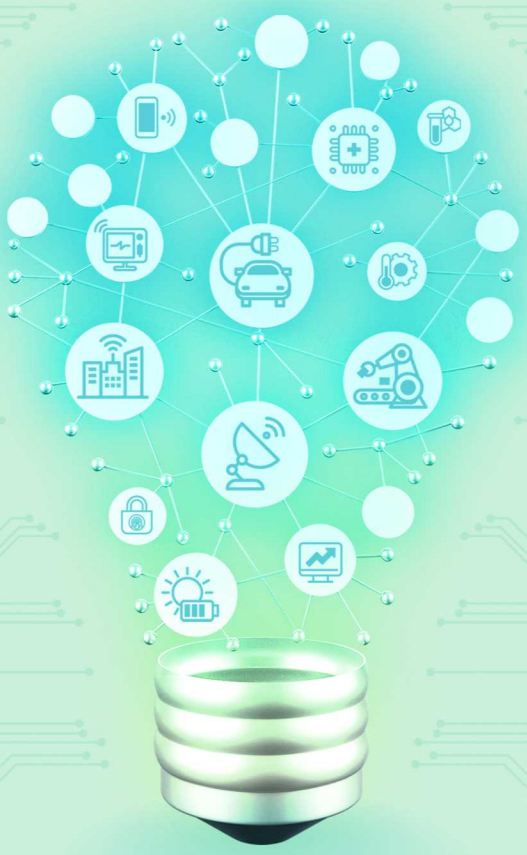
기술 2021-144

2021.03.18.

이 보고서는 코스닥 기업에 대한 투자정보 확충을 위해 발간한 보고서입니다.

기술분석보고서 YouTube 요약 영상 보러가기



에스에스알(275630)

소프트웨어/IT서비스

요 약
기업현황
시장동향
기술분석
재무분석
주요 변동사항 및 전망

작성기관	(주)NICE디앤비	작 성 자	최윤희 선임연구원

■ 본 보고서는 「코스닥 시장 활성화를 통한 자본시장 혁신방안」의 일환으로 코스닥 기업에 대한 투자정보 확충을 위해, 한국거래소와 한국예탁결제원의 후원을 받아 한국IR협의회가 기술신용평가기관에 발주하여 작성한 것입니다.

■ 본 보고서는 투자 의사결정을 위한 참고용으로만 제공되는 것이므로, 투자자 자신의 판단과 책임하에 종목선택이나 투자시기에 대한 최종 결정을 하시기 바랍니다. 따라서 본 보고서를 활용한 어떠한 의사결정에 대해서도 본회와 작성기관은 일체의 책임을 지지 않습니다.

■ 본 보고서의 요약영상은 유튜브로도 시청 가능하며, 영상편집 일정에 따라 현재 시점에서 미게재 상태일 수 있습니다.

■ 카카오톡에서 “한국IR협의회” 채널을 추가하시면 매주 보고서 발간 소식을 안내 받으실 수 있습니다.

■ 본 보고서에 대한 자세한 문의는 작성기관(TEL.02-2122-1300)로 연락하여 주시기 바랍니다.

한국IR협의회

에스에스알(275630)

취약점 진단 선도기업

기업정보(2021/03/11 기준)	
대표자	고필주
설립일자	2010년 08월 27일
상장일자	2018년 08월 06일
기업규모	중소기업
업종분류	시스템 소프트웨어 개발 및 공급업
주요제품	취약점 진단 솔루션 및 컨설팅

시세정보(2021/03/11 기준)	
현재가	5,630원
액면가	500원
시가총액	334억 원
발행주식수	5,930,038주
52주 최고가	7,130원
52주 최저가	2,705원
외국인지분율	2.70%
주요주주	
지란지교시큐리티 외 1인	32.5%

■ 취약점 진단 솔루션 개발 및 정보보호 컨설팅 전문기업

에스에스알(이하, 동사)은 과학기술정보통신부가 지정한 정보보호 전문서비스 기업으로, 공공 및 대기업, 금융, 교육, 의료기관 등을 대상으로 취약점 진단, 정보보호관리체계(Information Security Management System, ISMS) 수립, 개인정보보호 컨설팅, IT 보안솔루션 개발과 구축 등 종합 정보보호 서비스를 제공하고 있다.

■ 인적 자원을 대체하는 취약점 진단 솔루션 개발

동사는 전문가의 숙련도에 따라 평가속도와 결과가 상이한 컨설팅 방식을 대체하는 취약점 진단 솔루션을 개발하여 정보자산에 대한 취약점을 진단하고 있다. 동사의 취약점 진단 솔루션은 전체 정보자산에 대해 자동화 진단이 가능하며 수작업으로 이루어지는 컨설팅 진단 방법 대비 300배 빠른 진단 속도와 정확성을 확보하고 있다.

■ 우호적인 정보보안 시장환경

4차 산업혁명과 함께 ICT 기술이 발전하며 사이버(보안)위협이 급속도로 증가하고 있으며, 위협 대상도 확대되고 있다. 정보보안 시장은 보안강화를 위한 정부의 법·제도 정비, 보안사고 증가로 인한 경각심 고조, 정부 및 기업의 보안 투자 강화 등으로 성장이 지속되고 있다. 올해 1월 과학기술정보통신부는 “2021년, 달라지는 정보보호 제도와 지원 사업”을 발표하며 우호적인 시장환경을 이끌고 있다.

■ 2020년 코로나19로 인한 대면 활동 자제로 매출 감소, 적자전환

2020년 코로나19로 인해 대면 활동이 자제되면서 대면 비중이 높은 보안컨설팅 시장이 축소되어 동사의 매출도 전년 대비 25.9% 급감하였다. 또한, 동사는 협력업체 폐업 등으로 부실채권이 발생하며 영업이익도 적자전환된 것으로 공시(2021.01)하고 있다.

요약 투자지표 (K-IFRS 별도 기준)

구분 / 년	매출액 (억 원)	증감 (%)	영업이익 (억 원)	이익률 (%)	순이익 (억 원)	이익률 (%)	ROE (%)	ROA (%)	부채비율 (%)	EPS (원)	BPS (원)	PER (배)	PBR (배)
2017	113.3	37.3	26.3	23.3	25.2	22.2	43.0	19.6	67.3	661	2,173		0.0
2018	125.5	10.8	11.1	8.8	11.6	9.3	7.2	5.4	18.7	241	4,096	37.3	2.2
2019	136.5	8.8	5.7	4.2	11.2	8.2	4.7	4.0	14.0	194	4,265	31.5	1.4

기업경쟁력

연구개발역량 및 관련 인증 확보

■ 동사만의 방법론을 정립하고, 컨설팅 기획부터 솔루션 개발까지 자체 기술력으로 수행 중

■ CC인증(공통평가기준), GS인증(굿소프트웨어), ISO27001인증, 이노비즈인증 등 보유

■ 특허권 4건, 상표권 24건, 디자인권 1건, 저작권 4건 보유 (국내 2021.2. KIPRIS DB 기준)

긍정적인 정부정책과 시장 상황

■ 2015년 정보보호산업법이 제정된 이후 동사에게 우호적인 정부정책 지속적 발생

■ 사이버보안 위협이 증가하며, 경각심이 고조로 기업과 정부의 투자 강화

핵심기술 및 적용제품

화이트 해커 보유, 정보보호 컨설팅 수행

■ 과학기술정보통신부로부터 정보보호 전문서비스 기업 지정

■ 350건 이상(2018 기준)의 정보보호 컨설팅 레퍼런스 보유

취약점 진단 솔루션 개발 기술 보유

■ 국내·외 법령 및 규칙을 대응할 수 있는 진단항목 내포, 50여 개의 다양한 플랫폼 환경 지원

■ 다수의 정보자산을 동시에 진단할 수 있고, 안정적인 서비스 제공이 가능한 아키텍처 구조 설계

■ 컨설팅(수작업) 진단 방법 대비 300배 빠른 진단 속도

취약점 진단 솔루션 개요

최근 매출실적

■ 2020년 3분기(누적) 사업부문별 비중 (K-IFRS 별도 기준)

