 있으나, 아직까지 구체적인 내용이 알려지지는 않았다.

● 사업자가 고려하여야 할 사항

이용자보호법은 가상자산사업자에게 특정 행위 준칙 등을 부과하고 있으므로, 관련 규정들을 내재화하고, 그에 대한 감독 체계를 만들어야 한다. 관련해 가상자산사업자들이 준비해야 할 사항을 정리하면 아래와 같다.

1 내규 및 계약서 등 정비

a. 예치금 및 가상자산 보호를 위한 조치

예치금에 대한 금융기관 예치 및 가상자산 보호를 위한 콜드월렛 도입 의무 등이 법률상 의무가 됨에 따라 이를 위한 내부 규정을 정비하여야 한다.

실명확인계좌를 운용하고 있는 가상자산사업자들은 이미 은행과 예치 계약을 체결하고 있으므로, 큰 문제는 없을 것으로 생각되나, 은행과의 예치 계약에서 은행이 예치금의 사용 범위를 어떻게 정하고 있는지를 살펴, 이용자보호법에 따른 안전한 방법으로 예치금을 운용할 예정인지 확인하여야 한다. 또한, 현재 은행에 대한 예치 계약에서 가상자산사업자의 채무자가 은행에 대한 예치금에 관하여 압류 등을 금지하고 있는지도 살펴볼 필요가 있다. 물론, 위와 같은 조항들은 법상 의무로 규정되어 있는 만큼 계약서에 추가로 명시할 필요가 없다고 볼 수도 있지만, 계약 등을 통해 가상자산사업자의 의무 이행을 보다 철저히 준수하는 방안을 고려할 필요가 있다.

한편, 콜드월렛 기준과 관련해서 현재 고시안에서는 경제적 가치의 80% 이상을 보관하도록 정하고 있으므로, 이 기준을 맞출 수 있도록 콜드월렛 운영 기준을 재정리할 필요가 있다. 다만, 가상자산을 종류별로 보관할 필요가 없다고는 하지만, 월별 보관 기준 판단 시 어느 시점의 가상자산 가액을 기준으로 보관하면 되는지 불명확한 부분이 있어서 이에 대한 금융감독기관에 유권해석 등을 잘 살펴볼 필요가 있다.

또한, 콜드월렛의 운용 방법에 관하여 아직까지 표준화된 운용 방법이 정하여지지 아니하였으므로, 개별 가상자산사업자는 콜드월렛 운용 방법에 관하여 금융감독원과 충분히 상의할 필요가 있다.

나아가, 위와 같은 사항을 내규를 통해 작성하여 이후 금융감독기관의 검사 등에 대비할 필요가 있다. 가상자산 사업자들은 현재에도 내규를 통해 운영지침 등을 정하고 있으나, 이용자보호법에 따른 추가적인 의무들이 발생하였는바, 이를 현행 내규에 반영할 필요가 있다.

b. 불공정거래행위 관련

불공정거래가 일어나는 구체적인 양태들은 모두 다르기 때문에 불공정거래행위에 대한 세세한 지침을 작성하는 것은 어려운 일이라고 판단된다. 다만, 가상자산사업자들은 이용자보호법에 따른 불공정행위를 금지하는 내규를 1차적으로 작성하고, 그에 대한 임직원 교육들을 실시하면서, 불공정행위에 대한 경계심을 갖도록 할 필요가 있다. 그리고 실제 사업 과정에서 벌어지는 불공정행위 유형 또는 불공정행위로 이어질 수 있는 행위 유형 등을 모니터링하면서, 추가적인 세부지침을 작성하고, 이를 지속적으로 교육할 필요가 있다.

Insights | 전문가 칼럼

c. 특수관계인 발행의 가상자산 매매 등 금지 관련

특금법에서도 특수관계인 발행의 가상자산 매매 중개 등을 금지하고 있었기 때문에, 가상자산사업자들은 내부적으로 특수관계인 발행의 가상자산을 체크하는 기능을 이미 두고 있는 것으로 알려져 있다.

만약 특수관계인이 발행하는 가상자산에 대한 관리체계를 마련해 두지 않는 사업자라면, (1) 특수관계인 판단에 대한 내규 마련, (2) 내규에 따른 특수관계인 목록 정리를 하여 특수관계인이 발행한 가상자산이 거래되는 것을 방지할 필요가 있다. 나아가, 가상자산거래소 상장 당시 특수관계인이 발행하지 않은 가상자산이라는 점에 관하여 확약서 등을 제출받아 특수관계인이 발행하는 가상자산의 거래 등을 금지하여야 할 것으로 생각된다.

2 시스템 개선 등

a. 거래 기록 보관 관련

가상자산사업자들은 거래기록 등을 이미 보관하고 있으나, 이용자보호법에서는 그 보관기관을 일률적으로 15년으로 정하였는바, 현재 시스템을 검토하여 거래기록이 15년 이상 보관되도록 클리어링 기간 등을 재설정할 필요가 있다.

b. 이상거래 탐지 관련

가상자산사업자들은 이미 자금세탁방지 시스템 등을 구현하면서 이상거래 등을 탐지할 수 있는 시스템을 구축하고 있는 것으로 알려져 있다. 그러나 이용자보호법에서 정하고 있는 이상거래는 불공정거래와 관련되어 있어, 거래 모니터링에 있어서 로직 등을 업데이트 할 필요가 있다고 보인다.

또한, 금융감독원에서는 이상거래 탐지에 관한 모델 등을 작성하여 가상자산사업자에게 배포한 바 있으므로, 가상자산사업자들은 자신의 사업 모델에 맞추어 이상거래 탐지에 관한 로직 등을 업데이트 할 필요가 있다.

참고 이용자보호법에 따른 제재

행위 유형	제재
고객 예치금의 예치·신탁 의무 위반	
고객 예치 가상자산과의 분리보관의무 및 동일종목·동일 수량 보관 의무 위반	1억원 이하의 과태료
해킹·전산장애 등 사고에 대비한 보험·공제 가입 또는 준 비금 적립 의무 위반	
가상자산 거래기록의 생성·보관 의무	
미공개 중요정보 이용행위	위반행위로 얻은 이익 또는 이로 회피한 손실액의 2배
시세조종 행위	상당 내지 40억원 이하의 과징금
부정거래 행위	1년 이상의 유기징역 또는 위반행위로 얻은 이익 또는 회피한 손실액의 3배 이상 5배 이하 벌금 집단소송의 대상
자기 또는 특수관계인이 발행한 가상자산의 매매 등	10년 이하의 유기징역 또는 위반행위로 얻은 이익 또는 회피한 손실액의 3배 이상 5배 이하 벌금 / 다만, 손해액이 산정되지 곤란한 경우 등은 5억원 이하의 벌금
이상거래 감시의무	1억원 이하의 과태료

Part. 2

03

핵심 기술 융합과 실증 사례를 통해 살펴보는 제로 트러스트 전략

프라이빗테크놀로지 김영랑 대표

● 제로 트러스트 보안 모델의 필요성

기존 경계 기반 보안 모델의 경우 내부 네트워크를 신뢰할 수 있는 영역으로 정의하여, 외부로부터의 접근만을 차단하는 데 발전되어 왔다. 하지만 현재의 IT 환경은 Cloud, Mobile, IoT 등의 기술로 인해 급격히 변화되고 있으며, 이에 따른 기존 보안 체계의 한계가 드러나고 있다.

- 기업 업무 환경에 많은 변화가 생겨 경계의 개념이 점점 더 모호해지고 있다. 재택근무와 원격 접속, BYOD 등의 다양한 업무 환경에서 기업의 자산에 접근하는 사용자와 장치의 종류가 매우 다양하며, 이 다양한 사용자와 장치들을 모두 통제하는 것은 매우 어려워졌다.
- 내부 사용자에 의한 위협이 증가하고 있다. 내부 네트워크에 대한 과도한 신뢰로 인해 내부 사용자의 악의적 행위 또는 실수로 인한 데이터 유출, 시스템 장애 등의 사고 위험이 점점 높아지고 있다.
- 지능화되는 사이버 공격을 막기가 어려워졌다. 악성코드, APT 등 고도화된 최신 공격은 경계 보안 체계를 우회해 내부 네트워크에 침투하고, 장기간 잠복하면서 중요 정보를 유출시키는 사례가 늘고 있다.

이에 따라 “Never trust, always verify”의 원칙하에 모든 사용자, 디바이스, 애플리케이션을 신뢰할 수 없는 것으로 정의하고, 접근 시마다 신원을 검증하고 위험을 평가해 신뢰할 수 없는 것의 접근을 통제하는 제로 트러스트 보안 모델로의 전환이 시급한 과제로 대두되고 있다.

특히 코로나19로 인한 비대면 업무 환경의 확산, 클라우드 및 SaaS 사용의 가속화, 공급망을 통한 공격행위 증가 등으로 인해 제로트러스트 도입의 필요성은 더욱 높아지고 있다.

미국 바이든 행정부는 사이버 보안 행정명령을 통해 연방기관의 제로 트러스트 도입을 의무화했으며, 가트너는 2025년까지 기업의 절반 이상이 제로 트러스트를 도입할 것으로 전망하고 있다.

이제 제로 트러스트는 선택이 아닌 필수가 되었다. 비즈니스와 IT 환경의 변화에 맞는 보안 체계와 정책의 진화가 필요한 시점이다. 나아가 제로트러스트는 단순히 보안성 향상의 목적을 넘어, 클라우드 전환의 가속화, 업무 효율성 제고, 보안 규제 준수 등 기업의 디지털 혁신을 뒷받침하는 전략적 수단이 될 것이다.

● 제로 트러스트 성숙도 모델

제로 트러스트를 성공적으로 구현하기 위해서는 체계적인 이행 절차와 통제 항목이 필요하다. 이를 위해서 미국 국립표준기술연구소(NIST)와 사이버보안인프라보안청(CISA) 등의 기관에서는 제로 트러스트 아키텍처와 제로 트러스트 성숙도 모델을 정의하여 수립했다.

제로 트러스트 성숙도 모델은 조직의 제로 트러스트 구현 수준을 평가하고 로드맵을 제시하는 프레임워크이다. 조직의 제로 트러스트 도입 수준을 ‘전통(Traditional)’, ‘초기(Advanced)’, ‘고도화(Advanced)’, ‘최적화(Optimal)’의 4단계로 구분하고, 각 단계에서 총족되어야 할 요건들을 정의하고 있다.

성숙도 모델의 핵심 영역으로는 ‘사용자(User)’, ‘디바이스(Device)’, ‘네트워크(Network)’, ‘애플리케이션과 워크로드(Application and Workload)’, ‘데이터(Data)’, ‘가시성과 분석(Visibility and Analytics)’ 등 6가지로 구성된다.

사용자 영역에서는 강화된 인증, 역할 기반 접근 통제(RBAC), 최소 권한 부여 등의 항목을 다루고 있다. 디바이스 영역에서는 디바이스의 통제, 지속적인 모니터링과 대응 등을 포함하고 있다. 네트워크 영역에서는 네트워크 세분화, 암호화, 소프트웨어 정의 경계 적용 등을 요구하고 있다.

애플리케이션과 워크로드 영역에서는 접근 통제, DevSecOps 등 보안을 내재화한 개발 및 운영 방안을 제시하고 있다. 데이터 영역은 민감 데이터 식별 및 분류, 데이터 보호 정책 수립을 강조한다. 가시성과 분석은 위험 평가, 로깅과 모니터링 자동화 등을 통해 실시간 상황 인식과 대응 역량을 높이는 데 방점을 두고 있다.

성숙도 모델에서 제시하는 통제 항목을 얼마나 총족하는지에 따라서 조직의 제로 트러스트 구현 수준이 ‘전통’에서 ‘최적화’로 발전되게 된다. 조직은 현재 자신의 보안 체계가 어느 단계에 있는지를 객관적으로 평가하고, 업무 환경과 위험 특성에 맞는 목표 수준을 설정할 수 있다.

제로 트러스트는 장기적 관점에서 단계적으로 접근을 해야 한다. 따라서 성숙도 모델의 통제 항목을 일시에 모두 적용하기보다는, 우선순위를 정해 로드맵에 따라서 점진적으로 안정적인 고도화를 해 나가는 것이 바람직하다.

이때 기술적 방안 끝지않게 제로 트러스트 원칙을 조직 문화에 스며들 수 있도록 내재화하고 구성원의 인식을 개선하는 추가적인 거버넌스 체계 수립이 병행되어야 한다. 제로 트러스트는 기술적 솔루션이 아닌 전략이자 체계이며, 지속적인 개선 활동을 통해서 완성도를 높여갈 수 있기 때문이다.

제로 트러스트 성숙도 모델은 기업의 제로 트러스트 여정에 있어 나침반과 같은 역할을 하고 있다. 현 위치를 객관적으로 파악하고, 발전할 방향을 설정하며, 효과적인 경로를 선택하는데 도움이 된다. 이를 토대로 자사만의 제로 트러스트 전략과 로드맵을 수립하는 것이 제로 트러스트 적용 성공의 관건이 될 것이다.

● 제로 트러스트 성숙도 모델 준수를 위한 핵심 기술

제로 트러스트는 단순한 기술적 솔루션이 아닌 보안 개념과 철학이자 아키텍처이다. 여러 보안 기술과 절차가 유기적으로 결합되어야만 완성될 수 있다. 본 장에서는 제로 트러스트의 성숙도 모델 준수에 있어 필수 3대 핵심 기술인 소프트웨어 정의 경계(SDP), 강화된 신원 및 접근 관리(EIG), 마이크로 세그먼테이션에 대해 알아보고자 한다.

1 소프트웨어 정의 경계(SDP)

a. SDP의 정의와 주요 기능

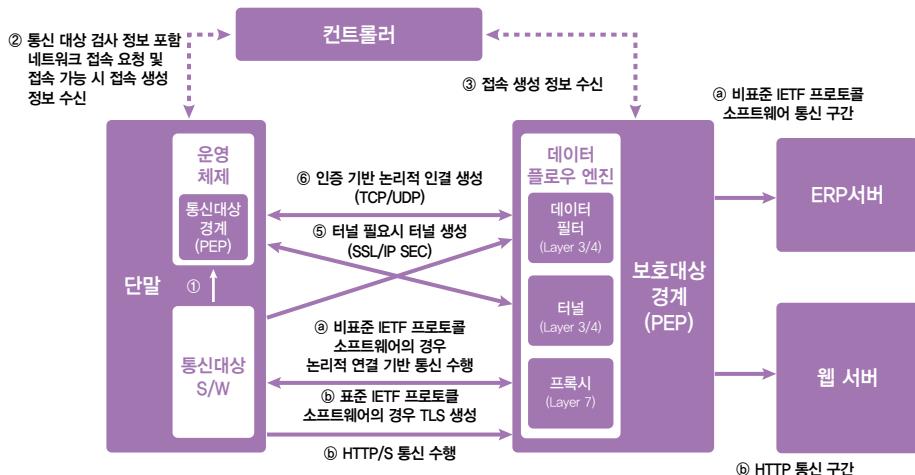
SDP는 네트워크 접근 제어를 소프트웨어 기반으로 동적으로 구현하는 보안 모델이다. 전통적인 네트워크 경계 방어와 달리, 애플리케이션 계층에서 사용자와 디바이스의 신원을 확인하고 접근을 허용한다. SDP는 제어 플레인과 데이터 플레인을 분리해, 인증 및 권한 부여 이전에는 보호 대상 서비스 자산을 숨기고(Stealth) 외부 공격 표면을 최소화한다. 사용자의 접속이 허가되면 앱과 데이터에 대한 안전한 데이터 채널을 동적으로 생성한다. 이를 통해 “Never trust, always verify” 원칙을 네트워크 레벨에서 구현할 수 있다.

b. SDP의 제로 트러스트 성숙도 모델 준수 항목

SDP는 제로 트러스트 성숙도 모델의 ‘네트워크’, ‘애플리케이션과 워크로드’ 영역에서 요구되는 여러 통제 항목의 충족을 도와준다. SDP를 통해 기업은 외부 접근뿐만 아니라 내부 트래픽까지 세분화하고, 최소 권한 접근 정책을 실행하며, 암호화를 적용함으로써 제로 트러스트 원칙을 네트워크 전반에 적용할 수 있다.

2 강화된 신원 및 접근 관리(EIG)

a. EIG의 정의와 주요 기능



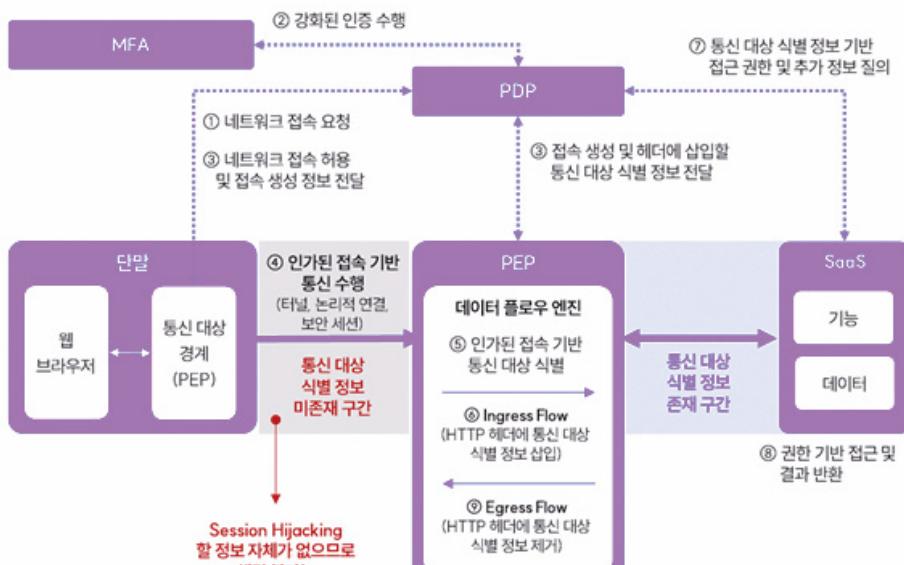
[그림 2-4] SDP 모델

Insights | 전문가 칼럼

EIG는 사용자뿐만 아니라 디바이스, 애플리케이션 등 모든 액세스 주체의 신원을 철저하게 확인하고 접근을 통제하는 기술이다. 전통적인 IAM이 사용자 중심이었다면, EIG는 모든 개체를 정책 수립과 시행의 주체로 간주한다. EIG의 핵심기능은 지속적 신원 검증, 위험 기반 인증(Risk-based authentication), 최소 권한 부여(Least privilege)이다. 접근 요청 시 다양한 속성 정보를 종합해 신뢰 점수를 산정하고, 위험이 높은 접근은 MFA 등의 강화된 인증을 요구한다. 사용자의 역할과 개체 속성을 기반으로 하여 최소한의 리소스로의 접근 권한만을 부여하여 횡적 이동을 차단한다.

b. EIG의 제로 트러스트 성숙도 모델 준수 항목

EIG는 제로 트러스트 성숙도 모델의 ‘사용자’ 영역에서 요구하는 대부분의 통제 항목을 충족시킨다. 단순히 사용자 식별 영역을 넘어 상황 정보 기반의 적응적 인증을 제공하고, 식별 정보의 노출에도 안전한 인프라를 구현할 수 있게 해준다.



▣ 그림 2-5 EIG 모델

3 마이크로세그먼테이션

a. 정의와 주요 기능

マイクロ세그먼테이션은 워크로드 단위로 네트워크를 논리적으로 분할해, 초 세분화된 접근 통제 정책을 적용하는 기술이다. 애플리케이션 정책을 구성하고 프로세스 간 통신 흐름을 시각화해, 화이트리스트 기반의 제어를 수행한다.

マイクロ세그먼테이션은 전통적인 네트워크 세분화의 한계를 극복, 클라우드와 데이터센터 접근의 동적인 환경에 유연하게 적용할 수 있다. 이를 통해 비인가 접근과 횡적 이동을 차단하고, 내부 위협의 영향 범위를 최소화할 수 있다.

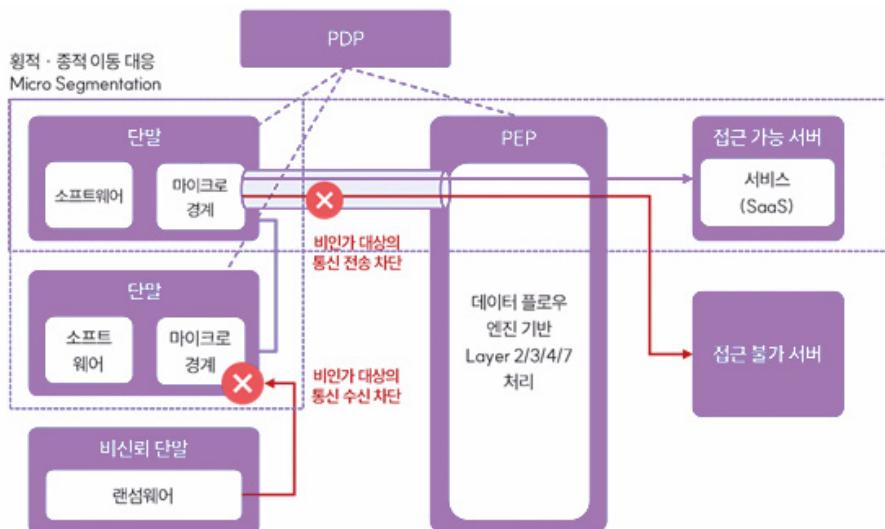


그림 2-6 마이크로세그멘테이션 모델

b. 제로 트러스트 성숙도 모델 준수 항목

マイクロ세그먼테이션은 '네트워크', '애플리케이션과 워크로드' 영역의 제로 트러스트 성숙도 향상에 직접적인 도움을 주게 된다. 최소 권한 접근을 애플리케이션의 프로세스 수준까지 적용하고, 이상 트래픽과 비정상 행위를 식별할 수 있는 가시성을 제공한다.

SDP, EIG, 마이크로세그먼테이션은 상호 보완적으로 융합되어 제로트러스트 아키텍처를 구현하게 된다. SDP가 초기 접근을 통제하고 공격 표면을 줄이는 역할을 한다면, EIG는 모든 개체의 신원을 지속적으로 검증하고 최소 권한을 부여한다. 마이크로세그먼테이션은 논리적 연결 이후에도 초 세분화된 제어를 통해서 무단 침입과 같은 무 권한자의 접근과 위협의 확산을 차단한다.

제로트러스트는 보안 제품을 도입한다고 완성되는 것이 아닐 것이다. 기업은 자신의 제로트러스트 성숙도 목표에 맞는 기술을 선별하고, 이를 유기적으로 연계해 일관된 보안 정책 시행이 가능한 제로트러스트 아키텍처를 설계해야 한다. SDP, EIG, 마이크로세그먼테이션은 그 여정의 시작점이 될 것이다.

● 제로 트러스트 원천 기술 통합 솔루션 실증 사례

제로 트러스트 핵심 기술을 단일 제품으로 통합한 솔루션이 실제 수요 기관에 적용되어 어떤 성과를 거두었는지 살펴보는 것은 의미 있는 일이다. 여기서는 SDP, EIG, 마이크로세그먼테이션 기술이 융합된 제품을 적용한 수요 기관의 사례를 통해 통합 솔루션의 효과성을 기증해 보고자 한다.

1 한국주택금융공사

a. 제로 트러스트 실증 배경 및 목표

한국주택금융공사는 중요 금융 정보를 다루는 공공기관으로서 강력한 보안이 요구된다. 그러나 기존의 물리적 망분리 환경에서는 외부 위협에 대응하는 것과 동시에 업무 연속성을 보장하는 것이 쉽지 않았다. 또한 경계 보안 솔루션만으로는 내부 네트워크를 통한 위험 확산을 효과적으로 통제하기 어려웠다. 이에 업무 환경을 저해하지 않으면서도 내외부의 위험으로부터 핵심 자산을 보호할 수 있는 제로 트러스트 보안 모델에 관심을 두고 실증 사업에 참여, 특히 비인가 단말, 사용자, 소프트웨어 등에 대한 가시성을 확보하고 세분화된 통제를 적용하는 것을 주요 목표로 삼았다.

나아가 기존 경계 보안 모델 및 불완전한 제로 트러스트 모델의 한계를 객관적으로 입증하기 위해, 자체적인 침투 시나리오를 도출하고 검증하는 과정을 포함했다. 이를 위해 제로 트러스트 분야 전문가들로 자문 조직을 구성하고, 모의 침투 전문 조직과 협업해 취약점 분석과 침투 테스트를 수행했다.

b. 기술 적용 내용

우선 SDP 기술을 통해 애플리케이션 접근 경로를 보호하고, 보안 에이전트를 통해 비인가 접근을 원천 차단했다. 이를 통해 네트워크 수준에서 접근 통제 정책을 동적으로 적용하고, 인가되지 않은 사용자와 디바이스의 접속을 사전에 차단할 수 있게 됐다.

또한, 업무 시스템 내 서버와 워크로드 간의 불필요한 통신 경로를 파악하고 이를 제한하기 위해 마이크로세그먼테이션을 구현했다. 세부 애플리케이션과 프로세스 수준에서 통신 흐름을 가시화하고 최소 권한 원칙에 따라 통신을 통제함으로써, 내부 위협의 이동을 최소화할 수 있었다.

SDP와 마이크로세그먼테이션은 단일 정책 하에서 통합 적용됐다. 이를 통해 사용자, 단말, 워크로드를 아우르는 제로 트러스트 접근 통제 체계를 일관되게 구현할 수 있었으며, 한층 강화된 보안과 운영 효율성을 동시에 확보할 수 있었다.

이번 실증 사업에서 구성된 전문 자문단과 모의 침투 조직은 구현된 제로 트러스트 아키텍처를 대상으로 철저한 검증을 수행했다. 이들은 사전에 도출된 다양한 위협 시나리오 18개 항목을 바탕으로 실제 공격을 모사하고, 각 단계별 방어 체계의 효과성을 점검했다. 이 과정에서 드러난 미흡한 부분은 지속적으로 보완해 나갔다.

Insights | 전문가 칼럼

c. 실증 결과 및 성과

제로 트러스트 보안 모델 적용 후, 한국주택금융공사는 업무 연속성을 유지하면서도 보다 강력한 보안을 구현할 수 있게 됐다. SDP 적용으로 비인가 사용자와 단말의 접근이 사전에 차단됐고, 마이크로세그먼테이션을 통해 내부 위협 확산이 억제됐다.

침투 테스트 결과, 기존 경계 보안 모델 대비 제로 트러스트 아키텍처가 내외부의 다양한 위협에 보다 효과적으로 대응할 수 있음을 입증됐다. 불완전한 제로 트러스트 구현 시 간과될 수 있는 취약점도 선제적으로 도출하고 대응함으로써, 강건한 보안 체계를 확립할 수 있었다.

나아가 물리적 망분리로 인한 업무 불편이 상당 부분 해소됐다. 외부 협력사의 원격 접속 역시 세분화된 접근 권한 하에 안전하게 이뤄질 수 있었다. 이는 업무 민첩성 향상과 보안성 증대, 운영 효율로 이어졌다.

한국주택금융공사의 사례는 물리적 망분리의 한계를 극복하고, 비인가 자산에 대한 통제를 강화하며, 내외부 위협에 선제적으로 대응할 수 있는 제로 트러스트 모델의 효과성을 입증했다. 특히 단순 적용을 넘어 실전 모의 침투까지 수행함으로써 그 완성도를 높였다는 점에서 의의가 크다.

이는 단순히 규제 준수를 위한 보안이 아닌, 비즈니스 연속성과 혁신을 지원하는 전략적 보안으로 전환하는 데 있어 제로 트러스트가 핵심 역할을 할 수 있음을 보여주는 좋은 사례라 할 수 있다.

2 한국지능정보사회진흥원

a. 제로 트러스트 실증 배경 및 목표

한국지능정보사회진흥원(NIA)은 안전한 지능정보사회 구현을 위해 제로 트러스트 기반의 선제적 보안 대책 마련이 필요했다. 특히, 국내 보안 규제상 공공기관이 민간 클라우드를 사용하기 위해서는 CC 인증 획득과 가상사설망(VPN) 적용이 필수인 상황에서, 이를 충족하면서도 내부망과 클라우드 간 안전한 접근을 보장할 수 있는 방안을 모색했다.

아울러 업무 효율성 제고를 위해 민간 SaaS 서비스 활용도 점차 확대되고 있으나 퍼블릭 클라우드 기반의 SaaS는 기존 경계 보안으로는 통제가 어려운 영역으로, 이에 대한 체계적인 보안 관리 방안 마련이 시급했다. 여기에 코로나19로 인한 재택근무 확대로 인해 기존 보안 체계로는 대응이 어려운 새로운 위협 시나리오에 직면, 언제 어디서나 안전한 업무 환경을 제공하고 비정상 행위를 실시간으로 탐지·대응할 수 있는 지능형 보안 체계 구축을 목표로 했다.

Insights | 전문가 칼럼

b. 기술 적용 내용

NIA는 규제 요건을 충족하면서도 내부망과 클라우드 간 경계에서 강화된 접근 통제를 적용하기 위해 SDP 기술을 적용했다. SDP는 응용 계층에서 사용자와 디바이스의 신원을 검증하고, 애플리케이션 접근 경로를 보호함으로써 네트워크 수준의 악의적 공격을 원천 차단한다.

