스몰캡

권명준 스몰캡
myoungchun.kwon@yuantakorea.com

종목	투자의견	목표주가 (원)
지니언스	Not Rated (I)	(I)
라온시큐어	Not Rated (M)	(M)

2025 K-사이버 보안 주목받을 수 있을까?

사이버 보안최근 이슈

지난 3월 19일 구글이 사이버보안 스타트업 위즈(Wiz) 인수를 공식 발표했다. 인수금액은 320억달러로 구글 인수 대금으로는 역대 최대 규모이다. 2024년에도 50억달러를 상회하는 사이버 보안기업들의 M&A Big-Deal들이 다수 이뤄졌다.

국내 사이버 보안사고는 늘어나고 있다. 한국인터넷진흥원(KISA)에 따르면 신고된 2024년 국내 유형별 사이버 침해사고는 총 1,887건으로 전년대비 47.8% 증가했다. 2023년의 전년대비 증가율(+11.8%)와 비교해 볼 때 30.0%p 상승한 수치이다.

국내 사이버 보안 기업들이 주목받지 못하는 이유

개인. 한국은 사이버 보안에 대한 인식이 낮다고 판단한다. 노드VPN은 사이버보안 인식테스트(NPT)를 매년 발표하고 있다. 한국은 2023년에 이어 2024년에도 사이버보안과 개인정보보호인식이 여전히 심각하게 부족하다고 평가되었다

기업. 2024년 정보보호 산업 실태조사가 2024년 10월에 발표되었다. 2023년 국내 정보보호 산업 전체 매출액은 16.8조원으로 전년대비 4.0% 증가했다. 하지만 수출로 한정해 살펴보면 2023년 2.0조원에서 2024년 1.68조원으로 16.3% 감소했다. 국내 매출액 성장률 대비 수출액 감소율이 더 크다는 점에서 심각성을 확인할 수 있다.

정부. 과기부의 사이버위협 대응 관련 R&D 예산 현황에 따르면 2025년도 정부안에서 총 1,049억원이 책정되었다. 2024년에 책정된 1,141억 500만원 대비 92억 500만원 감소된 수치이다. 다양하고, 복합적이고, 국내외에서 사이버 위협이 발생할 수 있다고 전망하고 있지만 정부 예산은 감소되었다.

국내 사이버 보안 기업 주목받을 수 있을까?

제로트러스트 2.0을 통해 국내 기업들은 새로운 먹거리 확보 및 글로벌 경쟁력을 갖출 수 있는 시기라고 판단된다. 제로트러스트의 주요 수단은 생체인식(FIDO)을 기반한다. 2025년 사이버 위협 전망을 통해서는 클라우드와 관련된 보안, AI를 활용한 공격(랜섬웨어, 딥페이크, 스미싱 등) 등을 주목하고 있다는 것을 알 수 있다.

라온시큐어와 지니언스를 주목한다. 라온시큐어(042510)는 FIDO 생체인식 기술을 보유하고 있으며, 모바일 ID Biz의 해외 진출이 기대된다. 지니언스(263860)는 오프레미스와 클라우드 방식을 모두 지원하는 보안 솔루션(NAC, ZTNA)을 보유하고 있으며, 해외시장에서 신규 고객사를 확대하고 있다.

사이버 보안 관련 최근 이슈!

1. 구글, 클라우드 사이버보안 위즈 인수 추진

지난 3월 19일 구글이 사이버보안 스타트업 위즈(Wiz) 인수를 공식 발표했다. 인수금액은 320억달러로 구글 인수 대금으로는 역대 최대 규모이다. 위즈는 클라우드 환경에서 위험요소를 신속히 식별 및 제거해 보안 사고를 예방하는 플랫폼을 제공하고 있다. 인수 후 구글 클라우드에 합류할 것으로 예상된다.

2024년 주요 사이버보안 M&A를 살펴보면 다음과 같은 특징을 보였다. 첫째. 외형 확대. 마임캐스트(Mimecast)는 3개 기업(엘러베이트시큘리티(1월), 코드42(7월), 어웨어(8월)) 인수를 진행했다. 포티넷(Fortinet), 아르미스(Armis), 프로텍트AI(Protec AI) 등의 기업은 2개 기업 인수를 발표했다. 둘째, Big-Deal. 2024년 50억달러를 상위하는 3건의 Big-Deal이 2024년에 이뤄졌다. HPE의 주니퍼네트웍스(Juniper Networks) 인수(140억달러), IBM의 하시코프(HashiCorp) 인수(64억달러), 토마브라보의 다크트레이스(Darktrace) 인수(53.2억달러) 등이 이에 해당된다.

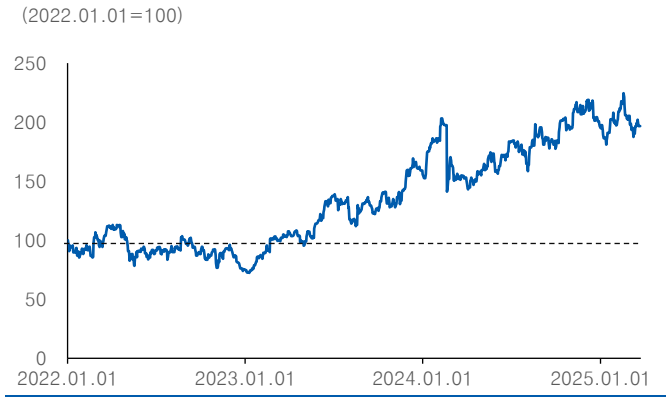
2025년 구글-위즈 인수와 연계해서 생각해본다면 외형확장에 따른 Big-Deal이 이어질 것으로 기대된다.

[표 1] 2024 년 글로벌 보안기업 M&A Deal

월	인수기업	피인수기업	인수대금
1월	5G네트웍스	시큐리티쉬프트	260만달러
1월	HPE	주니퍼네트웍스	140억달러
3월	클라우드스트라이크	플로우시큐리티	2억달러
3월	깃랩	옥스아이	3,000~4,000만달러
3월	지스케일러	아발러	3.5억달러
4월	아르미스	실크시큐리티	1.5억달러
4월	IBM	하시코프	64억달러
4월	토마브라보	다크트레이스	53.2억달러
9월	마스터카드	레코드퓨처	26억달러
10월	엑스페리안	클리어세일	3.5억달러
10월	소포스	시큐어웍스	8.6억달러
11월	위즈	대즈	4.5억달러

자료: 보안뉴스, 유안타증권 리서치센터

[그림 1] 팔로알토 상대주가 추이

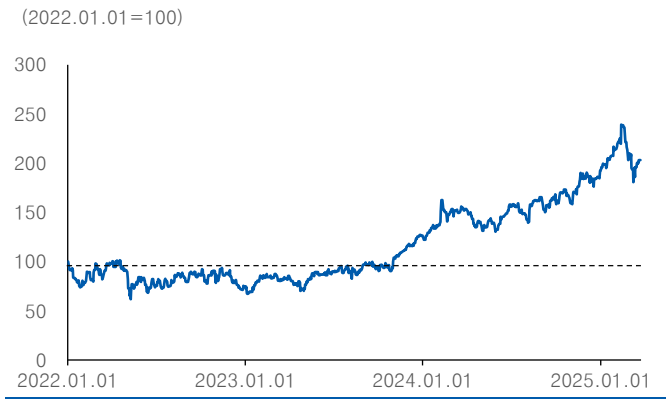


자료: Bloomberg, 유안타증권 리서치센터

[그림 2] 인포시스 상대주가 추이

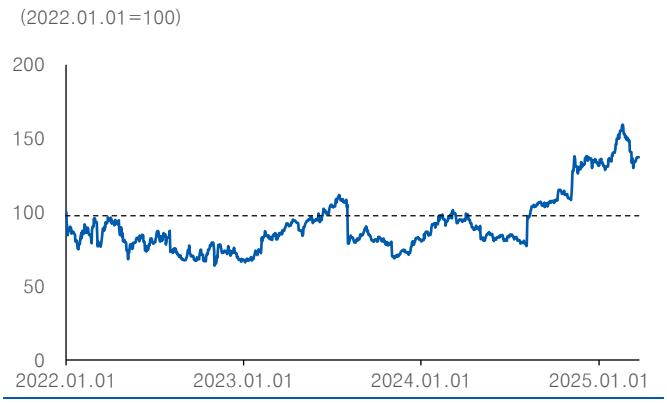
자료: Bloomberg, 유안타증권 리서치센터

[그림 3] 사이버아크 상대주가 추이



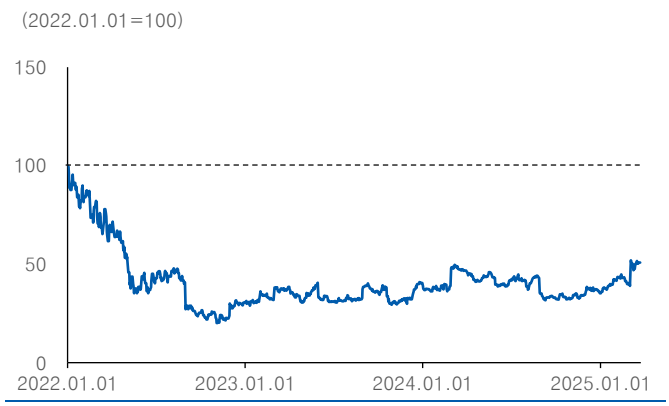
자료: Bloomberg, 유안타증권 리서치센터

[그림 4] 포티넷 상대주가 추이



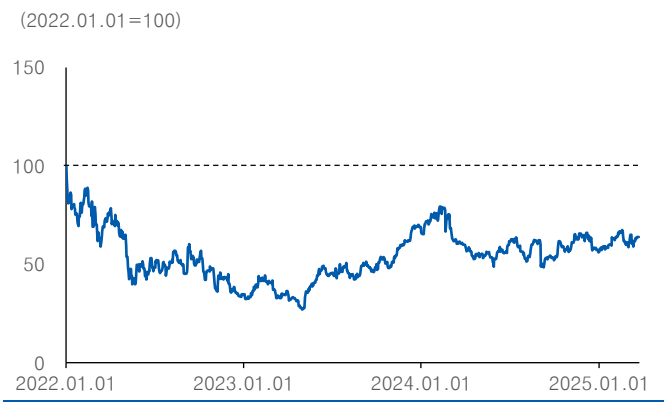
자료: Bloomberg, 유안타증권 리서치센터

[그림 5] 옥타 상대주가 추이



자료: Bloomberg, 유안타증권 리서치센터

[그림 6] 지스케일러 상대주가 추이



자료: Bloomberg, 유안타증권 리서치센터

2. 증가하고 있는 국내 사이버 보안 사고

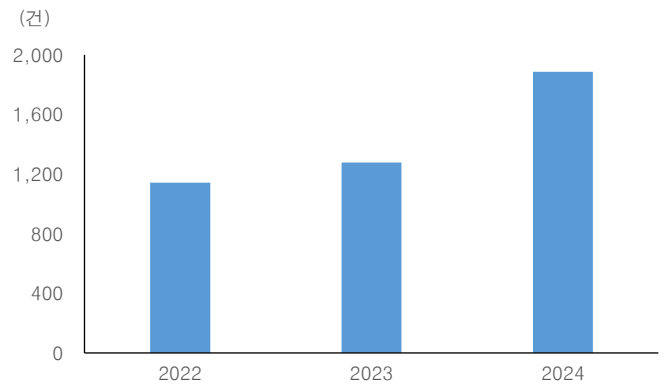
한국인터넷진흥원(KISA)에 따르면 신고된 2024년 국내 유형별 사이버 침해사고는 총 1,887건으로 전년대비 47.8% 증가했다. 2023년의 전년대비 증가율(+11.8%)와 비교해 볼 때 30.0%p 상승한 수치이다.