사업부문	품목	매출액(억 원)	비중(%)
솔루션	취약점 진단	26.1	47.4
	웹 해킹 방지	3.0	5.4
용역	기술 컨설팅	17.9	32.5
	관리 컨설팅	7.0	12.7
	기타	0.2	0.4
상품		0.5	0.9
기타		0.4	0.7
총 합계		55.1	100.0

시장경쟁력

국내 보안관리 시스템 시장규모

년도	시장규모	성장률
2015년	1,930억 원	연평균 14.2% ▲
2019년	3,278억 원	

국내 보안컨설팅 시장규모

년도	시장규모	성장률
2015년	1,131억 원	연평균 29.8% ▲
2019년	3,215억 원	

사업분야 시장동향 및 특징

■ ICT 기술 발전으로 사이버위협 증가, 보안위협에 대한 경각심 고조

■ 정부 및 기업의 보안 투자 강화와 우호적인 정책속에 지속적인 성장 예상

■ 다만, 정부정책에 많은 영향을 받는 시장이며, 신뢰성 확보를 위한 레퍼런스가 필요한 산업

최근 변동사항

2020년 매출급감 및 적자전환 공시

■ 코로나19로 대면 활동이 많은 보안컨설팅 시장이 축소되면서 매출 급감

■ 협력사들의 폐업으로 부실채권 발생, 적자전환

대표이사 변경

■ 지난해 3월 공동대표(정진석, 윤두식)에서 각자대표(정진석, 고필주)로 한차례 경영체제가 변경되었으며, 같은 해 6월 창업주인 정진석 대표 사임으로 고필주 대표 단독 경영체제로 전환

Ⅰ. 기업현황

취약점 진단 솔루션 개발 및 정보보호 컨설팅 전문기업

동사는 과학기술정보통신부가 지정한 정보보호 전문서비스 기업으로, IT인프라에 대한 정보보호 컨설팅과 취약점 진단 솔루션 개발 및 구축 사업을 영위하고 있다.

■ 회사 개요: 연혁, 주요주주

동사는 2010년 8월 ㈜에스에스알팀으로 설립되었으며, 2012년 2월 현 법인명인 에스에스알로 상호를 변경하였고, 2018년 8월 코스닥 시장에 상장되었다. 동사는 2020년 6월 정진석, 고필주 각자대표이사 체제에서 고필주 대표이사 단독체제로 변경되며, 창업주가 경영에서 물러나게 되었다.

동사의 최대주주는 ㈜지란지교시큐리티(최대주주 지란지교, 41.3% 지분 보유)로 동사 지분의 31.9%를 보유하고 있으며, 이 외 동사 임원인 이항연이 0.6%의 지분을 보유하고 있다.

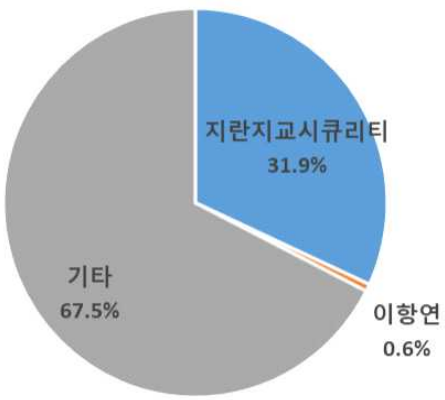
한편, 동사는 2대 주주였던 프리미어성장전략 엠앤에이사모투자합자회사(이하, 프리미어)는 투자금 회수를 목적으로 의무 보호예수 기간 해제 후(2019.2)부터 현재까지 동사의 지분을 지속적으로 매각 중이다. 프리미어는 2020년 3분기까지 동사 지분의 8.1%을 보유하고 있었으나 2021년 1월 추가 매각을 진행하며 현재 3.2%의 주식만을 남긴 상태로, 팍스넷뉴스(2021.1.8.)는 프리미어가 투자자금 엑시트(투자회수)를 위해 남은 잔여 지분에 대해서도 매각할 가능성이 높을 것이라는 견해를 보이고 있다.

[표 1] 동사 연혁

품목	비중
2010.08	㈜에스에스알팀 설립
2012.02	에스에스알로 상호변경
2012.10	솔리드스텝, 메티아이즈 출시
2014.03	현) 정보보호전문서비스기업 선정
2017.07	최대주주 변경(정진석->(주)지란지교시큐리티)
2017.07	공동대표이사 취임(정진석, 윤두식)
2020.03	각자대표이사로 변경(정진석, 고필주)
2020.06	정진석 대표이사 사임, 고필주 대표이사 단독

*출처: 동사 분기보고서(2020.09), NICE디앤비 재구성

[그림 1] 동사 주주현황



*출처: 동사 공시자료(2021.02), NICE디앤비 재구성

■ 주요 사업 및 매출실적

동사는 과학기술정보통신부가 지정한 정보보호 전문서비스 기업으로 공공 및 대기업, 금융, 교육, 의료기관을 대상으로 취약점 진단, 정보보호관리체계 수립, 개인정보보호 컨설팅, IT 보안솔루션 개발과 구축 등 종합 정보보호 서비스를 제공하고 있다.

동사의 주요 보안솔루션 제품으로는 취약점 진단 솔루션인 솔리드스텝(Solidstep)과 웹 해킹 방지 솔루션인 메티아이즈(MetiEye)가 있으며, 정보보호 컨설팅 사업은 IT인프라 취약점 진단과 침투분석, 모의해킹과 같은 기술적 관리 정보를 기반으로 고객 맞춤형 컨설팅 서비스를 제공하는 기술 컨설팅 부문과 ISO27001, ISMS와 같은 주요 정보보호 인증 취득, 정보침해 위협에 대응하기 위한 보안관리 대책을 도출, 설계, 내재화를 지원하는 관리 컨설팅 서비스가 있다.

[그림 2] 동사 사업 영역

*출처: 동사 IR 자료

동사의 매출실적은 취약점 진단과 웹 해킹 방지 솔루션으로 구성된 솔루션 부문과 기술 컨설팅 및 관리 컨설팅, 기타로 구성된 용역 부문, 상품 부문, 기타 부문으로 구성되어 있다. 동사의 매출은 2019년 기준 솔루션 매출이 36.9%, 용역 매출이 38.7%, 상품매출이 24.0%, 기타 0.4%를 차지하고 있다. 솔루션 부문 중 취약점 진단 솔루션은 전체 매출의 34.2%, 솔루션 부문 매출 중에서는 92.8%를 차지하고 있다.

