스몰캡

권명준 스몰캡
myoungchun.kwon@yuantakorea.com
서석준 Research Assistant
seokjun.seo@yuantakorea.com

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

정보유출 예방위해 사이버 보안투자 必

개인정보 유출 과징금 매출 10% 국회 통과

지난 2월 12일, 개인정보보호법 개정안이 의결되었다. 국무회의 의결을 거쳐 공표되면 6개월 후부터 적용 및 시행된다. 개정안 제64조에는 ▶고의 또는 중대한 과실로 과징금 처분을 받은지 3년이 지나기 전에 법 위법을 한 경우, ▶고의 또는 중대한 과실로 위반행위를 해 1,000만명 이상 대규모 피해가 발생한 경우, ▶시정조치 명령을 따르지 않아 유출이 발생한 행위에 대해 전체 매출액의 10% 범위 내에서 과징금을 부과할 수 있도록 하는 조항이 추가되었다. 단, 개인정보 보호를 위해 예산/인력/설비/장치 등을 투자하고 운영하는 등 사유가 있는 경우에는 과징금을 감경하되, 고의 또는 중대한 과실로 인한 위반행위에는 적용치 않도록 했다. 사이버 보안에 대한 투자가 연내 즉각적으로 진행될 것으로 예상된다.

위 내용을 통해 개인정보보호 관련 규제가 강화되었다는 것을 알 수 있으며, 이에 대응하기 위해 기업들은 예산/인력/설비/장치 투입을 통해 정보보호에 대한 대응 및 과징금을 감경하려는 노력이 이행될 것으로 예상된다.

제2차 정보보호 종합대책

아래 내용을 통해 기업들의 적극적인 투자를 유도하며, AI에 기반한 예방 및 신속한 취약점 파악이 기본적으로 수반되어야 한다. 이에 관련 기업으로 지니언스(263860), 라온시큐어(042510) 등이 있다.

정보보호 환경은 급변하는데 반해 관련 제도는 정체, 관행은 지속되어 중요 해킹사고가 통신/금융/공공 등 전방위적으로 발생하고 있다는 점이 제2차 정보보호 종합대책 추진 배경이다. 특히 침해사고는 AI를 활용한 해킹 기술의 발달 등으로 지속적으로 증가될 것으로 전망하고 있다. 1차 정보보호 대책을 24.10.22일 제시했으며, 지난 25.1.28일 제2차 정보보호 종합대책을 공개했다. 주요 추진 과제는 다음과 같다.

소비자 보호 및 투자유도. 소비자 피해에 대한 손해배상을 강화하고 기업의 적극적인 보안투자를 유인한다. 이용자 보호를 위해 침해사고로 인한 개인정보 유출 이외의 소비자 피해에 대해서도 분쟁 조정 제도를 도입(정보통신망법 개정)할 예정이며, 개인정보 유출 가능성이 있는 경우 통지 의무화, 통지항목을 추가할 예정이다. 투자 확대를 위해서는 개인정보 보호법상 안전조치 의무 수준을 뛰어넘는 개인정보보호에 대한 과징금을 경감할 계획이다.

대응강화. 진화하는 해킹에 대응하여 AI기반 예방 및 대응시스템으로 전환과 신속한 취약점 파악으로 선제적 대응한다. 이를 위해 ①사이버 공격 전 과정에 AI를 도입하여 대응, 국가/공공기관/민간의 취약점 분석/관리 및 재발방지 대책 수립 등을 AI로 효율화한다. ②AI분야별 보안 모델 개발 및 AI 레드팀 본격 운영을 통한 AI 취약점 점검 수행, ③데이터를 보호하면서 활용성을 높이는 암호화 기술개발 및 상용화를 추진하고, 민/관이 중요 데이터를 암호화하도록 인증기준(ISMS) 등 개정, ④개인정보 거래/확산 우려에 대응하여 개인정보 불법유통 처벌 근거를 신설하고, 다크웹 모니터링을 확대, ⑤민/관이 자율적으로 취약점 신고/조치/공개 제도를 도입 및 확대할 수 있도록 가이드라인 마련 및 인센티브를 강화한다.

