

스몰캡

SKT 해킹 사태 이후...

과기부

SKT 침해사고와 관련하여 2차례의 조사결과(4/29일, 5/19일)를 발표했다. 1차 조사결과 발표 직후인 5/1일 SKT에 해킹사고 발생에 따른 추가 피해 방지를 위해 보다 강도 높은 해결책 추진을 촉구했다, 5/8일에는 제조업과 에너지, 통신 분야를 비롯해 금융기관과 문화 콘텐츠 분야까지 국내 기업 6천여 곳에 SKT 서버에 발견된 악성 코드 12종이 각 사의 정보통신 설비에 잠복해 있는지 여부에 대한 보안 점검을 당부하면서 사이버 위협 대응 태세 강화를 요청하는 협조 공문을 보냈다. 5/23일 국내기업 및 기관과 보안투자 확대 방안 및 보안 업계 동반성장 방안을 논의하기 위한 간담회를 개최했다.

개인정보보호위원회

국내 주요 공공기관과 기업의 개인정보보호책임자(CPO) 55명을 대상으로 한 설문 결과에 따르면 63%가 개인정보 보호예산이 부족하다고 답변했다. 57%는 최근 3년간 개인정보 예산이 변화없이 일정 수준으로 유지되고 있다고 응답했다. 예산이 확보되기 어려운 이유는 낮은 우선순위(85%), 보안 및 IT 예산과 혼재(83%), 경영진의 낮은 관심(70%) 순서였다.

개인정보 정책포럼(5/21일)을 통해 SKT 해킹 사건을 계기로 전 산업군 조직에 적용할 종합적인 안전관리 대책을 마련할 필요가 있다고 언급했다. 1)즉각적/기술적 조치사항, 2)상시적/전사적 내부통제 강화, 3)정보 주체의 권리구제 실질화 등 크게 3가지 정책 방향을 수립하고 이를 적용하기 위한 과제를 공유했다.

입법조사처

입법조사처의 [이동통신사 해킹 사전 예방을 위한 정보보호 강화 방안]에 따르면 이동통신사는 광범위하고 민감한 개인정보를 보유하고 있어 이동통신사의 해킹사고가 발생할 경우 대규모 개인정보 유출로 이어질 수 있다. 또한, 특정국가나 조직이 이동통신사의 핵심 시스템을 해킹해 통신망을 장악하거나 마비시킬 경우 국가적 사이버 안보 위협으로도 확산될 수 있다. 반복적으로 발생하고 있는 이동통신 해킹 사고를 예방하기 위해 제도적 보안이 필수적이라고 언급했다.

관련기업

과기부, 개인정보보호위원회, 입법조사처 등의 내용을 요약해보면 다음과 같은 요인들을 주목해야 한다고 판단된다. 첫째, 정보보호 관련 예산 확대 및 기업들의 관련 투자 확대이다. 둘째, ZT(Zero Trust) 적용 확대도 예상된다. 셋째, 세부적으로는 개인정보보호위원회에서 제시한 이상행위 탐지 시스템, 취약점 점검, 모의해킹 등을 주목할 필요가 있다고 판단된다. 관련기업으로는 슈프리마(236200), 지니언스(263860), 라온시큐어(042510) 등이 있다.



권명준 스몰캡
myoungchun.kwon@yuantakorea.com

조혜빈 Research Assistant
hevin.cho@yuantakorea.com

종목	투자 의견	목표주가 (원)
지니언스	Not Rated (M)	- (M)
라온시큐어	Not Rated (M)	- (M)
슈프리마	Not Rated (M)	- (M)

SKT 해킹사태 이후 한달

과기부. 과기부는 SKT 침해사고와 관련하여 2차례의 조사결과(4/29일, 5/19일)를 발표했다.

4월 29일. SKT 침해사고 1차 조사결과를 발표했다. SKT가 공격을 받은 정황이 있는 3종, 5대 서버들을 조사, 가입자 전화번호, 가입자식별키(IMSI) 등 유심 복제에 활용될 수 있는 4종과 유심 정보 처리 등에 필요한 SKT관리용 정보 21종을 조사, 악성코드 4종을 발견했다. 단말기 고유식별번호(IMEI) 유출이 없는 것으로 발표했다.