[표 2] 동사 사업별 매출 현황 (K-IFRS 별도기준, 단위: 억 원, %)

매출유형	품목	2020년 3분기(누적)		2019년		2018년	
		매출액	비중	매출액	비중	매출액	비중
솔루션	취약점 진단	26.1	47.4	46.7	34.3	47.8	38.1
	웹 해킹 방지	3.0	5.4	3.6	2.6	3.2	2.5
	소계	**29.1**	**52.8**	**50.3**	**36.9**	**51.0**	**40.6**
용역	기술 컨설팅	17.9	32.5	36.8	27.0	27.0	21.5
	관리 컨설팅	7.0	12.7	11.8	8.6	11.0	8.8
	기타	0.2	0.4	4.2	3.1	0.0	0
	소계	**25.1**	**45.6**	**52.8**	**38.7**	**38.0**	**30.3**
상품		**0.5**	**0.9**	**32.8**	**24.0**	**35.9**	**28.6**
기타		**0.4**	**0.7**	**0.6**	**0.4**	**0.6**	**0.5**
합계		**55.1**	**100.0%**	**136.5**	**100.0%**	**125.5**	**100.0%**

*출처: 동사 분기보고서(2020.09), NICE디앤비 재구성

Ⅱ. 시장 동향

ICT 기술 발전으로 사이버위협이 증가하며 이를 방어할 정보보안 시장도 성장 중

미국의 사이버범죄 피해액은 2015년 이후 3배가 넘게 증가하였으며, 국내에서도 사이버위협으로 인한 피해사례가 증가하고 있다. 사이버위협에 대응하기 위한 정보보안 제품 구입 및 IT인프라에 대한 보안컨설팅이 증가하며 정보보안 시장도 성장 중에 있다.

■ ICT 기술 발전과 함께 사이버위협 증가

유·무선 인프라의 고도화, 스마트기기 보급 확대, 모든 사물이 인터넷으로 연결되는 초연결사회(IoT)가 도래하는 등 ICT 기술 발전과 함께 사이버상의 공격과 범죄가 기하급수적으로 증가할 것으로 전망되고 있다.

사이버공격의 양태는 공격 목적, 대상의 단계, 침입 방법 등에 따라 다양하게 구분되며 해커들이 나날이 지능화·고도화하면서 공격 방법 및 루트가 복잡하고 예측 불가능하게 진화하고 있다. 미연방수사국(FBI)의 내부 범죄 대응 센터(IC3)가 발표한 2019 사이버 범죄 동향 분석 보고서에 따르면, 미국의 사이버범죄로 인한 피해액은 2015년 11억 달러(약 1조 3천억 원)에서 2019년 35억 달러(약 4조 2천억 원)로 3배가 넘게 증가하였으며, 2015년부터 2019년까지 피해자들이 신고한 총 피해액은 102억 달러(약 12조 2천억 원)에 달하는 것으로 조사되었다. 신고건수도 2015년 29만 건에서 2019년 47만 건으로 증가한 것으로 나타나고 있다.

최근 국내에서도 사이버위협이 증가하고 있다. 작년 11월 이랜드가 랜섬웨어 공격을 받으며 자체 서버 셧다운을 진행한 바 있으며, 10월에는 신세계아이앤씨가 디도스 공격을 받아 편의점 택배 서비스가 마비되는 사례가 있었다.

■ 정부정책에 따른 국내 정보보안 시장 우호적 전망

동사의 사업은 정보보호산업 시장 중에서도 컴퓨터 또는 네트워크상 정보 유출, 훼손 등을 방지하기 위한 정보보안(사이버보안) 시장에 포함되며, 정보보안 시장은 크게 정보보안 시스템 개발 및 공급(舊. 정보보안 제품)과 정보보안 관련 서비스 시장으로 구분된다.

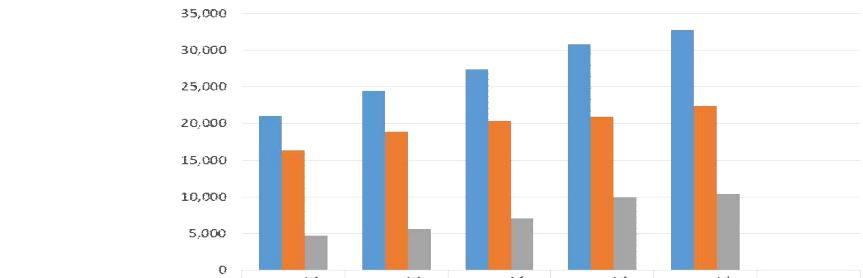
한국정보보호산업협회가 발간한 국내 정보보호산업 실태조사 보고서에 따르면, 전체 정보보안 시장규모는 2015년 2조 1,087억 원에서 2019년 3조 2,777억 원으로 연평균 11.7% 증가한 것으로 조사되었다. 정보보안 시장의 성장은 보안강화를 위한 정부의 법·제도 정비, 보안사고 증가로 인한 경각심 고조, 정부 및 기업의 보안 투자 강화 등에 기인한 것으로 분석되고 있다.

또한, 정보보안 시장의 세부시장인 정보보안 시스템 개발 및 공급 시장은 2019년 2조 2,406억 원 규모를 형성하고 있으며, 2015년 이후 연평균 8.2%씩 증가한 수치이다. 정보보안 관련 서비스 시장은 2015년 4,763억 원에서 2019년 1조 371억 원 규모로 2배 이상 성장(CAGR:21.5%)하였다.

정보보안 시장은 정부정책과 법/규제에 민감한 시장이며, 고객의 정보자산에 직접적으로 영향을 미치는 만큼 제품의 성능과 안정성, 컨설팅 인력에 대한 전문성, 신뢰성 등이 제품 및 컨설팅 업체 선정에 영향을 미친다. 이러한 이유로 다양한 레퍼런스를 확보하고 있는 것이 경쟁력되며, 신규 업체의 시장진입이 쉽지 않은 시장이다.

정부는 2015년 정보보호산업법이 제정된 이후 정보보호산업 확대를 위해 2016년 제1차 정보보호산업 진흥계획(K-ICT 시큐리티2020)을 발표하였으며, 이 계획을 이어가기 위해 2019년에 민간부문 정보보호 종합계획을 발표하였다. 올해도 대상기업과 예산을 확대하는 지원 방안이 추가적으로 게시되는 등 시장상황에 우호적인 정부정책이 지속적으로 발표되고 있다.

[그림 3] 정보보안 시장규모 (단위 : 억 원)



	2015년	2016년	2017년	2018년	2019년	CAGR
정보보안	21,087	24,540	27,449	30,829	32,777	11.7%
정보보안 시스템 개발 및 공급	16,324	18,952	20,357	20,937	22,406	8.2%
정보보안 관련 서비스	4,763	5,588	7,092	9,892	10,371	21.5%

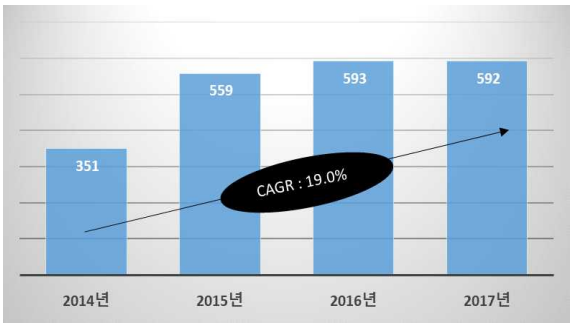
*출처: 한국정보보호산업협회, 국내 정보보호산업 실태조사 보고서(2016-2019), NICE디앤비 재구성

동사는 정보보안 시스템 개발 및 공급 중에서도 보안관리 시스템 제품을 개발하여 판매하고 있으며, 세세분류로는 취약점 분석 시스템에 해당되는 제품(“솔리드스텝”)을 출시하였다.

한국정보보호산업협회의 국내 정보보호산업 실태조사 보고서에 따르면, 국내 보안관리 시스템 시장의 규모는 2015년 기준 1,930억 원에서 연평균 14.2% 증가하여 2019년 3,278억 원 규모를 형성하였으며, 국내 취약점 분석 시스템 시장은 2014년 351억 원 규모에서 연평균 19.0% 증가하며 2017년에는 592억 원의 규모를 형성하고 있는 것으로 확인된다.