보안 내재화. 디지털 제품 보안 등 국민 일상과 역량이 부족한 중소기업에 정보보호 내재화를 추진한다. 국민 사생활 밀접 제품과 유통/플랫폼에 대해 개인정보 관리 등 실태점검을 강화하고, 정보보호 실천 홍보를 강화한다. 중소기업 스스로 보안환경을 점검/개선할 수 있는 훈련 플랫폼을 확대, 영세/중소기업 대상 정보보호 지원사업을 확대한다. 산업/사회의 디지털/AI 융합에 따라 디지털 요소를 포함한 모든 일반제품에 대한 보안정책을 마련한다.

[표 1] 제 2 차 정보보호 종합대책(안) 추진일정

주요과제	일정	소관
1. 기업 책임을 명확히 하고, 기업의 정보보호 투자 유도		
▶개인정보 외 침해사고 피해에 대해서도 분쟁조정 제도 도입	1H26	과기부
▶개인정보 유출 우려시에도 통지 의무 부과, 손해배상 등 안내 사항 강화	26 년	개보위
▶개인정보 보호 투자 노력에 따른 과징금 경감	26 년	개보위
2. 진화하는 해킹에 대한 대응 역량 강화		
▶민간/공공 사이버 위협 탐지/대응시스템 AI 기반으로 전환	26 년~	과기부, 국정원 등
▶AI 모델/서비스의 보안성 강화	26 년	과기부, 국정원 등
▶중요 데이터 암호화 관련 규정/인증기준 개정	26 년~	과기부, 국정원
▶주요 암호화 기술개발 투자 강화 및 사용화 촉진 지원	26 년~	과기부, 국정원 등
▶다크웹 모니터링 확대 및 상시적 취약점 점검 제도화	26 년	개보위, 과기부, 국정원
▶개인정보 불법유통 처벌 근거 신설	26 년~	개보위
▶화이트 해커를 통한 취약점 신고/조치/공개 제도 기반 조성	26 년	과기부, 국정원
▶민/간 사이버 위협정보 공유시스템을 통한 신속정보 공유 추진	26 년~	과기부, 국정원
▶정부의 침해사고 조사역량 강화	26 년	과기부
3. 정보보호가 내재화된 사회		
▶국민 사생활 밀접 제품 대상 보안 실태점검 강화	26 년~	과기부, 개보위
▶온라인플랫폼에 안전하고, 간편한 인증수단 적용	26 년~	개보위, 금융위
▶정보보호 실천 캠페인 및 홍보 강화	26 년~	과기부, 국정원, 개보위
▶영세/중소기업 대상 정보보호 지원사업 확대	26 년~	과기부, 개보위
▶중소기업 자율적 보안 환경 점검/개선 지원	26 년~	과기부, 개보위
▶중소기업 개인정보 유출 예방을 위한 기술지원 서비스 제공	26 년~	개보위
▶디지털 요소를 포함한 일반 제품에 대한 보안정책 마련	26 년	과기부
▶중소기업 제품/서비스의 SW 명세서 관리체계 구축 지원 강화	26 년~	과기부

자료: 관계부처 합동, 유안타증권 리서치센터

[Appendix] 제1차 정보보호 종합대책

10.22일 과기부와 관계부처는 전방위적 해킹사고로 국민 불안이 가속화되는 현 상황을 신속히 극복하고 국가전반의 정보보호 역량을 강화하기 위해 범부처 정보보호 종합대책을 수립하여 발표했다. 이후 중장기 관계를 망라하는 [국가 사이버안보 전략]을 연내 수립할 계획이다. 세부 내용과 관련기업을 제시한다.

