주주총회소집공고

2022년 11월 30일

회 사 명 : (주)파수

대 표 이 사 : 조규곤

본 점 소 재 지 : 서울특별시 마포구 월드컵북로 396, 누리꿈스퀘어17층

(전 화)02-300-9000

(홈페이지)http://www.fasoo.com

작 성 책 임 자 : (직 책)경영지원본부장 (성 명)이지수

(전 화)02-300-9000

주주총회 소집공고

(제23기 임시주주총회)

주주 여러분의 건승과 댁내의 평안을 기원합니다.
주식회사 파수는 상법 제363조 및 정관 제17조에 근거하여 임시주주총회를 아래와 같이 개최하오니 참석하여 주시기 바랍니다.(상법 제542조의 4 및 정관 제18조에 의거하여 발행주식총수의 1% 이하 소유주주에 대하여는 이 공고로 소집통지를 갈음하오니 양지하여 주시기 바랍니다)

- 아 래 -

1. 일시 : 2022년 12월 15일 목요일 오전 09시 00분

2. 장소 : 누리꿈스퀘어 비지니스타워 6층 대회의실(서울시 마포구 월드컵북로 396)

3. 회의목적사항
부의 안건
-제1호 의안 : 자본준비금 감액을 통한 이익잉여금 전입의 건

4. 주주총회 소집통지 공고사항 등의 비치
상법 제542조의4 등 관련 법령에 의거하여, 주주총회 소집통지・공고 및 경영참고사항을 당사의 인터넷홈페이지(www.fasoo.com) 및 전자공시시스템에 게재하고, 당사의 본점, 금융위원회, 한국거래소에 비치하오니 참조하시기 바랍니다.

5. 전자투표 및 전자위임장권유에 관한 사항
우리회사는 「상법」 제368조의4에 따른 전자투표제도와「자본시장과 금융투자업에 관한 법률 시행령」 제160조제5호에 따른 전자위임장권유제도를 제 22기 정기 주주총회부터 활용하기로 결의하였고, 이 두 제도의 관리업무를 삼성증권에 위탁하였습니다. 주주님들께서는 아래에서 정한 방법에 따라 주주총회에 참석하지 아니하고 전자투표방식으로 의결권을 행사하시거나, 전자위임장을 수여하실 수 있습니다.

가. 전자투표· 전자위임장권유관리시스템
- 인터넷 및 모바일 주소 : https://vote.samsungpop.com

나. 전자투표 행사 전자위임장 수여기간
: 2022년 12월 05일 오전9시 ~ 2022년 12월 14일 17시
- 기간 중 24시간 시스템 접속 가능(단, 마감일은 17시까지 가능)

다. 전자투표시스템에서 주주 본인인증 후 의안별 의결권 행사
- 본인인증 방법 : 공동인증, 카카오페이, 휴대폰인증 등

라. 수정동의안 처리 : 주주총회에서 상정된 의안에 관하여 수정동의가 제출되는 경우 전자투표는 기권으로 처리

주주총회 참석시 준비물
-직접행사: 주주총회 참석장, 신분증
-대리행사: 주주총회 참석장, 위임장(주주와 대리인의 인적사항 기재, 인감날인, 대리인의 신분증)

I. 사외이사 등의 활동내역과 보수에 관한 사항

1. 사외이사 등의 활동내역

가. 이사회 출석률 및 이사회 의안에 대한 찬반여부

회차	개최일자	의안내용	사외이사 등의 성명	
			이지화 (출석률: 100%)	홍석모 (출석률: 100%)
			찬 반 여 부	
1	2022.02.10	[보고] - 내부회계관리제도 운영실태 보고 [부의] 제1호 정관 일부 변경의 건 제2호 전자위임·전자투표 채택의 건 제3호 제22기 재무제표 승인의 건 제4호 제22기 영업보고서 승인의 건 제5호 이사 선임의 건 5-1호 사내이사 이지수 5-2호 사외이사 이지화 제6호 감사 선임의 건 제7호 제23기 이사보수한도 승인의 건 제8호 제23기 감사보수 한도 승인의 건 제9호 주식매수선택권 부여의 건 제10호 Fasoo, Inc. 자본금 출자의 건	-	찬성
2	2022.02.10	[부의] 제1호 제22기 주주총회소집 결의	-	찬성
3	2022.11.04	[부의] 제1호 제23기 임시주주총회 소집 결의 제2호 임시주주총회 권리주주확정을 위한 기준일 설정 제3호 자본준비금 감액을 통한 이익잉여금 전입의 건	찬성	-

당사는 제22기 정기주주총회에서 사외이사 이지화를 선임하였으며, 사외이사 홍석모는 임기만료에 따라 퇴임하였습니다.

나. 이사회내 위원회에서의 사외이사 등의 활동내역

위원회명	구성원	활 동 내 역		
		개최일자	의안내용	가결여부
-	-	-	-	-

2. 사외이사 등의 보수현황

(단위 : 백만원)

구 분	인원수	주총승인금액	지급총액	1인당 평균 지급액	비 고
사외이사	1	2,000	39	20	-

인원수는 현재 기준으로 작성하였으며, 상기 주총승인금액은 이사보수한도 총액입니다. 지급총액은 2022년 1월 ~ 10월 까지의 지급액이며 현재는 사임한 사외이사 지급분이 포함되어있으며 1인당 평균지급액은 사임한 이사를 포함하여 2인으로 계산하였습니다.