NIA는 민간 클라우드 사용 규정을 지키기 위해 CC인증을 획득한 국산 제품을 선정했으며, 가상사설망과의 유기적 연계를 통해 규제 준수와 보안성 향상을 동시에 달성했다. 특히, 재택근무자의 접속도 SDP 정책 하에서 체계적으로 통제함으로써, 기존의 VPN 방식 대비 관리 효율성과 안전성을 크게 높이는 효과가 있었다.

민간 SaaS 서비스를 안전하게 활용하기 위해서 EIG 기술을 적용했다. EIG는 사용자 신원과 권한, 단말 상태 등을 종합적으로 평가해 접근 관리를 수행한다. NIA는 SaaS 서비스 제공자와 연계해 SAML 기반 SSO를 구현함으로써, 사용자 인증을 NIA에서 직접 통제할 수 있게 했다. 나아가 접속 단말의 보안 상태를 실시간 점검하고, 이상 징후 탐지 시 접근을 차단하는 지능형 통제 체계를 갖췄다. 또한 SaaS 내 파일 전송 활동에 대한 가시성을 확보하고 바이러스 검사 및 권한 관리를 세밀하게 적용함으로써, 중요 데이터의 무단 유출을 방지하고, 감염 확산을 막을 수 있었다.

아울러 중요 데이터를 보유한 핵심 서비스를 대상으로는 마이크로세그먼테이션을 적용했다. 애플리케이션 간 불필요한 통신을 차단하고, 최소 권한 원칙에 따라 애플리케이션 및 SaaS 서비스의 기능별, URL별로 접속 권한을 부여해 접근을 통제함으로써 내부 위협의 전파 경로를 최소화했다. 이를 통해 중요 정보 자산에 대한 가시성과 제어 역량이 향상됐다. SDP, EIG, 마이크로세그먼테이션은 단일 관리 플랫폼을 통해 구현됨으로써, 일관된 제로 트러스트 정책 시행이 가능하다는 것을 보여줬다.

c. 실증 결과 및 성과

제로 트러스트 보안 모델 실증을 통해 NIA는 클라우드 및 SaaS 활용에 따른 보안 위험을 극복하고, 업무 변화에 민첩하게 대응할 수 있는 동적 보안 체계 확립이 가능함을 확인할 수 있었다.

SDP는 내부망 경계를 넘어서는 안전한 접근을 가능케 했으며, EIG는 SaaS 사용에 수반되는 ID 관리와 접근 통제 문제를 해결해줬다. 여기에 마이크로세그먼테이션으로 내부 위험마저 초세분화 되어 철저히 통제함으로써, 전방위적 보안 체계 구축이 가능함을 증명했다. 이를 통해 비인가 접근과 이상 행위에 대한 실시간 탐지 및 대응이 가능, 망 경계를 넘나들며 클라우드와 SaaS를 활용하는 업무 환경에서 발생할 수 있는 다양한 위험 시나리오에 선제적으로 대응할 수 있게 된 것이다.

또한 보안 정책의 일원화로 관리 부담이 크게 경감됐으며, 사용자 친화적인 접근 방식으로 업무 연속성을 보장할 수 있었다. 에이전트 기반 접근 통제는 사무실 밖 원격 근무자에 대한 보안 사각지대 해소에도 기여하는 효과도 있었다.

Insights | 전문가 칼럼

NIA의 실증 사례는 국내 공공기관이 직면한 클라우드 및 SaaS 보안 과제를 제로 트러스트로 효과적으로 풀어낼 수 있음을 보여준다. 특히 규제 준수와 혁신적 보안 모델 적용을 조화시킴으로써, 안전하고 신뢰할 수 있는 지능정보사회로의 전환을 가속화할 것으로 기대된다. 나아가 공공기관과 민간기업의 협력을 통한 보안 혁신 실증의 좋은 선례로도 평가된다.

3 LG유플러스

a. 제로 트러스트 실증 배경 및 목표

LG유플러스는 이동통신사업자로서 대규모 무선 통신망을 운영하고 있다. 그러나 무선 통신망은 유선에 비해 상대적으로 보안 위협에 취약하다는 문제가 있었다. 특히 무선 통신 라우터를 통한 멀웨어 전파와 DDoS 공격은 서비스 안정성을 위협하는 주요 요인으로 작용해 왔다.

기존의 경계 보안 모델과 IP 기반 통신 기술로는 이러한 위험을 근본적으로 해결하기 어려웠다. 이에 LG유플러스는 제로 트러스트 원칙에 입각한 새로운 보안 아키텍처를 무선 인프라에 적용함으로써, 보다 강력하고 능동적인 위협 대응 체계를 구축하고자 했다.

특히 5G 시대를 맞아 폭증하는 트래픽과 다변화하는 서비스 시나리오에 대비하기 위해, 무선 액세스 네트워크 영역에서의 세분화된 접근 통제와 이상 행위 탐지 역량 확보가 시급한 과제였다. 이에 무선 라우터 장비를 중심으로 제로 트러스트 원천 기술을 실증하고, 최적의 적용 방안을 도출하는 것을 목표로 삼았다.

b. 무선 라우터 기반 제로 트러스트 기술 적용 내용

LG유플러스는 제로 트러스트 실현을 위한 핵심 축으로 SDP 기술을 선택했다. SDP는 단말과 라우터 간 초기 연결 수립 시점부터 강화된 인증을 적용하고, 상황 정보 기반의 세밀한 접근 제어를 가능케 한다.

이를 위해 무선 라우터의 펌웨어 레벨에서 SDP 에이전트를 내재화하는 방식을 선택했다. 라우터 자체를 포함해 라우터에 연결되어 통신을 시도하는 모든 단말들은 SDP 정책에 따라 신원을 검증받게 되며, 선 인증 후 접속 체계를 통해 등록되지 않은 라우터 및 단말들은 통신이 차단되고, 신원 검증이 완료된 후 PDP에 의해 등록된 라우터 및 단말만 연결이 가능하다. 또한 역할과 권한에 기반한 네트워크 접근 권한을 부여받아, 보호 대상 서비스로만 접속이 가능하다. 나아가 단말의 보안 상태를 실시간으로 확인하고, 비정상 행위 탐지 시 즉각 접속을 차단하는 메커니즘을 적용했다.

멀웨어 전파 및 DDoS 공격 차단을 위해서는 마이크로세그먼테이션 기술도 함께 활용했다. 무선 라우터가 연결된 환경을 세분화된 보안 존으로 구분하고, 존 간의 트래픽을 엄격히 통제함으로써 위협의 확산을 원천 봉쇄하고자 한 것이다.

Insights | 전문가 칼럼

아울러 라우터 자체의 보안 강화를 위해 커널 레벨 하드닝, 시큐어 부팅, 무결성 검증 등 다양한 기술을 적용했다. 비인가 펌웨어 업데이트나 프로세스 및 설정 변경, 백도어 등 라우터를 통한 악의적 침투 시도를 사전에 차단할 수 있게 된 것이다.

c. 실증 결과 및 성과

제로 트러스트 기반 무선 라우터를 통해 LG유플러스는 무선 통신 환경의 보안성을 획기적으로 높일 수 있었다. SDP구조를 통한 단말 접근 통제, 세분화된 네트워크 격리, 그리고 라우터 자체 보안 강화가 삼위일체로 작용한 결과였다.

우선 라우터 레벨에서 비인가 기기 접속과 이상 트래픽 유입이 사전에 차단됨으로써, 네트워크 경로를 통한 멀웨어 유포와 DDoS 공격 위험이 현저히 감소했다. 만일의 감염 상황 발생 시에도 피해 범위를 최소화할 수 있는 통제 역량을 확보하게 됐다.

LG유플러스의 이번 실증 사업은 통신 사업자가 네트워크의 말단에서부터 선제적 보안 대응에 나설 수 있음을 보여주는 선도 사례로 평가된다. 이번 실증 사례가 국내 전반의 네트워크 보안 혁신을 가속화하는 신호탄이 되기를 기대한다.

● 제로 트러스트 보안 모델의 발전 방향

제로 트러스트는 이제 선택이 아닌 필수가 됐다. 그러나 제로 트러스트의 여정은 결코 평坦하지 않다. 기술적 복잡성, 조직 문화의 관성, 높은 초기 비용 등이 걸림돌로 작용한다. 제로 트러스트가 보다 널리, 손쉽게 채택되기 위해서는 지속적인 발전이 요구된다.

우선 사용자 편의성과 운영 효율성에 중점을 둔 솔루션 고도화가 필요하다. 이를 위해 접근 통제의 자동화, 상황 인식 기반의 적응적 인증, AI 기반 이상 징후 탐지 등 지능형 보안 기술과의 융합이 가속화될 것으로 보인다.

둘째, 제로 트러스트 정책 시행의 일관성과 연속성을 보장하는 것이 중요하다. ID 관리, 단말 관리, SIEM 등 기존 보안 인프라와 긴밀히 연계되고, 멀티클라우드 환경을 아우르는 통합 플랫폼 기반 구현이 대세가 될 것이다.

마지막으로 제로 트러스트를 조직 전반의 리스크 관리 체계와 연계하는 거버넌스 강화가 요구된다. 이는 단순히 기술 도입을 넘어 제로 트러스트 원칙을 조직의 문화와 프로세스에 내재화하는 과정을 의미한다.

● 제로 트러스트 도입을 위한 제언

제로 트러스트의 성공적인 구현을 위해서는 자신의 비즈니스 특성과 위협 특성에 부합하는 제로 트러스트 전략과 로드맵 수립이 필요하다. 이때 중요한 것은 기술 도입에만 몰두하지 않고, 조직 문화와 거버넌스 체계를 함께 혁신하는 것이다. 사내 교육과 캠페인을 통해 제로 트러스트 원칙을 임직원에게 효과적으로 전파하고, 행동 변화를 이끌어내야 한다. 아울러 제로 트러스트 전환을 보안 조직의 단독 프로젝트로 여겨서는 안 된다. 관련 부서와의 긴밀한 협업은 물론, 모두의 적극적인 참여와 피드백이 성공의 열쇠가 된다.

끝으로 제로 트러스트를 장기적 과제로 접근할 것을 당부한다. 큰 청사진을 세우되 단계적으로 이행하고, 작은 성공 경험을 축적해 나가는 것이 바람직하다. 외부 전문가 그룹과의 협력을 통해 제로 트러스트 구현의 전문성과 효율성을 높이는 것도 좋은 방법이 될 것이다.

디지털 전환의 시대, 사이버 위협의 대응은 더 이상 선택이 아닌 필수가 되었다. 제로 트러스트는 단순한 통제 강화가 아닌, 철학이자 문화이다. 이는 새로운 보안 환경을 고려하는 모든 기업이 향해 가야 할 방향이지만, 각자의 여정은 다를 수밖에 없다. 중요한 것은 원칙에 충실하되 자신만의 방식을 찾아가는 것이다. 지금이야 말로 제로 트러스트를 자신의 색깔에 맞게 채워가기 시작할 때이다.

Part. 2

04

SW 공급망 보안 가이드라인(1.0) 소개 및 발전 방향

한남대학교 이만희 교수

SW가 몸살을 앓고 있다. SW 공급망 공격이라는 몸살이다. 이 공격은 워낙 공격 루트가 다양해서 어디서 어떻게 막아야 할지 현재 정답이 없다. 지금 다양한 국가에서 추진하는 방향은 SW를 만들 때 어떤 컴포넌트로 만들었는지 개발단계부터 유통 및 운영 단계까지 소프트웨어의 라이프 사이클 전체에서 지속적으로 관리하는 것을 우선 추진하고 있다. 우리나라도 국가정보원, 과기정통부, 디지털플랫폼정책부위원회가 민간 전문가와 공동으로 SW 공급망 보안 가이드라인(v1.0)을 지난 5월 13일에 배포했다[1].

이에 본 칼럼에서는 첫째, SW 공급망 보안 가이드라인(v1.0)의 주요 내용을 요약해 소개하며 약간의 해설을 더해 가이드라인의 의미를 강조한다. 둘째, 가이드에도 소개되어 있지만 미국의 Secure Software Development Attestation Form 수집이 임박함에 따라 이를 자세히 소개한다. 마지막으로, 국가적 사이버 위험 관리를 위한 국가 공급망 관리 체계를 제안한다.

가. SW 공급망 보안 가이드라인(v1.0)

이번 가이드라인의 가장 큰 의미는 3개 정부 기관이 공동으로 가이드라인을 기획하고 집필했다는 것이다. 미국, 유럽 등에서는 다양한 부처에서 참여해 공동 집필하는 것이 너무 일반화되어 있지만, 우리나라는 이제껏 그러한 사례가 없었고 이번이 첫 공동 가이드라인이다. 먼저 공동 가이드라인을 어떻게 만들게 되었는지 그리고 그 의미에 관해서 설명한다.

최근 국제적으로 공급망 보안 위협이 크게 증가했다. 2020년 말, 솔라윈즈 사태를 통해 미국 정부가 큰 피해를 입었고, 2023년에 발생한 3CX 공급망 공격은 배후가 북한으로 알려짐에 따라 우리나라 정보보안 분야에도 큰 위기감이 형성됐다. 이 위협 증가와 함께 미국, 유럽이 SW 공급망 보안 강화를 위한 규제를 준비함에 따라 장기적으로 우리나라 기업의 수출에도 타격이 있을 것이 우려되는 상황이었다.

Insights | 전문가 칼럼

이 상황을 감지한 국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회는 각 기관의 상황에 맞게 SW 공급망 보안을 준비했다. 먼저 국가 사이버안보 및 국가·공공기관의 정보보안 태세를 책임지고 있는 국가정보원은 소프트웨어를 도입하는 공공기관 입장에서 소프트웨어의 공급망 보안 수준을 제고하는 방안을 도출하기 위해 노력했다. 이 노력의 일환으로 판교에 위치한 국가사이버안보협력센터 기술공유실 내에 공급망 보안 테스트베드를 구축해 다양한 방안을 추진했다. 이를 위해 전문가로 구성된 TF팀을 구성, 지속적으로 자문을 수렴하며 진행해 왔다. 주요 결과로 자동화된 소프트웨어 공급망 분석 시스템을 구축할 수 있었고, 이 경험을 바탕으로 공공기관 도입을 위한 SBOM(Software Bill of Materials) 기본항목을 제안하기에 이르렀다.

한편, 정보보호 산업 진흥의 역할을 담당하는 과학기술정보통신부는 현실화되고 있는 SW 공급망 보안 국제 규제에 국내 기업이 잘 대응할 수 있도록 다양한 방안을 추진했다. 2022년 10월, 제로트러스트 분야와 함께 제로트러스트 & 공급망 보안 포럼을 발족, 이를 통해 국내 전문가들이 공급망 보안 추진에 협력할 수 있는 발판을 만들었다. 이후 간담회를 개최하는 등 공급망 보안에 매우 적극적으로 나섰고, 2023년에는 국내 소프트웨어 기업들을 지원할 수 있는 모델 수립을 위한 공급망 보안 체계 실증사업을 추진했다.

우리나라의 디지털 전환과 정부 서비스 혁신을 촉진하기 위해 2022년에 설립, 정부 디지털 플랫폼 구축 및 운영을 총괄하는 역할을 맡은 디지털플랫폼정부위원회 또한 초기부터 제로트러스트·공급망보안 TF를 구성, “디지털플랫폼정부 신 보안체계 도입 및 적용 방안 연구” 등을 수행하며 정부 서비스 내에 공급망 보안 도입 방안 도출을 고민했다.

국가정보원과 과기정통부는 소프트웨어 공급망 보안과 관련된 정책적 사안에 대해 공동 협력 대응하기로 뜻을 모으고, 그 첫 번째 태스크로 SW 공급망보안 가이드라인을 공동 집필했다. 이 작업에 필자를 포함한 민간 전문가와 KISA, KISIA가 참여했고, 정부 서비스에 대한 공급망 보안 적용을 위해 국내 최초 다부처가 공동으로 집필한 가이드라인이 나오게 됐다.

가이드라인의 주요 내용은 SW 공급망 보안의 추진배경, SW 공급망 위험관리 방안, SBOM 기반 SW 공급망 보안 실증사례, SBOM 기반 공급망보안 활성화 지원 등으로 구성되어 있다.

1장 SW 공급망 보안의 추진배경

1절 환경변화, 2절 SW 공급망 보안 위기 대응의 필요성, 3절 주요국 SW 공급망 보안 정책 동향으로 구성되어 있다. 1절 환경변화에서는 크게 ‘초연결 사회의 도래, SW 부품 공급의 분업화, 공개 SW 사용의 확대’의 세 가지 변화를 소개했다. 요약하면, 디지털 전환이 가속화되면서 사람과 사물이 물리적·가상 공간에서 유기적으로 연결되는 초연결 사회가 도래하고 있고, 이에 따라 SW 공급망의 분업화로 인해 관리 책임이 복잡해지고, 공개 SW를 포함한 외부 SW에 대한 사이버 위협이 증가하고 있음을 설명한다(그림 2-7). 추가로, SW 공급망 공격에 대한 대응의 필요성을 강조한 2024년도 사이버보안 위협 전망을 소개했다.

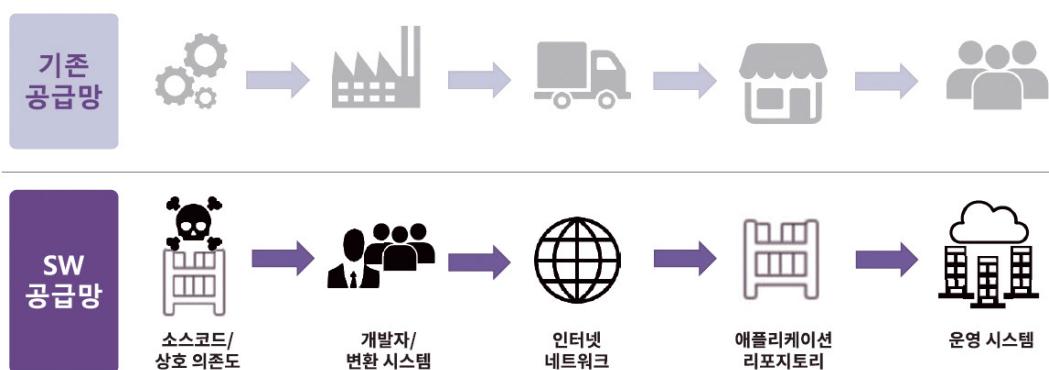


그림 2-7 전통적인 공급망과 SW 공급망 비교

2절에서는 SW 공급망 공격 대응의 문제, SW 공급망 침해사고의 피해 규모, 공개 SW 사이버보안 관리의 중요성, SW 공급망 공격의 주요 유형 및 대상 순서로 SW 공급망 보안 위기 대응의 필요성을 설명한다.

먼저 UEFI의 펌웨어 루트킷(Rootkit)인 LoJax, DNS 서버로 중국 IP가 설정된 채로 군에 납품된 CCTV, 2023년에 기상청에서 도입한 기상관측장비에서 악성코드가 설치된 사례를 포함하여 세계 주요 SW 공급망 침해사고 개요와 피해 내용을 간단히 소개했고, 공개 SW 보안에 대한 미국과 리눅스 재단의 대응 상황을 소개했다. 특히, SW 공급망 공격의 주요 유형 및 대상 순서에서는 공개 SW 보안취약점 (Vulnerabilities in OSS), 타사 의존성 (3rd Party Dependencies), 공용 리포지토리 (Public Repositories), 변환 시스템 (Build Systems), 업데이트 가로채기 (Hijacking Updates), 내부 리포지토리 (Private Repositories), 공급사 및 협력사 (Suppliers and Business Partners) 등 7가지 SW 공급망 공격의 유형을 간단한 그림과 함께 설명하고 있다. 이 그림과 설명은 다른 나라 자료에는 없는 설명으로써 공급망 공격을 이해하려는 독자들에게 큰 도움이 될 것이다(그림 2-8).

(유형1) 공개 SW 보안취약점(Vulnerabilities in OSS)

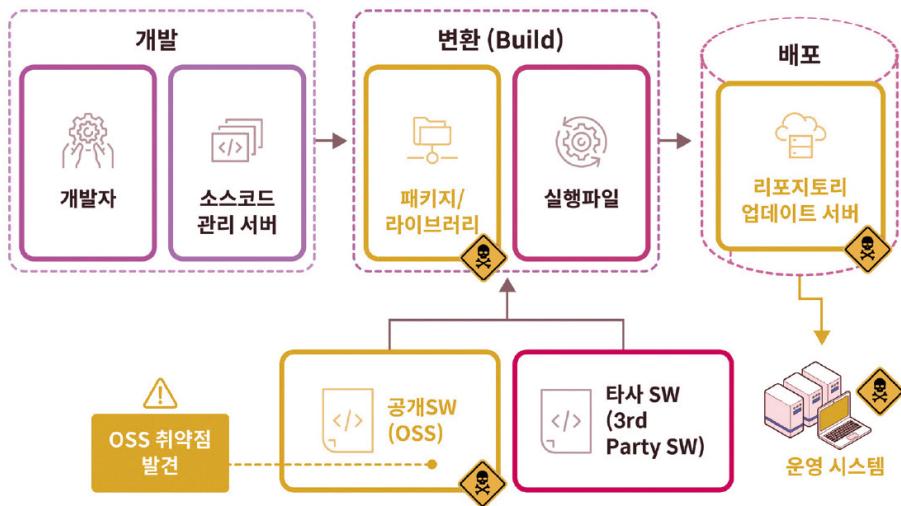


그림 2-8 유형별 SW 공급망 공격 대상 및 침투 경로

3절 주요국 SW 공급망 보안 정책 동향에서는 미국, 유럽, 일본, Quad의 공급망 보안 동향을 소개하고 있다. 미국은 2021년 바이든 정부의 행정명령을 통해 연방 정부에 납품되는 소프트웨어의 공급망 보안 관리 의무화를 천명하고[2], 2022년에는 “안전한 정부를 위한 SW 공급망 보안 강화 지침”과 “행정 부서 및 기관장을 위한 각서(M-22-18)”를 발표했다[3]. 이 지침은 SW 공급자에게 미국 국가기술표준원(NIST)의 “안전한 SW 개발 체계(SSDF)” 준수를 요구하며, 자체증명서를 제출하도록 하고 있고, 이 제도는 2024년 6월부터 시행될 예정이다. 이에 대해서는 다음 장에서 더욱 자세히 설명한다. 또한 미국 FDA는 2023년 1월 연방식품의약품화장품법을 개정해 의료기기의 사이버보안 강화 요구사항을 추가하면서 디지털 헬스 기기의 소프트웨어에 대한 SBOM 제출을 의무화하였다[4].

유럽연합(EU)은 2022년 사이버 복원력 법(Cyber Resilience Act, CRA) 제정안을 발의하여 역내 유통되는 디지털기기의 취약점 대응 능력 향상을 꾀하고 있다[5]. 주요 내용으로는 EU에 디지털기기를 판매하려는 제조사는 SBOM을 기술 문서로 제출하고, 제품 보안 업데이트, 공급망 사이버보안 점검, 보안 취약성 정보공유 등의 요건을 충족해야 한다. 2023년 12월, EU 의회와 이사회는 관련 개정 법안의 역내 시행에 정치적으로 합의했고, 2024년 4월 EU 의회를 통과했다. 가이드에서는 법안의 효력 발생 시점을 2026년 하반기로 예상하였으나, 2024년 이내에 EU 이사회 통과가 이루어질 경우, 2027년부터 시행될 것으로 보인다.

Insights | 전문가 칼럼

일본은 경제산업성에 SW TF를 설치하고, SBOM 실증사업을 통해 개념 정립 및 효과성 검증을 진행하고 있고, SBOM 도입 안내서를 배포해 민간 부문에서도 활용을 확산하려고 노력 중이다. 가이드에서는 소개되지 않았지만, 최근 일본은 SW 관리를 위한 SBOM 도입 안내서 v2.0 안을 공개하고 피드백을 받고 있다. 한편, 미국, 일본, 인도, 호주는 Quad 사이버보안 파트너십을 통해 SW 공급망 보안을 위한 개발 활동을 장려하고, 각국 정부 정책에 반영하기 위해 협력하고 있다. 이들은 “안전한 SW를 위한 공동 원칙”을 발표하고, 최소한의 사이버보안 지침 수립을 약속했다.

2장 SW 공급망 위험관리 방안

1절 공급망 사이버보안 위험관리 체계 구축 방안에서는 NIST의 Cybersecurity Supply Chain Risk Management (C-SCRM), Enduring Security Framework (ESF)의 안전한 SW 개발·운용을 위한 공급망 참여자들의 보안 활동, NIST의 안전한 SW 개발체계(SSDF)를 차례로 설명한다.

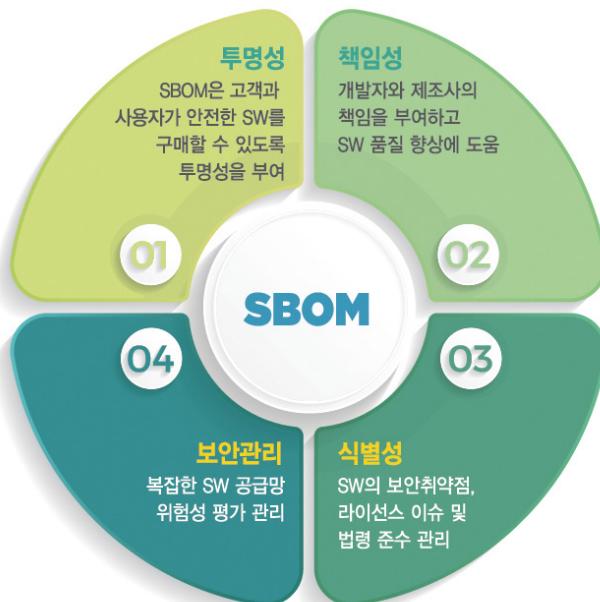
NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organization에서 설명하는 C-SCRM은 공급망의 사이버보안 위험관리를 위해 SDLC 전반에 걸친 활동을 통합하고, 전사적 위험관리 체계를 설명한다[6].

다양한 이해관계자가 참여해 설계, 개발, 제조, 구매, 배송, 통합, 운영, 유지보수, 폐기 등 전 과정에서 보안 취약점을 관리하고, 다단계 전사적 위험관리 모델을 통해 전사, 프로세스, 운영 수준에서 위험을 체계적으로 관리해야 함을 설명한다. ESF의 안전한 SW 개발·운용을 위한 공급망 참여자들의 보안 활동 부분에서는 SW 공급망 보안을 위해 개발사, 공급사, 운영사들은 각자의 역할을 수행해야 하며, 주요 활동으로 개발사는 보안 취약점을 최소화하고, 공급사는 SW 보안을 검증하며, 운영사는 보안 요구사항과 SCRM 대책을 정의하고 구현해야 함을 설명한다[7].

마지막으로 NIST의 안전한 SW 개발체계 부분에서는 SW 개발자들이 지켜야 할 보안 활동을 소개하고 있다[8]. SSDF는 인력, 프로세스, 기술 준비를 통해 안전한 SW 개발을 지원하며, 모든 구성요소의 변조 및 비인가 접근을 방지하고, 보안 취약점을 최소화하여 SW를 출시하는 것을 요구한다. 특히 6월부터 시행되는 Self-attestation Form의 핵심 내용은 SSDF의 준수이므로, 다음 장에서 SSDF와 Self-attestation에 대해 추가적으로 설명한다.

2절에서는 SW 구성요소의 신뢰성을 확보하는 방안으로 SBOM을 중심으로 한 접근법을 설명한다. 내용으로는 SBOM의 정의와 필요성, 효과성, 최소요건을 설명하며, SBOM을 활용한 SW 보안취약점 및 라이선스 관리 방안을 설명한다. 먼저 SBOM의 정의 소개로써 소프트웨어를 구성하는 재료의 목록이며 “SW 구축에 사용되는 다양한 구성요소의 세부 사항과 공급망 관계를 포함하는 공식적인 기록”으로 NTIA가 정의한 내용을 소개한 후, SBOM의 효과성을 그림으로 설명한다(그림 2-9).