1. 핵심IT 시스템에 대한 대대적 점검과 상시 취약점 탐지 체계 구축

주요 내용은 다음과 같다. 해킹에 대한 불안감 해소를 위해 공공·금융·통신 등 국민 대다수가 이용하는 1,600여개 IT 시스템들에 대해 대대적인 **보안 취약점 점검**을 즉시 추진한다. 통신사의 경우 실제 해킹 방식의 강도 높은 불시 점검을 추진, IT 자산에 대한 식별 및 관리체계를 구축한다. **펨토셀(**소형기지국)은 안정성이 확인되지 않을 경우 즉시 폐기할 계획이다. 보안 인증제도를 현장심사 중심으로 전환한다. **모의해킹** 훈련과 화이트해커를 활용한 상시 취약점 점검 체계도 구축한다.

보안 취약점 점검. 보안 취약점과 관련하여 NAC가 활용될 것으로 예상된다. NAC(Network Access Control)은 네트워크에 연결되는 모든 단말기와 사용자의 인증, 보안상태, 접근권한을 실시간으로 점검 및 제어하며, 비인가 장치와 보안 위협을 차단하는 네트워크 보안 솔루션이다.

펨토셀. 안정성이 확인되지 않은 펨토셀이 확인되면 교체작업이 예상된다. 펨토셀(소형기지국)은 대형기지국보다 훨씬 작은 범위에서 통신 신호를 제공하는 중계장비이다. 통신세대 진화시 높은 주파수 대역이 필요하다. 높은 주파수 대역은 도달거리가 짧기 때문에 스몰셀 등의 장치가 필요하다. 최근 KT의 펨토셀이 불법 장비에 의해 통신망에 접속, 악용되어, 일부 가입자 대상으로 무단 소액결제 등 금융피해가 발생한 사고가 발생되었다. 이로 인해 펨토셀에 대한 안정성 확인 필요성이 확대되고 있다.

모의해킹. 실제 공격자 관점에서 시스템·네트워크·애플리케이션의 취약점검을 찾아내고, 그 취약점으로 실체 침투까지 시연해 위험도를 평가 및 개선방안을 제공하는 보안점검이다. 모의해킹과 관련하여 라온시큐어(042510)가 대표적이다. 20여명의 화이트해커를 보유하고 있다. 이를 기반으로 공공·금융기관·민간기업을 대상으로 실제와 동일한 방식의 프리미엄 모의해킹을 진행하는 기업이기 때문이다.

2. 소비자 중심의 사고 대응체계 구축 및 재발방지 대책 실효성 강화

기업의 보안해태(懈怠, 행동이 느리고 움직이거나 일하기를 싫어하는 태도나 버릇)로 인한 해킹 발생시 소비자 중심의 피해구제 체계를 구축한다. 해킹의 정황이 확보될 경우, 기업의 신고 없이도 정부가 신속히 현장 조사할 수 있도록 정부의 조사권한을 확대한다. 보안 의무 위반에 대해서는 과태료 상향, 이행강제금 및 징벌적 과징금 도입 등 제재를 강화하다.

3-1. 정보호호 투자확대 유도 및 중소기업 지원 강화

공공부터 정보보호 역량 강화 솔선수범 위해 공공의 정보보호 예산, 인력을 일정수준 이상으로 확보(1Q26), 위기 상황 대응역량 강화 훈련을 고도화한다. 민간의 경우 필수 투자로 전환할 수 있도록 정보보호 공시 의무 기업을 상장사 전체로 확대, 공시 결과를 토대로 보안역량 수준을 등급화하여 공개하는 제도를 도입한다. CEO의 보안책임 원칙을 명문화하고, 보안최고책임자의 권한을 대폭 강화하며, 자체 역량이 부족한 중소·영세기업 대상으로는 정보보호 지원센터 확대 등을 통해 지원한다.

3-2. 글로벌 변환에 부합하는 제도 마련 및 환경 조성

글로벌 변화에 부합하는 보안환경을 조성하기 위해, 금융 · 공공기관 등이 소비자에게 설치를 강요하는 보안SW를 단계적으로 제한(26년~)하는 대신 다중인증, AI기반 이상 탐지 시스템 등의 활용을 통해 보안을 강화한다. 획일적인 물리적 망분리를 데이터 보안 중심으로 본격전환(26년~)하고, 클라우드 보안 요건 개선 등 민간 사업자의 공공진출 요건 완화를 추진한다.