2024년의 사이버 침해사고를 세부 항목으로 살펴보면 디도스공격(yoy +33.8%), 악성코드(-23.7%), 서버해킹(+81.3%), 기타(+74.6%) 등으로 서버해킹이 가장 큰 폭으로 증가했으며, 랜섬웨어가 포함되어 있는 악성코드 관련 사이버 침해는 감소하는 모습을 보였다. 서버해킹은 전체 침해사고의 비중이 2024년 절반이상(56.0%)을 차지했다.

2023년과는 다른 모습을 보였다. 2023년에 디도스공격(+74.6%), 악성코드(-13.5%), 서버해킹(-0.3%), 기타(+105.7%)였다. 2023년에는 디도스공격에 따른 침해사고가 가장 많이 증가했다는 것을 알 수 있다. 한가지 더 특징적인 사항은 위 카테고리에 포함되지 않은 기타사례가 증가율이 높다는 점이다. 이는 사이버 보안사고 유형이 다양해지고 있다는 것을 알 수 있다.

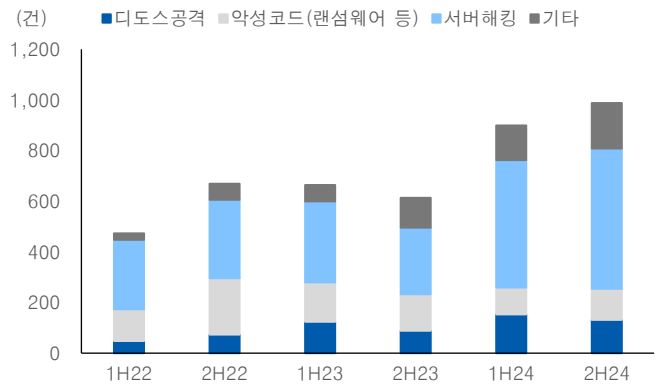
업종별 침해사고 신고 현황을 살펴보면 2024년에는 정보통신업(yoy +36.0%), 제조업(+35.9%), 도매 및 소매(+41.3%), 협회 및 단체(+71.8%)였다. 2023년은 정보통신업(+8.1%), 제조업(0.0%), 도매 및 소매(+17.9%), 협회 및 단체(+4.3%)였다. 이를 통해 다양한 업종으로 침해사고가 확산되는 것을 알 수 있다. 정보통신업이 가장 많은 신고를 받고 있지만 점유율은 하락(2022년 35.8%→2023년 34.6%→2024년 31.8%)하고 있다. 또한 기타의 비중이 2022년 22.9%에서 2024년 30.3%로 7.6%p 상향되었다. 이를 통해 사이버 보안사고 타겟 역시 다양해지고 있다는 것을 알 수 있다.

[그림 7] 유형별 침해사고 신고 현황(연도별)



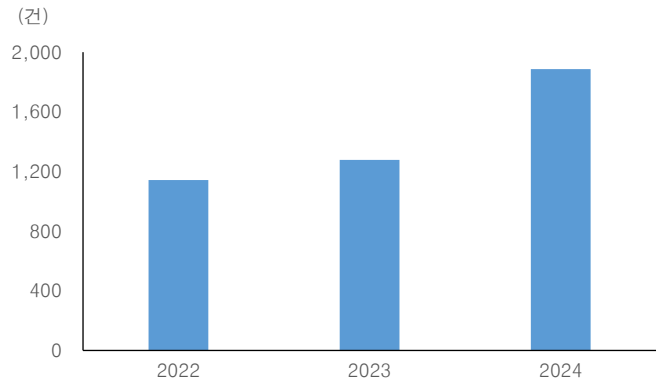
자료: 한국인터넷진흥원(KISA), 유안타증권 리서치센터

[그림 8] 유형별 침해사고 신고 현황(반기별)



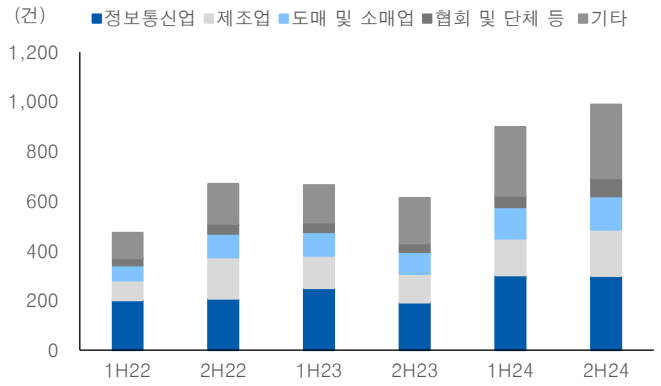
자료: 한국인터넷진흥원(KISA), 유안타증권 리서치센터

[그림 9] 업종별 침해사고 신고 현황(연도별)



자료: 한국인터넷진흥원(KISA), 유안타증권 리서치센터

[그림 10] 업종별 침해사고 신고 현황(반기별)

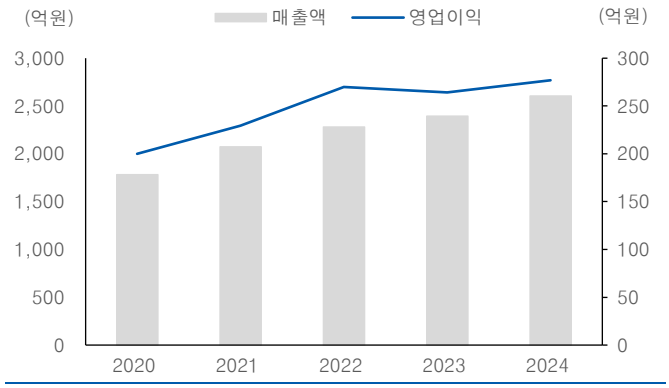


자료: 한국인터넷진흥원(KISA), 유안타증권 리서치센터

3. 국내 보안기업의 2024년 호실적

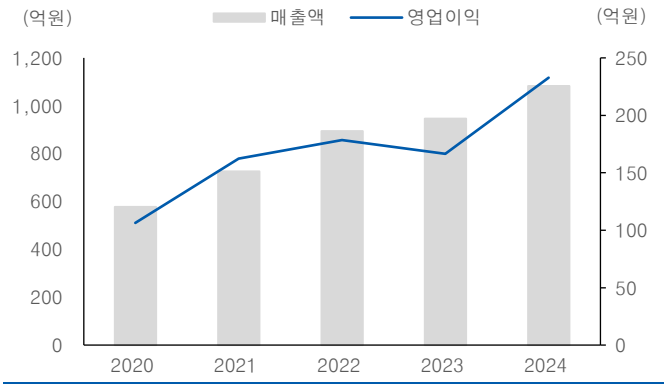
2024 년 국내 주요 보안기업들의 실적은 전년대비 성장하는 모습을 보였다. 매출액뿐 아니라 영업이익 역시 전년대비 성장했다. 아래기업 중 매출액은 라온시큐어, 영업이익은 지니언스가 전년대비 가장 높은 성장률을 보였다.

[그림 11] 안랩 연도별 매출액 및 영업이익 추이



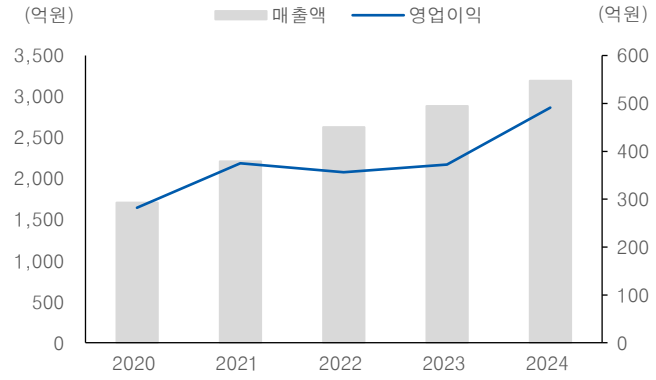
자료: Quantiwise, 유안타증권 리서치센터

[그림 12] 슈프리마 연도별 매출액 및 영업이익 추이



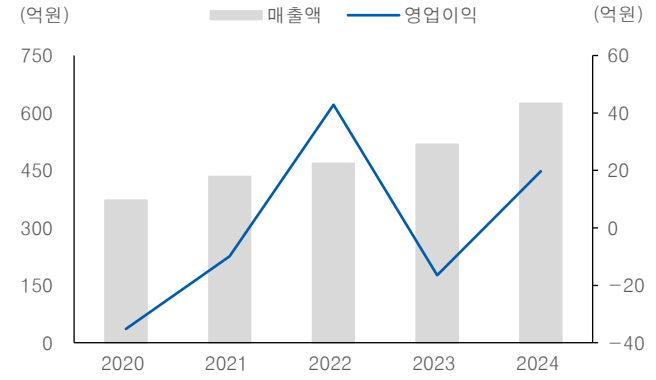
자료: Quantiwise, 유안타증권 리서치센터

[그림 13] 헥토이노베이션 연도별 매출액 및 영업이익 추이



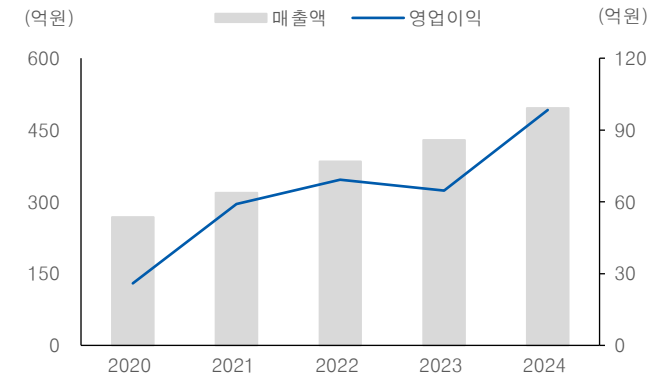
자료: Quantiwise, 유안타증권 리서치센터

[그림 14] 라온시큐어 연도별 매출액 및 영업이익 추이



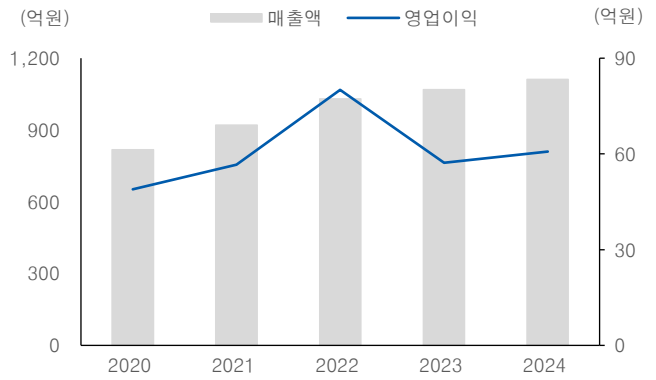
자료: Quantiwise, 유안타증권 리서치센터

[그림 15] 지니언스 연도별 매출액 및 영업이익 추이



자료: Quantiwise, 유안타증권 리서치센터

[그림 16] 이글루 연도별 매출액 및 영업이익 추이



자료: Quantiwise, 유안타증권 리서치센터

국내에서 사이버 보안기업들이 주목받지 못하는 이유!

국내 사이버 범죄가 증가, 2024년 국내 보안기업들의 호실적을 보였음에도 불구하고 2024년 국내 사이버보안기업들은 해외 사이버 보안기업들의 주가와 상이한 주가 흐름을 보였다. 개인, 기업, 정책 3가지 측면에서 고민해 보았다.