5월 19일. SKT 침해사고 2차 조사결과를 발표했다. 1차 발표 이후 공격을 받은 정황이 있는 서버는 추가로 18대(누적 23대)가 식별되었다. 해당 서버는 통합고객인증 서버와 연동되는 서버들로 고객 인증을 목적으로 호출된 단말기 고유식별번호(IMEI)와 다수의 개인정보(이름, 생년월일, 전화번호, 이메일 등)가 있다. 1차 조사결과와 달리 2차에서는 악성코드가 감염된 서버들에 대한 포렌식 분석 중 연동 서버에 일정기간 임시로 저장되는 파일 안에 단말기 고유식번호(IMEI) 등이 포함되고 있음이 확인되었다. 1차 조사결과 대비 피해가 확산되었다는 것을 알 수 있다.

5월 1일. 1차 조사결과 발표 직후 과기부는 SKT에 해킹사고 발생에 따른 추가 피해 방지를 위해 보다 다음과 같은 강도 높은 해결책 추진을 촉구했다. 1)국민입장에서 쉽게 설명, 정보를 투명하게 공개, 2)유심 교체 물량 부족 문제 해결위해 유심 물량공급이 안정화시까지 서비스 이용자 신규모집 전면 중단, 3)유심보호서비스 일괄 적용 방안의 이행계획 제출, 보상 방안 설명, 4)이용자 피해 보상 방안 마련 및 이행, 5)장애 발생시 즉각적인 상황공유 및 신속한 복구, 6)지원 인력 대폭 확대 등이다.

5월 3일. 과기부는 한국인터넷진흥원에 방문해 사이버 침해 모니터링 및 대응 현황과 통신3사 및 주요 플랫폼 기업의 정보보호 현황을 점검했다.

5월 8일. 제조업과 에너지, 통신 분야를 비롯해 금융기관과 문화 콘텐츠 분야까지 국내 기업 6천여 곳에 SKT 서버에 발견된 악성 코드 12종이 각 사의 정보통신 설비에 잠복해 있는지 여부에 대한 보안 점검을 당부하면서 사이버 위협 대응 태세 강화를 요청하는 협조 공문을 보냈다.

5월 23일. 2차 조사결과 발표 이후 과기부는 한국인터넷진흥원(KISA) 및 한국정보보호산업협회(KISIA)와 함께 최근 발생한 SKT 침해사고를 계기로 국내기업/기관의 보안투자 확대 방안 및 보안업계의 동반성장 방안을 논의하기 위한 간담회를 개최했다.

향후 보안과 관련된 구체적인 방안들이 제시될 것으로 예상된다.

개인정보보호위원회. 5월 21일 개인정보 정책포럼을 통해 SK텔레콤 해킹 사건을 계기로 전 산업군 조직에 적용할 종합적인 안전관리 대책을 마련할 필요가 있다고 언급했다.

과학기술정보통신이 국내 주요기업 646개사의 정보보호 공시 현황을 분석한 결과 전체 기술 투자 대비 정보보호 투자금액 비중은 평균 6.1%이다. 미국 26%, 독일 24%, 영국 23% 등 글로벌 주요국 대비 절반 수준에도 못 미치는 수치라는 점에서 심각성을 확인할 수 있다.

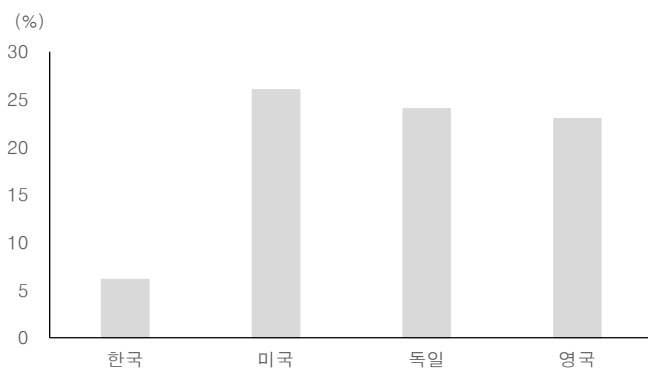
일시적으로 대응하는 사후 조치 위주의 체계로는 반복되는 유출 사고를 막기 어렵다고 진단했다. 대규모 개인정보 처리자를 중심으로 1)즉각적/기술적 조치사항, 2)상시적/전사적 내부통제 강화, 3)정보 주체의 권리구제 실질화 등 크게 3가지 정책 방향을 수립하고 이를 적용하기 위한 과제를 공개했다.