한편, 정보보안 시스템 개발 및 공급 분야는 통합보안관리, 취약점 분석, 로그 관리/분석 등의 세세분류 항목들으로 구분되었으나 최근 해당 시스템의 기능들이 통합되거나 분류가 모호하게 사용되며 2018년 이후부터는 세세분류 항목 시장들에 대한 조사가 이루어지지 않고 있다.

[그림 4] 국내 보안관리 시스템(좌) 및 취약점 분석 시스템(우) 시장규모 (단위 : 억 원)



*출처: 한국정보보호산업협회, 국내 정보보호산업 실태조사 보고서(2015-2019), NICE디앤비 재구성

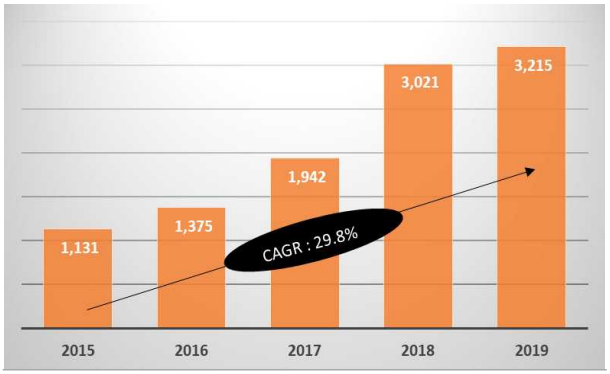
■ 취약점 점검 대상기업 증가로 긍정적인 보안컨설팅 서비스 시장

보안컨설팅 시장은 조직의 목적을 달성하는 데 있어 전산시스템과 네트워크 등 모든 IT 자산과 조직에 일어날 수 있는 위험을 분석하고 이에 대한 대책을 수립함으로써 관리자와 조직이 그 대책을 실현할 수 있도록 지원하는 독립적인 전문자문 서비스를 말한다. 보안컨설팅 서비스 시장은 정보보호 평가/인증(ISO/ISMS/CC 등), 진단 및 모의해킹, 개인정보보호컨설팅, 정보감사(내부정보유출방지컨설팅 등), 기타 보안컨설팅(기반보호, 보안SI 포함) 등을 포함한다.

정보보호산업 실태조사 보고서를 참고로 국내 보안컨설팅 시장규모를 살펴보면, 2015년 1,131억 원에서 연평균 29.8% 성장하며 2019년 3,215억 원 규모를 형성하고 있다.

2016년부터 정보보호관리체계(ISMS) 인증 의무화 대상이 상급종합병원, 고등교육기관, 매출액 100억 원 이상의 정보통신서비스업, 직전 3개월간의 일일평균 이용자 수가 100만 명 이상인 곳 들로 확대되면서 인증 취득을 위한 컨설팅 시장도 확대되었다.

[그림 5] 국내 보안컨설팅 서비스 시장



*출처: 한국정보보호산업협회, 국내 정보보호산업 실태조사 보고서(2015-2019), NICE디앤비 재구성

또한, 주요정보통신기반시설 및 전자금융기반시설, ISMS 의무 대상자는 1년 1~2회 취약점 점검을 실시하고, 보고해야 하는 의무를 가지고 있는 만큼 보안컨설팅 시장 성장에 높은 기여를 하고 있다.

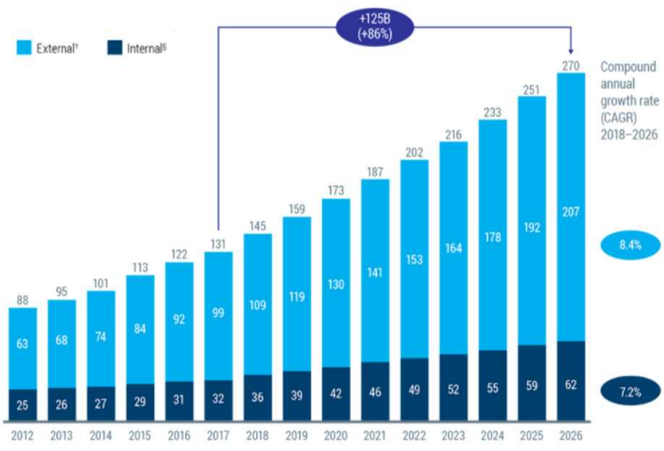
■ 글로벌 사이버보안 시장

우리나라의 정보보안 산업과 대응되는 사이버보안은 사이버상의 범죄, 테러, 해킹 목적의 접근 및 스파이 행위 등으로부터 정보, 시스템, 네트워크를 보호하는 IT 솔루션을 일컫는다.

암호, 인증, 인식, 감시 등의 정보보호 기술이 적용된 제품을 생산하거나, 해당 기술을 활용, 재난·재해·범죄 방지 서비스를 제공하는 산업을 말하고, 네트워크·시스템 기반의 정보보안과 보안기술 및 전통 산업간 융합으로 창출되는 융합보안을 포함한다.

AustCyber(2019)에 따르면 전 세계 사이버보안 시장규모는 2018년 기준 1,450억 달러이며, 2026년까지 86%가 증가하며 2,700억 달러의 시장을 형성할 것으로 전망하고 있다.

[그림 6] 글로벌 사이버보안 시장 전망 (단위 : 십억 달러)



*출처: AustCyber, Global cyber security spend(2019)

Ⅲ. 기술분석

인적 자원을 대체한 취약점 진단 솔루션 보유

동사는 수동적 취약점 진단(컨설팅 방식)을 대체하는 실시간 자동화 취약점 진단 솔루션을 개발하여 취약점 진단의 효율성을 높이고 있다.

■ 취약점 진단 방법 : 컨설팅 VS 솔루션

취약점 진단이란 정보보안 및 침해 사고 방지를 위해 서버, 데이터베이스, 웹 애플리케이션 서버, 웹, 네트워크 등 다양한 플랫폼의 'IT 취약점을 분석, 평가, 관리하는 제반 활동'을 말한다. IT 취약점이란 소프트웨어나 정보시스템 상에 존재하는 보안상의 결점으로서 프로그램을 본래의 기능과 다르게 동작하게 하고, 허용된 권한을 초과하여 사용할 수 있게 하거나 의도하지 않은 오류를 일어나게 할 수 있는 조건들을 말한다. 취약점으로부터 발생하는 피해 예방을 위해 정보통신기반보호법 제9조 제1항, 정보통신망법 제28조, 전자금융거래법 제21조 31항, 개인정보보호법 제29조, 정보통신망법 제47조 2항의 보안 기준에 해당하는 기관 및 기업은 매년 취약점 진단 관리를 받아야 한다.

취약점 진단 방법은 정보보호 컨설팅을 통한 방식과 취약점 진단 솔루션 도입 방식으로 나뉠 수 있다. 컨설팅 방식은 운영 중인 정보자산이 소규모이거나 매년 정보자산의 변동이 없는 경우, 단기간에 높은 수준의 취약점 진단이 필요할 때, 관리 인력이 부재할 때 주로 사용되며, 취약점 진단 솔루션은 반대로 취약점 진단 대상 정보자산의 수가 많고 지속적인 정보자산의 관리가 필요하며 상시적이고 즉각적인 취약점 진단 체계가 필요한 경우 사용된다.