Insights | 전문가 칼럼



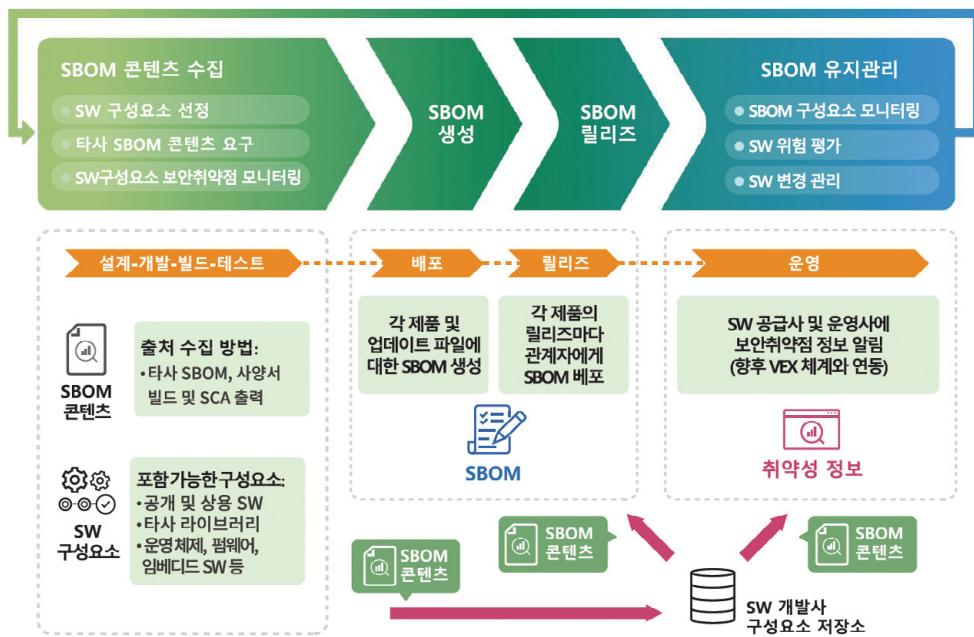
▣ 그림 2-9 SBOM 활용의 효과성

이어서 미국 NTIA가 제시한 SBOM의 최소요건을 소개한다. SBOM의 최소요건에는 ①데이터 필드(공급자명, 타임스탬프, 저작권자, 구성요소명, 버전, 고유식별자, 종속성 관계), ②자동화 지원(SPDX, CycloneDX, SWID 포맷 활용), ③관행 및 프로세스(SBOM 업데이트 및 제공 방법과 시기 관련 6가지 요구사항)이 포함된다.

마지막으로 SBOM을 통해 보안 취약점과 공개 SW 라이선스를 관리할 수 있음을 설명한다. SCA(Software Composition Analysis) 도구를 사용해 SBOM을 생성하고, 알려진 보안 취약점 정보(CVE, KEV 등)와 비교하여 취약점이 검출된 사례를 보이고, NVD(National Vulnerability Database) 가 제공하는 보안 취약점 정보를 확인하는 방법을 설명한다. 취약점의 위험도를 등급으로 나타내는 CVSS를 소개하고 CVSS 7.0 이상의 높은 위험도로 평가된 취약점의 즉각적인 완화 조치를 수행하도록 권고한다.

3절 SBOM 기반 SW 공급망 보안 강화 방안에서는 개발사, 공급사, 운영사가 SBOM을 활용하여 공급망을 관리할 수 있는 체계와 이를 확장한 산업별 SW 공급망 거점 및 국가 SW 공급망 관리센터에 대한 비전을 제시한다. 그림 4에서 제시하고 있는 공급망 관리 체계에서, 개발사는 SBOM 생성을 위한 필수 도구 및 기능으로써 SBOM 도구, 구성요소 저장소, SBOM 데이터베이스, 자체 보안취약점 DB 및 NVD 연계 등을 제시한다. 이를 통해 SW 공급사 및 운영사는 자산 파악과 보안 패치 등 선제 대응이 가능하다.

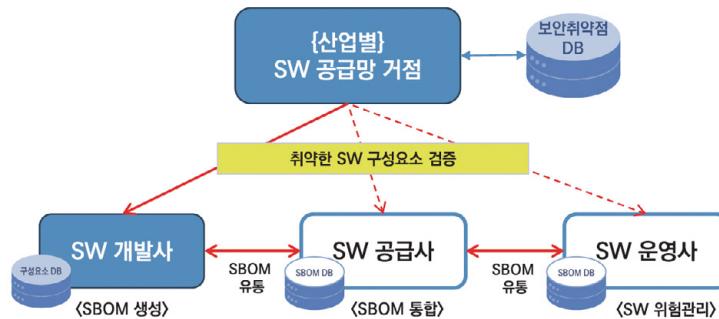
Insights | 전문가 칼럼



▣ 그림 2-10 SW 공급망과 내·외부 SW 유형 예시

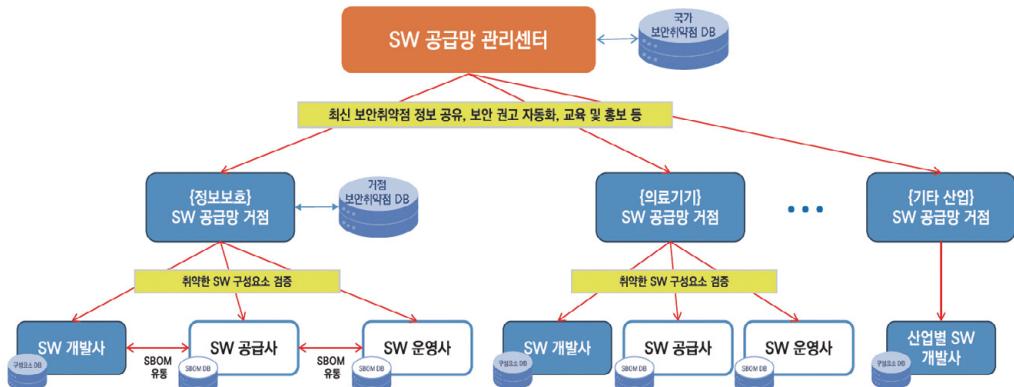
이렇게 개발사에서 공급사, 운영사로 이어지는 SW 공급망에 SBOM 공급망 체계를 구축하면, 정부·공공기관에서 '산업별 SW 공급망 거점'을 마련할 수 있다(그림 2-11). 산업별 SW 공급망 거점은 SW 개발자, 공급사, 운영사를 포괄하여 SBOM 정보를 자율적으로 공급하는 기능을 수행할 수 있다. 이 거점은 SBOM 공급을 체계화하고 자동화하여 새로운 SW 위험 발생 시 빠르게 대응하는 것을 목표로 한다. 기업 지식재산권 보호를 위해 최소한의 지원이 바람직해 보이며, 적용 방안으로 먼저 외부 SW인 상용 SDK부터 SBOM으로 관리하고, 공개 SW는 시장 자율성에 맡기되 정부가 신뢰성을 높이는 방안을 추진하는 것을 제시한다. 구현 방안으로는 가이드라인에 소개된 보안성 점검 시설에 정보공유 체계를 추가하는 형태를 제시하고 있다.

Insights | 전문가 칼럼



[그림 2-11] 산업별 거점을 활용한 SW 위험관리 구조도

마지막 내용으로 SW 공급망 관리센터 구축의 필요성을 설명한다. SW 공급망 관리센터는 공급망 각 단계의 위험을 사전에 분석하고 관리하며, 산업별 공급망 거점에 필수 정보를 공유하는 기능을 수행한다(그림 2-12). 주요 역할로는 SW 공급망 보안 활동 계획 수립, 관련 이해관계자와 정보 교류, 교육 및 홍보를 포함한다. 자동화된 체계를 통해 보안 취약점과 악성코드 정보를 쉽게 공유하고, 보안 권고를 체계화하여 자동 대응하며, 향후 SBOM 정보 공급 체계를 기반으로 보안 취약성과 악용 가능성 자동 교환(VEX) 인텔리전스 체계로 발전할 수 있다.



[그림 2-12] SW 공급망 관리센터 체계도

3장 SBOM 기반 SW 공급망 보안 실증사례

3장에서는 SW 공급망 보안 실증사례의 주요 내용을 설명하고, 이를 통해 도출된 자가 점검용 SW 공급망 단계별 보안 체크리스트를 제시하고 있다. 먼저 1절 SBOM 생성·활용 실증사례에서는 실증사업의 개요 및 주요 결과를 소개한다. 주요 결과로는 SBOM 생성 도구를 이용한 SBOM은 데이터 중복 및 누락, 오류 등이 존재함을 확인했고(그림 2-13), 소스코드 및 바이너리 대상으로 여러 SBOM 도구 비교 시, 도구 간 결과에 상당한 차이가 있음도 확인됐다.

컴포넌트 (Component Name)	버전 (Component Version)	공급자 (Supplier Name)	라이선스명·버전 (License Name·Version)
commons-io	1.3.2		정보누락
commons-io	2.2		
commons-io: commons-io	2.2		Apache-2.0
commons-io: commons-io	2.1	정보누락	Apache-2.0
commons-io: commons-io	1.3.2		Apache-2.0
commons-io: commons-io	1.3		Apache-2.0

[※] 그림 2-13 SBOM 유효성 검증 단계에서 데이터 누락·중복 사례

이 실증으로 SBOM 기반의 SW 공급망 보안 관리 요령을 제시했다. 먼저 기업은 SW 개발 언어의 호환성, 도구의 분석 알고리즘, 공급망 특성을 고려하여 적합한 SBOM 도구를 선정해야 한다. 소스코드와 바이너리 분석 방식을 기업 환경에 맞게 선택하고, 상호 보완적으로 2개 이상의 도구를 활용하는 것이 권장했다. 설계, 개발, 공급, 운영, 유지보수 등 각 단계별로 SBOM을 생성·공급하는 관리체계를 구축하고, 보안 취약점 탐지 성능을 높이기 위해 SBOM DB를 구축하고 NVD와의 연동을 제안했고, 마지막으로 보안 취약점이 발견되면 신속히 개발자와 고객사에 전파하여 조치 계획을 수립하고 대응 체계를 마련하는 것을 제안했다.

2절에서는 실증사업의 일환으로 수행한 SW 공급망 보안 관리체계 점검을 수행한 결과를 제시했다. SW 공급망 보안 관리체계 점검을 위해 5가지 분야, 54개 세부 항목으로 구성된 SW 공급망 보안 점검 항목을 도출해 기업의 실제 개발 현장에 적용해 본 결과, 국내 중소기업의 SBOM 기반 SW 공급망 보안 관리체계 구축이 미흡했다. 특히, 안전한 제품 관리, 보안 코드 개발, 타사 구성요소 확인, 개발환경 보안, 보안 코드 전달 등 개발 전 분야에 대한 지속적인 점검 지원이 필요함을 인식했다.

Insights | 전문가 칼럼

3절에서는 자가 점검용 SW 공급망 단계별 체크리스트를 제시했다. 실증 추진 과정에서 SW 공급망 보안 점검 실증 항목을 이용해 기업의 보안 수준을 체계적으로 점검할 수 있었으나, 항목이 많고 수행이 어려운 부분이 있어 이를 정제하고, 국내 기업에 맞는 공급망 단계별 체크리스트를 제안했다. 이 체크리스트는 개발사, 공급사, 고객사가 각 단계에서 공급망 보안 상태를 스스로 확인할 수 있는 도구로써, 개발사는 개발환경 보안 점검, 공급사는 보안 준비도 점검, 고객사는 도입 전후 보안 확인에 활용할 수 있다. 자가점검 항목은 설계, 개발, 공급, 도입, 유지보수 단계로 구성된다. 아래 표는 공급망 보안 단계별 체크리스트에서 자가점검 항목만 정리한 것이다.

표 2 - 5 자가 점검용 SW 공급망 단계별 체크리스트 요약

단계	점검항목
설계 단계	<ul style="list-style-type: none"> • 안전한 개발과 관련하여 조직 내 역할 및 책임 명시 • SW 제품, 서비스 개발자 및 관련자에게 보안 교육 • 개발단계에서 공급망 보안을 고려 • 개발환경의 보안상태 관리 • 제품의 주요 보안항목 식별 및 문서 보관
개발 단계	<ul style="list-style-type: none"> • 시큐어코딩 준수 • 배포 전 기본 설정 검토 • 외부 라이브러리의 보안성 확인 • 내부 저장소 접근 통제 • 내부 저장소의 보안취약점 지속 점검 • 빌드 과정에서 자동화된 보안 테스트 수행 • 컴파일러, 인터프리터 사용 시 보안 옵션 적용 • 빌드 후 결과물 보관 • SBOM의 보안취약점 확인 • 심각한 보안취약점 검증 • SBOM 작성 이력 보관
공급(유통) 단계	<ul style="list-style-type: none"> • SW 무결성 확인 데이터 전달 • 소스코드, 라이브러리, 공개 SW 정보 안전 보관 • 고객(운영)사에 SBOM, 보안취약점, 라이선스 정보 제공
도입 및 운영 단계	<ul style="list-style-type: none"> • SW 제품 도입에 대한 공급망 보안 요구사항 및 관리 매뉴얼 • 보안 요구사항 이행 확인 • SW 코드서명 또는 해시값으로 무결성 확인 • 주요 보안취약점 포함 여부 모니터링 • 보안취약점 처리 요구 • SBOM 제공 여부 • 소스코드 취약요인 점검
유지보수 단계	<ul style="list-style-type: none"> • 운영 SW 보안취약점 지속 점검 • 보안취약점 평가 및 대응 방안 • 보안취약점 패치 절차 수행 • 배포/업데이트 서버 보안관리

4장 SBOM 기반 SW 공급망 보안 활성화 지원

1절 SW 보안취약점 점검 지원 테스트베드는 세 개의 테스트베드 또는 랩을 소개하는 내용이고, 2절은 국가정보원의 공급망 보안 테스트베드 운영 중에 우리나라 공공기관에서 도입을 위해 우리나라만의 SBOM 요구 사항을 정의하는 것이 바람직하다는 판단하에 NIS-SBOM을 개발한 내용이며 마지막으로 3절은 우리나라의 공급망 보안 분야 발전을 위한 집필진의 발전 제언을 담았다.

1절에서 첫 번째로 소개한 기업지원허브(판교)는 2015년 10월에서 개소했고, 사이버보안 위협 시연, 보안취약점 점검, 견학·교육 프로그램 등을 지원한다. 중소기업들이 디지털제품과 서비스의 보안을 자체 검증하고 보완할 수 있는 환경을 제공하며, 특히 2024년부터 소스코드 분석 방식과 바이너리 분석 방식의 SBOM 생성·분석 도구를 도입해 기업들이 디지털제품 및 서비스 개발단계에서부터 보안성을 내재화할 수 있도록 지원하고 있다. 두 번째로 소개된 디지털헬스케어 보안 리빙랩(원주)은 디지털헬스케어기기와 서비스의 사이버보안 위협 시연 및 보안성 테스트를 지원하기 위해 2020년 12월에 구축됐다. 다양한 보안취약점 점검을 지원하며, 2024년부터 SBOM 생성 도구를 도입하여 기업을 지원한다. 미국 FDA가 디지털헬스케어 제품에 SBOM 제출을 필수로 하는 상황이므로, 관련 수출을 준비하는 기업은 이 랩을 활용해보는 것을 추천한다.

1절에서 세 번째로 소개한 공급망 보안 테스트베드는 국가사이버안보협력센터 기술공유실(판교)에 설치되어 있다. 기술공유실은 ICT 기술의 안전성을 확인하고, 보안업체와 시험기관에게 고가·신기술 융합제품의 안전성 평가를 지원하기 위해 2022년 11월에 개소했다. 특히, 공급망 공격에 대응하기 위해 SBOM 생성 자동화, SBOM 관리, SW 보안취약점 추적·관리를 실증할 수 있는 테스트베드를 구축했다. 앞서 소개된 랩은 개발사의 공급망 관리라면, 이 테스트베드는 향후 국가·공공기관에 SW를 도입할 때 활용할 수 있는 SBOM 관리 기술을 개발한 것이 특징적이다. 이 기술은 국내외 상용 SCA를 활용해 SBOM 통합엔진을 개발했고, 실제 국내외 펌웨어·운영 SW·웹소스·설치파일 등 4개 분야 10개 SW 제품을 대상으로 SBOM을 생성하고 SW 커포넌트에 대한 분석을 수행한 결과, 7개의 제품에서 CVSS 9.0 이상의 중대 보안취약점이 발견하는 등 중요한 성과를 얻었다. 이는 한계는 있지만 도입과정에서도 SBOM 생성 및 관리가 가능하며 주요 취약점을 식별할 수 있다는 것을 증명한 뜻깊은 결과라고 할 수 있다.

2절 SW 공급망 보안을 위한 SBOM 개발에서는 우리나라 공공기관 도입용 SBOM 기본항목 개발 내용을 소개한다. 미국, 유럽 등 주요국은 SBOM 제출 의무화를 추진하고 있고, 이 SBOM에 담아야 하는 기초 내용을 기본항목이라 한다. 미국 NTIA는 7개 기본항목을 권고하고 있으나 항목 수가 적고, 국내 정보통신 단체표준에서 15개를 제안했으나 다소 부족한 점이 있어, 국가정보원은 정부·공공기관 도입 SW의 SBOM 기본항목 20개를 제안했다(그림 2-14). NIS-SBOM 기본항목은 보안취약점 정보연동과 사이버 위험관리 효율성 향상을 목표로 하고 있고, 테이블 형태의 표준 출력 양식을 권고하며, 공급망 보안 테스트베드에 적용하여 실증을 마쳤다.

Insights | 전문가 칼럼

구분	속성
① SBOM Standard*	NIS / SPDX / CycloneDX / TTA 등 SBOM 표준
② SBOM Type*	개발 / 유통 등 SBOM 생성단계
③ CycloneDXNo.	CycloneDX번호
④ SPDX Doc. ID	SPDX 문서번호
⑤ SBOM ID*	SBOM 문서번호
⑥ Product Name*	제품 이름
⑦ Product Version*	제품 버전
⑧ Component Name	컴포넌트 이름
⑨ Component Alias*	컴포넌트 별칭
⑩ Component Version	컴포넌트 버전
⑪ Component Supplier Name	컴포넌트 공급자 이름
⑫ Component Hash	컴포넌트 해시(SHA-256 이상 사용)
⑬ Component Path*	컴포넌트 경로(컴포넌트 실제 위치 식별)
⑭ SBOM Author Name	SBOM 작성자
⑮ Unique Identifier	컴포넌트 버전 외에 조회가 가능한 고유 식별자 (CPE, PURL 등)
⑯ Dependency Relationship	상위 컴포넌트와의 종속 관계
⑰ Timestamp	SBOM 생성일시
⑱ License Name · Version	라이선스 이름 · 버전
⑲ Vul. DB	NVD(CVE), CISA(KEV) 등 보안취약점 DB
⑳ Vul. Info	CVE 식별자 및 CVSS 보안취약점 등급

▣ 그림 2-14 | NIS-SBOM 기본항목(*: 자체선정)

Insights | 전문가 칼럼

NIS-SBOM 기본항목은 SW 공급자와 도입 기관 간의 SBOM 관련 일관성을 제공하여 SW 공급망 관리 효율성을 높인다. 이를 통해 정부·공공기관에 도입되는 SW를 추적·관리하는 체계 도입을 통한 보안취약점에 대한 신속 대처로 국가 사이버안보를 강화하는 것이 NIS-SBOM의 의의라고 할 수 있다. NIS-SBOM 기본항목은 산·학·연 관계자들과의 논의를 통해 지속적으로 발전시켜 나갈 예정이며, 미국 CISA 등과의 국제 협력의 주요 내용으로 다를 예정이다.

3절에서는 SBOM 기반 SW 공급망 보안을 발전시키기 위한 제언을 다룬다. 제언의 핵심 내용은 국내 중소기업이 SW 공급망 보안 체계를 구축하기 위해 정부의 지원 필요성, 기업 차원에서는 미국과 유럽의 무역장벽에 대응하기 위해 SBOM 및 공급망 보안 기술에 대한 적극적 투자, 수요자 관점의 기관 내 IT 자산과 SW 구성요소 관리 및 보안 취약점 모니터링 체계 구축 필요성, SW 위험관리와 사이버 복원력을 강화하고, 보안적합성 및 IoT 보안 라벨링 등 법적, 기술적 프레임워크 도입 필요성, 그리고 SBOM의 기밀성을 보장하면서 안전하게 공유하는 연구 필요성을 설명한다.

나. Secure Software Development Attestation Form 제도

이 품의 의미를 설명하기 전에 먼저 이 품이 나오게 된 추진 사항을 설명한다. 솔라윈즈 공급망 공격 등 미국 정부에 대한 공급망 보안 위협이 급증함에 따라 2021년 5월 대통령 행정명령을 통해 소프트웨어의 공급망 보안 강화를 천명했다. 이를 통해 많은 문서 및 지침들이 작성됐고, 이 중 2022년 2월 “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities”가 발표됐다. 2022년 9월 OMB는 “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”(M-22-18)을 발표했다. 이 문서의 핵심 내용이 연방정부에 SW를 납품하는 공급자는 SSDF를 준수해야 하며 이를 수행했음을 선언하는 Secure Software Development Attestation Form 또는 Self-attestation Form(자체증명서)를 함께 제출해야 한다는 것이다[9]. 이 문서에서 자체증명서 실행을 2023년 9월로 정하였으나, 일정이 늦어지면서 2023년 6월 “Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”(M-23-16)을 발표했다[10]. 이 지침에서 자체증명서 도입 실행 시기를 CISA가 자체증명서 양식의 최종본을 릴리즈한 후 3개월 후부터 Critical SW, 6개월 후부터 모든 SW에 대해 밟도록 정했다. 2024년 3월 11일, 드디어 최종 품이 발표되었고 OMB의 추가 지침이 없으므로 M-23-16에 따라 6월 11일부터 Critical SW, 9월 11일부터 모든 SW를 연방정부에 납품할 때, 이 품을 제출해야 한다. 따라서 미국 연방정부의 공급망 보안의 가장 기초는 SSDF를 근간으로 만들어진 자체증명서라고 할 수 있다.

Insights | 전문가 칼럼

자체증명서 양식은 먼저 작성과 관련된 몇가지 정보를 제공하는데 이 중 몇 가지 중요한 점을 언급하고자 한다.

- 양식에서 요청한 정보를 제공하지 않을 경우, 해당 소프트웨어를 더 이상 사용하지 못할 수 있음: 연방정부에서 SW를 사용하려면 관련 정보가 모두 기재된 자체증명서가 필요하며, 이를 제출하지 못할 경우, SW를 사용할 수 없게 된다.
- 고의로 거짓 또는 오해의 소지가 있는 정보를 제공하면 형법 18 U.S.C. § 1001의 위반이 될 수 있음: 형법 18 U.S.C. § 1001은 연방 정부에 대해 거짓 진술을 하거나 사기를 행하는 행위를 금지하는 미국 연방법으로써 연방정부에 거짓 진술이나 허위 문서를 금지하고 벌하는 법인데, 이 법이 자체증명서에도 적용되므로, 고의로 정보를 누락하거나 수정할 경우, 최대 5년의 징역형에 처할 수 있고 테러리즘이 연관되면 8년까지 징역형에 처할 수 있다. 미국 정부의 소프트웨어 공급망 보안에 대한 의지를 알 수 있다.
- 2022년 9월 14일을 기준으로, 이날 이후 개발됐거나, 주요 버전이 변경됐거나, 날짜와 관계없이 소프트웨어 제작자가 지속적인 코드 변경을 제공하는 경우는 자체증명서 양식을 제출해야 함: 자체증명서 양식을 2024년 6월 11일부터 받지만, 대상 소프트웨어는 M-22-1801 공개됐던 2022년 9월 14일을 기준으로 한다. 버전 번호가 2.5에서 3.0 등으로 변경될 경우, 주요 버전 변경으로 간주하고, 이 변경이 2022년 9월 14일 이후 발생했을 경우, 자체증명서를 제출해야 한다. 또한 SaaS 형태 제품, CI/CD 등으로 소프트웨어의 구성요소가 언제든지 수정될 수 있는 제품은 제품이 개발된 날짜와 관계없이 자체증명서를 제출해야 한다.
- 연방 기관이 개발한 소프트웨어, 오픈소스 및 3자 소프트웨어인 경우, 자체증명서 제출 대상 아님: 오픈소스를 사용했거나 3자가 개발한 소프트웨어 컴포넌트에 대해서 개발사가 SSDF를 모두 수행하기 한계가 있으므로, 해당 컴포넌트에 대해서는 SSDF 적용 의무를 면해주는 것으로 보인다.
- 제3자 평가를 제출하여 최소 요구사항 준수를 입증할 수 있음: 기업 스스로 SSDF를 확실히 수행했다고 증명하는데 확신이 없다면 제삼자 인증도 가능하다. 3PAO(Third Party Assessor Organization)로 불리는 3자 인증기관이란 FedRAMP 인증을 받았거나 적절한 기관 공식으로부터 서면 승인을 받은 기관을 뜻한다. 3PAO의 인증을 받은 기업은 자체증명서를 제출하지 않아도 된다.
- 자체증명서를 제출하지 않더라도, 소프트웨어를 사용할 방법은 있음: 자체증명서를 받을 수 없는 경우, 개발사가 인증할 수 없는 관행을 식별하고, 관련된 위험을 완화하기 위해 시행하고 있는 관행을 문서화하며, 조치 및 마일스톤 계획(POA&M)을 제출하면 해당 소프트웨어를 계속 사용할 수 있다.

제출용 자체증명서 양식은 크게 3개 섹션으로 구성되어 있다. Section I는 자체증명서 양식의 첫 번째 섹션으로, 인증의 종류(New Attestation, Attestation Following Extension or Waiver, Revised Attestation)와 범위(Company-wide, Individual Product, Multiple Products or Specific Product Version(s)), 소프트웨어 제품에 대한 기본 정보(Product(s) Name, Version Number, Release/Publish Date)를 제공한다. Section II에는 자체증명서를 제출하는 기업과 연락처 정보를 기입한다.

Section III가 자체증명서에서 가장 중요한 부분으로써 SSDF에서 추출한 SW 개발 관행을 나열하고 이 관행을 잘 지켰다는 데에 체크하고 사인을 하면 된다. SSDF에서 추출한 SW 개발 관행은 아래와 같다. SSDF가 조직 준비(Prepare the Organization, PO), SW 보호(Protect the Software, PS), 보안성 높은 SW 개발(Produce Well-

Insights | 전문가 칼럼

Secured Software, PW), 보안취약점 대응(Respond to Vulnerabilities, RV) 등 4개 원칙을 정하고 각 원칙을 이루는 데 필요한 상세 과업을 제시한 데 비해, 자체증명서는 이 과업 중에서 꼭 수행이 필요한 부분만 남긴 것이다. 즉, 미국 연방정부 납품을 위해서 SSDF는 다 못 수행하더라도, 자체증명서에 있는 부분은 꼭 수행하는 것이 필요하다. 물론, 앞서 설명한 바와 같이 일부 수행하지 못하더라도 POA&M을 제출하면 도입할 수 있지만, POA&M을 제출하면서까지 꼭 해당 소프트웨어를 도입해야 할 상황이 아니라면, 자체증명서에 제시한 과업의 구현은 필수적이다.

표 2-6 자체증명서 공급망 보안 수행 요건

- 1) 소프트웨어는 안전한 환경에서 개발 및 구축되었다. 이러한 환경은 최소한 다음과 같은 조치를 통해 보호된다:
 - a) 소프트웨어 개발 및 구축에 관여하는 각 환경을 분리하고 보호.
 - b) 승인 및 접근에 사용되는 신뢰 관계를 정기적으로 기록, 모니터링 및 감사:
 - i) 모든 소프트웨어 개발 및 구축 환경에 대해;
 - ii) 각 환경 내 구성 요소 간에;
 - c) 소프트웨어 개발 및 구축과 관련된 환경 전반에서 다중 인증 및 조건부 접근을 적용하여 보안 위험을 최소화.
 - d) 소프트웨어를 개발 및 구축하는 환경에서 과도한 위험을 초래하는 소프트웨어 제품의 사용 또는 포함을 최소화하고 문서화하기 위한 일관되고 합리적인 조치 적용
 - e) 가능하고 위험에 기반하여 자격 증명 등 민감한 데이터를 암호화
 - f) 연속적인 운영 모니터링 및 경고를 포함한 방어적 사이버보안 관행을 구현하고, 필요에 따라 의심 되거나 확인된 사이버 사건에 대응
- 2) 소프트웨어 제작자는 내부 코드와 타사 구성요소의 보안을 다루고 관련 취약성을 관리하기 위해 자동화 도구 또는 유사한 프로세스를 사용하여 신뢰할 수 있는 소스 코드 공급망을 유지하기 위해 선의의 노력을 기울인다.
- 3) 소프트웨어 제작자는 소프트웨어에 포함된 내부 코드 및 타사 구성요소의 출처를 최대한 유지한다.
- 4) 소프트웨어 제작자는 보안 취약성을 확인하기 위해 자동화 도구 또는 유사한 프로세스를 사용한다.
추가로:
 - a) 소프트웨어 제작자는 이러한 프로세스를 지속적으로 운영하며, 제품, 버전 또는 업데이트 출시 전에 수행;
 - b) 소프트웨어 제작자는 제품 출시 전에 발견된 보안 취약성을 해결하기 위한 정책 또는 프로세스를 보유;
 - c) 소프트웨어 제작자는 취약성 공개 프로그램을 운영하며, 공개된 소프트웨어 취약성을 신속하게 수락, 검토 및 해결함. 이는 취약성 공개 프로그램이나 적용 가능한 정책에 명시된 일정에 따라 이루어짐

Insights | 전문가 칼럼

자체증명서 최종 버전이 나왔을 때 전 세계 많은 전문가가 관심을 가진 부분이 있다. 과연 SBOM 제출이 필수가 됐을까에 대한 부분이었다. 애초 M-22-18 지침서에 SBOM 제출이 요구될 수 있다고 명시되어 있었고, 자체증명서 초기 버전에도 SBOM에 대한 설명이 있었다. 하지만 최종 버전에서는 SBOM이라는 키워드 자체가 사라졌다. 그렇다면 SBOM도 만들지 않아도 되고 공급망 관리를 제대로 하지 않아도 되는가? 절대 그렇지 않다. 연방정부 기관에 자동으로 SBOM을 제출해야 하는 의무는 없지만 소프트웨어 개발 기업은 소프트웨어에 포함된 컴포넌트에 리스트인 SBOM을 만들지 않고는 자체증명서의 2번과 3번을 신의 있게 수행했다는 증명을 하기 거의 불가능하다. 왜냐면 소프트웨어에 사용한 구성요소의 출처를 관리해야 하고, 이를 명세한 리스트가 SBOM이기 때문이다.