II. 최대주주등과의 거래내역에 관한 사항

1. 단일 거래규모가 일정규모이상인 거래

(단위 : 억원)

거래종류	거래상대방 (회사와의 관계)	거래기간	거래금액	비율(%)
-	-	-	-	-

2. 해당 사업연도중에 특정인과 해당 거래를 포함한 거래총액이 일정규모이상인 거래

(단위 : 억원)

거래상대방 (회사와의 관계)	거래종류	거래기간	거래금액	비율(%)
-	-	-	-	-

III. 경영참고사항

1. 사업의 개요

가. 업계의 현황

(1) 정보보호산업의 개요

정보보호산업법에서는 정보보호산업을 '정보보호를 위한 기술 및 정보보호기술이 적용된 제품을 개발·생산 또는 유통하거나 이에 관련한 서비스를 제공하는 산업'으로 정의하고 있습니다.

정보보호산업은 정보보호제품을 개발, 생산 또는 유통하거나 정보보호에 관한 컨설팅, 보안관제 등 서비스를 수행하는 산업으로서 기술의 적용영역, 제품의 특성 등에 따라 정보보안, 물리보안, 융합보안(정보보안+물리보안,정보보안+他산업)으로 분류됩니다. 이는 크게 컴퓨터 또는 네트워크상 정보유출, 훼손 등을 방지하기 위한 정보보안, 재난, 재해, 범죄 등을 방지하기 위한 물리보안, 자동차나 항공해상 보안 등의 융합보안으로 구분됩니다.

국내 정보보호산업의 시장 동향은 다음과 같습니다

정부는 제1차 정보보호산업 진흥계획(K-ICT 시큐리티 2020)을 수립·발표하면서 창업활성화를 통한 글로벌경쟁력 강화, 투자확대 및 신시장 창출, 내수위주에서 글로벌 진출로 시장확대, 지속성장 생태계 조성 등을 중점 추진키로 하였습니다. 이후 2차 계획에서는 2021년부터 향후 5년간 정보보호산업을 차세대 핵심 산업으로 육성하기 위한 계획을 마련하였습니다. 이를 통해 정부는 정보보호 신규시장 발굴과 동시에 정보보호 성장 생태계를 조성해 정보보호 산업육성을 추진하고 있습니다. 2025년까지 정보보호시장이 20조원, 매출 300억 이상 기업이 100개까지 증가하는 것을 목표로 하고 있습니다.

정보보호산업 경쟁력 강화를 위한 10대 정책과제로

비대면 서비스 관련 보안시장 활성화

정보보호 데이터 활용기반 조성

AI기반 물리보안 산업 육성
5G + ICT 융합보안 산업 저변 확대
공공 및 민간분야 정보보호 투자 확대
정보보호기업 성장 지원
정보보호기업 해외진출 및 국제협력 강화
차세대 보안 신기술 확보
정보보호산업 규제 및 법, 제도 개선
정보보호 전문인력 양성

이처럼 정부가 적극 나서기로 한 정보보호산업은 초연결사회가 도래함에 따라 사물인터넷(IoT)이 미래의 새로운 경쟁성장 동력으로 부상하고 있는 가운데 향후 우리나라의 미래를 좌우할 최첨단 기술집약적 산업입니다. 국내에 정보보호 관련 기업들이 본격적으로 설립된 것은 1990년 중반으로 다른 국가 기간산업에 비해 월등히 역사가 짧다고 할 수 있습니다. 그럼에도 그동안 우리나라의 정보보호산업은 비약적인 발전을 통해 경쟁력도 확보했으며 수출도 매년 증가하고 있고 전체 IT 산업에서 차지하는 비중 역시 향후 첨단기술의 발달과 함께 급증할 것으로 예상됩니다.

전 세계 정보보호산업 시장 규모는 향후 해마다 증가할 것으로 예상되는데, 이는 기존 인터넷 및 스마트폰 이용부터 융합보안과 새롭게 떠오르고 있는 IoT(사물인터넷)의 등장으로 인한 보안의 중요성이 커지고 있기 때문입니다. 북미, 유럽, 일본 등 주요 선진국이 정보보호 시장의 90% 가량 차지하고 있으며, 최근에는 중국이라는 새로운 보안 시장이 대두되고 있습니다.

(2) 정보보호산업의 특징 및 국가경제에서의 중요성
정보보호산업은 '창과 방패'처럼, 진화하는 보안위협에 대응하여 지속적인 R&D가 필요한 분야이며, 보안위협의 대응과 우수한 제품 개발을 위해서는 암호, 인증, 인식, 감시 등의 보안 분야 학문 외에 인문학, 공학 등 多학제적인 연구 및 인재가 필요한 분야입니다.