이번 추진 과제에는 공공/민간 등 전 분야를 대상으로 개인정보보호 인력과 예산 기준을 구체화하는 내용도 포함되어 있다. 인력기준에 따르면 기업/기관 등 조직은 최소 1명 이상의 전담 직원을 개인정보 보호 업무에 배치해야 하며, 전체 정보기술 인력의 최소 10%는 개인정보 보호 업무를 병행 또는 전담하도록 권고한다.

2027년까지 전체 IT 예산의 최소 10%, 2030년까지는 15%를 개인정보 보호 관련 예산으로 확보하도록 의무화할 방침이다. 해당 예산에는 이상행위 탐지 시스템 구축, 취약점 점검, 모의해킹 등 정보보호를 위한 핵심 보안 활동에 필요한 투자 항목이 포함된다.

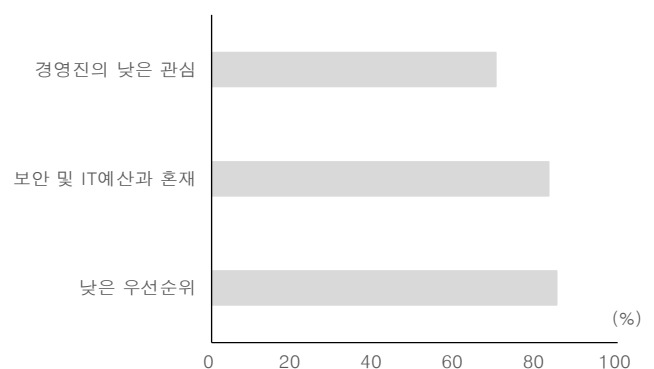
국내 주요 공공기관과 기업의 개인정보보호책임자(CPO) 55명을 대상으로 한 설문 결과에 따르면 63%가 개인정보 보호예산이 부족하다고 답변했다. 57%는 최근 3년간 개인정보 예산이 변화 없이 일정 수준으로 유지되고 있다고 응답했다. 예산이 확보되기 어려운 이유는 낮은 우선순위(85%), 보안 및 IT 예산과 혼재(83%), 경영진의 낮은 관심(70%) 순서였다. 예산이 필요한 영역은 인력확충(90%), 개인정보 처리시스템에 대한 기술적 보호조치(81%) 등의 순이었다.

[그림 1] 국가별 전체 기술 투자 대비 정보보호 투자금액 비중



자료: 과학기술정보통신, 유안타증권 리서치센터

[그림 2] 국내 개인정보 보호예산이 확보되기 어려운 이유



자료: 개인정보위, 유안타증권 리서치센터

입법조사처. 5월 21일 발간한 [이동통신사 해킹 사전 예방을 위한 정보보호 강화 방안]에 따르면 반복되는 이동통신사 대상 사이버 공격을 예방하기 위해 정보보호 체계를 개선할 필요가 있다고 지적했다.

국내 통신사는 모두 해킹사고를 경험했다. 2025년 4월 18일 SKT 홈가입자서버가 해킹된 정황이 발견되었다. 이번 사고는 유심 복제에 활용될 수 있는 주요 정부를 관리하는 중앙서버가 해킹되었다. KT는 2012년 영업시스템이 뚫리며 약 870만명의 이름/주민등록번호/사용 요금제 등 가입자 정보가 유출되었고, 2014년에는 홈페이지 취약점을 통한 해킹으로 약 1,200만명의 이름/주민번호/계좌번호 등이 외부로 유출되었다. 2018년 LGU+ 고객인증시스템에서는 약 30만명의 이름/전화번호/주소/유심 정보 등이 유출, 이는 불법거래 사이트에서 2023년에 발견되었다.

이동통신사는 광범위하고 민감한 개인정보를 보유하고 있다. 이에 이동통신사의 해킹사고가 발생될 경우 대규모 개인정보 유출로 이어질 수 있다. 특정국가나 조직이 이동통신사의 핵심 시스템을 해킹해 통신망을 장악하거나 마비시킬 경우 국가적 사이버 안보 위협으로도 확산될 수 있다. 반복적으로 발생하고 있는 이동통신 해킹 사고를 예방하기 위해 제도적 보안이 필수적이다.