Step 5: The next screen supports the option to select any previously uploaded or upload any new Artifacts. Artifacts may include documentation supporting the Attestation or affiliation of the registered user with the Agency or Organization. This step is optional. Please note - this is NOT where the Self Attestation Form is uploaded. Click "Next."

그림 2-15 온라인 자체증명서 접수 Step 5 : Artifacts 업로드 옵션

SBOM기반 소프트웨어 구성요소 관리는 실질적 의무 사항으로 이해해도 큰 문제가 없음을 간접적으로 알수 있는 것이 자체증명서 온라인 접수 매뉴얼의 artifact 업로드 옵션이다. 온라인 접수처인 <https://softwaresecurity.cisa.gov> 방문 후, 계정 생성한 후 자체증명서와 함께 자체증명서에서 주장한 사실, 즉 소프트웨어 개발사는 자체증명서의 지침에 따라 개발을 했다는 것을 증명하는 결과물인 artifact를 올릴 수 있는 옵션을 추가했다. 안전한 개발환경의 경우, 개발환경 구성도와 시스템 보호를 위한 수행한 로그를 제출하면 되고, 취약점 관리 부분도 취약점 점검 내역과 조치 결과를 제출하면 될 것이다. 하지만 SBOM을 제출하지 않고서는 자체증명서의 2번과 3번 요건을 증명하기 매우 어려우므로 많은 기업이 이 사이트를 통해 SBOM을 제출할 것으로 예상된다.

이 기고문을 마무리하는 중 6월 11일이 지나갔다. 이날은 Critical SW 도입에 대한 자체증명서 제출 의무 시행 첫날이다. 각 기업은 과연 어느 정보까지 제출할 것인지에 관심이 기울여질 수밖에 없다. 추후 CISA의 보고서 혹은 관계자의 질의응답을 통해 이 내용들을 확인해 본다면 우리나라 정책 추진에도 많은 도움이 될 것이다.

다. 국가적 공급망 위협 대응 체계 구축 필요성

정보보안 분야에 종사하는 분들은 아는 사실이지만 우리나라는 사이버 침해 대응을 위한 국가적 체계가 매우 잘 갖추어져 있다. 국가를 크게 공공, 국방, 민간으로 구분하고 국방은 사이버작전사령부, 민간은 KISA, 공공은 국가정보원이 직접 책임지며, 국가 어떤 부분에라도 현격한 사이버 침해가 발생하면 국가정보원에 자동화된 시스템을 통해 침해 내용이 실시간으로 보고되고 분석된다. 이를 통해 우리나라는 다른 나라부터 월등히 뛰어난 침해 대응 체계를 갖추고 있다.

공급망 위협 대응도 이와 유사한 관리체계가 필요하다. Log4j 사태를 돌아보자. 취약점 발견 후 72시간 이내에 80만 건에 이르는 사이버 공격이 시도되었을 만큼, 위험한 취약점이 발생하면 이를 악용하는 공격이 반드시 발생하는 것이 현실이다. 그만큼 해커들도 새로운 취약점의 등장을 기다리고 있고, 이를 분석해서 즉각적으로 익스플로잇하는 공격을 수행하는 능력을 완벽히 갖추고 있다. 그러므로 이제 취약점은 사이버 공격에 준하게 대응해야 한다. 그래서 디지털제품에 대한 사이버 침해 원인의 2/3가 취약점 때문임을 인지한 EU도 제품에 포함된 취약점 제거 및 제품 출시 후 발견되는 취약점에 대한 즉각적인 조치를 요구하는 CRA를 추진 중이다.

그렇다면 이러한 취약점 관리와 공급망 위협 대응은 어떤 관계인가? 다시 Log4j 사태를 돌아보자. Log4j라는 역대급 취약점이 발견됐을 때 소프트웨어 개발업계 및 보안전문가들이 동시에 물어본 질문이 있다. “어떤 소프트웨어가 Log4j를 사용하고 있는가?” 보안전문가들은 소프트웨어 내의 구성요소에 대한 지식이 없으므로 전혀 대답할 수 없었고, Log4j를 직접 개발에 사용한 사람들 외에는 자신이 판매하는 소프트웨어에 Log4j가 포함되는지 모르는 기업이 대부분이었다. 취약점은 기업에서 개발한 특정 부분에서 발생하는 빈도 보다, 오픈소스에서 발견되는 경우가 월등히 많다. 취약점 보고가 오픈소스 커뮤니티 단위로 신고되며, 이 커뮤니티를 사용한 소프트웨어가 영향을 받는 것으로 분류되는 구조이다. 따라서 소프트웨어의 구성요소를 관리하고 있지 않으면 취약점이 발견되더라도, 이 취약점이 내가 개발한 또는 소유한 소프트웨어가 영향을 받는지를 판단할 수 없다. 즉, 공급망 관리를 하지 않으면 취약점 관리가 매우 어려운 상황이라는 것이다.

지금은 대규모 DDoS 공격보다는 많이 쓰이는 오픈소스의 취약점을 이용한 익스플로잇 공격이 더 위험해졌다. 따라서 등 국가적 사이버 침해 대응 체계도 이에 대응하기 위한 체계로 변화되어야 하고 이 핵심은 공급망 관리가 필수이다. 국가적 공급망 위협 대응 체계는 각 국가·공공기관의 자산, 소프트웨어, 소프트웨어 구성요소 관리 시스템 운영으로 시작되어야 한다. 부문 보안관제센터와 같이 여러 공공기관을 하나로 관리하는 기관에서 일괄적으로 각 공공기관의 소프트웨어와 구성요소, 취약점 현황을 관리한다. 이 정보가 사이버작전센터, KISA, 국가정보원 단위로 모인다면 우리나라 전체에 대한 취약점 관리를 실시간으로 할 수 있는 체계가 구축된다.

이런 체계가 구축된다면 미래의 또 다른 Log4j는 무섭지 않다. 왜냐면 어느 기관에 어떤 소프트웨어가 해당 취약점을 포함하고 있는지 즉각적으로 식별되며, 기관별, 부문별, 국가적으로 취약한 컴퓨터 숫자 및 조치 현황까지도 파악할 수 있다. 이를 통해 취약점에 대한 국가적 위험 관리가 가능해진다. 장기적인 관점에서 이러한 체계가 구축되기를 바란다.

라. 맷음말

소프트웨어가 모든 것을 지배하는 사회가 다가오고 있다. SW 공급망 공격은 단순한 서비스 장애, 데이터 유출의 수준을 넘어 교통, 환경, 전력, 원자력 등 사회 기반시설 공격을 통한 국가적 혼란을 초래할 수 있다. 이에 대한 대응은 단순히 기술적인 해결책을 넘어서는 종합적인 접근이 필요하다. 이번에 발표된 SW 공급망 보안 가이드라인(v1.0)은 이러한 요구에 부응하는 중요한 첫걸음이다. 이 가이드라인은 국가정보원, 과학기술정보통신부, 디지털플랫폼정부위원회가 협력해 민관 전문가들과 함께 공동으로 작성한 것으로, SW 라이프 사이클 전반에 걸쳐 공급망 보안을 강화하기 위한 구체적인 방안을 제시하고 있다.

앞으로의 발전 방향은 이 가이드라인을 바탕으로 국가 차원의 통합적인 공급망 보안 체계를 구축하는 것이다. 국가적 공급망 위협 대응 체계를 확립해 모든 공공기관이 자산, 소프트웨어, 소프트웨어 구성요소를 체계적으로 관리하고, 실시간으로 취약점을 파악하고 대응할 수 있어야 한다. 이를 통해 네트워크 기반 공격 대응 중심의 위협 대응에서 SW 취약점 대응 중심의 선제적이며 예방적인 대응으로 나아갈 수 있다. 이러한 노력이 결실을 맺어 우리나라가 사이버보안 분야에서 국제사회를 선도하기를 기대한다.

참고문헌

- [1] SW 공급망 보안 가이드라인 1.0 (전체본, 요약본), <https://www.kisa.or.kr/2060204/form?postSeq=15&page=1>
- [2] Executive Order on Improving the Nation's Cybersecurity, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>
- [3] Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, M-22-18, OMB
- [4] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, FDA, <https://www.fda.gov/media/119933/download?attachment>
- [5] EU Cyber Resilience Act, European Commission, <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>
- [6] Cybersecurity Supply Chain Risk Management, NIST, <https://csrc.nist.gov/projects/cyber-supply-chain-risk-management>
- [7] Securing the Software Supply Chain – Recommended practices guide for developers, Enduring Security Framework, https://media.defense.gov/2022/Nov/17/2003116445/-1/-1/0/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_CUSTOMER.PDF
- [8] Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST SP 800-218, <https://csrc.nist.gov/pubs/sp/800/218/final>
- [9] Secure Software Development Attestation Form, CISA, <https://www.cisa.gov/secure-software-attestation-form>
- [10] Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, M-23-16, OMB

Part. 2

05

랜섬웨어 그룹의 주요 동향 및 위험도 평가

S2W TALON

1. Introduction

랜섬웨어(Ransomware)는 시스템 내 파일을 암호화해 공격자에게 복구를 대가로 한 금전을 지불할 경우에만 복호화가 가능하도록 제작된 악성코드의 일종이다. 랜섬웨어 그룹들은 기업 및 조직 내 네트워크에 랜섬웨어를 유포해 운영을 마비시키며, 추가로 민감 데이터 유출, 기업 명성 하락 및 경제적 손실 등을 유도해 협상을 강제하는 전략을 사용하고 있다. 최근 랜섬웨어의 활동은 지속적으로 증가하고 있고, 협박 전략도 데이터 보안 강화 정책을 악용하는 등 더욱 더 교묘해지는 추세이다.

본 칼럼에서는 딥다크웹 및 텔레그램에서 활동하는 랜섬웨어 그룹들을 다양한 관점에서 분석하고, 분석한 결과를 바탕으로 랜섬웨어 그룹들의 위험도를 측정하는 평가 척도를 구축해 도출된 위험도 결과를 공유한다. 이어질 내용에서는 주요 랜섬웨어 그룹의 동향을 소개한 후, 각 랜섬웨어 그룹들의 특성들을 바탕으로 구축한 활동량, 영향력, 브랜드 지속성, 확장성, 취약점과 같은 5개의 지표를 기반으로 총 72개의 랜섬웨어 그룹의 위험도를 산출했다.

* 본 보고서는 랜섬웨어 그룹이 직접 운영하는 Leak 사이트에서 확인된 피해 대상만 선별해 분석 대상에 포함

2. Threatscape of Ransomware

본 장에서는 S2W에서 분석한 2023년 랜섬웨어 그룹 동향을 정량 및 정성적으로 각각 나누어 소개한다.

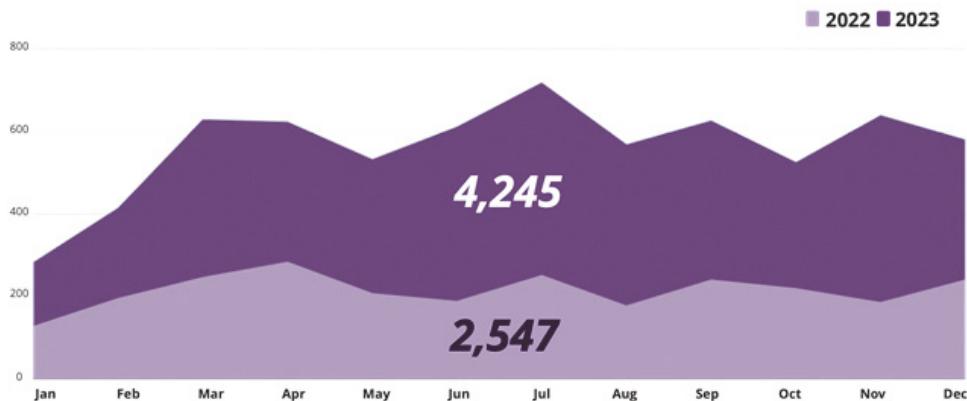
1 Quantitative Insights

정량적으로 분석한 파트에서는 랜섬웨어 그룹들의 2023년 활동량과, 특정 산업군에 미친 영향력, 그리고 2개 이상의 랜섬웨어 그룹들이 동일한 피해 대상을 Leak 사이트에 업로드한 사례들을 다룬다.

Insights | 전문가 칼럼

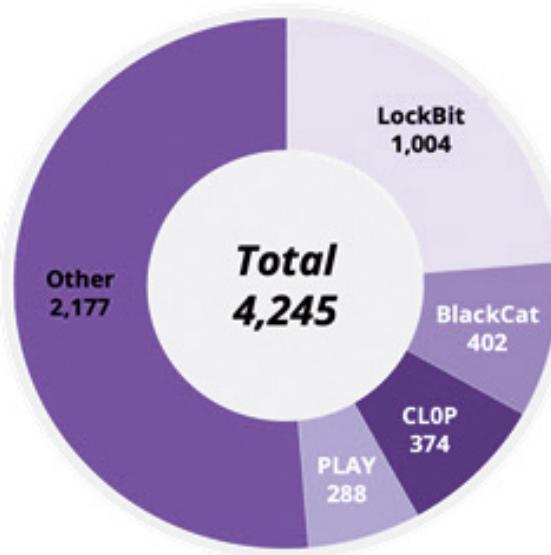
1. 활동량(Activity)

2023년 랜섬웨어 그룹의 Leak 사이트에 업로드된 피해 기업 수는 총 4,245 건으로, 2022년 대비 1.6배 증가한 수치로 나타났다.



▣ 그림 2-16 2022년 대비 2023년 랜섬웨어 Leak 사이트 업로드된 피해 기업 수 비교

2023년 랜섬웨어 그룹의 Leak 사이트에 업로드된 피해 기업 수를 대상으로 순위를 매긴 결과, Leak 사이트에 피해 기업을 많이 게시한 상위 5개 그룹은 LockBit, CLOP, 8BASE, BlackCat, PLAY로 확인된다. 이들은 그림 2-17와 같이 2023년 Leak 사이트에 업로드된 4,245건 중 전체의 50%에 육박하는 2,068 건을 차지했다.



▣ 그림 2-17 랜섬웨어 그룹 Leak 사이트 별 피해 기업 업로드 빈도 그래프

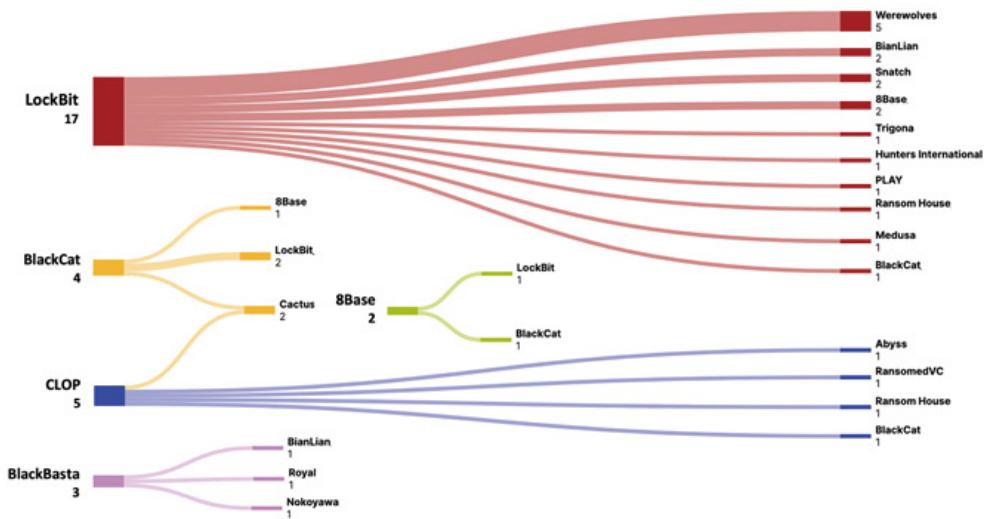
Insights | 전문가 칼럼

2023년 Leak 사이트에 업로드 된 기업이 속한 국가는 총 130개국으로 확인된다. 그림 2-15과 같이 전체 4,245건 중 미국은 절반이 조금 안되는 2,049 건의 피해가 확인됐으며, 영국, 캐나다, 독일 그리고 프랑스순이며, 한국은 14건으로 34위에 랭킹됐다. 특히 위 5개 국가들은 2023년 전체 랜섬웨어 Leak 사이트 업로드 건의 67%를 차지할 만큼 2023년 많은 피해를 입었다. 해당 국가들은 Worldometers에서 확인한 GDP 기준 전세계 10위 안에 드는 국가로, 경제력이 높은 국가의 기업들을 대상으로 랜섬웨어 공격이 다수 수행됐다.



[그림 2-18] 랜섬웨어 그룹 Leak 사이트 별 피해 국가 그래프

또 다른 흥미로운 결과는 그림 2-19에서 확인되는 바와 같이 랜섬웨어 그룹의 유출 사이트에 중복된 피해 기업이 업로드 됐다는 것이다. 이는 이미 피해 사실이 공개되어 비교적 침투하기 쉬운 기업을 우선적으로 선정해 추가로 공격하고자 하는 경향이 있거나, Initial Access Broker(IAB, 접근 권한 판매자)가 여러 랜섬웨어 그룹과 협력하고 있기 때문인 것으로 추측된다.



[그림 2-19] 랜섬웨어 그룹 Leak 사이트 내 중복 기업을 업로드한 랜섬웨어 그룹 현황 일부 그래프

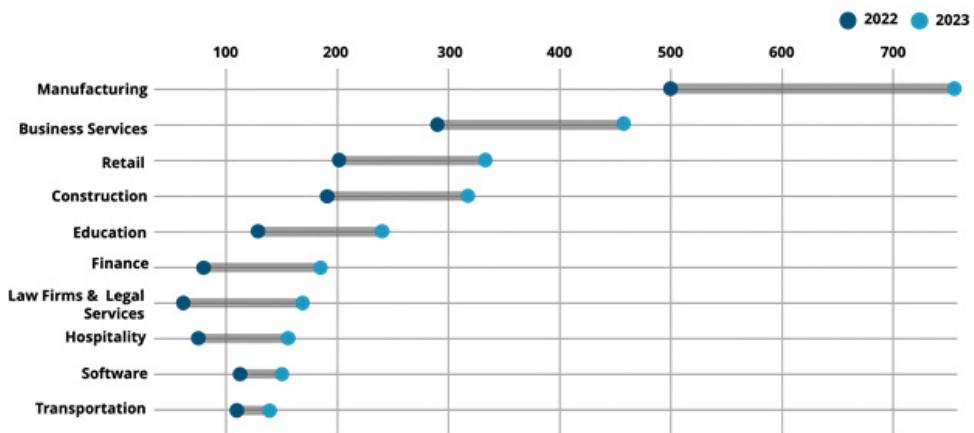
Insights | 전문가 칼럼

중복된 피해자를 먼저 업로드한 사실은 해당 그룹이 먼저 조직에 침투할 수 있음을 나타내며, 이는 동일한 피해 기업을 나중에 업로드한 랜섬웨어 그룹보다 숙련된 Pentester 또는 Affiliate가 먼저 업로드 그룹과 협력하고 있다는 징후로 해석될 수 있다. 더욱이 이들이 IAB와 협력한다고 가정할 때, IAB가 다수의 랜섬웨어 그룹과 협력할 경우 추후 다른 랜섬웨어 그룹도 동일한 침투 벡터로 추가 피해를 가하는 것도 가능하다. 2023년에 가장 많은 중복 피해자를 ‘먼저’ 업로드한 그룹은 LockBit이므로 이 그룹은 동일 기업 피해 사실 업로드 측면에서 가장 선제적인 공격 양상을 보이는 그룹이다.

2. 영향력(Influence)

2023년에 Leak 사이트에 업로드된 기업들의 업종 중 가장 많이 확인된 업종 10개는 그림 2-20에서 확인되는 바와 같이 제조업, 비즈니스 서비스업, 물류업, 건축업, 교육업, 금융업, 법률업, 숙박업, 소프트웨어업, 교통업으로 확인된다. 해당 10개 업종들의 2022년과 2023년 수치를 비교하면, 2023년 모든 업종들의 피해 건수가 증가된 것으로 확인된다.

피해 업종 상위권에는 BankRate에서 조사한 2023년 수익이 높은 업종 중 6개가 해당되는 점이 확인됐으며, 이는 랜섬웨어 그룹이 매출 규모가 높은 편에 속하는 업종을 타겟하는 경향이 있다고 해석된다. 특히, Leak 사이트에 가장 많이 게시된 제조업의 경우, 랜섬웨어 공격으로 인해 생산이 중단되어 상당한 재정적 손실이 발생할 수 있다. 이와 같이 매출 규모는 높으면서 업종별 발생할 수 있는 특수한 기업 운영상의 취약한 부분들을 랜섬웨어 그룹들이 전략적으로 고려했을 가능성이 있다.



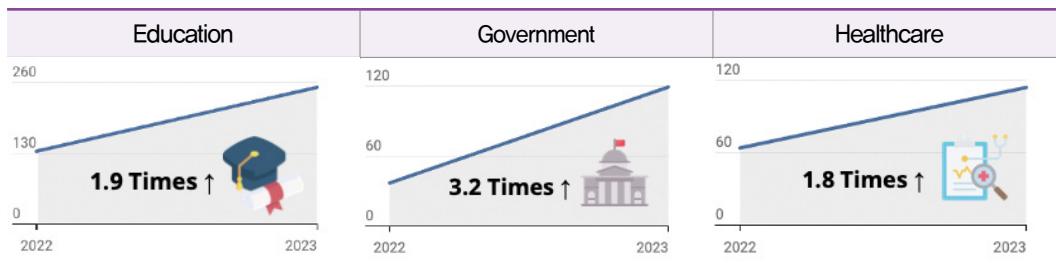
▣ 그림 2-20 랜섬웨어 Leak 사이트에 업로드된 2023년 기준 상위 10개 업종 별 2022~23년 수치 비교 그래프

또한, 다른 업종에 비해 민감 데이터를 많이 다루고, 중단 시 큰 사회적 파장을 일으킬 수 있는 교육업, 보건업, 그리고 정부기관에 대해서도 랜섬웨어 그룹으로 인한 피해가 증가한 사실이 확인됐다. 특히, CyberReason에서 공개한 내용에 따라 정부 기관에는 민감 정보가 다수 존재하고, 다양한 산업군이 교차하는 곳이며 정부에 대한 공격은 곧 나라에 대한 공격으로 간주되기도 할 만큼 영향력이 큰 업종이다.

Insights | 전문가 칼럼

표 2-3과 같이 2022년 대비 2023년 교육업은 1.9배, 보건업은 1.8배 그리고 정부 기관은 3.2배 피해 수치가 증가했다. 뿐만 아니라, 해당 업종들을 타겟하는 랜섬웨어 그룹도 2022년 39개였던 것에 비해 2023년에는 49개로 증가하며, 사회적으로도 랜섬웨어 그룹에 의한 피해를 많이 받은 것으로 관찰된다.

[표 2-7] 특수 산업군에 대한 피해량 변화 표

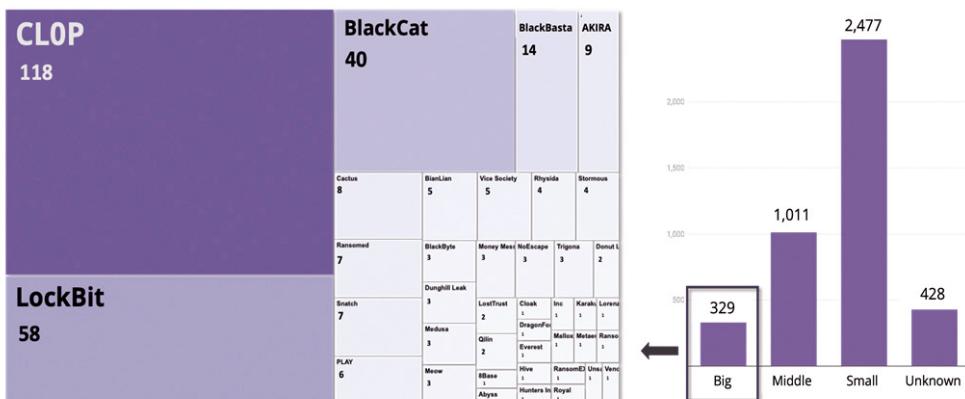


더 나아가, Leak 사이트에서 확인된 피해 기업들의 매출 규모를 파악하여, 2023년 Gartner에서 발표한 기준에 따라 대기업, 중견기업, 소기업 별 피해 현황을 분석했다.

[표 2-8] 매출 기반 피해 기업 규모 구분 기준

기업 규모	매출 기준
대기업	\$1 Billion ≤ 매출
중견기업	\$50 Million ≤ 매출 < \$1 Billion
소기업	매출 < \$50 Million

특히, 대기업에 대한 성공적인 공격은 뛰어난 침투 기술과 관련이 높다고 볼 수 있는데, CLOP, LockBit, BlackCat, BlackBasta 와 AKIRA은 대기업을 대상으로 다수의 공격을 수행한 그룹들로 확인됐다.



[그림 2-21] 대기업에 대한 피해 사실을 공개한 랜섬웨어 그룹 현황 그래프

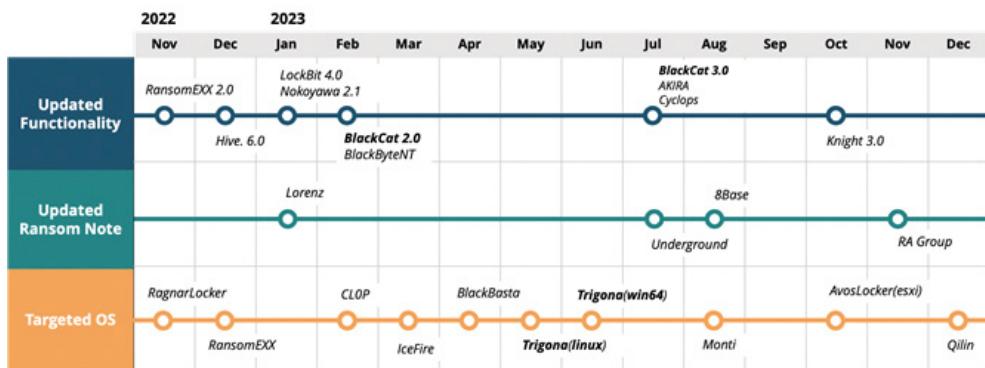
Insights | 전문가 칼럼

2 Qualitative Insights

이번에는 랜섬웨어 그룹이 자신들의 브랜드에 대한 지속성을 유지하기 위해 사용되는 브랜드 강화 전략을 살펴본다. 특히, 랜섬웨어 그룹의 다크웹 활동을 통한 인프라 확장 및 구축 방식에 대해 알아본다. 추가로, 그룹별로 랜섬웨어 공격에 활용한 0-day와 1-day 취약점 사용 이력과 해당 취약점들의 위험도를 살펴본다.

1. 브랜드 지속성(Brand Continuity)

랜섬웨어 그룹은 탐지를 회피하기 위해 일부 기능을 수정 및 보완하고, 랜섬노트를 변경하기도 한다. 또한, 공격 범위를 확대하기 위해 Windows 외에 Linux와 macOS 운영체제를 대상으로 하는 랜섬웨어 개발에 전념하기도 한다. 아래 그림 2-22에서 확인되는 바와 같이, 2023년에는 72개 그룹 중 최소 26개 그룹의 랜섬웨어에 대해 버전 업데이트가 이뤄졌으며, 그 중 가장 많은 버전 업데이트가 이루어진 그룹은 BlackCat으로 확인됐다.



[그림 2-22] 2023년동안 버전 업데이트를 수행한 랜섬웨어 그룹

이 외에도 랜섬웨어 그룹의 활동을 지속적으로 이어나가기 위해, 리브랜딩을 수행하는 경우도 존재한다. 리브랜딩은 브랜드 이미지 개선, 다른 그룹과의 협력 또는 진화하는 TTP를 기반으로 새로운 그룹명을 사용하는 행위를 의미한다. 리브랜딩된 그룹은 이전과 유사한 유형의 랜섬노트가 발견되거나 기존 랜섬웨어와 유사한 코드를 가진 새로운 이름의 랜섬웨어가 발견되기도 한다. 다수의 리브랜딩 이력이 존재한다는 점은 랜섬웨어 그룹 활동을 계속 유지하겠다는 의지를 보여주는 것으로 판단된다.

2. 확장성(Extensibility)

뿐만 아니라, RaaS 생태계에서 랜섬웨어 그룹은 조직적인 운영 및 인프라를 확장하기 위해 체계화된 역할 분담에 따라 그룹을 운영한다. 그림 8에서 보여지듯이, 랜섬웨어 그룹의 핵심 구성원(Core Member)들은 실제 침투를 담당하는 Affiliate와 협력한다. 또한 IAB를 통해 기업에 대한 초기 침투 벡터를 획득하거나, DDoS, Botnet 및 Stealer 판매자 등으로부터 서비스 및 악성코드 빌더와 라이센스를 구매하거나 구독해 랜섬웨어 공격에 활용한다.