[표 3] 취약점 진단 방법

구분	정보보호 컨설팅	취약점 진단 솔루션
대상	• 정보자산이 소규모 • 매년 정보자산의 변동이 없는 경우 • 단기간에 높은 수준의 취약점 진단 필요 • 관리 인력의 부재로 내부 관리가 어려운 경우	• 정보자산의 수가 많은 경우 • 지속적인 정보자산의 관리가 필요한 경우 • 상시적이며 즉각적인 진단 체계가 필요한 경우 • 매년 동일한 진단 수준의 유지 및 이력관리 필요
장점	• 외부 컨설팅 전문가의 취약점 진단으로 높은 전문성 보유 • 상세하고 세밀한 취약점 진단 가능	• 상시적인 취약점 진단 가능하여 높은 보안성 유지 • 장기적인 관점에서 컨설팅 비용 대비 절감 효과
단점	• 1회성 진단으로 매번 비용 소요 • 취약점 조치 후 이행진단 필요 시 추가 비용 발생 • 인력에 의한 작업으로 취약점 진단 과정 및 결과에 오류 발생 가능 • 컨설팅 전문가의 숙련도에 따라 진행 속도 및 결과 보고 상이	• 솔루션 도입의 초기 투자 비용이 높음 • 취약점 진단 결과에 대해 자체 판단 가능한 수준의 전문성 필요 • 컴플라이언스의 일부 개정 및 신설 시 즉각적인 대응 어려움

*출처: 동사 제품소개서, NICE디앤비 재구성

■ 정보보호 전문서비스 기업으로 지정되어 정보보호 컨설팅 진행

동사는 과학기술정보통신부로부터 정보보호 전문서비스 기업으로 지정(제2018-03호)되어 정보보호에 관한 컨설팅 등의 서비스를 제공하고 있다.

한국정보보호산업협회의 국내 정보보호산업 실태조사 보고서(2019)에 따르면, 국내 정보보안 관련 기업은 473개로 추정되며 이 중 보안컨설팅 서비스를 제공하고 있는 기업은 71개로 파악된다. 2021년 1월 기준 정보보호 전문서비스 기업으로 지정된 업체는 총 27개 업체로, 주요정보통신기반 시설의 취약점 분석·평가업무 및 보호대책의 수립업무에 대해 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 기업에게 지정 기준[1]을 만족할 시 주어진다.

동사는 2014년 3월 처음 지정(구. 지식정보보안 컨설팅 전문업체)되어 현재까지 정보보호 전문서비스 기업으로의 자격을 유지하고 있다.

[그림 7] 동사 정보보호 컨설팅 영역

*출처: 동사 회사소개서

동사는 웹, 모바일, 서버, 네트워크 등 각 분야의 보안 전문가를 보유하고 고객사 맞춤형 보안컨설팅 서비스를 제공하고 있다. 특히, 동사는 다수의 화이트해커들을 보유하고, 고객의 비즈니스에 따라 그에 맞는 시나리오 기법을 기반으로 예상 위협에 대한 모의해킹 서비스를 제공하고 있다. 해커 관점에서 악의적 해킹에 대한 취약점을 진단하는 것으로 취약점이 고객사의 정보자산에 끼치는 영향을 파악하여 대응방안을 제시하고 있다. 동사의 분기보고서(2020.09)에 따르면, 동사는 모의해킹 시 100% 침투 성공률을 보이고 있다.

1) 기술인력 10명 이상 보유(고급 또는 특급 인력 3명 이상 포함), 자본 총계 10억원 이상, 신원확인 및 출입통제를 위한 설비, 기록 및 자료를 안전하게 관리하기 위한 설비 보유 등의 설비요건, 업무 수행능력 심사 기준 70점 이상 획득, 정보보호 전문서비스 관리규정 보유 및 준수

동사는 기술적 진단 컨설팅 외에도 정보보호 관리를 위한 컨설팅을 진행하고 있다. 관리 컨설팅은 고객사의 정보침해 위협에 대응하기 위해 보안 관리 대책을 도출하고 이를 효과적으로 적용할 수 있도록 정보보호 체계 설계 및 내재화를 지원하여 가시적인 정보보호 관리해법을 제공하는 서비스이다.

동사는 이베이코리아, KB증권, 두산, 넥슨, 국립재활원 등 2018년 기준 약 350건 이상의 컨설팅 레퍼런스를 보유하고 있다.

■ 취약점 진단 솔루션 : 자동화 취약점 전수 진단

정보보호 컨설팅을 통한 취약점 진단 방식은 수작업으로 발생하는 다양한 문제점과 중요 자산만 선정하여 취약점 진단을 수행하는 표본진단으로 취약점 관리의 어려움이 발생한다. 동사는 이러한 컨설팅의 단점을 보완한 취약점 진단 솔루션을 개발하여 취약점 진단에 사용하고 있다.

동사의 취약점 진단 솔루션은 다년간의 기술/관리 컨설팅 노하우를 바탕으로 동사 직접 개발한 보안 솔루션이며, 국내·외 법령 및 규칙(컴플라이언스)에 대응하기 위해 1,000개 이상의 진단항목을 내포하고 있고, 취약점 항목(산업별, 목적별) 커스터마이징으로 내부 보안지침도 반영할 수 있는 것이 특징이다.

동사의 취약점 진단 솔루션은 운영체제, 데이터베이스 관리시스템, 네트워크, 웹 애플리케이션 서버, 웹의 다양한 플랫폼(50여 개) 환경을 지원하며 국내외 법령 및 규칙(컴플라이언스)을 준수하여 설계되어 있다.

[그림 8] 취약점 진단 솔루션 개요

*출처: 동사 제품소개서

특히, 동사의 솔루션은 취약점 정보 수집 및 분석을 분리 수행하여 취약점 진단 시 1% 이하의 CPU 점유율을 차지하는 안정적인 서비스 운영이 가능한 아키텍처 구조를 가지고 있다. 구체적으로, 진단 대상 시스템에 설치된 에이전트에서는 보안성 진단에 필요한 정보를 수집하여 전달하는 기능만을 수행하고, 리소스 소요가 많은 보안성 진단 분석 프로세스는 진단 대상 시스템이 아닌 보안성 진단 서버에서 별도로 이뤄지도록 함으로써, 보안성 진단 분석 프로세스 실행에 따른 진단 대상 시스템의 과부하의 부담을 해소할 수 있는 것이다.

동사의 제품소개서에 따르면, 동사의 솔루션은 컨설팅(수작업) 대비 300배의 빠른 진단 속도를 나타내고 있으며, 전체 자산에 대한 보안현황 관리를 가시적으로 관리할 수 있고,

취약점 분석평가의 계량화가 가능하며 체계적인 취약점 조치 이행관리 가능한 차이점을 보유하고 있다. 이러한, 동사의 취약점 진단 솔루션은 특허권(제10-1620601)을 통해 차별성을 인정받고 있으며, 컴퓨터 보안을 위한 국제 표준인증인 CC(Common Criteria)인증과 국산 소프트웨어의 품질을 증명하는 국가 인증인 GS(Good Software)인증을 획득하고 있고, 공공기관, 대기업, 금융권 등 다수의 레퍼런스를 확보하고 있다.

[그림 9] 기존 취약점 진단 방식과 동사 취약점 솔루션 차이

	방식	단위	정확도	속도	공수	금액	관리	보고서	안정성
기존 진단	샘플링	1M/M 100여대	±75%	보고서완료	1	1	기존결과와 비교불가	결과수정시 재진단 필요	수집 데이터 평문저장
SolidStep	전수 검사	무한대	100%	단시간에 보고서출력	1/300	1/10	누적통계 보고서 가능	다양한 양식의 보고서 출력	수집 결과 암호화

*출처: 동사 제품소개서

■ 웹 해킹 방지 솔루션 : 잠재적 위협까지 탐지

웹쉘(Web Shell)은 업로드 취약점을 통해 시스템에 명령을 내릴 수 있는 코드를 말하며, 해커들은 웹셀을 통해 공격 서버의 제어권을 장악하고 정보탈취, 위변조, 악성 스크립트 삽입, 인접 시스템 공격 등을 행할 수 있다. 웹쉘은 공격대상 서버에 업로드된 후 웹브라우저를 통해 시스템 명령어를 수행하게 되므로 다양한 공격이 가능하며, 기존 보안시스템(방화벽 등)으로 탐지가 어렵다.