향후 개선 과제로 3가지를 제시하였다. 1)정보보호 투자 확대이다. 이동통신사의 정보보호 투자 확대를 유도하기 위해 정보통신방법을 개정, 정보보호예산이 정부기술 부문 예산의 일정비율 이상이 되도록 노력할 의무를 명시하는 방안이다. 2025년 2월 정보보호 예산 투자 비율을 삭제하고 금융회사 또는 전자금융업자가 정보기술 및 정보보호 분야별 전문이력과 충분한 예산을 확보하도록 하는 방식으로 개정되었다. 한계점이 드러났다는 점에서 정보보호 예산의 최소 투자비율 명시가 필요하다.

2)인증제도 실효성 제고이다. 이를 위해서는 첫째, 이동통신 등 보안 관련 고위험 산업군에 대해 강화된 인증 기준을 적용하는 방안 고려이다. 둘째, 인증 취득 기업의 중대한 위법행위에 인한 해킹사고 발생시 인증 취소 등 엄중한 제재가 이뤄질 수 있도록 조치할 필요가 있다. 셋째, 연 1회 이상 서류중심의 사후관리에서 현장심사를 강화하는 등 인증에 대한 관리/감독으로의 개선이다.

3)주요정보통신기반시설 지정 확대 및 검토 강화이다. 이번 해킹사건은 국민 개인정보와 통신 안전을 지키는 국가적 기반시설임에도 불구하고 정보통신기반 보호법 상 주요정보통신 기반시설로 지정 받지 못하고 있었다는 지적이 제기되었다. 향후 정부는 이동통신사의 핵심 서버 등이 주요 정보통신기반시설 지정대상에서 누락되지 않도록 주요정보통신기반시설의 지정 범위를 확대하고 지정 절차를 강화할 필요가 있다.

SKT. 5월 23일 유심 해킹 사고 대응과 관련하여 SK그룹은 정보보호특별위원회를 구성해 그룹 사 모두를 대상으로 보안점검을 진행, 다음과 같은 대응을 진행하고 있다고 언급했다.

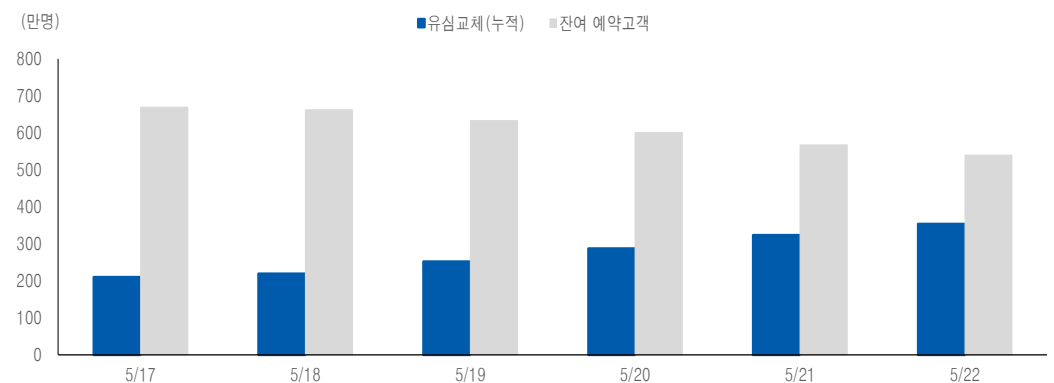
1) 기존 통신장비에 백신을 최대한 설치했다며 백신 설치 범위를 넓히고 있으며, 여기에 EDR이 포함된다고 밝혔다. 통신장비는 민감도가 높아 백신 설치에 어려움이 있어, 망 안정성을 고려해 EDR 설치 등 보안 시스템 강화책을 점진적으로 확대해야 한다는 계획이다.

2) SKT는 복제폰을 악용해 금융을 탈취하는 심스와핑 등 2차 피해를 방지하겠다고 강조했다. 심스와핑(SIM Swapping)은 피해자 휴대전화의 유심 정보를 복제해 피해자의 개인정보 또는 은행이나 가상화폐 계좌를 탈취 금융자산을 훔치는 신종 해킹 수법이다. 비정상인증차단시스템(FDS)으로 불법인증 시도를 차단하는 서비스를 제공하고 있다. FDS는 불법 복제된 유심 인증을 비롯한 다양한 비정상 인증 시도를 통해 통신망에서 실시간 감지 및 차단하는 기술이다.

3) 모의 해킹 등을 추진해 문제점이 발견되면 보안 체계 강화를 위한 투자 확대 등 후속조치를 할 것이다.