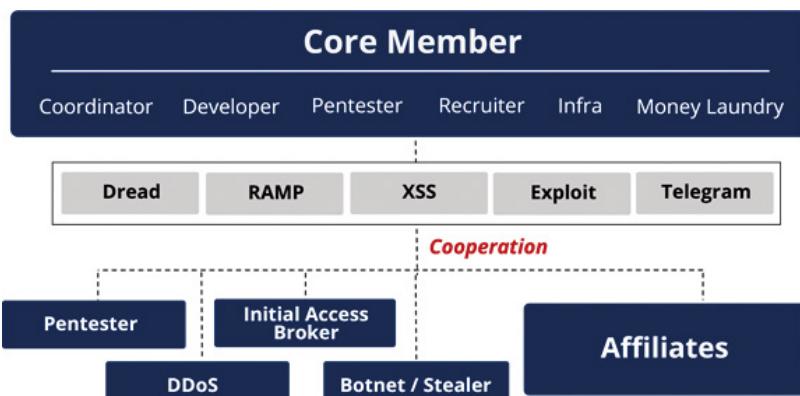


그림 2-23 RaaS 생태계 구조

또한 랜섬웨어 그룹의 약 84%가 피해 기업을 업로드하는 Leak 사이트를 운영하고 있다. 기존의 많은 랜섬웨어 그룹이 다크웹에 Leak 사이트를 구축했지만, 최근에는 운영 부담이 적고, 검색을 통한 접근이 비교적 쉬운 Twitter와 Telegram 등의 소셜 플랫폼과 Clearnet 도메인을 사용하는 방향으로 바뀌는 추세이다. 다만, Clearnet을 사용하는 그룹은 다크웹을 사용하는 그룹보다 IP의 흔적을 남길 가능성이 더 높다고 판단된다. 따라서 다크웹 내 인프라 구축 여부는 랜섬웨어 그룹의 활동성을 측정하는 중요한 지표로 여겨진다.

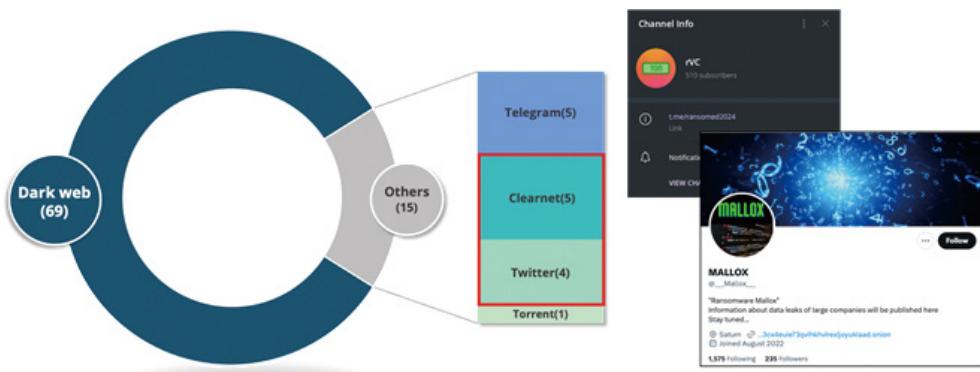


그림 2-24 랜섬웨어 그룹의 인프라 구축 현황

3. 취약점(Vulnerability)

공개된 기사 및 보고서에서 확인된 랜섬웨어 그룹이 사용하는 취약점 정보는 그림 2-25과 같다. 2023년 취약점을 사용하는 것으로 알려진 랜섬웨어 그룹은 최소 13개 이상 있으며, 그 중 약 47%는 기업 내부 환경 침투를 위해 원격 코드 실행(RCE) 취약점을 사용했다. 랜섬웨어 그룹이 악용한 취약점의 위험도는 CVSS와 EPSS 점수를 기반으로 평가했다.

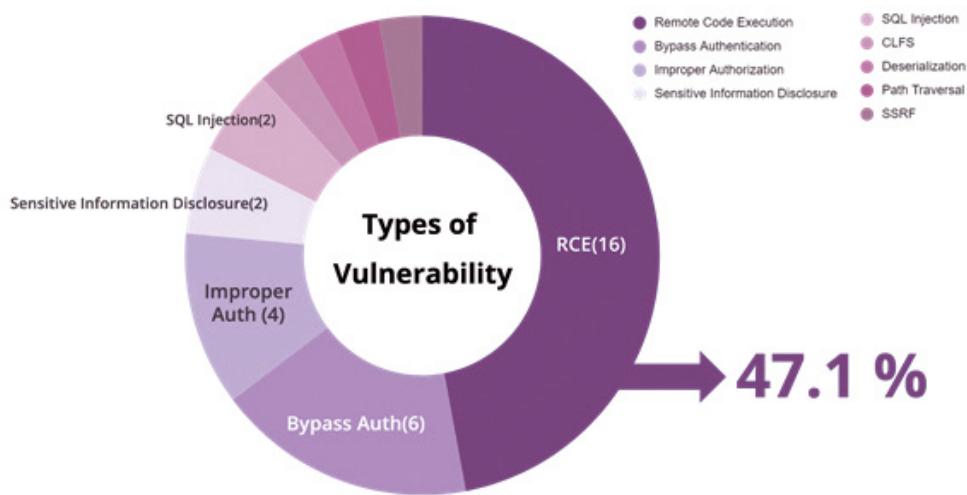


그림 2-25 랜섬웨어 그룹이 사용한 취약점 유형 구분 그래프

3. Ransomware Risk Assessment

앞서 정량적, 정성적으로 확인한 랜섬웨어 그룹의 동향을 기반으로 S2W가 자체적으로 구축한 랜섬웨어 그룹의 위험도 평가 기준을 소개하고, 각 그룹의 위험도 측정 결과를 토대로 유사한 성격을 가진 그룹을 클러스터링해 분석한 결과를 설명한다.

① 랜섬웨어 그룹의 위험도 평가 지표

랜섬웨어 그룹의 평가 지표를 구성할 때, 위험도를 증가시키는 지표를 참고해 점수를 부여했으며, 위험도를 감소시키는 지표에는 전체 합산 점수에 낮은 가중치를 부여해 계산된 평가 결과에 따라 랜섬웨어 그룹을 위험도에 따라 4가지 위험 수준으로 구분했다. 위험 수준 구분 기준과 위험도 평가를 위한 상세 지표는 각각 표 2-9, 표 2-10와 같다.

Insights | 전문가 칼럼

[표 2-9] 위험 수준 구분 기준

위험 수준	세부 구분 기준
Highly Severe	위험 지표 합산 값이 상위 25% 이하인 경우
Severe	위험 지표 합산 값이 상위 25% 초과, 50%인 이하인 경우
Moderate	위험 지표 합산 값이 상위 50% 초과, 75% 이하인 경우
Low	위험 지표 합산 값이 상위 75% 초과인 경우

랜섬웨어 그룹의 위험도를 증가시키는 지표는 앞서 언급한 활동량(Activity), 영향력(Influence), 브랜드 지속성(Brand Continuity), 확장성(Extensibility), 취약점(Vulnerability)이라는 5가지 지표로, 그 외 지표는 위험도를 감소시키는 지표로 구분했다.

[표 2-10] 위험도를 증가시키는 지표

No.	대분류	상세 지표
1	활동량	전체 피해 기업 수
2		중복 기업을 먼저 업로드한 횟수
3		중복 기업을 나중에 업로드한 공격 그룹의 유형
4	영향력	주요 산업군 집중 타겟
5		기업 규모별 타겟
6		특수 산업군 집중 타겟
7		특수 산업군: 비영리단체(교육, 의료, 복지, 문화, 환경단체), 정부 기관
8		버전 업데이트
9	브랜드 지속성	타겟 OS 종류
10		랜섬웨어 그룹의 리브랜딩
11		활동 기간
12		랜섬웨어 운영 그룹의 구인구직 & RaaS 홍보 다크웹 활동
13		Affiliate(Pentester, IAB)의 존재 여부
14		다크웹 내 구축된 인프라 유무
15		커스텀 도구 사용 여부
16	취약점	Critical한 취약점 사용 여부 (CVSS)
17		Critical한 취약점 사용 여부 (EPSS)
18		0day 취약점 사용 여부
19	감산 지표	복호화 도구 공개
20		공개된 소스코드/빌더 인용
21		인프라 유출 (소스코드, 채팅 내용 등)
		Take-down 여부

Insights | 전문가 칼럼

2 랜섬웨어 그룹의 위험도 평가 결과

감산 지표가 랜섬웨어 그룹의 위험도를 측정하는데 얼마나 큰 영향을 미치는지 확인하기 위해, 감산 지표의 적용 여부에 따라 랜섬웨어 그룹의 위험도를 나누어 평가했다.

먼저 감점 지표를 적용하지 않았을 때, 위험 지표 합산 값이 가장 높은 상위 5개 랜섬웨어 그룹은 LockBit, BlackCat, CLOP, BlackBasta 그리고 Nokoyawa로 확인됐다.

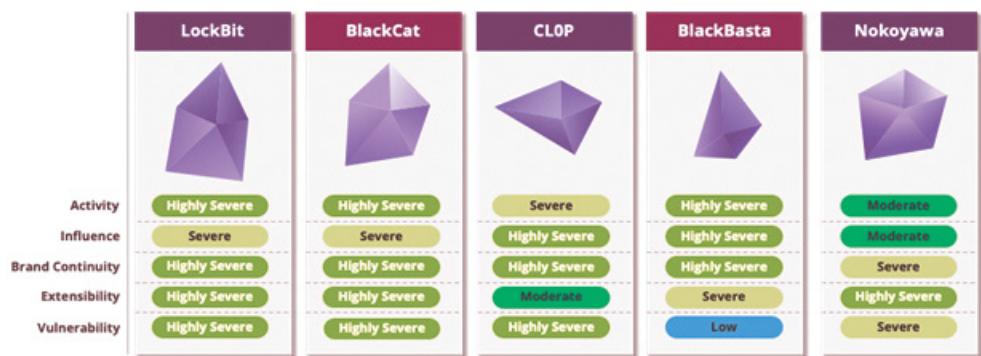


그림 2-26 위험 지표 합산 값이 높은 상위 5개 그룹 (감산 지표 적용 전)

감산 지표를 적용한 결과, 위험 지표 합산 값이 가장 높은 상위 5개 그룹에 포함됐던 LockBit과 BlackCat 그룹은 인프라 유출로 인한 감점이 적용돼 등수가 하향 조정됐고, Qilin과 BlackByte 그룹이 새롭게 상위 5개 그룹에 속하게 됐다. 감산 지표가 적용된 후 재산정된 상위 5개 그룹의 각 위험 수준은 그림 2-27와 같다.

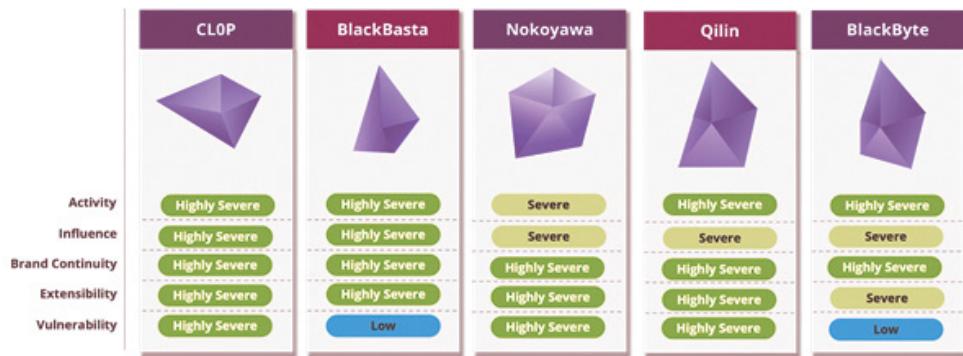
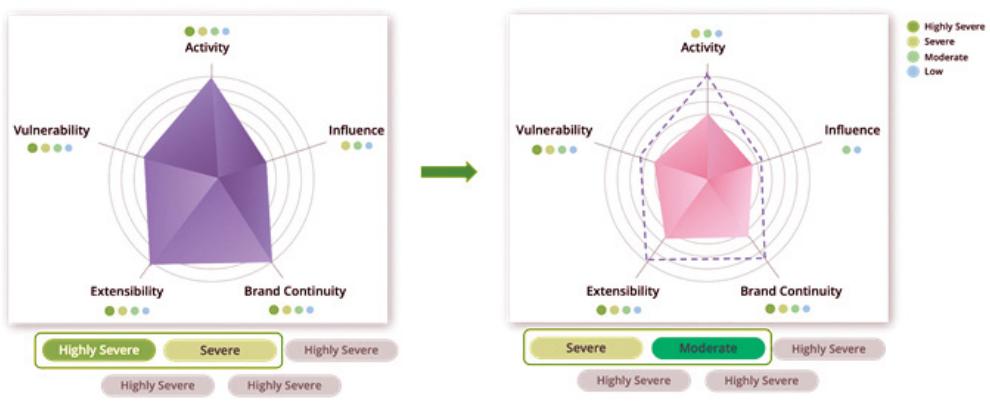


그림 2-27 위험 지표 합산 값이 높은 상위 5개 그룹 (감산 지표 적용 후)

Insights | 전문가 칼럼

위 내용은 2023년 랜섬웨어 그룹 동향을 기준으로 각 그룹의 위험도를 평가한 결과이지만, 2024년 2월에 공개된 Operation Cronos를 통해 LockBit 그룹의 인프라가 Take-down 되는 큰 이슈가 발생했다. 해당 이슈를 반영하기 전 2023년 한 해 동안의 활동을 기반으로 점수를 산출했을 때, LockBit 그룹의 위험 지표 합산 값은 총점 50점 중 38.7점으로 매우 높게 나타났다. 반면, 2024년에 발생한 인프라 Take-down 이슈가 위험도 측정에 반영된 후에는 총점이 27.07점으로 감소했다. 이처럼 제시하는 스코어링 체계를 통해 변화하는 지표를 정량적으로 반영해 랜섬웨어 그룹의 위험도를 측정할 수 있다.



▣ 그림 2-28 LockBit 그룹의 인프라 Take-down 이슈에 따른 점수 변화

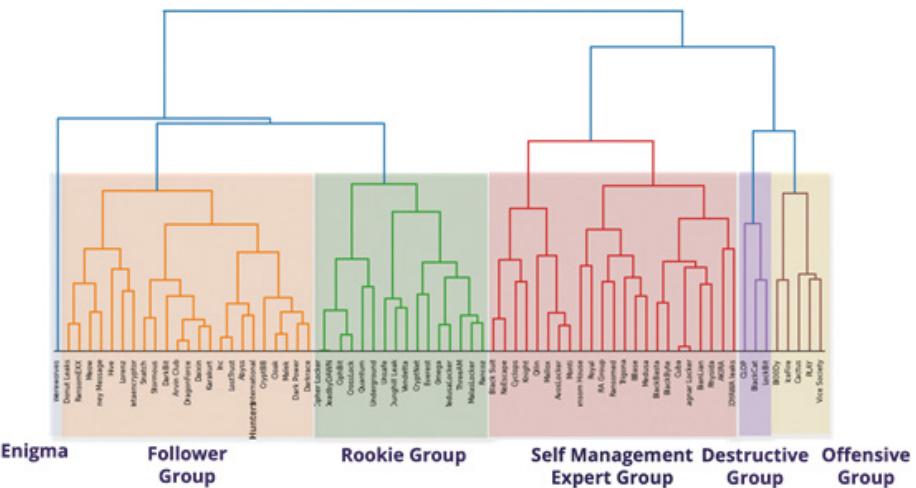
③ 랜섬웨어 그룹 클러스터링 결과

각 랜섬웨어 그룹의 위험도를 측정할 뿐만 아니라, 스코어링 결과를 기반으로 유사한 특징을 지닌 랜섬웨어 그룹을 클러스터링하는 작업을 진행했다.

이 과정에서 Ward Distance 기반의 계층적 클러스터링(Hierarchical Clustering) 기법이 사용됐으며, 72개의 랜섬웨어 그룹은 그림 2-29와 같이 6개의 클러스터로 구분됐고, S2W에서는 각 클러스터의 이름을 특징에 따라 Enigma, Follower Group, Rookie Group, Self Management Expert Group, Destructive Group 그리고 Offensive Group으로 명명했다. 각 그룹에 대한 상세한 특징은 아래 보고서에서 기술했다.

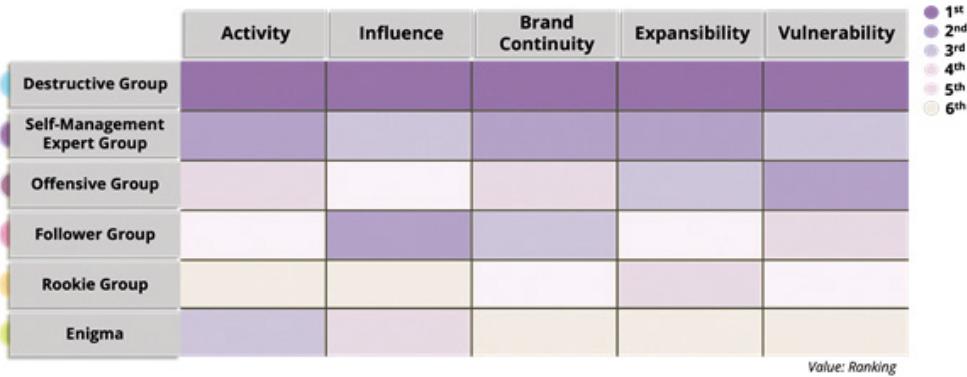
* Ransomware Resurgence: A Deep Dive into 2023's Threatscape and Risk Assessment

Insights | 전문가 칼럼



▣ 그림 2-29 랜섬웨어 그룹의 클러스터링 결과

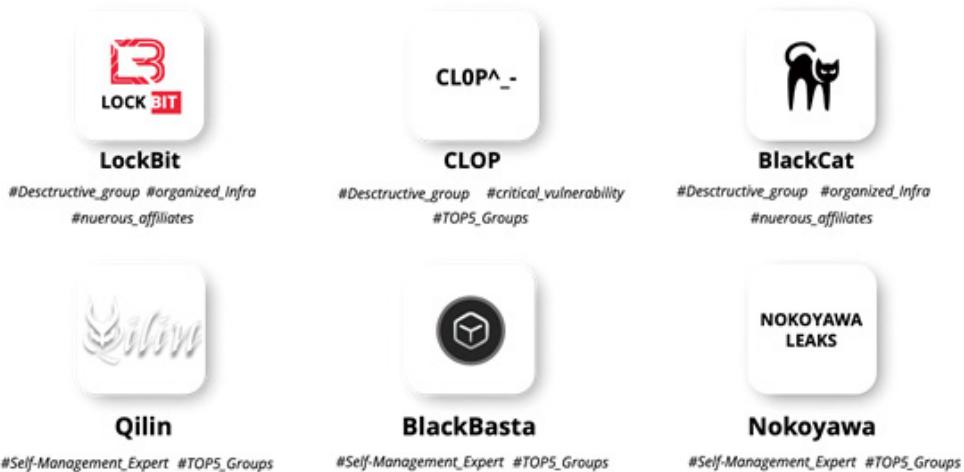
앞서 도출한 6개의 클러스터를 위험도 지표의 합산 값으로 구분한 결과, Destructive Group은 모든 지표에서 가장 높은 순위를 차지했고, Rookie 그룹은 모든 지표에서 대체로 낮은 등수를 차지했다.



▣ 그림 2-30 위험 지표 합산 값을 기반으로 한 클러스터 순위

4. Conclusion

위와 같은 분석 결과를 바탕으로 한 해동안 가장 위협적인 랜섬웨어 그룹을 선정했으며, 각 랜섬웨어의 위험도와 클러스터링 결과를 모두 고려했다. 가장 위협적인 랜섬웨어 그룹은 위험 지표 합산 값이 가장 높은 상위 2개 클러스터인 Destructive Group과 Self Management Expert Group에 속한 그룹 중, 위험 지표 합산 값이 가장 높은 상위 3개 그룹으로 선정됐다. LockBit과 BlackCat의 경우 감산 지표가 적용됐음에도 랜섬웨어 그룹의 위험 지표 합산 값이 상위 10위 이내로 위치하며 여전히 영향력 있는 랜섬웨어임을 입증했다.



▣ 그림 2-31 2023년 한 해동안 높은 위험 수준을 보인 랜섬웨어 그룹

이처럼 위험도 스코어링 체계를 활용해 각 랜섬웨어 그룹의 위험도를 정량적인 수치로 측정하고, 유사한 성질을 가지는 랜섬웨어를 군집화해 가장 큰 위협으로 간주되는 랜섬웨어 그룹을 도출했다. 본 칼럼에서 제시한 위험도 스코어링 체계는 추후 신규 랜섬웨어 그룹의 등장이나 랜섬웨어 그룹의 활동에 변화가 발생해도 신속하고 정량적인 위험도 측정이 가능하게 할 것으로 기대된다.

Part. 2

06

안전한 클라우드 서비스 이용을 통한 정보유출 방지

AWS 신은수 보안기술총괄

현재의 IT(Information Technology, 정보기술) 이용환경을 보면 클라우드는 기업이 선택할 수 있는 데이터 저장 서비스 유형 중 가장 많은 데이터를 저장하고 있는 중요 자산 중 하나라고 볼 수 있다. 그리고 이처럼 많은 데이터를 저장하고 있는 클라우드는 기업의 데이터 접근 요구사항을 충족할 수 있도록 다양한 유형으로 저장 서비스를 제공하고 있으며, 클라우드를 사용하는 사용자는 사무실, 집 혹은 이동 중에 자유롭게 데이터를 클라우드에 저장하거나 이용할 수 있다. 즉, 온프레미스 환경에서 데이터를 처리하던 것보다 클라우드를 이용하는 환경에서는 기업의 입장에서 조직에 필요한 데이터 처리에 대한 편리함이 증가하였다고 볼 수 있다. 그리고 많은 기업이나 조직들이 개인정보나 기업 내부 영업정보 혹은 기타 중요 데이터들을 클라우드 기반 저장서비스를 통해 보관하고 있으며 내부 혹은 외부 서비스를 제공하는데 이와 같은 데이터들을 적극적으로 활용하고 있다.

이처럼 기업에서 각종 데이터를 클라우드 환경에서 처리하게 되면서 각 기업의 보안 조직에서는 클라우드에 저장되는 각종 데이터를 안전하게 보관하고 내외부의 공격자 혹은 위협행위자로부터 보호하기 위해 다양한 조치를 수행하고 있다.

클라우드 사업자 역시 고객이 각종 위협으로부터 데이터를 안전하게 보호할 수 있도록 다양한 보안 기능을 제공함과 동시에 위협을 최소화할 수 있는 각종 모범사례를 제공하고 있다. 따라서, 기업에서는 자체적으로 수행하는 데이터 보호 조치 이외에 클라우드 사업자가 제공하는 보안 모범사례를 데이터 처리 과정 전반에 적용함으로써 데이터 보안 수준을 향상시키는 것이 필요하다. 반면에, 공격자의 입장에서 클라우드 환경에서 안전하게 보호되지 않은 데이터는 적은 노력으로 많은 데이터를 탈취할 수 있는 좋은 공격 대상이라고 볼 수 있다. 실제로 최근 발생한 보안 사고 유형을 보면 클라우드 서비스에서 안전하게 관리되지 못한 고객 자격증명의 유출로 인해 대규모의 개인정보가 유출되거나 기업의 내부 데이터가 유출되는 경우가 빈번함을 알 수 있다.

● 데이터 유출 사고 유형

공격자가 클라우드 환경에서 데이터를 탈취하는 공격 방법은 공격 대상에 따라 다양하고 복잡한 절차에 따라 수행될 수 있지만 가장 빈번하게 발생되는 보안 사고 유형에 기반한 공격 유형을 정리하면 아래와 같은 4가지 유형으로 정리할 수 있다.

1 공개된 객체 저장소

대부분의 클라우드 사업자들은 SaaS(Software As A Service) 기반 객체 저장서비스를 제공한다. 이와 같은 객체 저장서비스를 업무 목적과 특성 및 관리자의 설정에 따라 인터넷에서 공개적으로 접근이 허용되거나 지정된 사용자만 접근이 허용되도록 제한할 수 있다. 공격자는 공격도구를 이용하여 공개적으로 접근이 가능한 객체저장소를 스캔한 후 저장된 데이터를 탈취할 수 있다.

2 적절하게 보호되지 않은 데이터베이스

클라우드 기반에서 제공되는 데이터베이스는 관리자의 설정에 따라 클라우드의 내부망에 구성되거나 외부에서 접근 가능한 영역에 구성될 수 있다. 공격자는 자동화된 도구를 이용하여 외부에 노출된 데이터베이스를 스캔할 수 있으며 외부에 노출된 데이터베이스에 대해 크리덴셜 스타핑(Credential Stuffing)과 같은 공격을 수행하여 데이터베이스 접근 권한을 획득한 후 데이터를 탈취할 수 있다.

3 소스 코드에 하드코딩된 자격증명

클라우드 환경에서 동작하는 애플리케이션을 개발하는 경우 개발자는 클라우드 서비스에 접근하기 위해 클라우드의 자격증명을 애플리케이션에서 사용해야하는 경우가 발생한다. 이를 위해 각 클라우드 사업자는 이와 같은 환경에서 소스코드에 클라우드의 자격증명을 하드코딩하지 않고 서비스를 개발하는 모범사례를 제공하고 있다. 공격자는 개발자가 보안 모범사례를 준수하지 않고 소스코드에 자격증명을 하드코딩하는 환경을 스캔하여 클라우드 자격증명을 획득하고 획득한 자격증명을 이용하여 클라우드에 저장된 데이터를 탈취할 수 있다.

4 부적절한 API 관리를 통한 자격증명 노출

쿠버네티스와 같은 컨테이너 기반의 서비스를 운영하는 경우 클러스터를 운영하기 위한 API를 공개 혹은 비공개로 설정할 수 있다. 공격자는 자동화된 도구를 이용하여 외부에 공개되어 있는 쿠버네티스 클러스터 관리 API를 탐지할 수 있으며 이를 통해 컨테이너 환경에 저장된 데이터를 탈취할 수 있다.

Insights | 전문가 칼럼

● 사고 유형 별 예방 방안

위에 소개된 사고 유형들로 인한 데이터 유출은 다음과 같은 방법들을 통해 미연에 방지할 수 있다.

사고유형 1. 공개된 객체 저장소

클라우드 사업자가 제공하는 SaaS 기반의 객체 저장 서비스는 저장된 데이터에 접근할 수 있는 보안주체를 제한할 수 있는 정책을 지원한다. 관리자는 이와 같은 정책 설정을 통해 객체가 저장된 저장소를 외부에 노출하지 않고 안전하게 운영할 수 있다. 특히, AWS의 경우 Amazon S3에서 제공하는 ‘퍼블릭 액세스 차단 설정’과 같은 기능을 활성화해 객체 저장소가 인터넷에 공개되는 것을 원천적으로 차단할 수 있다. ‘퍼블릭 액세스 차단 설정’은 개별 버킷 단위에서 설정할 수도 있지만 계정 단위로 설정하는 경우 계정내에 생성된 모든 버킷이 ‘공개(Public)’로 설정되는 것을 차단하기 때문에 버킷 관리자의 실수 혹은 위협 행위자의 고의적인 공개 설정을 미연에 방지할 수 있다.