1. 개인

한국은 사이버 보안에 대한 인식이 낮다고 판단한다. 노드VPN은 사이버보안 인식테스트(NPT)를 매년 발표하고 있다. 한국은 2023년에 이어 2024년에도 사이버보안과 개인정보보호인식이 여전히 심각하게 부족하다고 평가되었다. 사이버보안 인식테스트는 디지털 습관, 위험 수용성, 개인정보 보호 인식 등의 국가별 점수를 측정하여 순위를 결정한다.

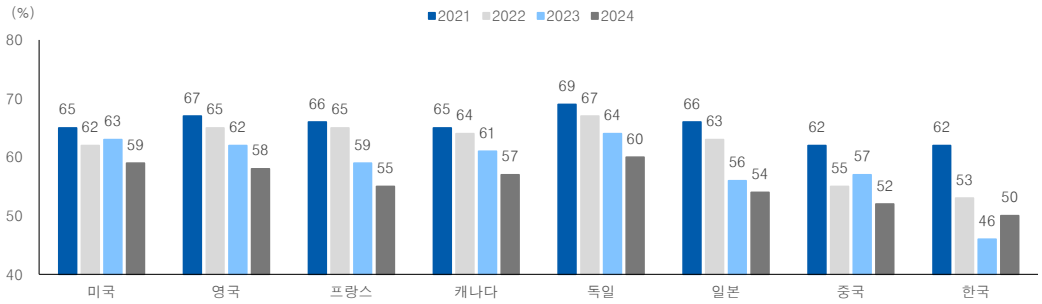
2024년 평균 점수가 58점인 반면 한국은 50점에 불과했다. 디지털 습관 50점, 위험 수용성 45점, 개인정보 보호인식 57점이었다. 2023년의 종합점수는 46점이었으며 디지털습관 36점, 위험 수용성 49점, 개인정보 보호인식 50점이었다. 전년대비 상승하는 모습이라고 생각할 수 있다. 하지만 2022년 종합점수 53점, 2021년 종합점수 62점과 비교해보면 하향 추세가 회복되었다고 판단하기 어렵다.

비교를 위해 7개국(미국, 영국, 프랑스, 캐나다, 독일, 일본, 중국)을 살펴보았다. 북미/유럽 등의 국가뿐 아니라 일본보다 낮으며, 중국보다도 낮은 점수를 받고 있다. 심각성을 확인할 수 있다. 참고로 2024년의 국가별 종합점수는 미국 59점, 독일 60점, 일본 54점, 중국 52점이었다. 지난 4년간(2021~2024년) 중국 평균점수와 비교시 3.8점 낮은 수치이다.

2024 사이버보안 인식테스트에서 한국 참여자가 더 자세히 알아볼 필요가 있는 사항으로 업무에 AI를 활용할 때 고려해야 할 개인 정보 보호 문제(정답비율 3%), 홈 Wi-Fi 네트워크를 보호하는 방법(8%), 인터넷 서비스 제공자(ISP)가 메타데이터로 수집하는 정보(10%) 등이다. 최근에 부각되고 있는 AI, 클라우드, IoT 등과 관련된 보안인식이 낮다는 것을 알 수 있다.

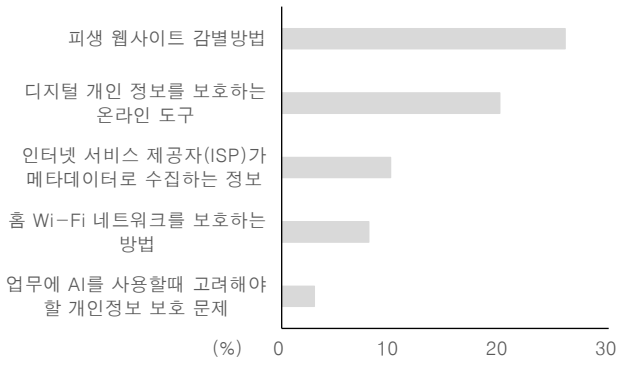
2023년과 비교해 보면 일부 개선되었다는 점은 긍정적이다. 2023년에서는 인터넷 서비스 제공자(ISP)가 메타데이터로 수집하는 정보(2%), 홈 Wi-Fi 네트워크를 보호하는 방법(2%), 디지털 개인정보 보호를 보호하는 온라인 도구(2%), 앱 및 온라인 서비스 이용약관 읽어보기의 중요성(10%) 등이 10%이하의 정답 비율을 보였다. 사용자 확대에 따른 관심 증가, 기업들의 교육 확대 등이 영향을 끼쳤을 것으로 추정된다.

[그림 17] 2021~2024년 국가별 사이버 보안 인식 테스트



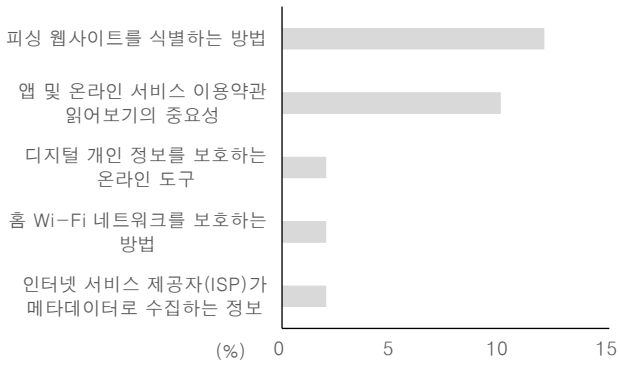
자료: NPT, 유안타증권 리서치센터

[그림 18] 한국 참여자가 더 자세히 알아볼 필요가 있는 사항(2024)



자료: NPT, 유안타증권 리서치센터

[그림 19] 한국 참여자가 더 자세히 알아볼 필요가 있는 사항(2023)



자료: NPT, 유안타증권 리서치센터

2. 기업

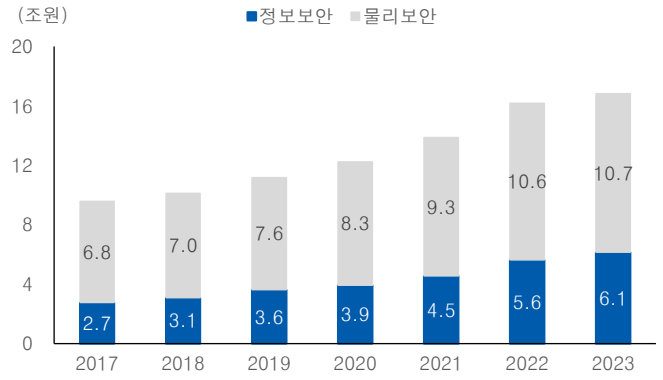
2024년 정보보호 산업 실태조사가 2024년 10월에 발표되었다. 2023년 국내 정보보호 산업 전체 매출액은 16.8조원으로 전년대비 4.0% 증가했다. 국내 정보보호 산업은 정보보안과 물리보안으로 구분된다. 정보보안은 6.1조원으로 전년대비 9.4%, 물리보안 10.7조원으로 1.2%증가했다. 하지만 수출로 한정해 살펴보면 2023년 2.0조원에서 2024년 1.68조원으로 16.3% 감소했다. 국내 매출액 성장률 대비 수출액 감소율이 더 크다는 점에서 심각성을 확인할 수 있다.

세부적으로 살펴보면 다음과 같다. 정보보안은 네트워크보안, 엔드포인트보안, 플랫폼보안/보안관리, 클라우드보안, 콘텐츠/데이터 보안, 공동인프라 보안 등으로 구분된다. 2023년 정보보안에서는 네트워크보안은 전년대비 19.5% 성장했지만 플랫폼보안, 콘텐츠/데이터, 공동인프라는 역성장하는 모습을 보였다. 정보보안 수출액을 살펴보면 네트워크보안은 2022년 714억원에서 2023년 500억원으로 감소하는 모습을 보였다. 네트워크보안 마저도 글로벌 경쟁력에 대해서는 의구심이 존재한다.

물리보안 세부항목을 살펴보면 보안용카메라, 보안용 저장장치, 출입통제 장비 등 출입보안과 관련된 항목 위주로 성장하는 모습을 보였다. 하지만 이 역시 수출액 추이를 살펴보면 보안용 카메라, 보안용 저장장치, 출입통제 장비 모두 감소하는 모습을 보였다. 특징적인 점은 생체인식 보안 시스템는 산업 전체 매출액은 감소했지만, 수출액은 2023년 1,015억원에서 2023년 2,136억원으로 2배 이상 성장하는 모습을 보였다.

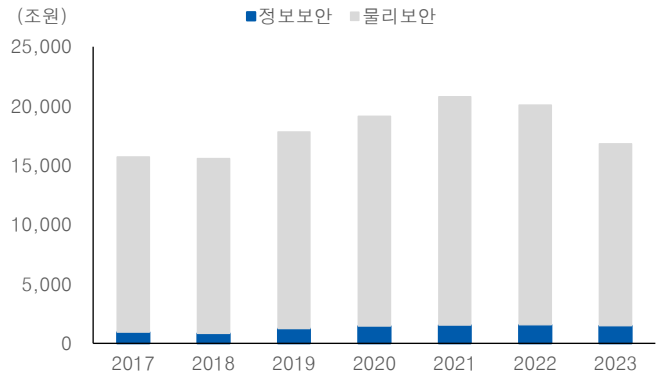
국내 정보보호산업 관련 2023년 전체 종사자는 6만 308명으로 전년(6만 4,831명) 대비 7.0% 감소했다. 정보보안 종사자수는 전년대비 4.1% 증가했지만, 물리보안 종사자는 13.1% 감소했다. 정보보안 종사자 중 연구개발 인력은 9.5% 증가했다는 점은 긍정적이지만, 관제와 관련된 종사자가 2,656명으로 15.9%감소. 기업들의 R&D 투자 확대영역이 제한적인 것으로 추정된다.

[그림 20] 국내 정보보호산업 매출액 추이(연도별)



자료: KISIA, 유안타증권 리서치센터

[그림 21] 국내 정보보호산업 수출액 추이(연도별)



자료: KISIA, 유안타증권 리서치센터

국내 보안기업들의 M&A도 활발하지 않다. 2024년 3월 국내 최초 사이버 보안전용 펀드 조성이 시작되었다. 2024년 정부가 200억원을 모태펀드에 출자하여 총 400억원 규모의 펀드를 조성, 2027년까지 4년간 출자를 통해 총 1,300억원 규모 이상의 펀드 조성을 목표로 하고 있다고 밝혔다.

펀드의 주 투자목적은 사이버보안 기술(AI, ZT, 융합보안, 클라우드 등)을 보유한 혁신 기업이거나 사업영역 및 규모 확대를 위한 M&A와 관련한 정보보호산업(물리보안 제외)에 해당하는 중소/벤처 기업에 50% 이상을 투자할 계획이다. 2025년 예산은 100억원 수준으로 절반 축소된 것으로 파악되고 있지만, 정책이 진행되고 있다는 점에서 2024년 보안기업들의 M&A가 부재했다는 점은 아쉬운 사안이라고 할 수 있다.