유심 교체와 관련해서는 이달 안으로 예약자의 절반의 유심교체를 완료할 계획이다. 5/19~5/22 일을 살펴보면 일간 30만명 이상(31~36만명) 교체가 진행되고 있다. 일 평균 30만명의 교체가 이어진다고 가정해보면 산술적으로 18일 후엔 6월 10일 이전에 교체가 완료될 수 있다.

[그림 3] 유심 교체 현황



자료: SKT, 유안타증권 리서치센터

관련기업

SKT 해킹사건 이후 1개월이 지났다. 단기적으로는 SKT의 고객들의 유심 교체와 관련된 기업들이 주목을 받았다. 지금부터는 과기부, 개인정보보호위원회, 입법조사처 등에 따른 다음과 같은 변화를 관심을 가질 필요가 있다.

첫째, 정보보호 관련 예산 확대 및 기업들의 관련 투자 확대이다. 과기부에서는 국내 기업 6천여 곳에 보안점검 당부 및 사이버 위협 대응 태세 강화 요청을 했다. 과학기술정보통신의 전체 기술 투자 대비 낮은 정보보호 투자금액 비중, 과기부의 국내 기업 6천여 곳에 사이버 위협 대응 태세 강화를 요청 등이 제기되었기 때문이다. 개인정보위원회에서는 SKT 해킹 사건을 계기로 전 산업군 조직에 적용할 종합적인 안전관리 대책 마련이 필요하다고 주장하고 있다. 사이버 보안과 관련된 대상 확대 및 투자금이 확대될 것으로 예상된다.

둘째, ZT(Zero Trust) 확대이다. SKT 해킹사태에서 확인할 수 있듯이 백신으로는 해킹침투를 효율적으로 방어하기 어렵다. 이상 상황에 따른 실효성 있는 감지 및 확산 방지는 지난 보고서 [2025 K-사이버 보안 주목받을 수 있을까?]에 언급한 ZT의 적용확대로 이어질 것으로 기대된다.

셋째, 세부적으로는 개인정보보호위원회에서 제시한 이상행위 탐지 시스템, 취약점 점검, 모의해킹 등을 주목해야 한다.

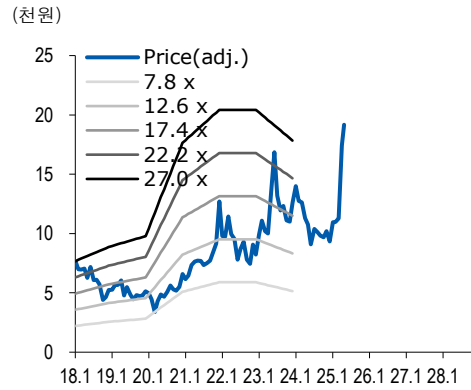
이상행위 탐지와 관련해서는 슈프리마(236200)이 주목받을 수 있다. 슈프리마는 CES2025에서 최고혁신상을 수상한 Q-Vision Pro 제품을 연내 출시할 예정이다. AI얼굴인식 기술과 AI행동분석 기술을 적용한 제품으로 은행 ATM 등에서 현금 일출시 듀얼인증 및 위협감시 분석이 가능하다.

취약점 점검과 관련 지니언스(263860)이 관심받을 수 있다. SKT에서 취약점을 점검을 위해 백신과 EDR설치 등 보안 시스템을 강화할 예정이다. 지니언스는 EDR을 국내 최초 출시했으며, 2024년말 기준 200여 곳에 넘는 국내 고객사를 보유, 국내 1위 사업자이다. 중소기업 시장 확대를 위해 EDR에 보안 및 네트워크 관제 서비스를 추가한 MDR 서비스도 확대되고 있다. 또한 단말기들을 중앙에서 관리 및 통제하는 기술 및 솔루션 NAC도 국내 1위 사업자이다. 이 역시 중소기업으로 영역확대를 위해 Cloud NAC를 출시(2020년)하였다.