ZT. 글로벌 사이버 보안의 트렌드이며 데이터 보안과 클라우드 보안 요건 개선과 관련된 사항이 ZT(Zero Trust)이다. ZT는 기업망 내 · 외부에 언제나 공격자가 존재할 수 있고, 명확한 인증 과정을 거치지 전까지는 모든 사용자, 기기, 네트워크 트래픽을 신뢰하지 않으며, 인증 이후에도 끊임없이 신뢰성을 검증함으로써 기업의 정보 자산을 보호할 수 있는 보안 모델이다.

ZT 핵심 요소에는 Identity, Device/Endpoint 등이 있으며, 다중인증 기법 도입, EDR 솔루션의 전사적 도입 등이 주요사항이다. ①ID/PW를 제외한 가장 활용도가 높은 ID 확인 방법은 생체인증을 활용하는 방법이다. FIDO(Fast Identity Online)은 국제 생체인증 표준 규격으로 사용자가 생체정보(지문, 얼굴 등)나 보안키를 이용하여 안전하게 로그인할 수 있도록 만든 글로벌 인증 표준이다.

②EDR(Endpoint Detection & Response)는 PC · 서버 · 노트북 등 엔드포인트 단말에서 발생하는 이상 행위를 감지 및 탐지하고, 침입에 자동 대응하는 보안솔루션이다. NAC가 접속 단계 이전이라면 EDR은 이미 연결된 단말 내부에서의 공격 탐지 및 대응단계이다.

3-3. 보안산업을 국가전략 산업화하고 사이버안보 인력 · 기술 육성

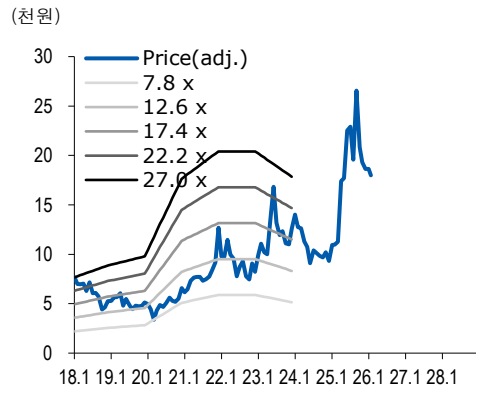
AI 에이전트 보안 플랫폼 등 차세대 보안기업을 집중 육성(연 30개 기업)하고 보안산업의 저변 확대를 위해 정보보호 서비스의 범위를 확대한다. 보안최고 전문가인 화이트해커(연 500여명) 양성 체계를 기업 수요로 재설계하고, 정보보호특성화대학, 융합보안대학원을 5극3특 권역별 성장엔진 산업에 특화된 보안 인재 양성 허브로 기능을 강화(26년~)하는 등 전주기 보안인력 양성을 체계화 · 고도화한다.

양자내성암호 기술 개발 등 국가적 암호체계 전환을 착수, 공공부문에서 자율주행차, 지능형로봇, 드론 등 신기술 모빌리티의 안전한 활용을 위한 보안 체크리스트 및 가이드라인을 수립(26년)한다.

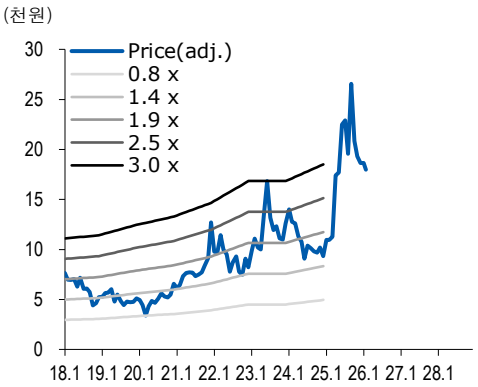
4. 범국가적 사이버보안 협력 강화

부처별로 파편화된 해킹 사고조사 과정을 체계화하여 현장혼선을 최소화하고, 민관군 합동 조직인 국가정보원 산하 국가사이버위기관리단과 정부 부처간의 사이버 위협 예상 · 대응 협력을 강화환다.