[그림 22] 사이버보안 펀드 출자사업계획

□ 펀드 결성규모

출자예산	결성 목표액	정부 출자비율	선정 운용사수	자조합별 최대출자액	신청가능 조합형태
200억원	400억원	50%	2개	200억원	벤처투자조합 신기술사업투자조합 기관전용 사모집합 투자기구

□ 투자 분야 및 조건

주요항목	주요내용
주목적투자 대상 및 의무비율	○ 정보보호산업(물리보안 제외)에 해당하는 중소·벤처 기업에 50% 이상 투자, 단, ①, ② 중 하나 이상의 조건을 충족하여야 함 ① **사이버보안 기술**(AI, ZT, 융합보안, 클라우드 등)을 보유한 혁신기업 ② 사업영역 및 규모 확대를 위한 **M&A**에 투자
투자/존속기간	○ 4년 / 8년
관리보수	○ {투자잔액(분기말 잔액) × 결성규모 적용요율} + (조합약정총액×1%)
기준수익률	○ 3% 이상
성과보수	○ 기준수익률을 초과하는 수익의 20%이내
인센티브	운용사는 인센티브를 선택하여 제안할 수 있으며, 출자심의회에서 최종 결정 ○ 손실 발생 시, 모태펀드가 민간출자자에게 모태펀드 납입출자금의 15% 이내에서 우선손실충당 가능 ○ 수익률이 펀드의 기준수익률을 초과하는 경우, 모태펀드가 수령할 초과수익의 30% 이내에서 민간출자자에게 지급 가능 구분 / 적용조건 / 추가성과보수율 초기 창업기업 / 「벤처투자 촉진에 관한 법률」에 의거한 초기창업기업 투자실적이 전체 투자금액 대비 40% 이상일 경우 / 모태펀드가 수령할 초과수익의 10% 이내 목적달성 / 펀드 결성액의 40% 이상을 M&A에 투자 ○ 기준 시점 투자목표비율을 1회 이상 달성한 조합 대상, 모태펀드 출자지분에 대한 기준수익률 0.5%p 하향 적용
선정우대기준	○ 정부출자비율보다 5%p 이상 하향하여 제안하는 경우 ○ 주목적 투자비율을 10%p 이상 상향하여 제안하는 경우 ○ 최종 선정 시, 최소결성금액의 20% 이상을 '24년 내에 투자하기로 제안하는 경우

자료: 과기부, 유안타증권 리서치센터

3. 정부

과기부의 사이버위협 대응 관련 R&D 예산 현황에 따르면 2025년도 정부안에서 총 1,049억원이 책정되었다. 2024년에 책정된 1,141억 500만원 대비 92억 500만원 감소된 수치이다.

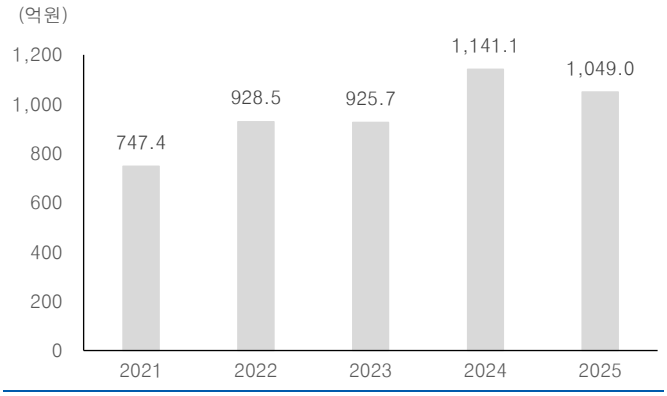
세부적으로 살펴보면 정보보호 핵심원천 기술개발 예산은 2024년 1,076억원에서 2025년 993억원으로 감소되었다. 2024년 예산(10억원) 책정되었던 사이버보안 챌린지 선도기술 개발, 데이터프라이버시 글로벌 선도기술 연구개발에는 예산이 배정되지 않았다.

비대면 서비스 물리보안 통합 플랫폼 운영체계 개발과 국방 무인 이동체 사이버보안 기술개발 관련 2025년 예산은 2024년과 동일하다. 암호화 사이버 위협대응 기술개발은 2024년 20억원에서 2025년 31.5억원으로 예산이 상승했다. 하지만 이 역시 2023년 30억원이었다는 점을 감안할 경우 예산이 상승했다는 평가가 무색하다.

정보보호 전문인력 양성 예산도 2024년 241.0억원에서 2025년 221.2억원으로 감소되었다. 2025년의 정규교육훈련과 정책기반 관련 예산은 전년과 동일했지만, 중단기교육훈련은 2024년 196.5억원에서 2025년 177.0억원으로 9.9%감소하였다.

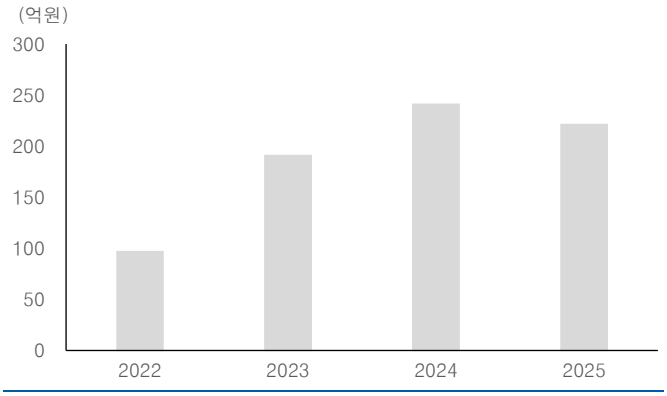
과기부의 「2024년 사이버위협 사례분석 및 2025년 전망」에 따르면 2024년도 사이버위협으로 ①사이버 사기(금융사기, QR사기 등)로 인해 국민 피해, ②S/W 공급망 공격 등 복합적이 공격 전술 사용, ③금품용구 악성 프로그램(랜섬웨어) 공격기번 고도화를 제시했다. 2025년 사이버위협으로는 ①공격자의 생성형 인공지능 활용 본격화, ②디지털 융복합 체계에 대한 사이버 위협 증가, ③국제 환경 변화에 따른 사이버 위협 증가 가능성, ④무차별(분산 서비스 거부) 디도스 공격 증가 예상 등이 될 것으로 전망했다. 다양하고, 복합적이고, 국내외에서 사이버 위협이 발생할 수 있다고 전망하고 있지만 정부 예산은 감소되었다.

[그림 23] 사이버 보안 관련 연도별 예산: 2025 년 전년대비 삭감



자료: 과기부, 유안타증권 리서치센터

[그림 24] 정보보호 전문인력 양성 예산



자료: KISA, 유안타증권 리서치센터

국내 보안기업 주목받을 수 있을까?

AI 산업 성장에 따라 사이버보안에 대한 글로벌 관심은 이어질 가능성이 높다. 반면, 국내에서는 개인들의 보안의식이 글로벌 국가대비 낮으며, 기업들은 글로별 경쟁력을 확보하고 있지 못한 상황이고, 2025년 예산은 축소되었다. 이런 상황에서 보안기업들이 주목을 받을 수 있을까? 주목을 받을 수 있다면 어떤 section일까? 이와 관련해서 다음의 내용을 우선적으로 살펴볼 필요가 있다.

1. 제로트러스트

제로트러스트(Zero Trust)는 기업망 내·외부에 언제나 공격자가 존재할 수 있고, 명확한 인증 과정을 거치기 전까지는 모든 사용자, 기기, 네트워크 트래픽을 신뢰하지 않으며, 인증 이후에도 끊임없이 신뢰성을 검증함으로써 기업의 정보 자산을 보호할 수 있는 보안 모델이다.

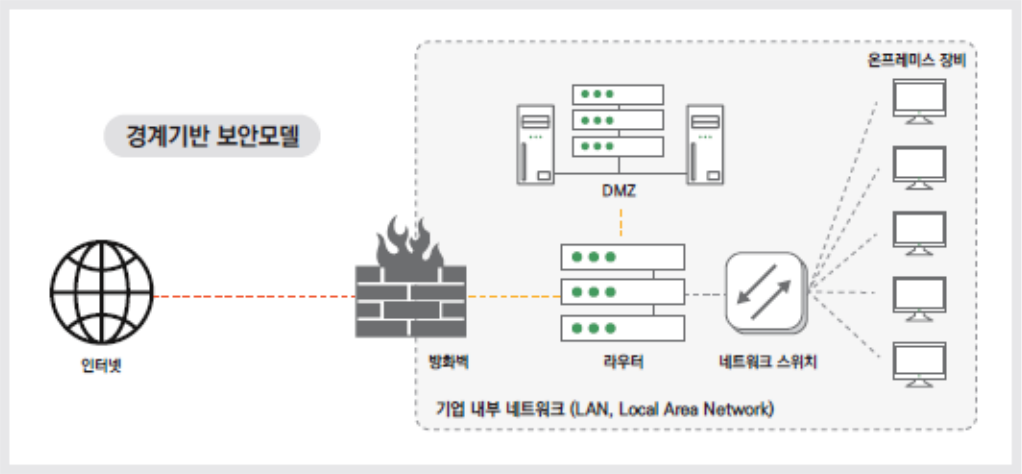
도입 배경. 전통적으로 기업은 업무를 위한 기업망을 두고, 기업망은 인터넷과 같은 외부망과 연동을 하되 경계선에서 보안 솔루션(방화벽, 침입탐지시스템 등)을 통해 해킹 공격에 대응하는 경계 기반의 보안 방식을 채택했다. 기존 기업망의 경우 기업망과 외부망으로 구분되는 구조가 단순하고 경계가 명확했기 때문이다.

다수의 기업들은 기존 보안기술을 일부 개선/보완/진화한 SIEM, SOAR, XDR 등의 보안관제 솔루션을 도입 및 운영하고 있다. 하지만 기업망 내부 사용자에 높은 신뢰를 부여함으로써 내부자는 기업내 서버 침투 및 데이터 유출이 상대적으로 용이하다.

모바일, IoT, 클라우드 확산으로 원격 재택 근무환경이 조성되었고, 코로나19 팬데믹으로 비대면 사회가 가속되어 기업망 보호를 위한 전통적인 사이버보안 체계의 변화가 야기되고 있다. 점점 늘어나는 사용자, 수많은 단말기와 장비, 이로 인해 복잡해지는 권한 권리 등 각 기관 및 기업의 사이버보안 관리가 어려워지고 있다. 고도화되고 있는 수많은 해킹 및 랜섬웨어 공격의 경우 피해가 확산되고 있다.

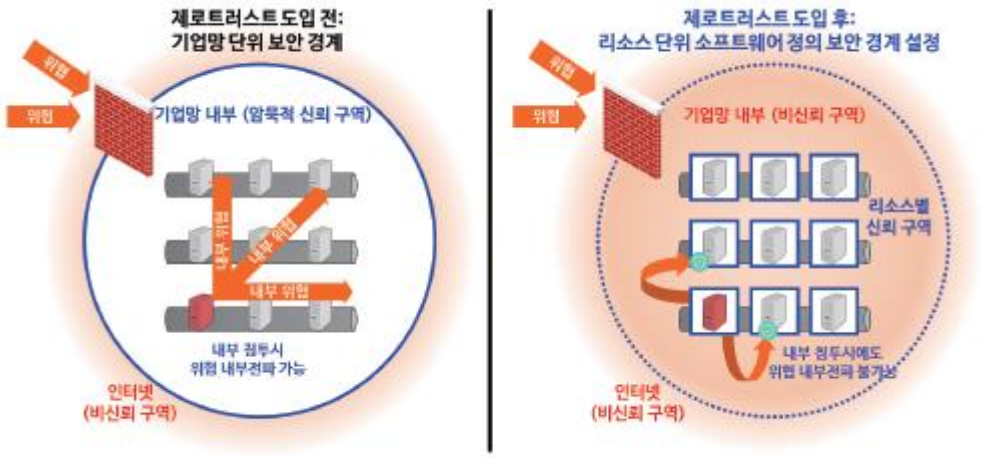
코로나19 팬데믹 당시 비대면/원격/재택근무 환경이 확대, 외부에서의 원격 접속을 위해 VPN(Virtual Private Network)망을 활용했다. 직원들의 원격 접속용 기기가 다양해지고, 직원이 생산 및 활용하는 데이터, 사내 업무 솔루션 등을 편리하게 접근할 수 있도록 클라우드 서비스도 확대되고 있다. 이 과정에서 ①보안과 비보안 영역의 경계, ②기업망 내외부의 경계가 모호해지면서 기존 경계 기반 보안 방식으로 기업망을 보호하는 것이 어려워졌다. 이러한 변화로 정부 시스템 및 서비스에 대한 접속요구가 발생시 네트워크가 이미 침해된 것으로 간주, 주어진 권한을 정확하고 최소한으로 부여하는데 있어서 불확실성을 최소화하도록 설계된 개념 및 아이디어인 제로트러스트가 주목받고 있다.