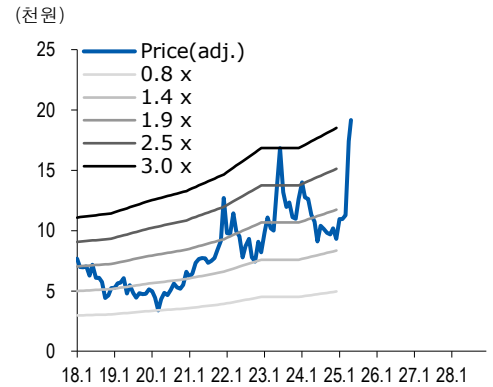
모의해킹과 관련해서는 라온시큐어(042510)이다. 국가 지정 정보보호 전문서비스 기업으로 국내에서 유일하게 기업 대상 프리미엄 모의해킹을 진행하고 있다. 국내외 해킹 관련 대회에서 수상한 다수의 인력을 보유하고 있으며, 민간/공공/금융 등 다양한 고객사를 보유하고 있다. 라온시큐어는 FIDO와 딥페이크 탐지 솔루션도 보유하고 있다.

SKT 해킹사태로 인해 다수의 기업들이 보안의 위협에 대한 심각성을 느꼈을 것으로 예상된다. 하반기에는 다수의 정책들이 제시될 것으로 예상되며, 과거 대비 의무성이 강화될 것으로 기대된다. 올해 하반기에도 국내 보안 기업들에 대한 관심을 이어가야 할 필요가 있다고 판단된다.

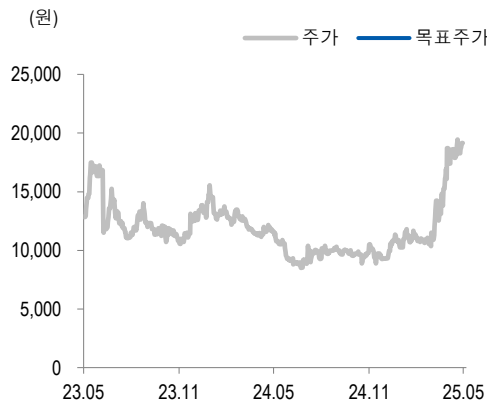
P/E band chart



P/B band chart



지니언스 (263860) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	과리율	
				평균주가 대비	최고(최저) 주가 대비
2025-05-27	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: 과리율 = (실제주가* - 목표주가) / 목표주가 X 100

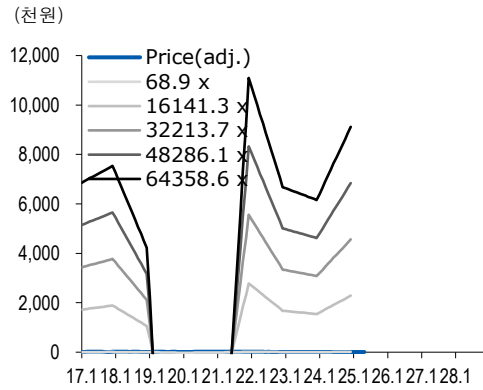
- * 1) 목표주가 제시 대상시점까지의 "평균주가"
- 2) 목표주가 제시 대상시점까지의 "최고(또는 최저) 주가"

구분	투자의견 비율(%)
Strong Buy(매수)	0
Buy(매수)	93.7
Hold(중립)	6.3
Sell(비중축소)	0
합계	100.0

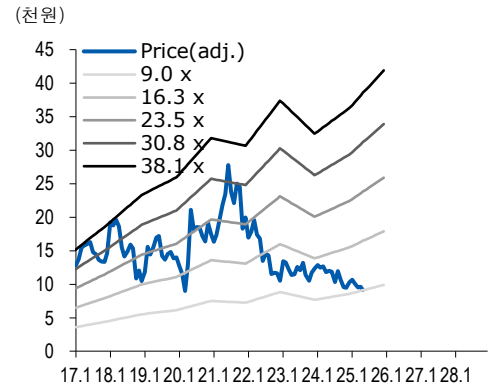
주: 기준일 2025-05-27

※해의 계열회사 등이 작성하거나 공표한 리포트는 투자등급 비율 산정시 제외

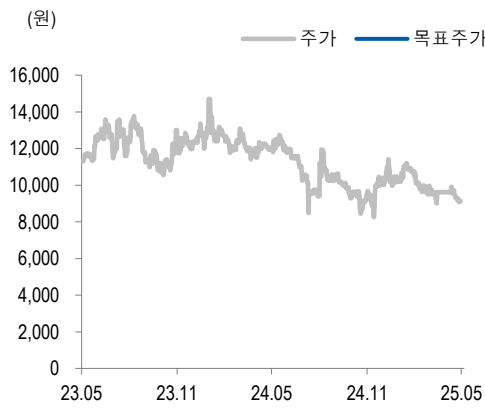
P/E band chart



P/B band chart



라온시큐어 (042510) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	과리율	
				평균주가 대비	최고(최저) 주가 대비
2025-05-27	Not Rated	-	1년		
2024-09-25	Not Rated	-	1년		