동사의 웹 해킹 방지 솔루션은 기존 보안시스템에서 탐지하지 못하는 신·변종 웹쉘을 정규식과 휴리스틱(의사결정과정 단순화한 지침) 탐지 기술을 사용하여 실시간으로 탐지하고 차단, 격리조치하는 실시간 웹쉘 탐지 솔루션이다.

동사의 웹 해킹 방지 솔루션은 실무경험이 많은 자사 컨설턴트들에 의해 웹쉘 패턴을 수집하고 수집된 패턴을 별도의 연구인력을 통해 최적화 및 관리하며 최신 동향을 빠르게 반영하고 있다.

[그림 10] 웹 서버 방어 솔루션 특징

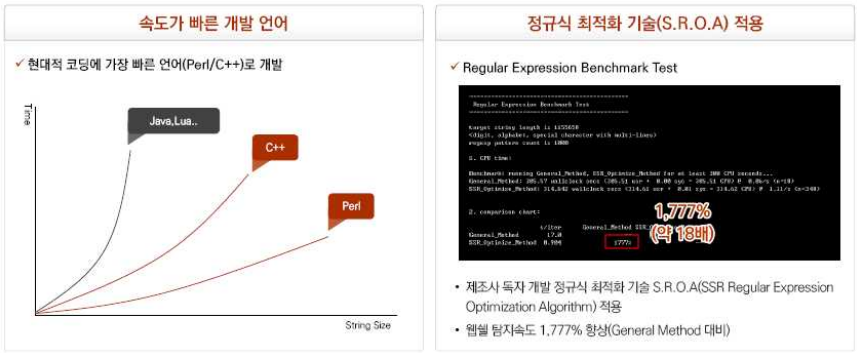
*출처: 동사 제품소개서

특히, 이미 알려진 웹쉘의 고유 패턴과 해시값을 DB화하여 매칭 탐지(정규식 패턴)를 통해 1차적으로 웹쉘을 탐지하고, 휴리스틱 엔진을 탑재하여 정규식 패턴탐지와는 별개의 독립된 검사를 수행하여 탐지율을 높이고 있. 동사가 개발한 휴리스틱 엔진은 웹쉘이 가진 기능 및 특성 유사도를 분석하여 웹쉘을 탐지하는 것으로 악성코드에 포함될 수 있는 기능의 종류에 따라 배정과 유형을 미리 정하여 악성코드 위험도를 산출하는 엔진이다.

또한, 동사는 자바 대신 C++, Perl 등으로 개발하여 솔루션 동작 속도를 높였으며, 정규식 패턴의 최적화 알고리즘을 자체적으로 개발하여 일반적인 방식 대비 약 18배 빠른 탐지 속도를 제공하고 있다.

웹 해킹 방어 솔루션 역시 특허권(제10-1461051) 취득을 통해 권리를 보호받고 있으며, CC인증 및 GS인증을 취득하고 있다.

[그림 11] 웹 해킹 방어 솔루션 특징



*출처: 동사 제품소개서

■ 정보보호 컨설팅 및 제품 개발을 위한 안정적 기술 개발 인프라 보유

동사는 2012년 기업부설연구소를 설립하고, R&D 인큐베이션팀, Core팀, UI팀, 항목개발팀, 디자인팀, Q.A팀, 기술지원팀으로 영역별 팀을 구성하고 있으며, 자체 개발한 각종 툴, 시제품, 프로세스 등이 공유될 수 있도록 유기적인 관리체계를 구성하여 업무 효율성을 높이고 있다. 또한, 지식관리시스템을 활성화하여 전문 지식과 경험을 축적하고 이를 구성원들에게 공유하여 검증된 기술력을 기반으로 안정적인 제품 개발이 가능하도록 개발 환경을 구축하고 있다.

동사는 기업부설연구소를 통해 보안취약점 통합관리 솔루션, 사용자 정의 피싱 템플릿 작성 기능 등 연구개발을 수행 중에 있으며, 올해 상반기에도 신제품 출시를 예정하고 있는 것으로 파악된다.

동사는 보고서 작성일 기준(2021.02) 특허권 4건, 상표권 24건, 디자인권 1건, 저작권(프로그램등록) 4건의 지식재산권을 보유하고 있다. 또한, GS인증, CC인증, 이노비즈인증, ISO27001, ISO9001, 벤처기업인증 등을 받으며 기술력을 인정받고 있다.

[그림 12] SWOT 분석

IV. 재무분석

정보보안에 대한 시장 수요 증가로 동사 매출 성장 전망

취약점 의무진단 대상 기업이 증가하고, 높아진 보안위협에 따라 정보보안을 위한 법/규제가 강화되고 예산확대 방안이 실시되며 동사의 수혜도 지속될 것으로 전망된다.

■ 정보보안 시장의 성장으로 동사의 매출 증가세 기대

동사의 사업 영역은 취약점 진단, 웹 해킹 방지 솔루션으로 구성된 솔루션 부문과 보안 관련 기술 및 관리 컨설팅을 진행하는 용역 부문으로 크게 나눌 수 있다. 2019년 연간 매출액 기준 솔루션 부문 36.9%, 용역 부문 38.7%, 상품 부문 24.0%, 기타 0.4%의 비중을 나타냈고, 2018년에는 솔루션 부문 40.6%, 용역 부문 30.3%, 상품 28.6%, 기타 0.5%를 기록하고 있다. 국내외 매출 비중은 국내 99.4%, 수출 0.6%(2018년 국내 99.9%, 수출 0.1%)로 대부분의 매출이 내수 판매를 통해 발생하고 있다.

한편, 정부는 2015년 12월 정보보호산업의 진흥에 관한 법률을 시행하였고, 이후 5년간 정보보호 예산확대 방안을 실시하였다. 이로 인해 은행, 보험회사, 협동조합 등을 포함한 전자금융기반시설과 더불어, 의료기관 및 교육기관도 의무대상으로 포함되어 우호적인 시장 분위기가 형성되며 과거 3개년 동사는 실적 수혜를 입은 것으로 확인된다. 최근 5G시장 가속화에 따른 트래픽 증가 등으로 정보보안에 대한 시장 수요가 증가할 것으로 전망되고 있어 시장 환경은 우호적인 수준이다.

[표 4] 동사 연간 및 3분기(누적) 요약 재무제표 (단위: 억 원)

항목	2017년	2018년	2019년	2019년 3분기	2020년 3분기
매출액	113.3	125.5	136.5	71.3	55.1
매출액증가율(%)	37.3	10.8	8.8	58.1	-22.7
영업이익	26.3	11.1	5.7	-13.1	-32.2
영업이익률(%)	23.2	8.8	4.2	-18.4	-58.4
순이익	25.2	11.6	11.2	-6.8	-16.7
순이익률(%)	22.2	9.2	8.2	-9.5	-30.3
부채총계	61.4	43.4	34.5	21.7	15.7
자본총계	91.3	232.0	247.1	228.6	234.9
총자산	152.6	275.3	281.6	250.3	250.6
유동비율(%)	250.7	557.8	716.5	1,053.4	1,355.2
부채비율(%)	67.3	18.7	14.0	9.5	6.7
자기자본비율(%)	59.8	84.3	87.7	91.3	93.7
영업현금흐름	12.2	1.1	24.7	8.5	16.0
투자현금흐름	-8.4	-102.4	-1.6	-0.6	3.6
재무현금흐름	1.9	109.8	-11.5	-10.6	2.0
기말 현금	28.2	37.0	48.6	34.3	70.2

※ 분기: 누적 실적 *출처: 동사 사업보고서(2019.12), 동사 분기보고서(2020.09)

다만, 2020년 3분기 누적 매출액이 전년 동기 대비 22.7% 감소한 55.1억 원 수준에 그쳤으며, 2020년 4분기 누적 매출액도 전년 대비 25.9% 감소한 101.1억 원 매출액 시현에 그친 것으로 공시하였다. 이는 코로나19 사태로 인한 대면 보안컨설팅 시장 축소, 신규제품 출시 지연에 따른 결과로 확인된다. 동사는 많은 수의 화이트해커를 보유하고 있어 취약점 진단 분야에서 우수한 기술력을 보유한 것으로 평가되는 점과 우호적인 시장 분위기 등을 고려할 시, 중장기적인 성장 모멘텀은 확보한 것으로 판단된다.