[그림 25] 경계 기반 보안 모델



자료: Digital.com, 유안타증권 리서치센터

[그림 26] 보안 패러다임의 변화: 기업망 단위 → 리소스 단위



자료: NIST(A.Kerman), KITA, 유안타증권 리서치센터

도입 효과. ①사용자 자격증명 도용. 악의적인 공격자는 정당한 사용자의 자격 증명을 위조하여 기업내 접근하고자 한다. 기존 기업망에서는 사용자의 자격 증명 위조만으로도 사내망 접근이 가능하다. 하지만 제로트러스트 환경에서는 접속기기 역시 신뢰를 확인하기 위한 대상으로 지정한다. 위장 기기의 경우 접근 권한이 부여되지 않는다. 해당 정보에 대한 로그 및 모니터링이 이뤄진다는 의미이다. 예를 들어 평상시 접속하지 않는 기기를 사용하여 접속하는 등 정상적인 경우가 아니라고 판단될 경우 해당 접속자에 대한 신뢰도 역시 충분하지 않다고 판단하다. 즉, 접속자의 다중 인증을 통해 안정성을 상향시킨다.

②원격 공격 혹은 내부자 위협. 공격자가 네트워크에 접속하여 권한 상승 이후 횡적 이동을 통해 다양한 리소스에 접근하거나 손상시킬 수 있다. 제로트러스트內 네트워크는 마이크로 세그멘테이션 되어 관리함에 따라 공격자의 횡적 이동을 제한한다. 데이터 접근은 보안 정책, 사용자 역할, 기기 속성 등에 따라 접근제어를 세밀화 한다. 민감한 데이터 접근도 제한적이다.

③공급망 침투. 공격자는 기업망에 있는 기기나 응용 프로그램에 악성코드를 삽입할 수 있다. 기존 기업망에서는 해당 접속에 대한 신뢰성이 부여된 이후에는 벌어지는 공격들에 대해서는 대응이 어렵다. 제로트러스트에서는 정상적인 기기에 정상적으로 배포된 프로그램이라고 하더라도 우선적으로 신뢰하지 않아 데이터 접근은 최소화로 이뤄져 피해를 최소화할 수 있다. 모든 네트워크 연결이 감시되어 허가 받지 않은 원격 접속을 통한 공격 명령/통제 및 데이터 전송 역시 대응이 가능하다.

[표 2] 시나리오별 제로트러스트 도입시 효과

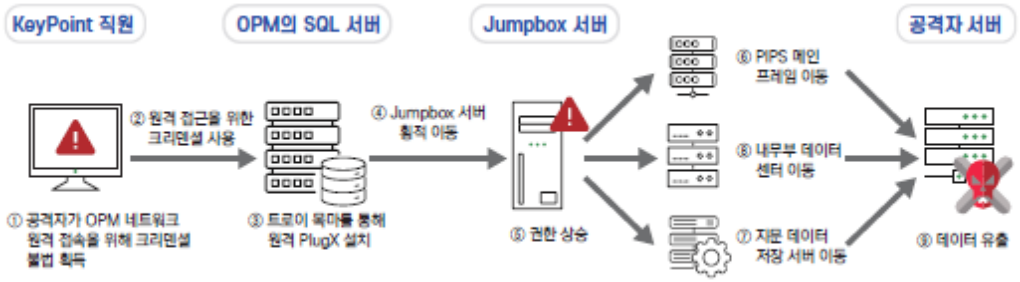
접근방법	세부내용	제로트러스트 보안 모델의 대응 시나리오
사용자 자격증명 도용	▶일반적으로 사용자 자격 증명 위조시 기기와 관계없이 기업망 내부 리소스 접근가능하여 피해 발생 ▶기업 외부 접속 시 강화된 다중 인증 등 인증 환경을 강화함으로써 일부 대응가능	▶위장 기기인 경우, 접근 권한이 부여되지 않고 해당 정보에 대한 로그 및 모니터링 ▶정상적인 자격 증명 후에도 신뢰도가 충분하지 않은 이벤트 발생 시 강화된 다중 인증 적용을 통한 대응
원격 공격 혹은 내부자 위협	▶네트워크에 접속, 권한 상승 후 횡적이동을 통해 다양한 리소스에 접근하거나 손상시키는 등 피해를 줄 수 있음	▶네트워크는 마이크로 세그멘테이션 되어 관리되므로, 공격자의 횡적 이동이 쉽지 않음 ▶ 데이터 접근은 보안 정책, 사용자 역할, 기기 속성 등에 따라 제한되며, 세밀한 접근제어를 통해 민감한 데이터 접근 불가 ▶사용자 행위에 대한 모니터링을 통해 비정상적인 활동시 추가 인증 요구 혹은 동적인 접근 제한 가능
공급망 침투	▶해당 접속에 대해 신뢰성이 부여되어, 이후 벌어지는 대다수 공격에 대한 대응불가	▶정상적인 기기에 정상적으로 배포된 프로그램이라 해도 일단 신뢰하지 않으므로, 데이터 접근은 최소화. 피해를 최소화할 수 있음 ▶모든 네트워크 연결이 감시, 허가받지 않은 원격접속을 통한 공격 명령/통제 및 데이터 전송 역시 대응 가능

자료: 과기부, 유안타증권 리서치센터

도입 및 발전. 2014~2015년 두 차례에 걸쳐 미국 연방정부의 인사관리처(OPM)에서 대량의 개인정보 유출사고가 발생했다. 미국 역사상 최악의 해킹 사례 중 하나로 알려져 있다. 2,150만명에 달하는 전/현직 직원 및 가족의 개인정보가 유출되었다. 美 하원 감독개혁위원회는 1년 5개월간(2015.4월~2016.9월간)의 조사후 채택한 보고서에서 해킹의 원인과 영향 등을 분석한 후 연방 정부에게 총 13가지 권고안을 제시했다. 2번째 권고안으로 지능적이고 지속적인 공격에 대응하기 위해 연방정부의 정보보안 및 IT아키텍처를 제로트로스트 모델로 이행할 것을 촉구했다.

18년 연방CIO위원회에서는 연방정부차원에서 제로트러스트 도입을 논의하기 위해 Zero Trust/SDN Steering Group을 설립했다. 19년 제로트러스트 아키텍처 프로젝트를 시작, 논리적 보안 모델 및 구현 방안에 대한 연구를 수행했다.

[그림 27] 美 연방정부의 인사관리처 개인정보 유출사고 해킹 방법



자료: H. Saleem et al, 유안타증권 리서치센터

[그림 28] 참고자료: 美 연방정부의 제로트러스트 관련 진행사항

시기	기관	미 연방정부 진행 사항
2019.04	ACT-IAC	제로트러스트 사이버 보안 동향 소개
2020.08	NIST	제로트러스트 아키텍처(SP 800-207) 발간
2021.02	DISA/NSA	국방부 제로트러스트 참조 아키텍처 버전 1.0 발간
2021.02	NSA	제로트러스트 보안 모델 수용 지침 발간
2021.05	바이든 대통령	'국가 사이버 보안 개선을 위한 행정 명령 (EO-14028)' 발표
2021.06	CISA	제로트러스트 성숙도 모델 (Pre-decisional Draft) 발간
2021.06	GSA	제로트러스트 아키텍처 – 구매자 가이드 발간
2021.07	NIST	행정 명령(EO-14028) 관련 주요 소프트웨어에 대한 보안성 관련 지침 발표
2022.01	바이든 대통령	'국가 안보, 국방부 및 정보 공동체 시스템의 사이버 보안 개선에 관한 각서 (NSM-08)' 발표
2022.01	OMB	'제로트러스트 사이버 보안 원칙을 향한 미 연방 정부 전략에 관한 각서' 발표
2022.02	NSTAC	'제로트러스트 및 신뢰할 수 있는 ID 관리' 대통령 보고서 발표
2022.03	CISA	엔터프라이즈 모빌리티에 제로트러스트 원칙 적용 (Draft for Public Comment) 발간
2022.05	NIST	제로트러스트 아키텍처 계획: 연방 관리자를 위한 계획수립 지침 (CSWP 20) 발간
2022.06	법무부	제로트러스트 도입을 포함하는 '2022-2024 회계년도를 위한 미국 법무부 정보기술 전략 계획' 발표
2022.07	DISA/NSA	국방부 제로트러스트 참조 아키텍처 버전 2.0 발표
2022.06~08	NIST	제로트러스트 아키텍처 구현 (SP 1800-35A~D, Preliminary Draft) 발간
2022.11	DoD	국방부 제로트러스트 전략, 기능 실행 로드맵 발표
2022.12	NIST	제로트러스트 아키텍처 구현 (SP 1800-35A~E, 2nd Preliminary Draft) 발간
2023.04	NSA	사용자 핵심요소를 통한 제로트러스트 성숙도 개선
2023.04	CISA	제로트러스트 성숙도 모델 2.0 발간

자료: H. Saleem et al, 유안타증권 리서치센터

제로트러스트 아키텍처란 제로트러스트의 개념을 활용하여 기업 내부의 네트워크, 시스템 및 리소스를 보호할 수 있는 추상적인 보안 구조이며, 해당 목적을 달성하기 위한 기업망의 구성 요소 간 인터페이스 정의와 인증, 접근제어, 보안 모니터링 및 가시화 등 보안 정책을 포함한다.

제로트러스트의 6가지 기본 원리는 다음과 같다. ①기본원칙. 모든 종류의 접근에 대해 신뢰하지 않을 것(명시적인 신뢰 확인 후 리소스 접근 허용). ② 일관되고 중앙 집중적인 정책 관리 및 접근제어 결정. ③ 사용자, 기기에 대한 관리 및 강력한 인증. ④리소스 분류 및 관리를 통한 세밀한 접근제어(최소 권한 부여). ⑤논리 경계 생성 및 세션 단위 접근 허용, 통신보호 기술 적용. ⑥모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증 및 제어다.

제로트러스트 아키텍처 접근 방법은 3가지 추상적인 요소(①인증체계 강화, ②마이크로 세그멘테이션, ③네트워크 인프라 및 소프트웨어 정의 경계)로 분류된다.

제로트러스트 도입을 위한 기업망의 6가지 핵심 요소는 ①식별자/신원(Identity)이다. 기업망에 접근하는 사용자는 기업에서 관리하는 식별정보를 이용하여 업무에 활용하는 응용에 접근한다. 피싱 등 다양한 공격에 강한 다중 인증(MFA, Multi-Factor Authentication) 기법을 도입하여 더욱 정교한 온라인 공격으로부터 사용자를 보호할 수 있어야 한다. 다중 인증 기술이 필요한 이유는 기존 인증방식의 취약점이 존재하기 때문이다. 패스워드 기반인증에 생체 혹은 OTP 기반의 인증방식을 추가로 활용함으로써 어느정도 극복이 가능하다.