자료: 유안타증권

주: 과리율 = (실제주가* - 목표주가) / 목표주가 X 100

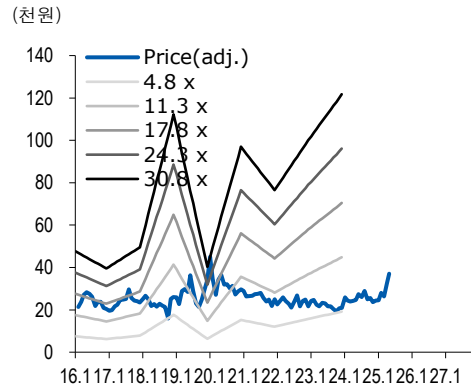
- * 1) 목표주가 제시 대상시점까지의 "평균주가"
- 2) 목표주가 제시 대상시점까지의 "최고(또는 최저) 주가"

구분	투자등급 비율(%)
Strong Buy(매수)	0
Buy(매수)	93.7
Hold(중립)	6.3
Sell(비중축소)	0
합계	100.0

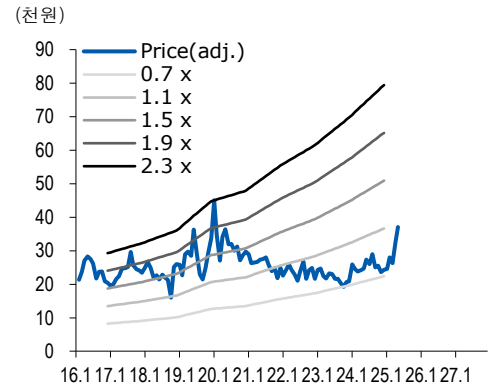
주: 기준일 2025-05-27

※해의 계열회사 등이 작성하거나 공표한 리포트는 투자등급 비율 산정시 제외

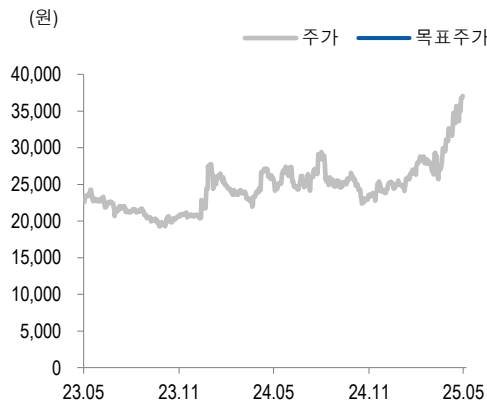
P/E band chart



P/B band chart



슈프리마 (236200) 투자등급 및 목표주가 추이



일자	투자 의견	목표가 (원)	목표가격 대상시점	과리율	
				평균주가 대비	최고(최저) 주가 대비
2025-05-27	Not Rated	-	1년		
2023-08-25	1년 경과 이후		1년		
2022-08-25	Not Rated	-	1년		

자료: 유안타증권

주: 과리율 = (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)	93.7
Hold(중립)	6.3
Sell(비중축소)	0
합계	100.0

주: 기준일 2025-05-27

※해의 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

본 자료는 투자자의 투자를 권유할 목적으로 작성된 것이 아니라, 투자자의 투자판단에 참고가 되는 정보제공을 목적으로 작성된 참고 자료입니다. 본 자료는 금융투자분석사가 신뢰할만 하다고 판단되는 자료와 정보에 의거하여 만들어진 것이지만, 당사와 금융투자분석사가 그 정확성이나 완전성을 보장할 수는 없습니다. 따라서, 본 자료를 참고한 투자자의 투자사결정은 전적으로 투자자 자신의 판단과 책임하에 이루어져야 하며, 당사는 본 자료의 내용에 의거하여 행해진 일체의 투자행위 결과에 대하여 어떠한 책임도 지지 않습니다. 또한, 본 자료는 당사 투자자에게만 제공되는 자료로 당사의 동의 없이 본 자료를 무단으로 복제 전송 인용 배포하는 행위는 법으로 금지되어 있습니다.