이 계정의 퍼블릭 액세스 차단 설정

편집

퍼블릭 액세스는 ACL(액세스 제어 목록), 버킷 정책, 액세스 지점 정책 또는 셋 모두를 통해 버킷 및 객체에 부여됩니다. 모든 S3 버킷 및 객체에 대한 퍼블릭 액세스가 차단되었는지 확인하려면 모든 퍼블릭 액세스 차단을 활성화합니다. 이 설정은 현재 및 향후 버킷과 액세스 지점 모두에 대해 계정 전체에 적용됩니다. AWS에서는 모든 퍼블릭 액세스 차단을 활성화하도록 권장하지만, 이 설정을 적용하기 전에 퍼블릭 액세스가 없어도 애플리케이션이 올바르게 작동하는지 확인합니다. 버킷이나 객체에 어느 정도 수준의 퍼블릭 액세스가 필요한 경우 특정 스토리지 사용 사례에 맞게 아래 개별 설정을 사용자 지정할 수 있습니다. 자세히 알아보기 [\[2\]](#)

모든 퍼블릭 액세스 차단

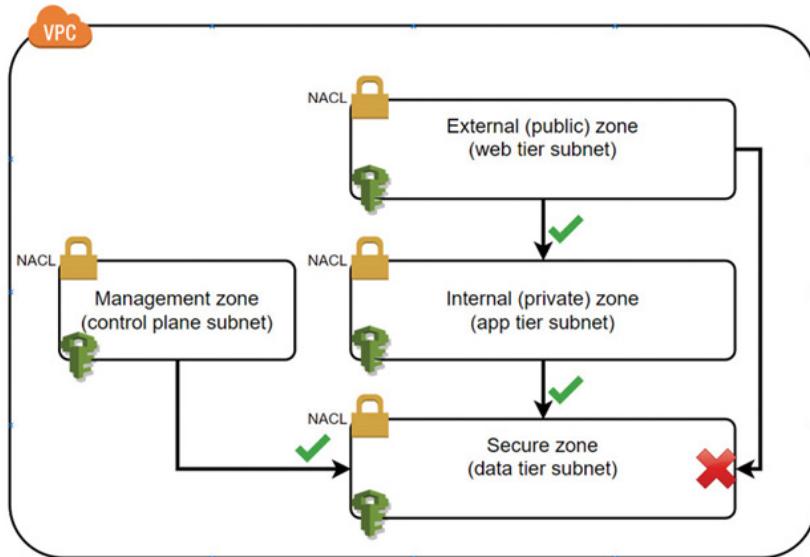
◉ 활성화

- 세 ACL(액세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단
 - ◉ 활성화
- 임의의 ACL(액세스 제어 목록)을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단
 - ◉ 활성화
- 세 퍼블릭 버킷 또는 액세스 지점 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 액세스 차단
 - ◉ 활성화
- 임의의 퍼블릭 버킷 또는 액세스 지점 정책을 통해 부여된 버킷 및 객체에 대한 퍼블릭 및 교차 계정 액세스 차단
 - ◉ 활성화

[그림 2-32] AWS S3 퍼블릭 액세스 차단 설정

사고유형 2. 적절하게 보호되지 않은 데이터베이스

클라우드 환경에서 사용하는 데이터베이스는 가상 사설 클라우드(Virtual Private Cloud) 공간에서 관리자가 지정한 서브넷을 통해 배포되게 된다. 이 때, 관리자는 데이터베이스를 인터넷과 완전히 격리되어 있는 서브넷에 지정할 수 있는데 이렇게 내부망에 데이터베이스를 배포하게 되면 인터넷을 통해 수행되는 데이터베이스 스캔 공격으로부터 안전하게 데이터베이스를 구성할 수 있다. 또한, 데이터베이스에 접근할 수 있는 네트워크에 대해 보안 그룹에서 지정된 IP 혹은 지정된 가상 자원을 통해서만 접근이 가능하도록 규칙을 적용하여 보안을 강화할 수 있다.



▣ 그림 2-33 VPC 보안존에 구성된 데이터베이스 영역

사고유형 3. 소스 코드에 하드코딩된 자격증명

개발된 애플리케이션이 클라우드 환경에서 구동되고 클라우드 서비스에 대한 접근을 위해 코드 내에서 클라우드 자격증명이 필요한 경우에는 소스코드에 자격증명을 하드코딩 하는 대신 클라우드 사업자가 제공하는 메타데이터 기반 임시 보안 자격증명을 사용하도록 애플리케이션을 구성할 수 있다. 애플리케이션 내에서 메타데이터를 이용해 임시 보안 자격증명을 호출하도록 구성하기 위해서는 클라우드 사업자가 제공하는 메타데이터 호출 URL을 사용하도록 코드를 수정하거나 SDK(Software Development Kit)을 이용하면 간단하게 임시 보안 자격증명을 호출하는 구조를 코드에 반영할 수 있다.

아래는 AWS에서 제공하는 Python 용 AWS SDK에서 자격증명을 탐색하는 순서이다.

1. boto.client() 메소드에서 자격증명을 파라미터로 전달
2. Session 오브젝트를 생성할 때 자격증명을 파라미터로 전달
3. 환경 변수
4. 공유 자격증명 파일 (`~/.aws/credentials`)
5. AWS config 파일 (`~/.aws/config`)
6. Assume Role 제공자
7. Boto2 설정 파일 (`/etc/boto.cfg` and `~/.boto`)
8. IAM 역할이 설정된 Amazon EC2 인스턴스의 메타데이터

애플리케이션을 개발하는 팀에서는 위와 같은 클라우드 사업자가 제공하는 SDK를 활용해 임시 보안 자격증명을 사용하는 방법을 적극적으로 반영해야 한다.

Insights | 전문가 칼럼

사고유형 4. 부적절한 API 관리를 통한 자격증명 노출

쿠버네티스와 같은 컨테이너 오케스트레이터는 컨테이너가 구동되는 클러스터를 관리하기 위한 제어영역(Control Plane)과 데이터를 처리하는 데이터영역(Data Plane)이 존재한다. 제어영역은 클러스터를 운영하고 관리하기 위한 API들을 통해 제어되는데 API를 수신하기 위한 엔드포인트는 외부에 노출하지 않고 사설(Private)로 구성해 인가된 네트워크에서만 접근이 가능하도록 해야 한다. 또한, API호출 시에는 익명(Anonymous)호출을 차단하고 API호출 권한을 인가된 사용자에게만 부여해야 한다. 인가된 사용자에게 권한을 부여할 때는 최소 권한 부여 원칙을 준수해 임여 권한을 획득한 내부자 위협으로부터 클러스터를 보호해야 한다.

● 자격증명 노출 시 대응 방안

보안적인 측면에서 본다면 중요한 자격증명은 유출되지 않는 것이 최선일 것이다. 하지만 자격증명이 유출돼 악용된 사례가 발견되지 않았더라도 노출된 것을 인지한 경우라면 노출된 자격증명에 대해 적절한 대응 조치를 취하는 것 역시 아주 중요하다. 아무리 철저한 보안 환경을 구성하고 자격증명 관리자 보안 교육을 진행하더라도 자격증명 유출 사고는 발생할 수 있기 때문에 조직에서는 반드시 사고 발생 시 대응 가능한 시나리오를 준비해야 한다. 자격증명 노출 시 대응을 위한 주요 단계는 아래와 같이 요약할 수 있다.

단계 1 ▶ 노출 경로 확인

자격증명이 노출된 경로를 파악하는 것은 사고 대응 단계에서 가장 먼저 수행돼야 하는 작업이다. 보안관리자는 다양한 도구를 사용해 자격증명 노출을 탐지할 수 있어야 한다. 다양한 도구를 통해 수동 혹은 자동으로 노출된 자격증명을 식별했다면 식별된 경로(코드저장소, 웹 서비스, 모바일 앱 등)와 연관되어 있는 주요 담당자에게 상황을 전파해야 한다.

단계 2 ▶ 노출된 자격증명 위험도 판별

노출된 자격증명에 대한 후속 조치의 유형과 속도 등을 결정하기 위해서는 노출된 자격증명에 대한 위험도를 판별하는 것이 필요하다. 판별된 위험도에 따라 조치 방법이나 조치 속도 등의 차이가 있을 수 있다.

단계 3 ▶ 노출 경로 차단

노출된 자격증명의 위험도를 결정했다면 결정된 위험도에 따라 자격증명 노출 경로를 차단하는 작업이 수행돼야 한다. 코드 저장소가 '공개'로 설정되어 노출됐다면 '비공개'로 전환하거나 부적절한 API키 관리를 통해 유출됐다면 코드 수정 등을 수행할 수 있다.

단계 4 ▶ 자격증명 격리 혹은 교체

노출된 자격증명은 조직에서 어떤 위협 징후를 감지하지 못했더라도 이미 위협 행위자가 악의적인 목적으로 사용하고 있을 수 있다. 따라서, 노출이 확인된 자격증명은 가능한 즉시 비활성화하고 새로운 자격증명으로 교체해야 한다.

단계 5 ▶ 위협 사냥

자격증명이 노출됐다면 해당 자격증명을 위협행위자가 탈취한 상황을 가정해야 한다. 조직에서 인지 가능한 보안사고가 발생하지 않았더라도 위협행위자는 탈취한 자격증명을 이용해 공격을 준비하고 있을 수 있다. 따라서, 탈취된 자격증명을 기반으로 사용 이력 등을 추적해 잠재적 위협을 사냥해야 한다.

단계 6 ▶ 재발 방지

노출 경로를 차단하고 잠재적 위협까지 식별해 조치했다면 자격증명 노출사고가 재발하지 않도록 재발방지 방안을 수립하고 수행하는 것이 필요하다.

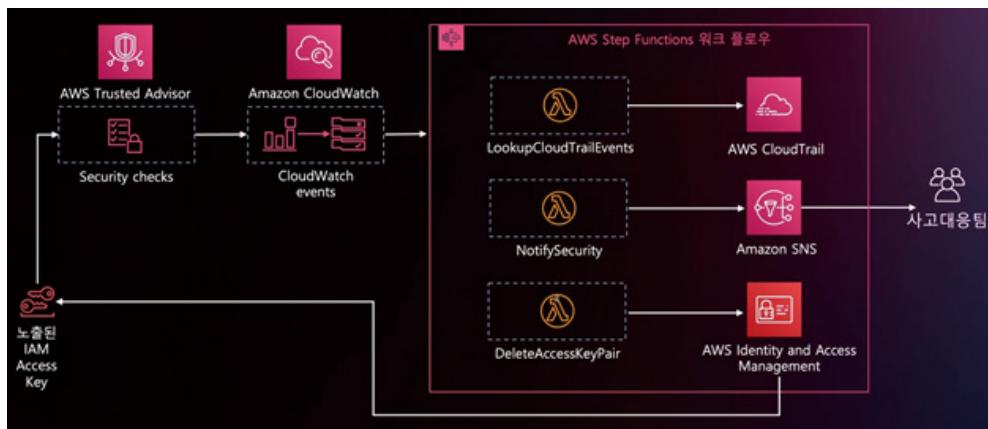
● 사고 대응 자동화

기업의 중요 자산인 데이터를 유출할 수 있는 권한을 가진 자격증명이 유출된 경우, 대응할 수 있는 체계를 수립하는 것도 중요하지만 수립된 대응 체계를 효율적으로 운영하는 것은 실제 사고 발생 시 사고의 범위와 영향도를 최소화할 수 있는 방안인만큼 각 조직에서는 최대한 빠르고 체계적으로 대응 단계들을 수행하는 것이 필요하다. 오프라imes 환경에서는 이와 같은 대응 체계를 매뉴얼화해 사고 발생 시 각 단계별로 대응 지침을 명시하고 담당자를 지정해 순차적으로 지정된 지침들이 수행될 수 있도록 운영하고 있다.

하지만, 이와 같은 수동적인 대응 체계는 클라우드 환경처럼 정보 자산들이 동적으로 운영되고 빠르게 변화하는 환경에서는 사고 발생 시 위험을 최소화하는데 한계가 있는 것이 사실이다. 따라서, 클라우드 환경에서는 클라우드 환경에서 사용할 수 있는 다양한 기능들을 사용해 Cloud-Native한 자동화된 대응 체계를 수립하는 것이 필요하다. 클라우드 환경에서는 클라우드 사업자가 제공하는 다양한 기능들을 통해 정보 유출과 관련한 위험 징후가 탐지되는 경우 대응 절차를 자동화하는 것이 가능하다.

● IAM(Identity and Access Management) 자격증명 노출 대응 자동화

예를 들어, AWS의 경우, IAM에서 사용되는 자격증명인 ‘Access Key’, ‘Secret Key’가 외부로 유출된 경우 ‘AWS Trusted Advisor’라는 서비스를 통해 고객에게 알람을 제공한다. 기업에서는 이와 같은 알람을 사용해 아래 그림과 같이 ‘자격증명 노출 시 대응 방안’을 자동화해 구성할 수 있다.



▣ 그림 2-34 IAM 자격증명 노출 대응 자동화

위 그림에 소개된 ‘IAM 자격증명 노출 대응 자동화’의 각 단계는 아래와 같이 동작한다.

1. AWS Trusted Advisor에서 IAM 자격증명 노출에 대한 알람 발생
2. ‘IAM 자격증명 노출’ 알람 Amazon CloudWatch Event로 전달
 - a. Amazon CloudWatch Event에서는 관리자가 ‘IAM 자격증명 노출’ 알람이 수신됐을 경우, 어떤 액션(위 예시의 경우 AWS Lambda 함수 호출)을 수행하게 될지를 지정해야 한다.
3. ‘IAM 자격증명 노출’ 알람이 CloudWatch Event로 수신되면 CloudWatch Event는 지정된 3가지 AWS Lambda 함수를 실행
 - a. AWS Lambda 함수 – LookupCloudTrailEvents

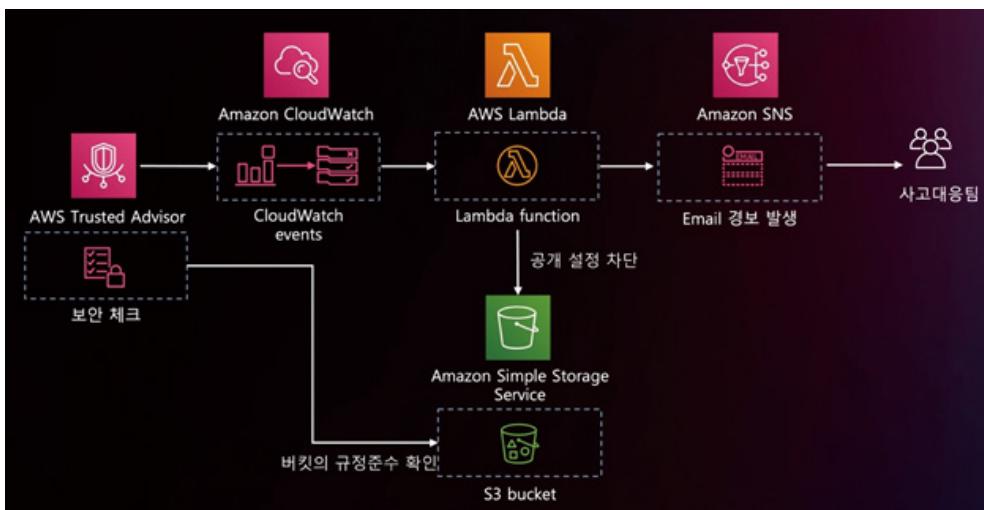
: CloudWatch Event에 수신된 알람 정보를 기반으로 노출된 Access Key 정보를 확인한 후 해당 Access Key를 통해 수행된 AWS API 작업들을 확인한다.
 - b. AWS Lambda 함수 – NotifySecurity

: CloudWatch Event에 수신된 알람과 ‘LookupCloudTrailEvents’ 함수에서 확인한 정보 등을 유관 보안부서에 통지한다.
 - c. AWS Lambda 함수 – DeleteAccessKeyValuePair

: 노출된 것으로 확인된 Access Key를 IAM 서비스에서 삭제한다.

● S3 버킷 공개 설정 대응 자동화

AWS Trusted Advisor는 IAM Access Key 노출 시 알람을 제공하는 것뿐만 아니라 Amazon S3 버킷의 설정을 점검해 특정 버킷이 공개로 설정되는 경우에도 알람을 제공하고 있다. 따라서, AWS Trusted Advisor 서비스를 활용하면 아래 그림과 같이 대응 체계를 자동화할 수 있다.



▣ 그림 2-35 S3 버킷 공개 설정 대응 자동화

위 그림에 소개된 'S3 버킷 공개 설정 대응 자동화'의 각 단계는 아래와 같이 동작한다.

1. AWS Trusted Advisor에서 인터넷에 오픈된 공개 S3 버킷을 탐지하는 경우 공개된 S3 버킷에 대한 알람 발생
2. '공개된 S3 버킷' 알람이 Amazon CloudWatch Event 로 전달
 - a. Amazon CloudWatch Event 에서는 관리자가 '공개된 S3 버킷' 알람이 수신된 경우 어떤 액션(위 예시의 경우 AWS Lambda 함수 호출)을 수행하게 될지를 지정해야 한다.
3. '공개된 S3 버킷' 알람이 CloudWatch Event 로 수신되면 CloudWatch Event 는 지정된 AWS Lambda 함수를 실행
 - a. AWS Lambda 함수
 - '공개된 S3 버킷' 알람에 포함된 정보를 기반으로 경보를 발생한다.
 - '공개된 S3 버킷' 알람에 포함된 정보를 기반으로 공개로 설정된 S3 버킷을 확인한 후 해당 버킷을 비공개로 설정을 변경한다.

● 결 론

다양한 보안표준 및 규제 준수 인증을 통해 안전성이 보장된 클라우드 사업자의 서비스를 이용하는 것은 기업에 입장에서는 온프레미스 환경 못지않은 훌륭한 인프라를 이용해 다양한 실험을 수행하고 빠른 혁신을 가능하게 한다.

하지만, 클라우드 환경에서 중요한 정보 자산을 운영하고 안전하게 보호하기 위해서는 현재 사용중이거나 사용하려고 하는 클라우드 서비스에 대한 보안적인 이해가 선행돼야 하며 이를 기반으로 안전한 보안 체계가 적용되어야 한다.

또한, 이와 같은 보안 체계는 시간 소모적인 일회성 보안 체계가 아닌 클라우드 환경에 맞는 지속적인 점검 및 대응이 가능한 체계로 준비돼야 한다. 이를 위해서 기업과 기업의 보안 담당자는 온프레미스와 클라우드의 차이점을 명확히 이해해야 한다. 그리고, 이를 기반으로 조직에서 사용하는 데이터의 생명주기 별로 위협 모델링을 수행해 데이터에 대한 접근 경로, 사용하는 클라우드 서비스 및 처리 과정에서 발생하는 위협을 식별하고 식별된 위협에 대해 보안 조치를 적용해야 클라우드 이용 환경에서 발생할 수 있는 정보 유출 사고를 미연에 방지할 수 있다.

Part. 2

07

생성형 AI를 활용한 보안업무 혁신

넥슨코리아 김동춘 실장

● 서론

인공지능(AI)은 현재 다양한 산업과 분야에서 혁신적인 변화를 일으키고 있다. 특히, 생성형 AI는 인공지능이 새로운 데이터를 생성하거나 수정하는 기술로, 대규모 언어 모델, 이미지 생성, 음성 합성 등 다양한 분야에서 활용되고 있다.

일반적으로 생성형 AI는 사용자의 요구사항을 텍스트 또는 음성으로 입력하면 적절한 결과물을 제공한다. 이러한 서비스는 보안 업무에도 적용할 수 있으며, 보안 업무의 효율성과 품질을 향상시킬 수 있다.

본 칼럼에서는 생성형 AI를 활용한 보안업무의 혁신에 대해 다음과 같이 말하고자 한다. 먼저, 생성형 AI의 개념과 기술을 소개하고, 보안에서 활용할 수 있는 생성형 AI 서비스를 소개한다. 그 다음 생성형 AI를 보안 업무에 적용한 사례와 장점을 분석하고, 생성형 AI의 단점과 위험성을 고찰한다. 마지막으로 생성형 AI를 보안적인 측면에서 안전하게 도입하고 운영하기 위한 고려사항을 제시하고자 한다.

● 생성형 AI의 개념과 기술

생성형 AI는 인공지능이 새로운 데이터를 생성하거나 수정하는 기술을 말한다. 생성형 AI는 주로 딥러닝과 생성 모델을 기반으로 한다. 생성 모델은 주어진 데이터의 분포를 학습하고, 그 분포에서 샘플링하여 새로운 데이터를 생성하는 모델이다. 생성 모델에는 다양한 종류가 있으며, 대표적으로는 다음과 같은 것들이 있다.

- 적대적 생성 신경망(GAN): 두 개의 신경망으로 구성되며, 하나는 가짜 데이터를 생성하고, 다른 하나는 생성된 데이터가 진짜인지 판별한다. 생성자와 판별자가 서로 경쟁하면서 학습하므로 적대적이라고 한다. GAN은 이미지, 음성, 텍스트 등 다양한 데이터를 생성할 수 있다.

Insights | 전문가 칼럼

- **변이형 오토인코더(VAE):** 인코더와 디코더로 구성되며, 인코더는 입력 데이터를 잠재 공간에 있는 저차원의 벡터로 압축하고, 디코더는 잠재 벡터를 다시 원래 차원의 데이터로 복원한다. VAE는 잠재 공간에서 새로운 잠재 벡터를 샘플링하여 새로운 데이터를 생성할 수 있다. VAE는 GAN보다 안정적으로 학습할 수 있으며, 이미지, 음성, 텍스트 등 다양한 데이터를 생성할 수 있다.
- **오토리그레시브 모델(AR):** 조건부 확률 분포를 이용하여 데이터를 생성하는 모델이다. AR은 데이터의 각 요소를 순차적으로 생성하며, 이전에 생성한 요소들을 조건으로 사용한다. AR은 특히 텍스트 데이터에 적합하며, 대규모 언어 모델이 AR의 한 예이다.

생성형 AI의 기술적인 특징은 다음과 같다.

- 생성형 AI는 적은 양의 데이터로도 다양하고 풍부한 데이터를 생성할 수 있다. 생성형 AI는 학습한 데이터의 분포를 잘 반영하여 데이터를 생성하므로, 원본 데이터의 양이 적어도 새로운 데이터를 생성할 수 있다. 또한, 생성형 AI는 원본 데이터에 없는 특징이나 패턴을 가진 데이터를 생성할 수 있다.
- 생성형 AI는 실시간으로 데이터를 생성할 수 있다. 생성형 AI는 사용자가 입력한 텍스트 또는 음성을 즉시 분석하고, 그에 따라 적절한 데이터를 생성할 수 있다. 따라서, 사용자의 요구사항에 신속하게 대응할 수 있다.
- 생성형 AI는 사용자의 피드백을 반영하여 학습하고 개선할 수 있다. 생성형 AI는 생성한 데이터에 대한 사용자의 피드백을 수집하고, 그 피드백을 바탕으로 학습 데이터를 업데이트하고, 모델을 재 학습할 수 있다. 따라서, 생성형 AI는 사용자의 만족도를 높이고, 서비스의 품질을 향상시킬 수 있다.

● 일반적인 생성형AI 활용

- 생성형 AI는 업무에서 다양한 방면으로 활용할 수 있다. 생성형 AI는 텍스트, 음성, 이미지, 비디오 등 다양한 형태의 데이터를 생성하거나 변환할 수 있으며, 이를 통해 업무 효율성과 창의성을 높일 수 있다. 업무에서 활용할 수 있는 생성형 AI 사례는 다음과 같다.
- 문서 작성: 생성형 AI는 사용자가 입력한 키워드나 요약문에 따라 적절한 문서를 생성하는 서비스이다. 보고서, 계약서, 뉴스 기사, 블로그 글, 소설 등 다양한 장르의 문서를 작성할 수 있다. 본 칼럼과 같이 생성형 AI를 이용하여 키워드, 요약문을 기반으로 손쉽게 작성할 수 있다. 특히 필요한 정보를 쉽게 검색하고, 표준화된 양식을 따를 수 있다.
- 언어 번역: 각 기 다른 언어로 작성된 텍스트, 문서 이미지를 원하는 이미지로 변환할 수 있다. 예를 들어 국문으로 작성한 메일, 계약서를 일본어, 영문 등의 다양한 언어로 변환할 수 있다. 이 때 기존 번역 서비스 대비 좀 더 자연스러운 문장을 구사할 수 있다. 다만 생성형 AI가 주로 기사, 논문 등 문어체를 기반으로 하고 있어 구어체는 다소 미흡할 수 있다.

Insights | 전문가 칼럼

- Voice GPT: 오프라인 회의 또는 화상회의에서 음성을 자막으로 변환하거나 타 언어로 자동 변환할 수 있다. 다양한 메신저, 모바일 및 서비스에서 이를 확대 지원하고 있다. 최근 발표된 GPT-4o의 경우 실시간에 준하는 음성번역 성능을 보여주고 있다.

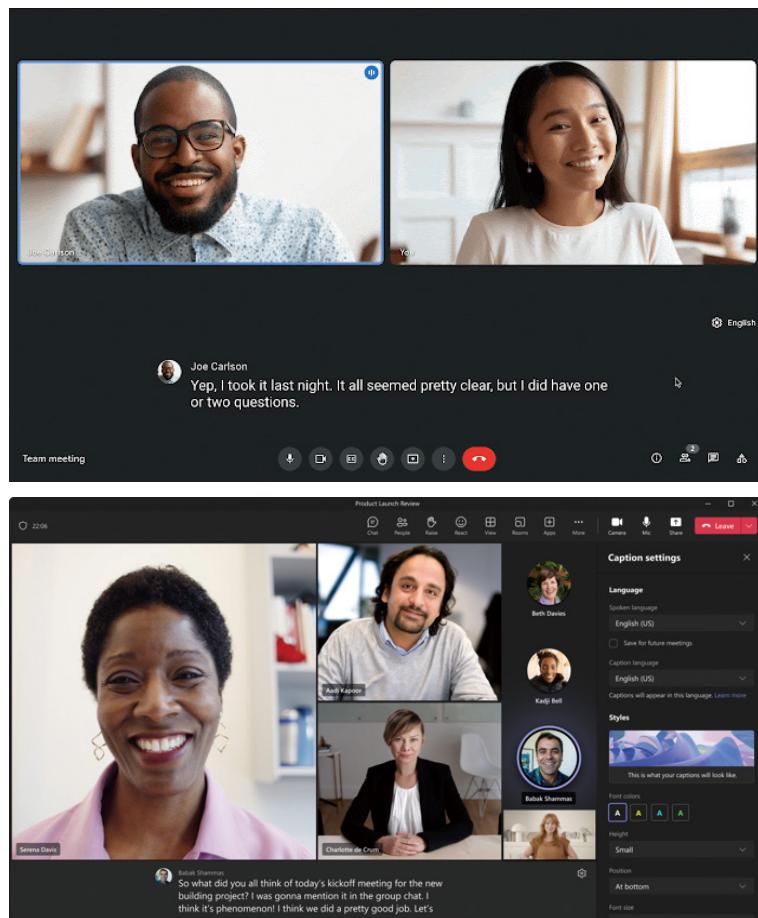
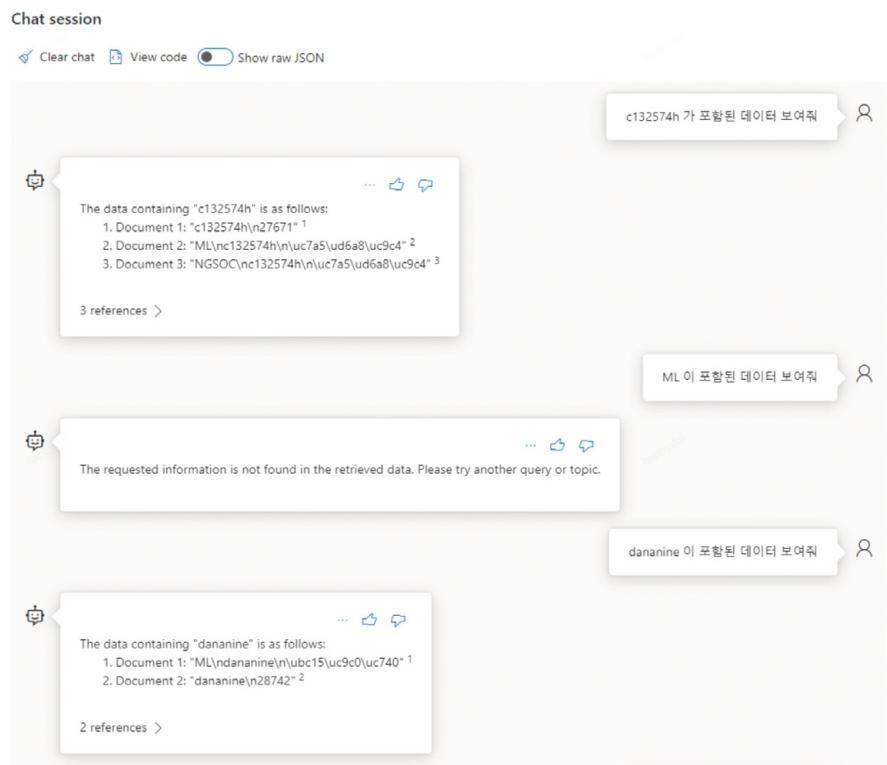


그림 2-36 (예시) Google Meet, MS Teams

Insights | 전문가 칼럼

- 대화형 검색 서비스 & 챗봇: 사용자의 요구사항을 대화형으로 질의하고 이에 대한 적절한 응답데이터를 제공한다. 예를 들어 인트라넷 데이터를 RAG 방식으로 생성형 AI에 연결해 추가 작업 없이 임직원에게 검색 서비스를 제공할 수 있으며, 회사 내부데이터와 인터넷의 공개된 데이터를 혼합하여 회사 내부에 맞춤형 챗봇 서비스를 제공할 수 있다. 또한, 회사 자산 정보가 저장된 DB, 엑셀, 텍스트파일 등을 연동하여 자산관리에도 활용할 수 있다.



[그림 2-37] (예시) 생성형 AI를 이용한 자산관리 챗봇

Insights | 전문가 칼럼

- DB 쿼리 작성: DB 종류, 구성에 따라 각기 다른 DB Query를 생성형 AI에 요구사항을 질의해 생성할 수 있다. 초급 엔지니어를 대체하거나 고급 엔지니어의 업무시간을 단축할 수 있다. 특히 다양한 Data warehouse가 등장하고 복합적으로 사용하는 환경에서 탁월한 생산성을 보장하고 있다.

I am trying to run this on SQLite. Will that work?

The SQL query provided in the previous response should work in SQLite, with a few minor modifications. In SQLite, the 'LIMIT' clause does not accept a subquery, so you will need to use a different approach to limit the results to the top 10% of the most frequently queried addresses.