②기기 및 엔드포인트(Device/Endpoint)이다. 기업은 업무용으로 인가되어 동작하는 모든 기기 목록을 관리, 해당 장치에서 발생하는 사고를 예방, 감지 및 대응가능해야 한다. 전략으로는 자산 목록화와 전사적 기기 탐지 및 대응(EDR)솔루션의 전사적 도입 등이 있다.

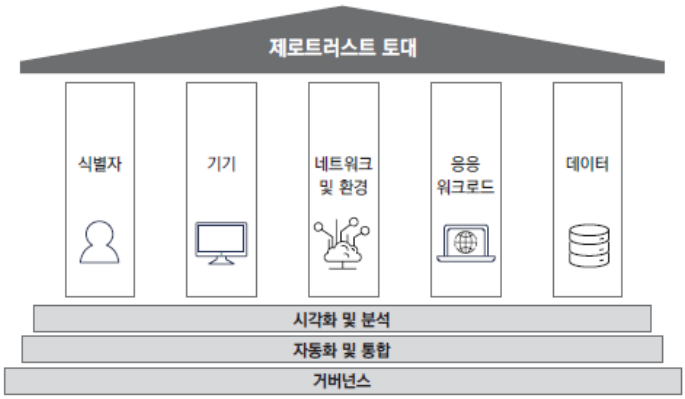
③네트워크(Network). 기업망 내에서 DNS, HTTP 트래픽을 암호화하며, 보안 경계를 격리된 환경으로 분할하는 계획이 필요하다.

④시스템(System). 기업이 보유하고 있는 서버 시스템에 대해 권한 사용자 레벨로 접속하는 경우 서버 시스템의 주요 파일 접근제어, 주요 사용 명령어 통제, 영역별 접근제어 등이 통제되고 관리됨으로써 외부 해커의 주요 서버 시스템 공격에 대해 대비해야 한다. 시스템 관리자 인증은 단순 ID 및 패스워드가 아닌 PKI, OTP, FIDO 등이 연동가능한 방식으로 지속해야 한다.

⑤응용 및 워크로드(Application & Workload). 기업은 모든 응용들이 인터넷에 연결되어 있다고 간주, 정기적으로 응용 프로그램을 엄격하게 심사, C-TAS와 같은 위부 취약성 보고서를 참고해야 한다.

⑥데이터(Data). 완전한 데이터 분류를 사용하는 보호 기능을 배포하기 위해 명확하고 공유된 경로를 따른다. 기관은 클라우드 보안 서비스 및 도구를 활용하여 민감한 데이터를 검색, 분류, 보호하고 전사적 로깅 및 정보 공유를 구현해야 한다.

[그림 29] 제로트러스트 토대



자료: CISA, 유안타증권 리서치센터

[그림 30] 각 기업/기관에서 정의한 제로트러스트 도입을 위한 기업망의 핵심 요소

Forrester[17]	Microsoft[18]	SAP[19]	DISA/NSA (DoD) [20]	CISA[21]
7가지 핵심 요소 ‣ Data ‣ Networks ‣ People ‣ Workloads ‣ Devices ‣ Visibility and Analytics ‣ Automation and Orchestration	**6가지 핵심 요소** ‣ Identities ‣ Devices ‣ Applications ‣ Data ‣ Infrastructure ‣ Networks	**6가지 핵심 요소** ‣ Identities ‣ Data ‣ Network ‣ Applications ‣ Infrastructure ‣ Endpoints	**7가지 핵심 요소** ‣ User ‣ Device ‣ Network/ Environment ‣ Applications and Workload ‣ Data ‣ Visibility and Analytics ‣ Automation and Orchestration	**5가지 핵심 요소** ‣ Identity ‣ Device ‣ Network/ Environment ‣ Applications Workload ‣ Data **3가지 교차 기능** ‣ Visibility and Analytics ‣ Automation and Orchestration ‣ Governance

자료: 해당기업, 유안타증권 리서치센터

[그림 31] 제로트러스트 아키텍처 도입 운영시 발생할 수 있는 위협 및 완화 방안

위협		내용
제로트러스트 아키텍처 결정 과정 무력화	위협 내용	▸ 정책 엔진의 규칙을 설정할 수 있는 기업 관리자가 승인없이 규칙을 변경하거나 기업 운영에 지장을 주는 실수 ▸ 정책 관리자에 대한 직접적인 침해를 통한 승인되지 않는 접근 허용
	위협 완화 방안	▸ 정책 엔진 및 정책 관리자를 적절하게 설정·모니터링 ▸ 모든 설정 변경을 반드시 기록·감사
DoS 또는 네트워크 장애	위협 내용	▸ 공격자가 정책집행지점, 정책 엔진 또는 정책 관리자에 대한 접근 방해/거부 (서비스 거부 공격 혹은 라우팅 가로채기) ▸ 호스팅 제공자에 의해 정책 엔진 또는 정책 관리자 오프라인 ▸ 알 수 없는 이유로 정책 관리자가 기업 리소스에 연결되지 못함
	위협 완화 방안	▸ 이들 시스템을 적절하게 보호되는 클라우드 환경에서 운영 ▸ 혹은 사이버 내성에 관한 지침에 따라 여러 위치에 복제 (단, 이러한 공격·장애는 기존 VPN에서도 발생할 수 있으며, 원천 봉쇄는 불가능)
인증 수단 도용 및 내부자 위협	위협 내용	▸ 중요한 계정의 인증 수단을 획득하기 위해 피싱, 사회 공학 등의 공격
	위협 완화 방안	▸ 컨텍스트 기반 신뢰도 평가 알고리즘을 통하여, 일반적인 패턴과 다른 리소스 접근 방지
네트워크 가시성	위협 내용	▸ 기업망의 일부 트래픽에 대한 분석의 어려움 (기업 소유가 아닌 접속 자산, 혹은 DPI 수행이 안 되거나 암호화된 트래픽을 조사할 수 없는 경우)
	위협 완화 방안	▸ 내용을 알 수 없더라도 메타데이터(출발지/목적지 IP 주소 등) 등을 활용하여 공격자 혹은 악성 코드 탐지 ▸ 머신러닝 기반 트래픽 분석 등
시스템/ 네트워크 정보 저장소	위협 내용	▸ 모니터링, 네트워크 트래픽, 메타데이터 등 분석용 데이터는 일반적으로 공격자의 타깃이 될 수 있음
	위협 완화 방안	▸ 중요 기업 데이터는 가장 엄격한 접근제어 정책 설정
전용 데이터 규격 또는 솔루션에 대한 의존	위협 내용	▸ 데이터(주체 식별정보, 자산, 위협 인텔리전스 등) 입력 요소들의 전용 데이터 규격 혹은 솔루션 사용으로 인한 상호 운용성 문제 발생 ▸ 혹은 보안 이슈 및 장애로 인한 막대한 교체 비용 및 시간 소요
	위협 완화 방안	▸ 데이터 입력 요소를 도입하기 전, 업체의 보안 통제, 교체 비용, 공급망 위험 관리, 성능, 안전성 등을 종합적으로 고려하여 평가 후 도입
비인간 객체에 의한 제로트러스트 아키텍처 관리	위협 내용	▸ 인공지능 혹은 소프트웨어 기반 에이전트의 인증 문제 ▸ 자동화된 기술이 기업의 보안 상태에 영향을 줄 수 있는 오탐과 미탐 가능성 ▸ 공격자가 비인간 객체 접속을 통해 권한이 없는 태스크를 수행하게 함
	위협 완화 방안	▸ 오탐, 미탐에 대해 정기적인 분석 및 수정·보완 ▸ 비인간 객체의 접근에 대한 모니터링 및 분석

자료: 과기부, 유안타증권 리서치센터

제로트러스트 관련 내용을 주목해야 하는 이유. 과기부와 KISA에서 대내외 환경변화 및 실증사업 결과 등을 반영하여 조직 의사결정자 및 담당자가 실질적으로 활용할 수 있는 가이드라인 2.0을 2024년 12월에 발표했다. 가이드라인 2.0은 성숙도 모델의 추상성을 극복하고 기업의 정보보호 담당자들이 제로트러스트를 실질적으로 적용 및 시행할 수 있도록 명확하고 구체적인 세부역량의 성숙도 수준별 특징을 정의했다. 이를 통해 국내 사업화가 구체화될 것으로 기대된다.

2024년 12월 과기부에서 K-제로트러스트 보안모형을 제시하여 공공 금융 서비스 대상 첫 도입 사례를 발표했다. 과기정통부는 국내 기업/기관들의 제로트러스트 도입을 지원하기 위해 시범사업을 마련하고 4개 연합체를 선정하여 추진하고 있다. 24.6월부터 수요기관별 맞춤형 보안모형 개발부터 신제 환경에서의 시범운영까지 지원하며 제로트러스트 도입/구현 사례를 발굴했다.

미국은 2020년 미국표준기술연구소(NIST)가 제로 트러스트 아키텍처를 발표한 것을 시작으로 연방정부 차원에서 도입을 본격화했다. 바이든 행정부는 2021년 행정명령을 통해 제로트러스트를 명문화했고, 각 연방 정부 주체와 기관을 대상으로 24년까지 관련 모델을 도입하도록 했다.

영국도 빠르게 생태계를 구축하고 있다. 영국은 국가사이버보안센터(NCSC)를 중심으로 2021년 제로트러스트 아키텍처 설계원칙을 제시했다. 일본 또한 2020년 정부 정보시스템에서 제로트러스트를 적용하기 위한 사고방식을 도입하면서 구현을 추진하고 있다. 2022년에는 제로트러스트 아키텍처를 적용하기 위한 정책을 제시한바 있다.

제로트러스트라는 개념이 해외에서 공통적으로 적용되는 개념이라는 것을 알 수 있다. 이는 국내 사업화를 통한 매출은 해외진출을 할 수 있는 교두보 역할을 할 수 있다는 것을 의미한다.

[그림 32] 2024 년 제로트러스트 도입 시범사업 주요 내용

구분	연합체 (수요기관)	주요 특징
공공 분야 (1개)	SGA솔루션즈 컨소시엄 (국가정보자원관리원, 공무원연금공단)	▪ **정부·공공기관 통합 전산센터** 대상 철통 인증(제로트러스트) 적용
민간 분야 (3개)	지니언스 연합체 (야놀자, 에스트래픽)	▪ **해외지사 등 원격접속**이 잦은 환경에서 철통 인증(제로트러스트) 구현
	앰진 연합체 (이브이시스, SK브로드밴드 등 6개사)	▪ 일반 사무환경이 아닌 **외부고객·특수단말 접속**이 많은 환경에 적용
	엠시큐어 연합체 (KB국민은행)	▪ **금융분야** 인터넷 기반 자원공유(클라우드) 업무환경에 철통 인증(제로트러스트)보안모형 구현