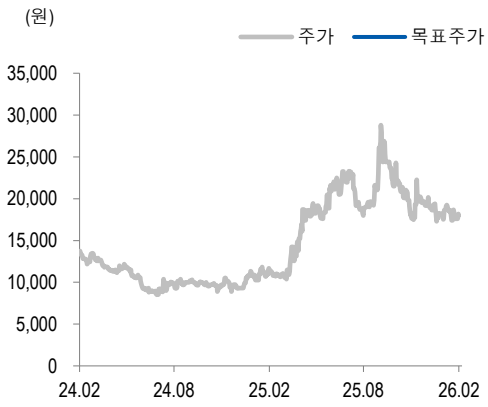
P/E band chart



P/B band chart



지니언스 (263860) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	괴리율	
				평균주가 대비	최고(최저) 주가 대비
2026-02-23	Not Rated	-	1년		
2025-04-23	Not Rated	-	1년		
2025-03-28	담당자변경 1년 경과 이후		1년		
2024-03-28	Not Rated	-	1년		

자료: 유안타증권

주: 괴리율 = (실제주가* - 목표주가) / 목표주가 X 100

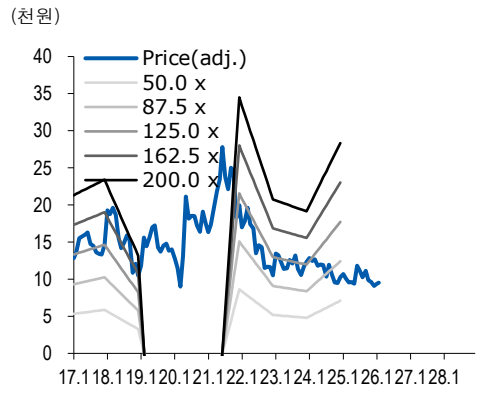
* 1) 목표주가 제시 대상시점까지의 "평균주가"
2) 목표주가 제시 대상시점까지의 "최고(또는 최저) 주가"

구분	투자의견 비율(%)
Strong Buy(매수)	0
Buy(매수)	94.2
Hold(중립)	5.8
Sell(비중축소)	0
합계	100.0

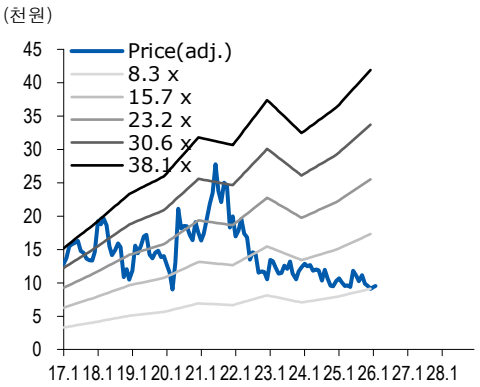
주: 기준일 2026-02-20

※해외 계열회사 등이 작성하거나 공표한 리포트는 투자등급 비율 산정시 제외

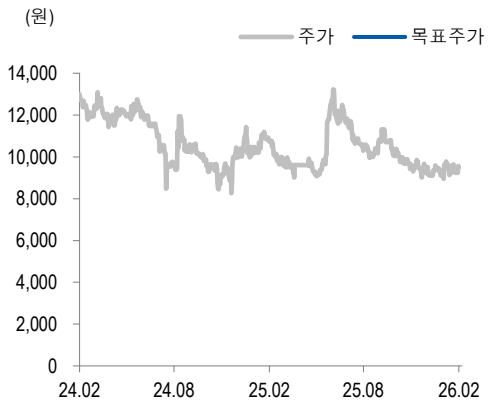
P/E band chart



P/B band chart



라온시큐어 (042510) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	괴리율	
				평균주가 대비	최고(최저) 주가 대비
2026-02-23	Not Rated	-	1년		
2025-09-25	1년 경과 이후		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)	94.2
Hold(중립)	5.8
Sell(비중축소)	0
합계	100.0

주: 기준일 2026-02-20

※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