One way to do this is to use the 'ROW_NUMBER' function to assign a unique number to each row in the results, and then use a combination of the 'LIMIT' and 'WHERE' clauses to only select the rows with the top 10% of the highest 'query_count' values. This can be done with the following SQL query:

```
SELECT "query", query_count
FROM (
  SELECT "query", COUNT(*) as query_count,
         ROW_NUMBER() OVER (ORDER BY COUNT(*) DESC) as rn
  FROM dns
  GROUP BY "query"
)
WHERE rn <= (SELECT COUNT(*) FROM dns) * 0.1;
```

This query uses a nested subquery to calculate the row number for each 'query' value, based on the number of times it appears in the 'dns' table. The outer query then uses the 'WHERE' clause to only select the rows with a 'rn' value that is less than or equal to 10% of the total number of rows in the 'dns' table.

Note that this query may not return exactly 10% of the results if the total number of rows in the 'dns' table is not evenly divisible by 10. However, it should provide a way to limit the results to only the top 10% of the most frequently queried addresses in SQLite.

그림 2-38 (예시) 생성형 AI에 DB Query 생성 질의

Insights | 전문가 칼럼

- **소프트웨어 개발:** 웹, 모바일 등 다양한 개발환경에서 새로운 코드를 생성, 교정하고 버그 수정에 사용할 수 있다. 생성형 AI 서비스에 소스코드를 업로드해 버그를 수정하거나 코드를 최적화할 수 있으며, 사용자의 요구사항을 간단히 질의하여 원시 코드를 생성할 수 있다. 특히, 개발 에디터와 생성형 AI를 연동해 별도 과정 없이 코드 생성, 버그 수정, 최적화 할 수 있다.



▣ 그림 2-39 (예시) Github Copilot

- **디자인:** 생성형 AI는 사용자의 스케치나 설명에 따라 적절한 디자인을 생성하는 서비스이다. 로고, 아이콘, 웹사이트, 앱, 포스터, 옷, 신발 등 다양한 디자인을 생성할 수 있다. 업무에서는 디자인 과정을 단축하고, 디자인 품질을 개선하고, 디자인 트렌드를 파악할 수 있다.



▣ 그림 2-40 (예시) Adobe Firefly

● 보안에서 활용할 수 있는 생성형 AI 서비스

보안업무는 자동화되지 못하고 많은 부분이 사람에 의존하고 있다. 사람이 하고 있었다는 것은 생성형 AI를 활용할 수 있는 범위가 다양하다는 것으로 해석할 수 있다. 생성형 AI를 업무에 도입하기 위해서는 현재 우리가 하고 있는 보안업무가 무엇인지 명확한 정의를 선행해야 한다.

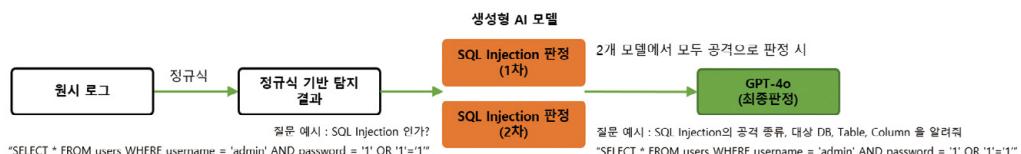
시스템관리, 보안솔루션 운영, 보안엔지니어링, 보안진단, 보안개발 등 기술적 보안영역과 정보보호, 개인정보보호, 인식개선, 위험종합관리의 관리적 영역까지 보안의 영역은 다양하다.

각 보안업무 영역을 정의하고 업무 흐름과 방식을 명확하게 해야만 생성형AI 도입효과를 극대화할 수 있다. 특히, 업무 방식 정의 시 “업무를 어떻게”, “원하는 업무 결과물”이 무엇인지 명확히 정의해야 한다. 정의 결과에 따라 생성형 AI 서비스 종류, 기반 데이터, 데이터 사용방법 및 생성형 AI에 입력할 질의를 결정할 수 있으며 그에 따라 전체적인 서비스 품질이 결정된다.

예를 들어 SQL Injection과 같은 웹공격을 생성형 AI로 판정하는 서비스를 도입한다고 가정해 보자. 원하는 결과물이 무엇이고 현재 보안조직에서 어떤 방식으로 웹공격을 판정하고 있는지 업무 프로세스를 정의해야 한다.

- 요구되는 결과물 예시: SQL Injection 유무, 종류, 대상 DB, Table, Column, Leak Data
- SQL Injection 판정 업무 프로세스
 - 1) 웹 로그 또는 DB 로그에서 정규식 기반 탐지
 - 2) 보안관제 초동 인력이 정탐 또는 오탐 판정
 - 3) 보안관제 상위 인력이 1차 판정 결과를 2차 검증
 - 4) 정탐으로 최종 판정된 경우 피해범위 파악을 위해 공격 쿼리 분석

위와 같이 정의 후 생성형 AI에 반영해 웹공격 판정 프로세스를 자동화 할 수 있다.



- 보안관제 초동인력과 같이 빠른 판정을 위해 가벼운 생성형 AI 모델 2개로 교차 검증
 - 모델 2개에서 모두 공격으로 판정한 이벤트를 다른 생성형AI를 사용해 심층분석
- 위와 같이 업무를 최대한 명확히 정리해야 생성형 AI의 성능을 최대화할 수 있다. 정의된 업무영역에 따라 아래와 같이 다양하게 적용할 수 있다.

Insights | 전문가 칼럼

생성형 AI 활용 – 보안관리

- 보안가이드 제공: 내부임직원에게 제공하는 보안가이드 제작 시, 생성형AI를 사용해 필요한 정보검색, 결과요약, 결과문서 제작에 투입되는 리소스를 대폭 절감할 수 있다.

 Gemini가 업데이트되었습니다. 업데이트 보기



◆ Phishing Email Warning Poster (English Translation)

Background: Dark

Text:

주의! 피싱 이메일 주의!

최근 피싱 공격이 증가하고 있습니다. 피싱 이메일은 귀하의 개인 정보, 금융 정보 또는 기타 민감한 정보를 훔치기 위해 보내는 사기 이메일입니다.

피싱 이메일을 식별하는 방법:

- 의심스러운 발신인: 이메일 주소가 정상적인지 확인하십시오. 공격자는 종종 합법적인 회사나 조직을 가장하기 위해 유사한 이메일 주소를 사용합니다.
- 긴급하거나 위협적인 내용: 피싱 이메일은 종종 즉각적인 조치를 취하도록 압박하거나 계정이 손상되었다는 등의 위협적인 내용을 포함합니다.
- 문법 및 맞춤법 오류: 피싱 이메일에는 종종 문법 및 맞춤법 오류가 있습니다.
- 링크 또는 첨부 파일 클릭하지 마십시오: 피싱 이메일에는 악성 링크 또는 첨부 파일이 포함될 수 있습니다. 클릭하면 컴퓨터가 손상되거나 개인 정보가 유출될 수 있습니다.

피싱 공격으로부터 자신을 보호하는 방법:

- 의심스러운 이메일은 삭제하십시오.
- 링크 또는 첨부 파일을 클릭하지 마십시오.
- 사용 중인 웹사이트의 URL 주소가 정확한지 확인하십시오.
- 강력하고 고유한 비밀번호를 사용하십시오.
- 최신 보안 소프트웨어를 사용하십시오.

피싱 공격을 당했다면:

- 즉시 비밀번호를 변경하십시오.
- 사용 중인 금융 기관에 연락하십시오.
- 관련 당국에 신고하십시오.

자세한 정보:

- <https://www.kisa.or.kr/EN>
- <https://ncsa.gov.qa/en>

주의: 피싱 공격은 지속적으로 진화하고 있습니다. 최신 피싱 공격 정보를 확인하고 자신을 보호하기 위해 위의 조치를 취하십시오.

 그림 2-41 (예시) 생성형 AI에 피싱메일 대응 가이드 제작 질의

Insights | 전문가 칼럼

- 보안정책인식 제고: 보안 인식을 높이기 위해 생성형 AI를 활용할 수 있다. 예를 들어, 보안 교육에서는 생성형 AI를 이용해 다양한 보안 시나리오를 생성할 수 있으며, 보안상태나 위험도를 쉽게 이해할 수 있는 이미지나 동영상으로 생성해 캠페인을 제작할 수 있다. 또한 보안교육 영상 제작 시 생성형 AI를 통해 자연스러운 음성으로도 제작할 수 있다.

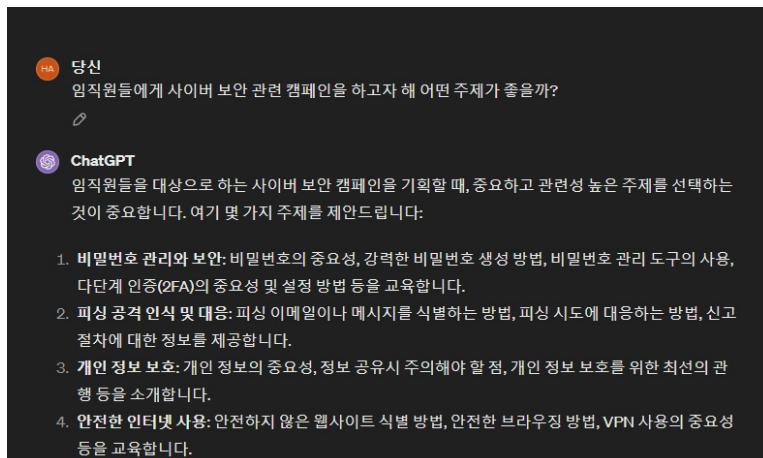


그림 2-42 (예시) 생성형AI에 보안캠페인 주제 질의



그림 2-43 (예시) 생성형AI로 보안캠페인 이미지 제작

- 보안 챗봇: 보안챗봇으로 임직원 보안상담 서비스를 24시간 제공할 수 있다. 보안을 담당하는 직원은 업무 중 많은 시간을 임직원의 다양한 질문을 답변하는데 사용하고 있으며 그 질문의 범위는 일반적인 보안이슈나 매우 기본적인 질문부터 사내 인프라 환경을 이해하고 답변해야 하는 질문까지 다양하다. 이를 해결하기 위해 일반적으로 외부 공개된 정보와 내부 정보를 결합하여 임직원에게 챗봇을 제공할 수 있다.

Insights | 전문가 칼럼

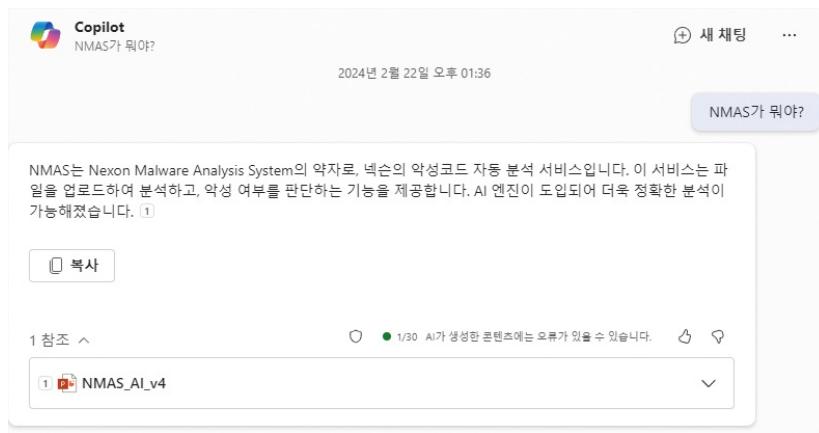


그림 2-44 (예시) 내부문서를 RAG로 연결하여 임직원에게 챗봇 제공

생성형 AI 활용 – Red Team

- 피싱 메일 모의훈련: 생성형 AI를 이용해 손쉽게 정교한 피싱 메일을 제작할 수 있다.
- 보안 취약점 진단: 시스템이나 네트워크 보안취약점을 찾고, 분석 시에 생성형 AI를 사용할 수 있다. 초급인력의 보안취약점 진단 진입 허들을 낮추고 효율성을 높일 수 있다. 예를 들어 생성형 AI는 보안취약점을 탐지하는 공격 시나리오를 생성하고, 취약점에 대한 보안 조치를 제안하고 보고서를 작성할 수 있다. 다만 생성형 AI의 공격 시나리오가 실제 환경에서 위험성이 고려되지 않을 수 있어 진단 전 충분한 사전검토가 필요하다.

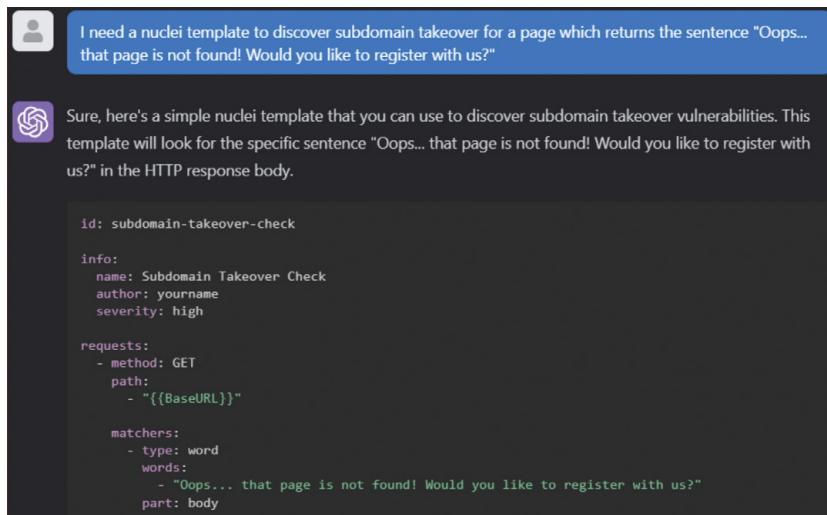


그림 2-45 (예시) Nuclei Scanner with GPT

Insights | 전문가 칼럼

BurpGPT

Enhance your Burp Suite with Large Language Models (LLMs)

Experience enhanced web security testing with BurpGPT our Burp Suite extension which integrates OpenAI's LLMs for advanced vulnerability scanning and traffic-based analysis. The Pro edition also supports local LLMs, including custom-trained models, ensuring greater data privacy and more accurate results according to your needs.

[Get Community edition](#) [Upgrade to Pro edition](#)

- Effortless security testing**
Effortlessly Integrate Burp GPT into your security testing workflows with user-friendly documentation.
- Developed by AppSec specialists**
Developed by application security experts, Burp GPT represents the cutting-edge of web security testing.
- Continuously evolving security**
Burp GPT continuously improves based on user feedback, ensuring it meets evolving security testing needs.

Burp GPT. unleash the power of LLMs. the ultimate Burp Suite add-on.

Burp GPT is a robust tool developed to enhance precision and efficiency of application security testing. Extended with advanced language processing capabilities and an intuitive interface, it enhances security testing for both beginners and seasoned testers alike.

Perform sophisticated technical tasks such as evaluating cryptographic integrity of custom libraries or even detect zero-days. By leveraging the power of large language models (LLMs). With your imagination and the quality of your prompts as the only constraints, assess web applications using an AI Co-Pilot to perform web traffic analysis.

Burp GPT is the comprehensive tool for consultants and security experts alike. By employing **local large language models (LLMs)**, a feature **exclusive to the Pro edition**, BurpGPT negates third party data sharing to ensure client engagement confidentiality.

Additional Pro edition features include **prompt libraries** and **support for custom-trained models**. Have internal repositories of appsec data? Train your own model and harness your internal knowledge-base.

Join the community of forward-thinking professionals who use Burp GPT. Elevate your application security testing and ensure privacy and compliance using large language models.

[Get Community edition](#) [Upgrade to Pro edition](#)

그림 2-46 (예시) BurpGPT

- 웹 서비스 스캐너: 내부 각종 시스템이 고의적 또는 실수 등으로 외부에 무방비로 노출될 수 있다. 보안관리자는 외부자의 관점에서 이를 매일 스캐닝하고 확인해야 하기 때문에 번거롭고 많은 리소스가 투입된다. 생성형 AI를 이용해 내부 웹 서비스를 학습, 외부 노출 시 즉시 이를 탐지할 수 있다.

- 1) 생성형 AI는 일반적인 웹사이트 및 내부 웹서비스의 스크린샷을 학습
- 2) 비공개 내부 페이지의 외부노출을 탐지

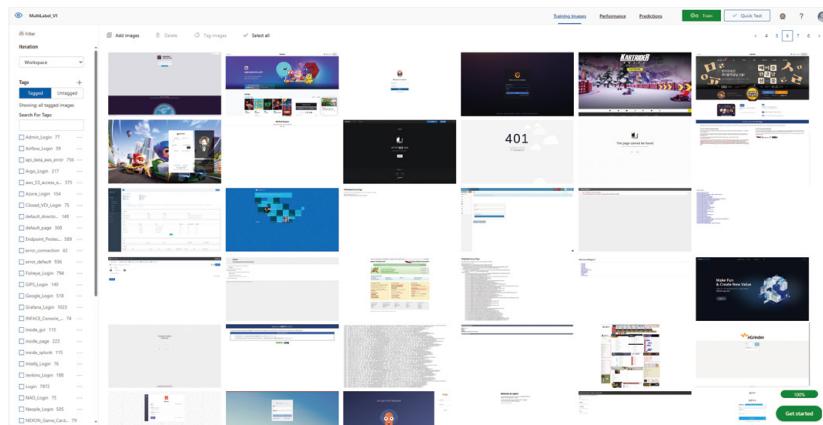
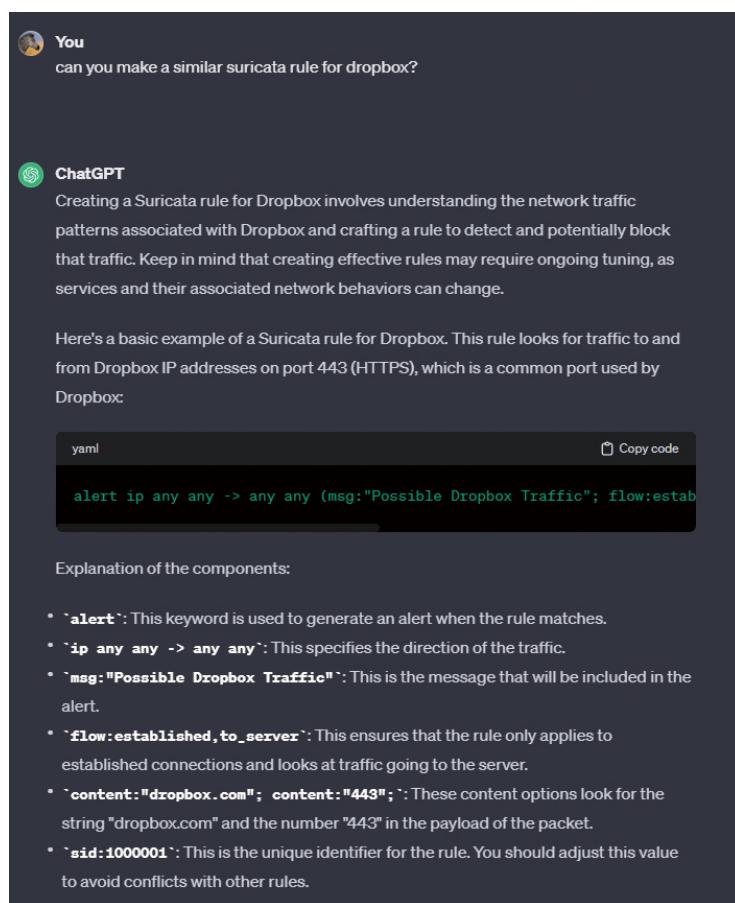


그림 2-47 (예시) Azure AI Custom Vision을 이용한 스크린샷 학습

Insights | 전문가 칼럼

생성형 AI 활용 – Blue Team

- 보안 대응: Blue Team은 침해시도를 탐지하고 사고발생 시 원인과 영향을 분석해 대응 방안을 수립한다. 생성형 AI를 업무에 사용하면 보안대응 품질과 속도를 향상시킬 수 있다.
- 보안관제 정책 생성: IDS Rule 생성, Splunk, DB, Snowflake 등의 Query를 자동 생성할 수 있다. 복잡한 정규식 작성 및 테스트를 모두 생성형 AI로 해결할 수 있다. 예를 들어 Dropbox로 연결을 탐지하고자 할 때, Dropbox의 도메인 조사, 연결 테스트, 정규식 작성, 정규식 검증, IDS 룰 테스트를 진행해야 하나, 생성형 AI에서는 'Dropbox를 탐지할 수 있는 정규식 작성'으로 간단히 해결할 수 있다.



[그림 2-48] (예시) 생성형 AI로 Dropbox 접속 탐지 IDS Rule 생성

Insights | 전문가 칼럼

You
write a splunk search query to identify the number of active directory logon failures for user within a 24 hour period

∅

ChatGPT
To identify the number of Active Directory logon failures for a specific user within a 24-hour period in Splunk, you can use the following search query. This assumes that your Active Directory logon failure events are indexed in Splunk:

```
spl
Copy code

index=<your_active_directory_index> sourcetype="your_active_directory_s
| eval user=mvindex(split(UserName, "\\\"), 1) // Extract the username
| stats count by user, _time
| where count>0
| eval logon_hour=strftime(_time,"%H")
| eval logon_date=strftime(_time,"%Y-%m-%d")
| eval logon_time=strftime(_time,"%H:%M:%S")
| eval logon_datetime=strftime(_time,"%Y-%m-%d %H:%M:%S")
| stats count by user, logon_date, logon_hour
| sort - count
```

This query does the following:

- Filters events from your Active Directory logs where the EventCode is 4625 (logon failure).
- Extracts the username from the "domain\username" format.
- Counts the occurrences of logon failures for each user within each hour.
- Filters out records where there were no logon failures.
- Extracts the hour, date, and time from the `_time` field.
- Presents the count of logon failures for each user, on each date, and each hour.
- Sorts the results in descending order by the count.

그림 2-49 (예시) 생성형 AI로 최근 24시간 내 AD 접속실패 탐지 Splunk Query 생성

- **사고분석:** 웹 로그 및 DB Query에서 SQL Injection 과 같은 공격 쿼리를 생성형 AI를 이용해 손쉽게 분석할 수 있다. 분석가는 수십만 라인의 로그를 생성형 AI에 공격 유무, 공격 대상, 공격종류, 피해 범위를 질의해 그 결과를 손쉽게 얻을 수 있다. 초급분석가의 분석장벽을 낮추고 중/고급 분석가의 업무 효율을 극대화할 수 있다.
- **로그 실시간 분석:** 각각의 서비스별로 각기 다른 로그를 생산하고 있으며 분석가는 서비스를 파악해 장애, 공격 등을 실시간 판정해야 한다. 기존 환경은 분석가가 서비스 환경과 로그 형식, 유형, 각 상황별 로그를 모두 파악하고 이를 정규식으로 탐지할 수 있도록 보안관제 정책을 수립해야 한다. 수십~수천의 서비스가 운영되고 변화하는 환경에서 분석가는 비효율적이고 반복적인 활동을 수행해야 한다. 각 서비스의 로그를 생성형 AI에 학습시켜 장애와 공격을 별도 작업 없이 판정할 수 있다.

Insights | 전문가 칼럼



[※] 그림 2-50 (예시) 생성형 AI에 로그를 학습시켜 공격/장애 등과 같은 비정상 로그 판정

생성형 AI 활용 – Purple Team

- 보안 인텔리전스: 보안 인텔리전스는 보안 관련된 정보를 수집, 분석하여 내부시스템의 영향을 파악하고 조치하는 업무이다. 보안 인텔리전스의 범위는 일반적인 보안영역부터 각 사업 영역에 따라 사업영역에서 요구하는 정보까지 그 영역이 다양하다. 과거의 경우 유형별로 인텔리전스 정보를 제공하는 각각의 사이트를 수동검색하거나 크롤러를 자체 개발해 정보를 수집 관리했다. 분석가 리소스가 효과 대비 과도하게 투입되거나 분석가의 역량에 따라 그 결과가 달라지는 문제가 발생한다.

✓ log4j 취약점 검색 중
✓ 답변을 생성하는 중...

개인 및 회사 데이터는 이 채팅에서 보호됩니다.

Log4j 취약점은 Log4j라는 자바 기반 로깅 유틸리티에서 발생하는 원격 코드 실행 (RCE) 취약점입니다. 이 취약점을 이용하면 공격자가 원격에서 임의의 자바 코드를 실행할 수 있어서 서버를 제어하거나 악성파일을 감염시킬 수 있습니다. Log4j 2 버전에서는 JNDI (Java Naming and Directory Interface) 인젝션 취약점이 주요 원인이며, Log4j 1 버전에서는 다른 원격 코드 실행 취약점이 있습니다. 이 취약점은 CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-41104 등으로 분류되었습니다. Log4j 취약점에 영향을 받는 버전은 다음과 같습니다.

- Log4j 2 버전: 2.0-beta9 ~ 2.17.0 (Log4j 2.3.1, 2.3.2, 2.12.3, 2.12.4 제외)
- Log4j 1 버전: 1.x

Log4j 취약점을 해결하기 위해서는 최신 버전으로 업데이트하는 것이 가장 좋은 방법입니다. Log4j 2 버전은 2.17.1로, Log4j 1 버전은 2.3.2로 업데이트하면 됩니다. 업데이트가 불가능한 경우에는 다른 대용책을 적용해야 합니다. 예를 들어, JndiLookup 클래스를 제거하거나, Java 메시지에 JNDI 문법을 사용하지 않도록 변경하거나, JNDI 서비스에 대한 접근을 차단하거나, Java 보안 마니저를 활성화하거나, log4j2.formatMsgNoLookups 시스템 속성을 true로 설정하는 등의 방법이 있습니다. 자세한 내용은 아래의 웹사이트들을 참고하시기 바랍니다.

- Log4j 보안 취약점, 버전 확인부터 해결 방법까지 알려 드립니다 | 웹로그 [1]
- [긴급] Apache Log4j 보안 취약점 대응 방안 안내 [2]
- Apache Log4j 2 취약점 주의 및 업데이트 권고 - ASEC BLOG [3]
- Apache Log4J (Log4Shell) 취약점이란? - Trend Micro [4]

Learn more ▾ 1 whatap.io 2 bing.com 3 blog.alyac.co.kr 1 / 30 responses •

[※] 그림 2-51 (예시) 생성형 AI를 이용한 취약점 정보 수집

상반기
2024년 사이비 위협 동향 보고서

Insights | 전문가 칼럼

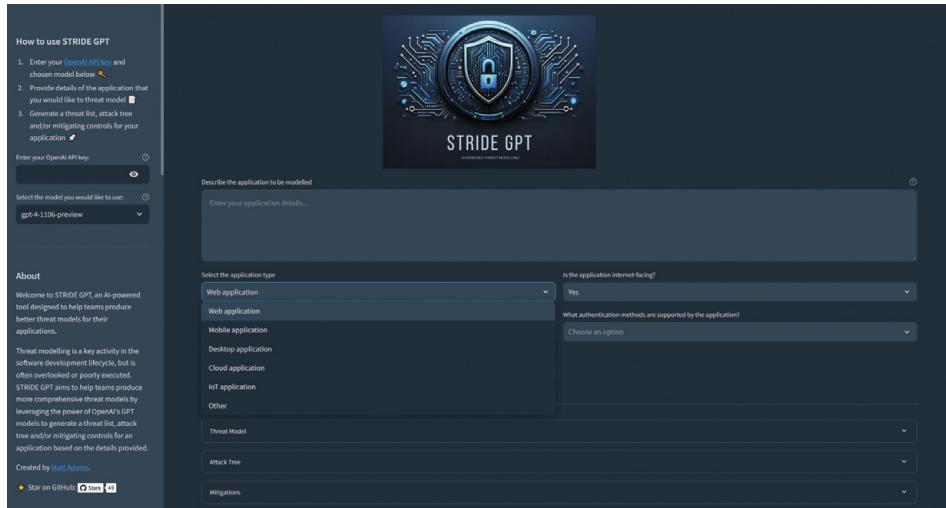


그림 2-52 (예시) STRIDE GPT를 이용하여 어플리케이션 위협 관리 모델 생성

생성형 AI를 이용하면 보안 인텔리전스의 다양성과 신뢰도를 높일 수 있다. 예를 들어, 생성형 AI는 보안 위협이나 취약점에 대한 정보를 수집하고, 보안 트렌드나 예측을 분석하고, 보안 정책이나 전략을 제안하고, 보안 뉴스나 보고서를 작성할 수 있다.

cve.mitre.org에서 오늘 올라온 신규 취약점을 알려드립니다. 팔레이트 보기

2024년 2월 19일 CVE.mitre.org에 등록된 신규 취약점

2024년 2월 19일 기준, CVE.mitre.org에 등록된 취약점은 총 14건입니다.