자료: 과기부, 유안타증권 리서치센터

[그림 33] 가이드라인 1.0 VS. 가이드라인 2.0

구분	가이드라인 1.0	가이드라인 2.0
제로트러스트 성숙도 모델	▸ **3단계**(기존-향상-최적화) **성숙도 수준** 정의 ▸ **기업망 핵심 요소별 20가지 기능** 정의	▸ '**초기**' 단계를 추가한 **4단계**(기존-초기-향상-최적화) **성숙도 수준** 정의로 **고도화** ▸ **기업망 핵심 요소별 27가지 기능** 정의 및 각 단계별 특징 **구체화** ▸ 기업망 핵심 요소 및 2가지 교차 기능에 대한 **52가지 보안 세부역량 및 각 세부역량의 성숙도 수준별 특징** 정의 ▸ 성숙도 모델에 기반한 **구현 방안 제시**
제로트러스트 도입 절차	▸ 제로트러스트 아키텍처 **도입 고려사항 정리**(성숙도 모델 관점 및 기업 내외부 환경 관점) ▸ **총 5단계의 제로트러스트 아키텍처 도입 단계 제시**(준비 → 계획 → 구현 → 운영 → 피드백 및 개선) ▸ **美OMB 문서를 참고하여 제로트러스트 구현에 따르는 핵심 요소별 초기 전략 제시**	▸ 제로트러스트 아키텍처 **도입 과정에서의 고려사항 구체화**(제로트러스트에 대한 명확한 이해 및 기업 내 인식 제고 등 추가) ▸ **제로트러스트 도입 준비 단계 구체화**(업무 구체적 기술 및 예시 제시) ▸ 제로트러스트 아키텍처 도입을 위한 **조직 구성 및 목표 설정 방안** 제시
기타	▸ **제로트러스트 구현에 관한 6가지 유스케이스** 및 목표·요구사항, 구현 방안 등 제시 ▸ 제로트러스트 도입 후 **보안 수준 평가 방안 부재**	▸ 제로트러스트 **도입 후 기업망 보안 수준을 평가할 수 있는 2가지 방안** 제시(성숙도 기반 도입 수준 분석을 위한 체크리스트, 침투시험 기반 제로트러스트 효과성 분석 방안) ▸ 부록에서 2023년도 **제로트러스트 실증 사례 소개**

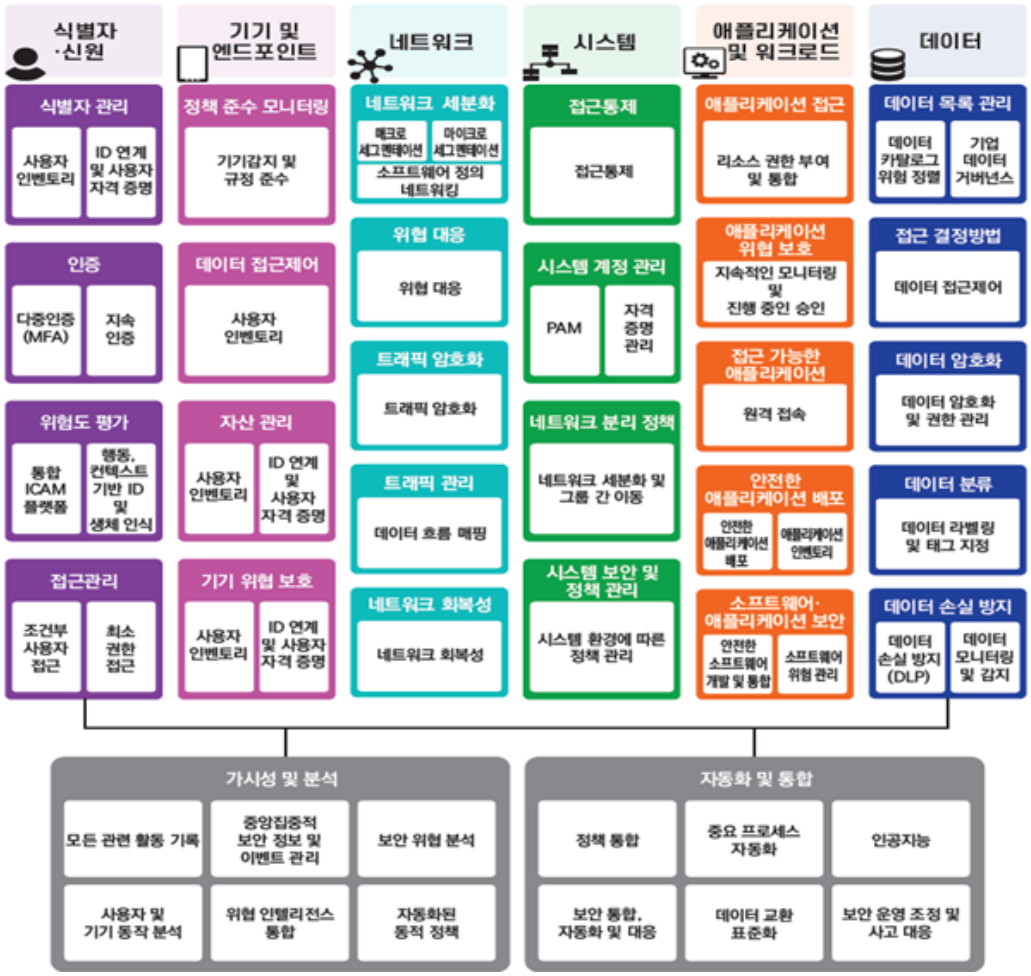
자료: 과기부, 유안타증권 리서치센터

[그림 34] 제로트러스트 성숙도 모델 2.0 요약

	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 · 신원	• 온프레미스ID 사용 • 패스워드 혹은 다중인증 방식 • 수동접근 및 자격증명 관리	• 클라우드와 온프레미스 기반 ID 연계 • 다중인증 및 FIDO 기반인증 • 수동 및 정적 규칙 기반 위험 판단	• 컨텍스트 기반 ID 인증 • 일부 자동화된 및 동적 규칙을 이용한 위험도 평가 • 세션 기반 접근 지원	• 클라우드와 온프레미스 시스템 전반에 걸친 글로벌ID • AI 기반 위험도 결정 및 지속적 보호 • 자동화된 적시·최소 권한 접근 적용
기기 및 엔드포인트	• 제한된 정책준수정보 • 단순하고 수동적 기기 목록 관리 • 수동적위협보호 기능 적용	• 대부분의 기기에 정책 준수 시행 메커니즘 사용 • 모든 기기에 대해 목록화 • 기기 보안솔루션 자동 관리	• 규정 준수 여부에 따른 접근 권한 부여 • 검증된 기기만 데이터 접근 • 자동화, 중앙집중식 위협 보호 및 자산관리 기능 통합	• 지속적인 기기 보안 상태 모니터링 및 검증 • 모든 환경에 걸쳐 자산 및 취약점 관리 통합 • 모든 기기에 대해 위협 보호
네트워크	• 경계분리 네트워크 구조 정의 • 알려진 위협 및 정적 트래픽 필터링 • 매우 중요한 애플리케이션 및 워크로드에 대한 기능 회복	• 소규모 경계를 통해 확장된 네트워크 구조 정의 • 내부 애플리케이션 모든 트래픽 및 외부 일부 트래픽 암호화 • 위험성이 없는 워크로드에 대한 탄력적인 네트워크 회복	• 마이크로 세그먼트를 통해 엔드포인트 및 애플리케이션 격리메커니즘 배포 • 비정상적인 데이터 흐름 격리 및 제거 • 자동화된 위협 인식 기반 동적 네트워크 규칙 생성	• 컨텍스트 기반 및 기계학습 기반 위협 보호 통합 • 암호화 민첩성 • 우선 순위 지정 가능한 동적 네트워크 규칙 생성
시스템	• 로컬 시스템 기반 ID/패스워드 등 단순인증 • 정적 속성 등 최소한의 권한 분리 정책 적용 • 온프레미스 시스템보안 패치 및 정책 수동 변경	• 독립적인 시스템으로 계정 관리 • 일부 중요도에 따르는 네트워크 세분화 • 온프레미스 및 클라우드 시스템에 대한 패치 수준 자동 확인 기능	• 동적 접근 권한 통제 • 등급 및 기능별 네트워크 분류 • 온프레미스 및 클라우드 시스템에 대한 자동화된 보안 패치	• 다중인증 및 신뢰도 기반 접근 인가 • 세분화된 리소스별 접근 정책 적용 • 온프레미스 및 클라우드 상의 모든 시스템 실시간 모니터링 및 자동화된 보안 패치
애플리케이션 및 워크로드	• 로컬 인가 및 정적 속성 기반 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대해 최소한의 통합 • 정적·수동테스트 수행	• 애플리케이션 워크플로우와 위협 보호에 대한 기본적인 통합 • CI/CD 파이프라인 DevSecOps, SBOM 적용 • 동적 테스트 방법 사용	• 확장된 컨텍스트 정보 및 최소권한 원칙의 애플리케이션 접근 • 애플리케이션 워크플로우와 위협 보호에 대한 강력한 통합 • 정기적인·자동화된 테스트	• 실시간 위험 분석을 통해 지속적 애플리케이션 인가 • 모든 애플리케이션에 사용자 및 단말 직접 접근 가능 • 자동화된 코드 배포 및 소프트웨어 검증
데이터	• 정적, 수동 데이터 분류 및 접근제어 • 온프레미스 및 암호화되지 않은 데이터 저장소 • 제한된 임시 데이터 분류	• 일부 자동화된 추적 기반 수동데이터 분류 및 목록화 • 최소한의 권한 요소를 통합한 데이터 접근 • 정적 레이블 및 수동 메커니즘 데이터 분류	• 속성에 기반한 최소 권한 제어기법으로 접근관리 • 저장소의 모든 데이터 암호화 • 레이블 지정 프로세스 계층화 및 데이터 목록화 자동화	• AI를 이용한 지속적인 데이터 분류 및 목록화 자동화 • 적시·최소권한 동적 데이터 접근 • 사용중인 데이터 암호화 및 최신 암호화 적용

자료: 과기부, 유안타증권 리서치센터

[그림 35] 제로트러스트 성숙도 향상을 위한 핵심 기능 및 세부역량



자료: 과기부, 유안타증권 리서치센터

2. 예상되는 2025년 사이버보안위협

삼성SDS는 매년 5대 사이버 보안위협을 발표한다. 2025년 5대 사이버 보안 위협으로는 ①AI 악용피싱에 대비해야..AI보안위협, ②장기 방치 자격 증명 클라우드 보안 위협, ③이중갈취 전략 진화 랜섬웨어 공격, ④오픈소스 악성코드 유입 SW공급망 보안 위협, ⑤초연결사회 독, OT(생산 시스템)/IoT 파고드는 보안위협 등이다.

2024년 5대 사이버 보안 위협으로는 ①AI를 활용한 보안 위협, ②하이브리드 환경에서의 클라우드 보안 위협, ③개인정보, 민간 정보 등의 주요 데이터 유출, ④지속적으로 진화하는 랜섬웨어, ⑤공격 대상 확장에 따른 네트워크 보안 위협 등을 제시했다.

2023년 5대 사이버 보안위협은 다음과 같다. ①랜섬웨어 조직, 양보다 질 전략 추구, ②조직의 핵심 정보를 장기간 유출하는 기생형 공격 대세, ③파급력 높은 잭팟 취약점 발굴과 악용 지속, ④공급망 공격, 모바일 환경으로 확대, ⑤개인의 가상 자산 지갑을 노린 공격 심화 등이다.

안랩에서도 매년 5대 사이버 보안위협을 제시한다. 2025년 5대 사이버 보안 위협 전망으로 ① 공격 표면의 확대-IoT와 클라우드 환경의 위험 증가, ②랜섬웨어 공격의 진화와 다변화, ③크리덴셜 스터핑(Credential Stuffing) 공격의 증가, ④인공지능 및 딥페이크 기술의 악용, ⑤공급망 보안 위협을 제기했다.

2024년에는 ①적대세력 간 사이버 공격 및 핵티비스트 활동 증가, ②RaaS(서비스형 랜섬웨어) 조직의 변화 가속화, ③가상화 플랫폼을 노리는 랜섬웨어 활개, ④금전 및 개인정보를 노린 안드로이드 악성 앱의 확산, ⑤암호화폐 탈취목적 개인 지갑을 노린 공격 심화 등을 제시했다.