■ 최근 3개년 매출 확대세를 보였으나 수익성은 저하

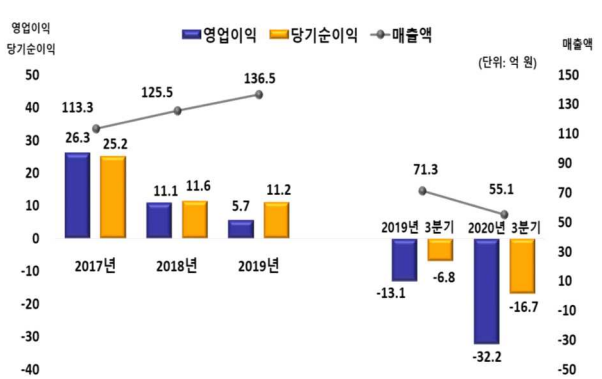
최근 3개년 매출액은 2017년 113.3억 원(yoy 37.3%), 2018년 125.5억 원(yoy 10.8%), 2019년 136.5억 원(yoy 8.8%)을 기록하며 최근 3개년 매출 증가세가 지속되었다. IT인프라 기업을 대상으로 취약점 의무진단이 법제화되었으며, 관련 법규도 신설로 의무진단 대상업체가 확대됨에 따른 수요 증가가 매출 확대를 견인한 것으로 조사된다.

한편, 동사가 속한 사업의 특성상 연구개발비용이 지속적으로 발생하고 있는 가운데, 연구개발비용이 2017년 9.2억 원(매출액 대비 8.2%), 2018년 10.6억 원(매출액대비 8.5%), 2019년 17.8억 원(매출액 대비 13.0%)으로 그 비중이 증가세를 보이고 있다. 이로 인해 최근 3개년 매출 증가에도 불구하고 영업비용(매출원가+판관비) 부담의 가중으로 수익성은 하락세를 보이며 2019년 영업이익 5.7억 원, 매출액영업이익률 4.2%를 기록하였다. 한편, 최근 2개년 말 영업외수지가 흑자를 지속하며 순이익률이 영업수익률을 상회하고 있는 가운데, 2019년 말 이자수익, 외환차익 등의 증가에 힘입어 순이익 11.2억 원, 매출액순이익률 8.2%를 기록하였다.

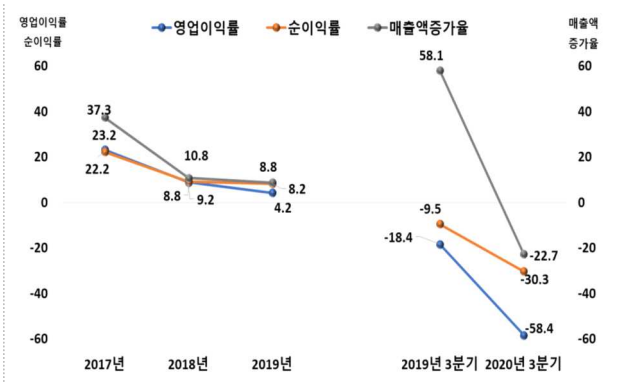
■ 2020년 3분기 전년동기 대비 매출 감소, 영업적자 확대

2020년 3분기 누적 매출액 55.1억 원을 기록하며 전년도 매출액의 40.4%, 전년 동기 대비 22.7% 감소한 실적을 나타냈다. 웹 해킹 방지 솔루션 및 관리 컨설팅 분야에서는 수주가 확대되었음에도 불구하고, 취약점 진단 솔루션 및 기술 컨설팅 수주가 부진함에 따른 결과이다. 한편, 영업손실 32.2억 원, 매출액영업이익률 -58.4%로 전년 동기 대비 영업적자 폭이 확대되었으나, 유형자산처분이익, 무형자산처분이익 등 영업외수지 흑자 발생으로 순손실 16.7억 원, 매출액순이익률은 -30.3%로 적자 폭이 축소되었다.

[그림 13] 동사 연간 및 3분기(누적) 요약 포괄손익계산서 분석 (단위: 억 원, %)



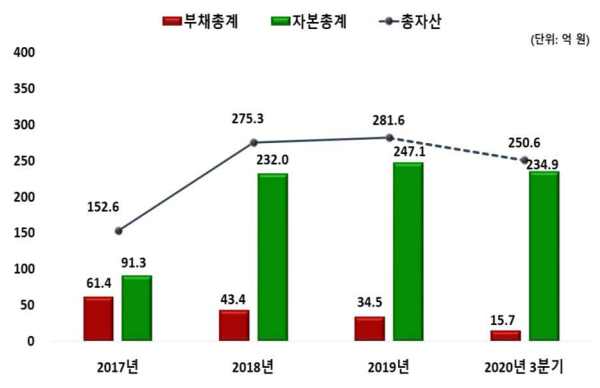
매출액/영업이익/당기순이익 추이



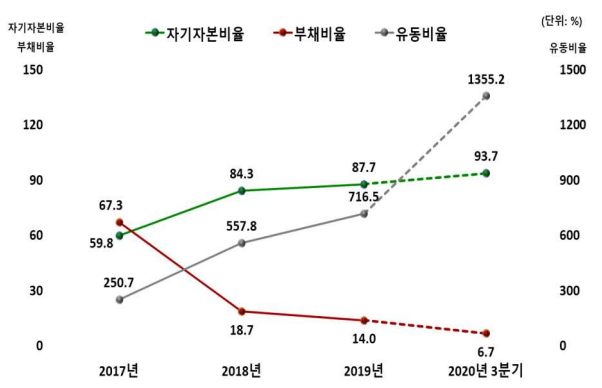
증가율/이익률 추이

*출처: 동사 사업보고서(2019.12), 분기보고서(2020.09), NICE디앤비 재구성

[그림 14] 동사 연간 및 3분기(누적) 요약 재무상태표 분석 (단위: 억 원, %)