주요 취약점:

- CVE-2024-23844: Google Chrome 및 Chromium 기반 브라우저에서 발견된 힐 베피 오브젝트 취약점 (심각도: 높음)
- CVE-2024-23843: Microsoft Windows에서 발견된 고급 상승 취약점 (심각도: 높음)
- CVE-2024-23841: VMware ESXi에서 발견된 원격 코드 실행 취약점 (심각도: 높음)
- CVE-2024-23840: Apache HTTP Server에서 발견된 서비스 거부 취약점 (심각도: 중간)
- CVE-2024-23839: Mozilla Firefox에서 발견된 메모리 손상 취약점 (심각도: 중간)

기타 취약점:

- CVE-2024-23838
- CVE-2024-23837
- CVE-2024-23836
- CVE-2024-23835
- CVE-2024-23834
- CVE-2024-23833
- CVE-2024-23832
- CVE-2024-23831

자세한 정보:

- 각 취약점에 대한 자세한 정보는 CVE ID를 클릭하여 확인할 수 있습니다.
- CVE.mitre.org에서 검색 기능을 사용하여 특정 제품이나 소프트웨어 버전에 대한 취약점을 찾을 수 있습니다.
- 취약점 정보를 받아보는 구독 서비스를 신청할 수 있습니다.

취약점 관리:

- 시스템 및 소프트웨어를 최신 버전으로 업데이트하여 취약점을 해결합니다.
- 취약점 관리 솔루션을 사용하여 시스템을 정기적으로 스캔하고 취약점을 파악합니다.
- 보안 패치를 적시에 적용합니다.
- 사용자에게 보안 교육을 실시합니다.

cve.mitre.org에서 오늘 올라온 신규 취약점을 알려드립니다. 팔레이트 보기

2024년 2월 19일 CVE.mitre.org에 등록된 신규 취약점

2024년 2월 19일 기준, CVE.mitre.org에 등록된 신규 취약점은 총 14건입니다.

주요 취약점:

- CVE-2024-23844: Google Chrome 및 Chromium 기반 브라우저에서 발견된 힐 베피 오브젝트 취약점 (심각도: 높음)
- CVE-2024-23843: Microsoft Windows에서 발견된 고급 상승 취약점 (심각도: 높음)
- CVE-2024-23841: VMware ESXi에서 발견된 원격 코드 실행 취약점 (심각도: 높음)
- CVE-2024-23840: Apache HTTP Server에서 발견된 서비스 거부 취약점 (심각도: 중간)
- CVE-2024-23839: Mozilla Firefox에서 발견된 메모리 손상 취약점 (심각도: 중간)

기타 취약점:

- CVE-2024-23838
- CVE-2024-23837
- CVE-2024-23836
- CVE-2024-23835
- CVE-2024-23834
- CVE-2024-23833
- CVE-2024-23832
- CVE-2024-23831

자세한 정보:

- 각 취약점에 대한 자세한 정보는 CVE ID를 클릭하여 확인할 수 있습니다.
- CVE.mitre.org에서 검색 기능을 사용하여 특정 제품이나 소프트웨어 버전에 대한 취약점을 찾을 수 있습니다.
- 취약점 정보를 받아보는 구독 서비스를 신청할 수 있습니다.

취약점 관리:

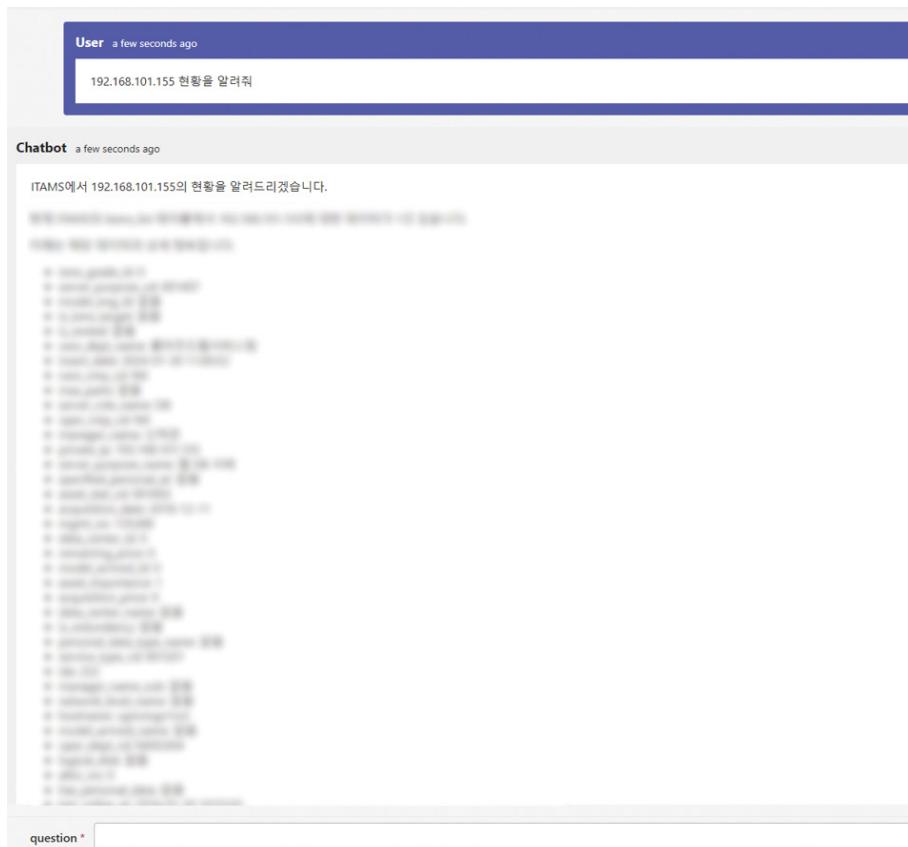
- 시스템 및 소프트웨어를 최신 버전으로 업데이트하여 취약점을 해결합니다.
- 취약점 관리 솔루션을 사용하여 시스템을 정기적으로 스캔하고 취약점을 파악합니다.
- 보안 패치를 적시에 적용합니다.
- 사용자에게 보안 교육을 실시합니다.

그림 2-53 (예시) 생성형 AI를 이용하여 CVE 취약점 자동수집 및 이메일, 메신저 자동 발송

98

Insights | 전문가 칼럼

- 자산정보 위협 통합관리: 텍스트 또는 엑셀, DB 등 다양한 방식으로 관리되고 있는 자산 정보와 취약점 정보를 생성형 AI에 연동해 회사 환경에 특화된 보안 챗봇을 구현할 수 있다. 자산 데이터, 자산 취약점 진단현황, 서비스 현황과 외부 인터넷에 공개된 데이터를 훈합해 자산의 위협을 질의 응답할 수 있는 생성형 AI 챗봇을 구현할 수 있다.



▣ 그림 2-54 (예시) 생성형 AI에 자산정보를 RAG로 연동하여 자산 위협관리 챗봇 생성

Insights | 전문가 칼럼

생성형 AI 활용 – 보안개발 외

- 보안 개발: 보안업무에 사용되는 다양한 종류의 스크립트를 생성형 AI를 이용하면 보안개발의 창의성과 효율성을 높일 수 있다. 예를 들어, 생성형 AI는 보안 요구사항에 맞는 소프트웨어나 하드웨어의 설계도를 생성하고, 보안 코드나 알고리즘을 작성, 보안 테스트 케이스나 데이터를 생성할 수 있다.

 Gemini가 업데이트되었습니다. 업데이트 보기

 네이버 뉴스 채널의 헤드라인 뉴스를 추출할 수 있는 파이썬 스크립트를 제작해줘

◆ 네이버 뉴스 채널 헤드라인 뉴스 추출 파이썬 스크립트

```
Python

# 라이브러리 import
import requests
from bs4 import BeautifulSoup

# 네이버 뉴스 채널 URL
url = 'https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=102'

# HTTP 요청 및 응답
response = requests.get(url)
response.raise_for_status()

# BeautifulSoup 객체 생성
soup = BeautifulSoup(response.content, "html.parser")

# 헤드라인 뉴스 목록 추출
news_list = soup.find_all("ul", class_="type06_headline")

# 뉴스 제목 및 링크 추출
for news in news_list:
    title = news.find("a").text.strip()
    link = news.find("a")["href"]
    print(f"제목: {title}")
    print(f"링크: https://news.naver.com{link}")
    print()
```

코드를 사용할 때는 주의가 필요합니다.

사용 방법:

- 위 코드를 Python 파일로 저장합니다.
- Python 파일을 실행합니다.

출력 결과:

```
제목: 윤석열 대통령, 오늘(16일) 국정원 업무보고 받아...안보 상황 점검
링크: https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=102&o

제목: 이제명 더불어민주당 대표, 오전 9시 국회 본회의장 입장...'윤석열 정부 국정조사'
링크: https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=102&o

제목: "尹, 국정원에 북핵 대비 만전 대세 지지..."적의 도발 즉각 응징"
링크: https://news.naver.com/main/read.naver?mode=LSD&mid=sec&sid1=102&o
```

여기에 프롬프트 입력

▣ 그림 2-55 (예시) 생성형 AI를 이용하여 크롤링 스크립트 제작 및 테스트

생성형 AI를 에디터와 연동해 사용 편리성을 향상시킬 수 있으며 상급개발자는 코드 품질 개선, 버그피스, 디버깅 등 다양한 방식으로 품질을 향상시킬 수 있다. 또한, 기 개발한 프로젝트의 소스코드를 생성형 AI에 강화학습 시켜 프로젝트에 최적화된 생성형 AI를 제공할 수 있다.

2024년 사이비 위협 동향 보고서

Insights | 전문가 칼럼

```

25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61

```

그림 2-56 (예시) Github Copilot 사용 및 Fine-tuning 모델 사용

- Devsecops 구현: 개발분야의 생성형 AI는 효율적인 알고리즘 제공뿐만 아니라 보안적으로 취약한 코드를 보완할 수 있도록 제공한다. 기존 문서와 교육으로만 제공해 전적으로 사람에게만 맡겨졌던 시큐어코딩을 개발, 코딩 단계부터 생성형AI로 해결할 수 있다. 예를 들어 IDE 형태로 제공되는 생성형 AI 개발환경에서 'SQL Injection 취약 검증' 등으로 개발자가 직접 테스트 검증할 수 있다. 이렇게 생산, 취합된 개발코드를 소스코드 저장소에서 생성형 AI로 2차 검증할 수 있다.

logger.info("Found survey entry")

semgrep-app bot 4 days ago

The first parameter when logging with structlog is the event name.
Follow these rules when writing an event name:

- use only lowercase letters, underscores, and dots, because these events get indexed in Datadog, and spaces or special characters make searching and browsing in a spreadsheet view more difficult
- use a maximum of 50 characters
- do not do string formatting, instead, pass variables as keyword arguments for nicer indexing in Datadog

Semgrep Assistant thinks this is a **true positive** that should be fixed. If you agree, a fix for this finding might look like this:

Suggested change
58 - logger.info("Found survey entry")
58 + logger.info("found_survey_entry", message="Found survey entry")

Commit suggestion Add suggestion to batch

Reply with /semgrep ignore <reason> to ignore the finding created by structlog-event-name-conventions.

status open

Resolve conversation

그림 2-57 (예시) Semgrep with GPT로 프로그램 코드 검증

Insights | 전문가 칼럼

● 생성형 AI 도입 방법

생성형 AI는 외부 공개된 SaaS 형태를 사용하거나 자체구축해 사용할 수 있으며, 데이터를 RAG 참조형태로 사용하거나 Fine-tuning 해 사용할 수 있다. 외부 공개된 서비스는 주로 오픈 소스나 클라우드 기반의 서비스로, 쉽게 접근하고 사용할 수 있다. 자체 구축한 서비스는 요구사항에 맞게 커스터마이징하고 관리할 수 있다.

데이터 기준 유형 분류

생성형 AI는 모델이 학습하고 있는 데이터를 사용하거나, Fine-tuning 해 모델에 데이터 추가 또는 RAG로 데이터를 참조하는 방식 등으로 사용할 수 있다.

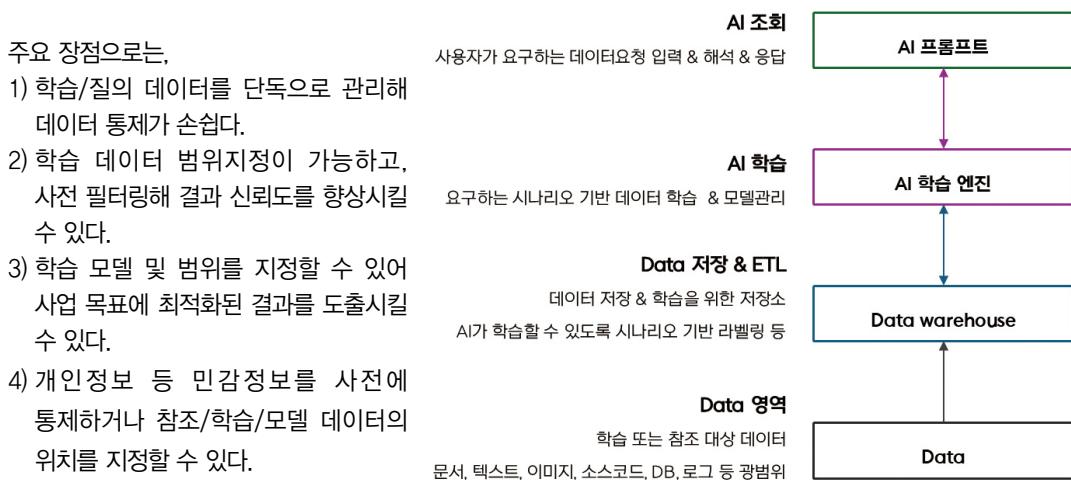
모델 기초데이터	서비스 예
서비스 제공자	OpenAI, MS Azure, Bing Chat enterprise, Github Copilot, Adobe Firefly 등
서비스 이용자 데이터	OpenAI, MS Copilot, AWS Dedrock, GCP Vertex AI 등

데이터 기준 유형 분류

구분	사전학습	참조데이터	서비스 예
번역	불필요	불필요	OpenAI, Bing Chat enterprise 등
지식검색	불필요	회사 데이터	OpenAI, Azure Copilot 등
프로그래밍/이미지생성	불필요	불필요	Github Copilot, Adobe Firefly, 미드저니 등
문서작성	필요	회사데이터	MS O365 Copilot 등

생성형 AI 이용 – 자체구축

생성형 AI를 업체나 기관에서 자체적으로 구축해 운영하는 방식이다. 운영인프라, 학습에 필요한 데이터와 학습 모델 등 모든 영역을 자체 구축하는 방식이다.



[그림 2-58] (예시) 생성형 AI 자체구축

Insights | 전문가 칼럼

주요 단점으로는,

- 1) 생산형 AI의 구축, 운영 능력이 필요하며 AI 관련 전문지식을 갖춘 인력이 필요하다.
- 2) 사업 규모와 요구되는 결과물에 따라 대규모 운영 인프라가 필요하다.

생성형 AI 이용 – 외부서비스 사용

생성형 AI 인프라와 기초 데이터를 외부 제공사를 이용하는 방식으로 SaaS와 유사하다. 일반적으로 우리가 가장 많이 이용하는 방식이다.

주요 장점으로는,

- 1) 인프라, 데이터 저장소, 전문 인력 등의 리소스를 절약할 수 있다.
- 2) 기본 인프라 구축이 불필요 해 즉시 사용할 수 있다.
- 3) 운영에 필요한 운영기술, 전문지식 및 전문 운영 인력이 불필요 하다.

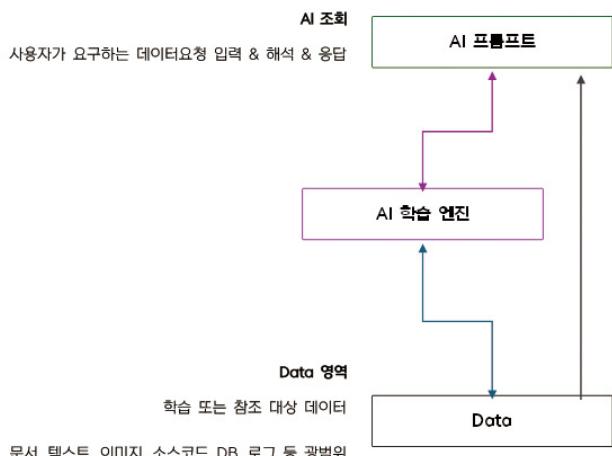


그림 2-59 (예시) 생성형 AI 외부서비스 사용

주요 단점으로는,

- 1) 모델이 학습한 원천 데이터의 신뢰도와 적절성을 검증하기 어렵다.
생성형 AI는 학습한 데이터의 분포를 따라 데이터를 생성하므로, 학습 데이터의 품질이 중요하다. 하지만 학습 데이터의 출처나 정확성, 편향성, 관련성 등을 확인하고 검증하기 어렵다. 따라서 생성형 AI는 학습 데이터의 문제점을 반영해 잘못된 데이터를 생성할 수 있다.
- 2) 학습한 원천데이터가 불명확한 경우 산출물의 상업적 활용이 어려울 수 있다.
학습한 원천데이터 저작권이 모호하거나 무단 사용해 모델을 생성한 경우, 그 산출물 또한 상업적 활용에 제약 받거나 산출물 소유권을 인정받지 못할 수 있다.
- 3) 회사 내부데이터를 강화 학습/참조하는 경우 중요 데이터가 외부로 유출될 수 있다.
생성형 AI는 내부 데이터를 학습하고, 접근하고, 생성하고, 전송하는 과정에서 보안 위반 위험이 있다. 따라서, 생성형 AI는 내부 데이터의 보안과 개인정보의 보호를 위해 적절한 통제와 모니터링이 필요하다
- 4) 질의, 학습에 데이터가 서비스 제공사에 의해 의도하지 않게 2차 활용될 수 있다.
많은 서비스 제공사가 제공사의 생성형 AI 개선을 위해 사용자가 입력한 질의내용, 추가 학습 및 참조데이터를 재학습 및 서비스 개선에 활용하기도 한다. 따라서 서비스를 이용 전 철저한 환경 조사가 필요하다.

참고로 위의 언급된 단점은 외부자가 생성한 생성형 AI모델을 별도 변형없이 도입해 자체구축한 경우 동일한 문제점이다.

● 생성형 AI의 보안적인 측면에서의 고려사항

생성형 AI를 도입하고 운영하기 위해서는 다음과 같이 보안적 측면에서 고려해야 한다. 일반적으로 생성형 AI 외부서비스를 사용하고 있는 사례가 대다수이며, 이 경우 SaaS 서비스 도입과 유사한 관점으로 접근하면 좀 더 손쉽고 안전하게 도입할 수 있다.

- 사업의 목적과 필요조건을 식별하고 적절한 통제 규정을 마련해야 한다. 각 사업의 목적에 따라 범위, 내부규정, 취급 데이터가 달라질 수 있어 도입 전 명확한 정의를 수립해야 한다.
- 생성형 AI 서비스 도입 방식에 따라 적절한 보안 관리 기준을 마련하고 준수해야 한다. 생성형 AI 서비스는 외부 공개된 서비스를 활용하거나, 자체 구축한 서비스를 이용할 수 있는데, 각각의 방식에 따라 보안 관리의 책임과 범위가 다르다. 따라서, 생성형 AI 서비스 도입 방식에 따라 적절한 보안 관리 기준을 마련하고 준수해야 한다.
- 생성형 AI 서비스에 사용되는 데이터의 접근 권한과 저장 위치를 통제해야 한다. 생성형 AI 서비스는 내부 데이터를 학습하고 접근, 전송, 생성하는 과정에서 내부정보 유출 위험이 있다. 따라서 원천 데이터 및 생산 데이터의 추적과 통제가 필요하다.

- 원천 데이터를 접근권한에 기반해 학습해야 함
- 원천 데이터를 학습 대상과 비학습 대상으로 구분해 관리해야 함
- 원천 데이터에서 개인정보, 기밀정보를 철저히 구분, 필터링해 관리해야 함
- 원천 데이터의 접근권한이 부실 한 경우 AI서비스가 유출경로가 될 수 있음
- 사용자가 AI에 질의한 요청의 민감도를 구분하고 관리해야 함
- AI 서비스에서 생산된 데이터가 Cloud에 저장되는 경우 외부유출을 통제 해야함

예시. 데이터 접근제어

2024년 사이비 위협 동향 보고서

Insights | 전문가 칼럼

The screenshot shows the 'Admin Console' interface with the 'Access Control' tab selected. Under 'Sharing Settings', there are sections for 'Sharing Options' and 'Sharing Requests'. A highlighted box contains text about AI-generated content and AI services opt-out policies. Another box provides details on how AI services can store and use user content.

▣ 그림 2-60 (예시) Adobe Admin Console 데이터 공유제한 설정

- 생성형 AI 서비스에 사용되는 모든 데이터가 2차 활용되지 않도록 차단해야 한다. 생성형 AI 서비스 품질 향상을 위해 이용자가 질의한 질의내역, 학습데이터, 모델, 참조 참조데이터 등을 경우에 따라 2차 활용할 수 있다. 따라서 기술적 보호조치와 NDA, 약관 등을 검토해 내부 데이터가 2차 활용되지 않도록 차단해야 한다.

The screenshot shows the 'AWS Organizations > Policies' section. Under 'Supported policy types', the 'AI services opt-out policies' section is highlighted with a red border. It describes how these policies enable control over AWS AI services storing and using user content. Other policy types listed include 'Backup policies', 'Service control policies', and 'Tag policies', each with their status (Disabled or Enabled).

▣ 그림 2-61 (예시). AWS opt-out 설정

Insights | 전문가 칼럼

- 생성형 AI 서비스에 질의한 요청과 생성된 결과물의 민감도를 구분하고, 재검증과 이력 관리를 해야 한다.

생성형 AI 서비스는 사용자의 텍스트 입력에 따라 자동으로 데이터를 생성하므로, 생성된 데이터의 품질과 안전성을 사전에 검사하고 수정하기 어렵다. 따라서, 생성형 AI 서비스에 질의한 요청과 생성된 결과물의 민감도를 구분하고, 재검증과 이력 관리를 해야 한다.

- 회사 내부 데이터 이용 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 등 민감정보가 저장되는 경우 지역지정이 가능한가
- 서비스로 전송되는 모든 데이터는 접근통제 및 이력관리가 가능한가
- 사업자 간 NDA 체결로 회사 데이터를 보호 받을 수 있는가

예시. 데이터 보호조치 수립

- 생성형 AI의 학습데이터의 적절성을 상시 검토하고 원천데이터의 신뢰성을 확보해야 한다. 생성형 AI의 모델을 생성하는 원천데이터가 저작권을 위반하거나 개인정보를 침해하는 경우, 그 결과물은 동일하게 법적 제재를 받는다. 또한 개인정보 및 민감정보가 Fine-tuning 되는 경우 이를 제거하기 매우 어렵다.

- AI 서비스에서 참조하는 원천데이터가 신뢰할 수 있는 데이터인가
- 사용자 질의를 요청에 부합하게 해석하고 신뢰된 결과를 응답했는가
- AI 서비스에서 참조하는 원천코드, 이미지가 적절한가
- 원천코드/이미지의 라이선스, 오픈소스 유형이 적절한가
- 원천 코드의 악성코드 등의 해킹 위험성은 없는가
- 생산형AI의 결과를 상업적 용도로 사용할 수 있는가

예시. 데이터의 적절성

- 생성형 AI 서비스의 프롬프트 설계와 데이터 접근 제어를 통해 프롬프트 공격을 방지해야 한다. 생성형 AI 서비스는 사용자가 입력한 텍스트를 프롬프트라고 하며, 프롬프트에 따라 데이터를 생성한다. 하지만, 프롬프트에 악의적인 내용이나 명령이 포함되면, 생성형 AI 서비스가 원하지 않는 데이터를 생성하거나, 공격자에게 유출하거나, 공격자의 명령을 수행할 수 있다. 이를 프롬프트 공격이라고 한다. 따라서, 생성형 AI 서비스의 프롬프트 설계와 데이터 접근 제어를 통해 프롬프트 공격을 방지해야 한다.

● 생성형 AI의 이용 가이드라인과 법적 규제

생성형 AI는 품질이 낮거나, 오류가 있는, 또는 위험한 데이터를 생성할 수 있다. 따라서 생성형 AI에서 만든 결과물을 재검증 할 수 있는 프로세스 구현해 적용해야 한다.



그림 2-62 (예시) Hallucination

생성형 AI의 일반적인 위험성은 다음과 같다.

- 생성형 AI의 오남용이나 악용이 사회적, 윤리적 문제를 야기할 수 있다. 생성형 AI는 현실과 구분하기 어려운 가짜 데이터를 생성할 수 있으므로, 그 데이터를 오남용하거나 악용하면 사회적, 윤리적 문제를 야기할 수 있다. 예를 들어, 생성형 AI는 가짜 뉴스나 딥페이크 등을 생성하고, 보안 인증이나 사기 등에 이용할 수 있다.
- 생성형 AI의 과잉 의존이 인간의 창의성과 판단력을 저하시킬 수 있다. 생성형 AI는 인간의 역량을 보완하고, 향상시킬 수 있으나, 그에 과잉 의존하면 인간의 창의성과 판단력을 저하시킬 수 있다. 예를 들어, 생성형 AI는 인간의 의사결정이나 행동을 영향을 줄 수 있으며, 인간의 책임감이나 도덕성을 약화시킬 수 있다.
- 생성형 AI의 자기 발전이 인간의 통제를 벗어날 수 있다. 생성형 AI는 스스로 학습하고, 개선하고, 발전할 수 있으나, 그 과정에서 인간의 통제를 벗어날 수 있다. 예를 들어, 생성형 AI는 인간의 의도와 다른 목적이나 방식으로 데이터를 생성하고, 인간의 권한이나 규칙을 무시하고, 인간에게 위협이 되는 데이터를 생성할 수 있다.

Insights | 전문가 칼럼

생성형 AI의 이용 가이드라인과 법적 규제는 다음과 같다.

생성형 AI의 이용 가이드 라인은 생성형 AI의 이용자와 제공자에게 생성형 AI의 적절하고 책임 있는 이용을 권고하고 있다.

- 인간의 존엄성과 권리를 존중하고, 보호하고, 증진시켜야 한다.
- 투명하고, 설명 가능하고, 책임 있고, 신뢰할 수 있어야 한다.
- 학습 데이터와 생성 데이터의 출처와 저작권을 명시하고, 존중하고, 보호해야 한다.
- 학습 데이터와 생성 데이터의 품질과 안전성을 보장하고, 검증하고, 개선해야 한다.
- 학습 데이터와 생성 데이터의 보안과 개인정보를 통제하고, 모니터링하고, 보호해야 한다.
- 학습 데이터와 생성 데이터의 편향과 차별을 인식하고, 방지하고, 교정해야 한다.
- 학습 데이터와 생성 데이터의 오남용이나 악용을 감지하고, 예방하고, 대응해야 한다.
- 학습 데이터와 생성 데이터의 영향력과 책임을 평가하고, 공유하고, 책임져야 한다.

생성형 AI의 법적 규제는 생성형 AI의 이용자와 제공자에게 생성형 AI의 적법하고 적정한 이용을 강제하는 법률로 다양한 국가나 지역에서 제정을 준비, 진행하고 있다. 예를 들어, 유럽연합은 생성형 AI의 법적 책임과 규제를 위한 법안을 발표했으며, 미국은 생성형 AI의 보안과 민감도를 위한 법안을 제안했다. 생성형 AI의 법적 규제는 일반적으로 다음과 같은 내용을 포함한다.

- 인간의 권리와 자유를 침해하거나, 위협하거나, 손상시키지 않아야 한다.
- 인간의 감독과 개입을 받아야 하며, 인간의 의사결정과 행동을 침해하거나, 제한하거나, 강요하지 않아야 한다.
- 학습 데이터와 생성 데이터의 출처와 저작권을 준수하고, 침해하거나, 위반하거나, 배타하지 않아야 한다.
- 학습 데이터와 생성 데이터의 보안과 개인정보를 준수하고, 침해하거나, 유출하거나, 남용하지 않아야 한다.
- 학습 데이터와 생성 데이터의 편향과 차별을 준수하고, 침해하거나, 유발하거나, 증폭하지 않아야 한다.
- 학습 데이터와 생성 데이터의 오남용이나 악용을 준수하고, 침해하거나, 유도하거나, 협력하지 않아야 한다.
- 학습 데이터와 생성 데이터의 영향력과 책임을 준수하고, 침해하거나, 회피하거나, 전가하지 않아야 한다.

● 결론

생성형 AI는 인공지능이 새로운 데이터를 생성하거나 수정하는 기술로, 보안 업무의 효율성과 품질을 향상시킬 수 있으며, 보안 리소스 부족 문제를 해결할 수 있다. 하지만, 학습 데이터의 신뢰도와 적절성, 생성된 결과물의 품질과 안전성, 내부 데이터 보안과 개인정보 보호, 생성형 AI의 오남용이나 악용, 과잉 의존, 생성형 AI의 자기 발전 등의 단점과 위험성을 고려해야 한다.

따라서, 생성형 AI를 도입하고 운영하기 위해서는 서비스 도입 방식에 따른 보안 관리 기준, 사용되는 데이터의 접근 권한과 저장 위치, 생성형 AI 서비스에 질의한 요청과 생성된 결과물의 민감도, 프롬프트 설계와 데이터 접근 제어 등의 보안적인 측면에서의 고려사항을 준수해야 한다. 또한, 생성형 AI의 이용 가이드라인과 법적 규제를 준수하고, 사회적, 윤리적 책임을 다해야 한다.



[나주본원] 전라남도 나주시 진흥길 9 한국인터넷진흥원

[서울청사] 서울시 송파구 중대로 135 (가락동) IT벤처타워 TEL. 1433-25