2023년은 ①랜섬웨어 조직, 양보다 질 전략추구, ②조직의 핵심 정보를 장기간 유출하는 기생형 공격 대세, ③파급력 높은 잭팟 취약점 발굴과 악용 지속, ④공급망 공격, 모바일 환경으로 확대, ⑤개인의 가상 자산 지갑을 노린 공격 심화를 제기했다.

과기부에서 매년 당해연도의 사이버위협 사례분석과 차기연도 사이버위협 전망에 대해서 분석한 내용은 아래 표에서 확인할 수 있다. 내용은 삼성SDS/안랩과 유사하다.

삼성SDS와 안랩의 2025년 사이버 위협 전망을 통해서 사이버 공격의 종류가 다양해지고 있으며 빠른 변화를 보이고 있다는 것을 알 수 있다. 세부적으로는 클라우드와 관련된 보안, AI를 활용한 공격(랜섬웨어, 딥페이크, 스미싱 등) 등을 대안이 필요한 상황이다.

[표 3] 2024 년 사이버 위협 사례분석 및 2025 년 사이버위협 전망

사이버 위협사례 (2024)	① 사이버 사기(쓰레기 편진, 금융 사기, 큐알사기 등)로 인한 국민 피해
	② SW 공급망 공격 및 복합적인 공격 전술 사용
	③ 금품요구 악성 프로그램(랜섬웨어) 공격기법 고도화
사이버 위협전망 (2025)	① 공격자의 생성형 인공지능 활용 본격화
	② 디지털 융복합 체계에 대한 사이버 위협 증가
	③ 국제 환경 변화에 따른 사이버 위협 증가 가능성
	④ 무차별(분산 서비스 거부) 디도스 공격 증가 예상

자료: 과기부, 유안타증권 리서치센터

[표 4] 2023 년 사이버 위협 사례분석 및 2024 년 사이버위협 전망

사이버 위협사례 (2023)	① 보안프로그램 취약점과 SW 개발자 대상 공급망 공격 확대
	② 개인정보를 노려 진화하는 메신저 사칭 공격과 피해 재확산
	③ 랜섬웨어 공격과 산업 기밀정보 공개를 빌미로 하는 금전 협박
사이버 위협전망 (2024)	① 피해 자체를 모르게 하는 은밀하고 지속적인 SW공급망 공격
	② 생성형 인공지능(AI)를 악용한 사이버 범죄 가능성 증가
	③ OT(Operational Technology)/ICS(Industrial Control System) 및 IoT 환경의 보안 위협 증가
	④ 정치/사회적 이슈를 악용하는 사이버 위협 고조

자료: 과기부, 유안타증권 리서치센터

[표 5] 2022 년 사이버 위협 사례분석 및 2023 년 사이버위협 전망

사이버 위협사례 (2022)	① 국가/사회 혼란을 야기하는 사이버 공격
	② 재택근무, 인터넷기반자원 공유(클라우드) 전환 등 정보기술 환경 변화를 악용한 공격
	③ 디지털 사회를 마비시키는 금품 요구 악성프로그램(랜섬웨어), 분산서비스 거부(디도스) 공격
사이버 위협전망 (2023)	① 국가/산업 보안을 위협하는 국제 해킹 조직의 공격 증가
	② 재난, 장애 등 민감한 사회적 현안을 악용한 사이버 공격 지속
	③ 지능형 지속 공격과 다중 협박으로 무장한 금품요구 악성프로그램의 진화
	④ 디지털 시대 인터넷기반 자원 공유 전환에 따른 위협 증가
	⑤ 갈수록 복잡해지는 기업의 소프트웨어 공급망과 위협 증가

자료: 과기부, 유안타증권 리서치센터

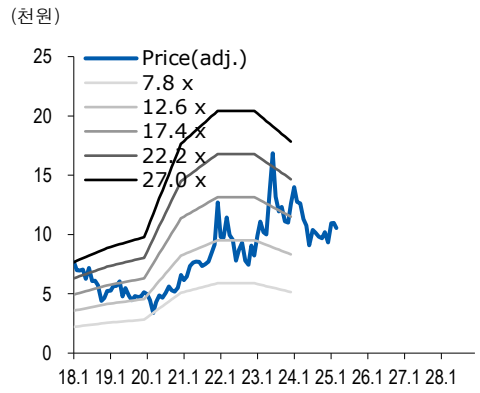
3. 결론

제로트러스트 2.0을 통해 국내 기업들은 새로운 먹거리 확보 및 글로벌 경쟁력을 갖출 수 있는 시기라고 판단된다. 제로트러스트의 주요 수단은 생체인식(FIDO)을 기반한다. 삼성SDS/안랜의 2025년 사이버 위협 전망을 통해서는 클라우드와 관련된 보안, AI를 활용한 공격(랜섬웨어, 딥페이크, 스미싱 등) 등을 주목하고 있다는 것을 알 수 있다.

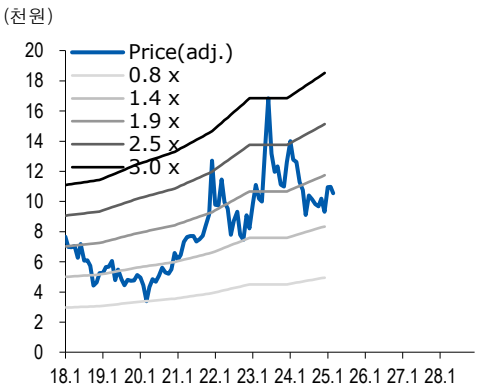
국내 기업들도 이러한 변화를 인지, R&D를 확대하고 있으며, 향후 적극적인 M&A를 진행할 계획을 보유하고 있다. 이런 사항들이 구체화되는 올해 하반기에는 시장에서 주목받을 수 있을 것으로 기대된다. 국내 관련 기업 라온시큐어와 지니언스를 주목한다.

라온시큐어(042510)는 FIDO 생체인식 기술을 보유하고 있으며, 모바일 ID Biz를 국내 뿐 아니라 해외 진출을 모색하고 있다. 지니언스(263860)는 오프레미스와 클라우드 방식을 모두 지원하는 보안 솔루션(NAC, ZTNA)을 보유하고 있으며, 해외시장에서 신규 고객사를 확대하고 있다.

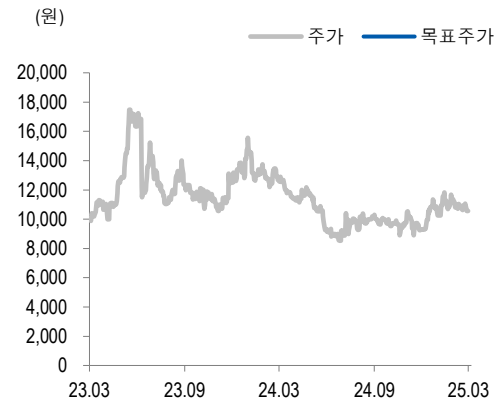
P/E band chart



P/B band chart



지니언스 (263860) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	괴리율	
				평균주가 대비	최고(최저) 주가 대비
2025-03-25	Not Rated	-	1년		
2024-03-28	Not Rated	-	1년		

자료: 유안타증권

주: 괴리율 = (실제주가* - 목표주가) / 목표주가 X 100

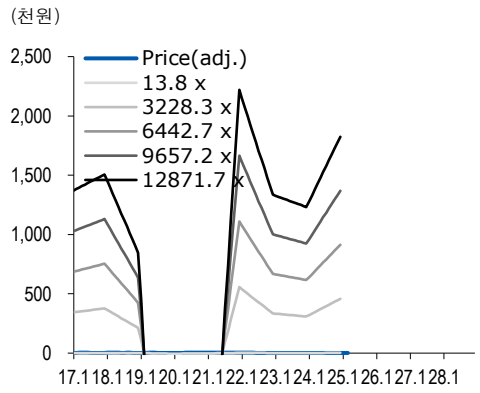
* 1) 목표주가 제시 대상시점까지의 "평균주가"
2) 목표주가 제시 대상시점까지의 "최고(또는 최저) 주가"

구분	투자의견 비율(%)
Strong Buy(매수)	0
Buy(매수)	93
Hold(중립)	7
Sell(비중축소)	0
합계	100.0

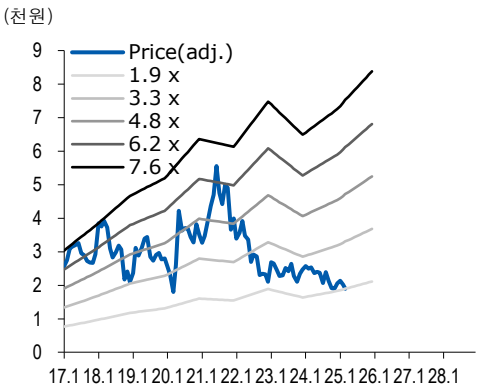
주: 기준일 2025-03-25

※해외 계열회사 등이 작성하거나 공표한 리포트는 투자등급 비율 산정시 제외

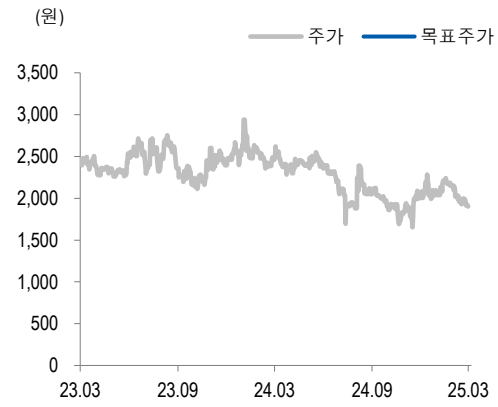
P/E band chart



P/B band chart



라온시큐어 (042510) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	괴리율	
				평균주가 대비	최고(최저) 주가 대비
2025-03-25	Not Rated	-	1년		
2024-09-25	Not Rated	-	1년		

자료: 유안타증권

주: 괴리율 = (실제주가* - 목표주가) / 목표주가 X 100

* 1) 목표주가 제시 대상시점까지의 "평균주가"
2) 목표주가 제시 대상시점까지의 "최고(또는 최저) 주가"

구분	투자의견 비율(%)
Strong Buy(매수)	0
Buy(매수)	93
Hold(중립)	7
Sell(비중축소)	0
합계	100.0

주: 기준일 2025-03-25

※해외 계열회사 등이 작성하거나 공표한 리포트는 투자등급 비율 산정시 제외

Appendix

- 이 자료에 게재된 내용들은 본인의 의견을 정확하게 반영하고 있으며 타인의 부당한 압력이나 간섭 없이 작성되었음을 확인함. (작성자: **권명준**)
- 당사는 자료공표일 현재 동 종목 발행주식을 1%이상 보유하고 있지 않습니다.
- 당사는 자료공표일 현재 해당 기업과 관련하여 특별한 이해관계가 없습니다.
- 당사는 동 자료를 전문투자자 및 제 3자에게 사전 제공한 사실이 없습니다.
- 동 자료의 금융투자분석사와 배우자는 자료공표일 현재 대상법인의 주식관련 금융투자상품 및 권리를 보유하고 있지 않습니다.
- 종목 투자등급 (Guide Line): 투자기간 12개월, 절대수익률 기준 투자등급 4단계(Strong Buy, Buy, Hold, Sell)로 구분한다
- Strong Buy: +30%이상 Buy: 15%이상, Hold: -15% 미만 ~ +15% 미만, Sell: -15%이하로 구분
- 업종 투자등급 Guide Line: 투자기간 12개월, 시가총액 대비 업종 비중 기준의 투자등급 3단계(Overweight, Neutral, Underweight)로 구분
- 2014년 2월21일부터 당사 투자등급이 기존 3단계 + 2단계에서 4단계로 변경