자산/부채/자본 비교



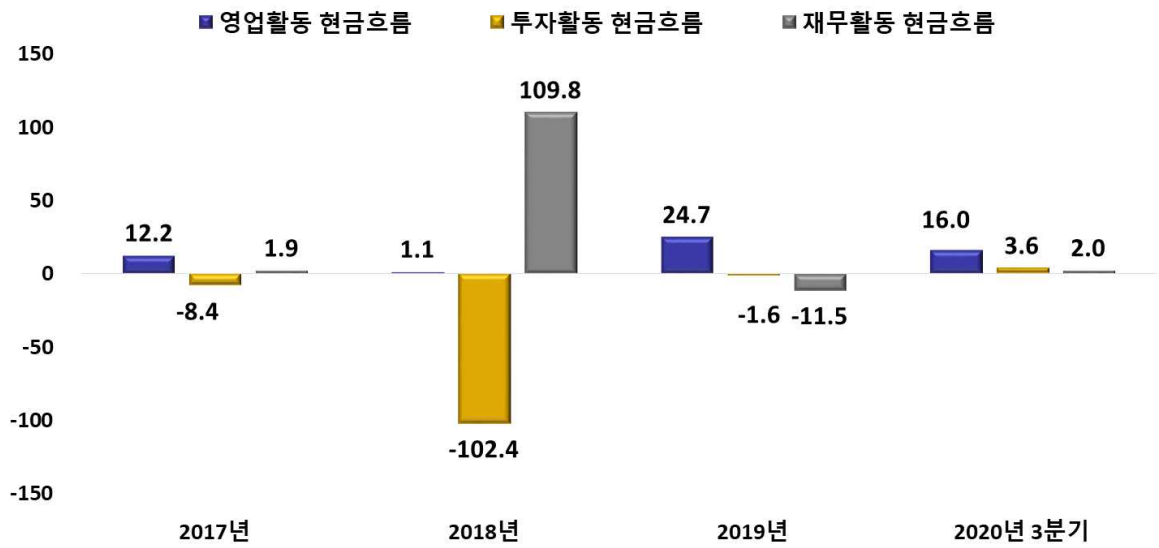
자본구조의 안정성

*출처: 동사 사업보고서(2019.12), 분기보고서(2020.09), NICE디앤비 재구성

■ 2019년 투자활동현금 유출이 크게 감소, 기말 현금성자산 증가

동사는 최근 3개년 말 흑자 수익 지속과 더불어 현금 유출이 없는 비용의 가산으로 영업활동현금흐름이 최근 3개년 양(+)의 값을 지속하였고 그 규모는 2017년 12.2억 원, 2018년 1.1억 원, 2019년 24.7억 원으로 등락세를 나타냈다. 2018년 장단기금융상품의 취득 등으로 인한 투자활동현금유출 수준이 높았으나, 2019년 해당 값이 감소하며 투자활동현금흐름은 -1.6억 원에 그쳤다. 결과적으로 동사는 투자활동과 재무활동에 필요한 자금을 영업활동현금으로 충당하는 모습을 나타낸 가운데, 2019년 기준 기초현금 37.0억 원에서 기말현금 48.6억 원으로 증가하는 모습을 나타냈다.

[그림 15] 동사 현금흐름의 변화 (단위: 억 원)



*출처: 동사 사업보고서(2019.12), 분기보고서(2020.09), NICE디앤비 재구성

V. 주요 변동사항 및 향후 전망

코로나19로 인한 수요 감소로 적자전환하였으나, 시장환경은 여전히 우호적

코로나19로 인해 대면으로 진행되는 보안컨설팅 시장이 축소되고, 협력업체의 폐업 등으로 인해 2020년 적자전환되었으나, 정보보호 산업을 지원하는 정부정책이 추가적으로 발표되는 등 시장환경은 여전히 우호적이다.

■ 과학기술정보통신부, 정보보호 지원 사업 추진 내용 발표

올해 1월 과학기술정보통신부는 ICT 중소기업 정보보호 안전망 확충, 정보보호제품 평가·인증 부담완화, 정보보호관리체계(ISMS) 간편 인증 신설 등을 골자로 중소기업 정보보안 강화와 안전한 정보보호 제품 이용 촉진을 위한 "2021년, 달라지는 정보보호 제도와 지원 사업"을 발표하였다.

이번 지원 사업 중 하나로 정부는 ICT 중소기업 정보보호 안전망 확충을 위해 정보보호 컨설팅 및 보안제품 도입지원 사업 대상 기업을 300개에서 600개로 확대하고, 지원 금액도 기업당 1,000만 원에서 1,500만 원으로 확대한다는 계획이다. 해당 정책은 올해 4월부터 시행되며, 대상 기업이 확대되고 금액이 증가하는 만큼 모의해킹 등의 컨설팅과 취약점 지원 솔루션 등을 제공하는 동사의 사업에도 긍정적인 영향을 미칠 것으로 예상된다.

또한, 기존 중견기업 이상을 대상으로 인증 항목과 평가방법이 설계되어 있던 정보보호관리체계(ISMS) 인증을 영세·중소기업 규모에 적합하도록 경량화한 ISMS-P 간편 인증 제도를 신설하는 계획도 발표하였다. 경량화된 인증 제도는 인증절차가 축소됨에 따라 비용과 시간에 대한 부담이 완화되어 인증 취득을 위한 기업이 증가할 것으로 보이며, 이는 동사에도 간접적인 영향을 미칠 것으로 예상된다. 다만, ISMS-P 인증은 올해 인증기준 수립 및 법령 개정을 준비하고 2022년 3월부터 시행할 예정에 있다.

한편, 동사의 취약점 진단 솔루션과 웹 해킹 방지 솔루션과 같은 정보보호제품은 국가·공공기관에 납품하기 위해선 CC인증이 필수적이다. CC인증 취득을 위해서는 많은 시간이 소요되며 버전이 다를 경우 인증을 새로 취득해야 하고, 3년마다 갱신해야 했다. 이번 정보보호 지원 사업 추진 내용에 따르면 평가자 양성, 대기적체 기관의 신청 수요 조정 등을 통해 평가 대기시간을 단축시키고, 변경 승인 요건 확대와 CC인증 유효기간을 3년에서 5년으로 확대시키며 정보보호 기업의 적시, 적기에 제품 조달이 가능하도록 하겠다는 입장이다.

■ 코로나19로 인한 대면 컨설팅 수요 감소로 적자전환

동사의 공시자료(2021.01)에 따르면, 2020년 동사는 코로나19로 인해 대면으로 진행되는 보안컨설팅 시장이 축소되면서 매출액이 전년 대비 25.9% 감소하고, 협력업체의 폐업 등으로 인해 부실채권이 발생하며 영업이익이 적자전환되었다. 동사 매출의 상당수가 보안컨설팅(용역부문, 2019년 기준 38.7%)에서 발생되고 있으며, 솔루션 부문도 컨설팅 과정에서 연계되어 판매되는 경우가 많아 대면 컨설팅 수요감소가 많은 영향을 미칠 것으로 판단된다.

다만, 하나금융투자 보고서(2020.12)에 따르면 동사는 취약점 진단 종류의 다양화(자율주행차, 로봇 등)와 정부 정책지원 확대 등 우호적인 시장 환경이 조성되고 있고, 기존 제품의 업그레이드 버전과 신규 솔루션 출시가 예정되어 있으며, 클라우드 서비스를 통한 서비스 대상 기업 확대 등으로 중장기적인 성장모멘텀을 확보하고 있다는 견해를 밝히고 있다.

■ 각자대표이사에서 고필주 단독대표이사 체제로 변경

지난해 3월 공동대표이사였던 윤두식 대표이사가 등기이사로 물러나고, 고필주 대표이사가 각자대표이사로 취임하였다. 그러나 각자대표이사 체제로 변경된지 3개월 만인 지난해 6월 정진석 대표이사가 사임하며 경영에서 완전히 물러났다.

동사의 창업주인 정진석 대표이사는 2017년 경영권을 지란지교시큐리티에 매각한 후에도 동사의 공동대표이사로 취임하여 동사 경영을 지속하였으나 일신상의 이유로 사임하였고, 현재 동사는 고필주 대표이사 단독체제로 변경되었다.

■ 증권사 투자의견

작성기관	투자의견	목표주가	작성일
하나 금융투자	Not Rated	-	2020.12.08
	■ 국내 최다 화이트해커 보유한 취약점 진단 보안업체 ■ 2021년 신제품 출시, 보안시장 확대에 따른 수혜 기대 ■ 2020년 매출액 124억 원, 영업이익 -11억 원 전망		