또한 보안사고 발생시 개인,사회,국가 등 전 영역에 영향을 주는 등 파급력이 매우 크고 최근 전 산업의 IT화로 대부분의 산업에 보안기술 적용이 요구되고 있으며, 평상시에는 중요성을 인식 못하지만 사고 발생시에는 높은 수준의 품질을 요구하게 되는

특징을 가지고 있습니다.

우리나라의 정보보호의 자주성을 확보하고 국가의 중요정보 유출을 미연에 방지하기 위해서는 무엇보다 국내 정보보호업체의 기술수준을 향상시키고 이를 활용하는 것이 필요하다고 할 수 있습니다. 특히 정보보호산업은 다음과 같은 특성이 있습니다.

첫째, 정보보호산업은 성장발전 가능성이 높은 신성장 산업으로, 시스템 네트워크 보안 중심의 정보보안과 CCTV・DVR・무인경비서비스 등의 물리보안, 타 산업 군에 보안기술이 적용되는 활용분야(융합보안)로 구분됩니다. 향후 지능화된 보안위협 및 자동차・안전 등 타 분야의 신규 보안 이슈의 확대로 시장은 더 커질 것으로 전망됩니다.

둘째, 정보보호산업은 국가의 안위를 지켜주는 방위산업입니다. 협의의 개념으로는 개인의 안전과 재산을 지켜주는 보안산업이고, 광의의 개념으로는 각종 테러와 보이지 않는 전쟁(사이버테러 및 정보화 전쟁)으로부터 국가의 안위를 지켜주는 방위산업입니다. 정보보호산업은 밖으로는 금융기관의 IT보안 서비스, 국제범죄, 국제해커로부터의 침입차단 등 국가를 위험으로부터 지켜주고, 안으로는 주정차 차량 감시 CCTV 등을 활용하여 질서 확립 및 각종 범죄 예방 및 치안을 담당하므로 방위산업이라 할 수 있습니다.

셋째, 정보보호산업은 차세대 고부가가치 미래지향 산업입니다. 최근 국내 IT 산업은 스마트폰, 태블릿 PC 등 스마트 모바일 기기 시장 뿐만 아니라 IoT(사물인터넷) 및 클라우드 컴퓨팅 등 큰 변화가 있어 왔습니다. 이에 정보보안 및 무선통신망의 안전성 강화에 대응해야 할 것이며, IT산업을 기반으로 한 미래 생활에 정보보호산업 기술이 포함되어 응용되고 있습니다.

나. 시장 여건

(1) 데이터보안 시장

데이터보안은 암호화 기술을 이용하여 허가된 사용자가 허가된 권한 내에서 콘텐츠를 사용하도록 통제하는 권한 제어 기술(Digital Rights Management) 입니다.

최근에는 클라우드 컴퓨팅의 발전에 따라 각종 플랫폼을 지원하는 클라우드 환경에서의 보안이슈가 증가하여 클라우드 데이터보안 서비스 분야도 신규산업으로 떠오르고 있습니다. 과거 해킹이나 바이러스에 의한 정보유출 사고의 대부분이 최근에는 허가된 내부자나 관계자에 의해 금전적 목적을 동반한 사고로 확대되면서, 보안의 중심이 네트워크 보안에서 콘텐츠 보안으로 패러다임이 변화되었으며, 콘텐츠 자체를 직접 암호화하고 사전에 정의된 권한에 따라 사용을 통제하는 디지털저작권관리(DRM) 솔루션이 보안 현안을 해결하는 기업 보안의 핵심 인프라로 제시되고 있습니다.

DRM솔루션은 보안 영역별로 특화된 타 보안 솔루션들이 가지는 한계점을 보완하고 핵심 정보 자체에 대한 원천적이고 지속적인 보안 해법을 제시하며, 전 산업 군에 걸쳐 빠르게 수요가 확산되고 있는 실정입니다. 이는 외부는 물론, 허가된 내부자에 의한 불법 유출까지 방지할 수 있는 근본적인 보안 해법으로 떠오르면서, 기업보안에 있어 더 이상 선택이 아닌 필수적으로 도입해야 하는 보안 인프라로 자리 잡고 있습니다. 특히 보안 투자 여력이 높고, 정보 인프라의 표준과 통합을 중시하는 대기업 및 그룹사들이 이 시장의 가장 큰 고객입니다. 또한, 기술력을 가지고 있는 중소 제조업체들도 자사 기술에 대한 외부유출 방지를 위해서 도입하고 있는 추세입니다.

당사의 주력 사업분야인 데이터보안 시장은 크게 대기업, 공공기관, 금융기관, 병원, 제조업체 및 중소기업 등으로 나눌 수 있으며 각각 주력제품과 시장의 특성은 조금씩 다른 모습을 보이고 있습니다. 공통적인 특징은 기업의 요구사항이 복잡하고, 기업 내 다양한 시스템과의 연동, 한컴오피스 등 국내 전용 애플리케이션 지원 이슈 등 외산 제품이 가지고 있는 자원 및 연동 한계로 인해 국내 제품이 선호되고 있다는 점입니다. 1차 도입이 이루어졌던 곳은 업그레이드, 교체, 확산, 모바일 등 플랫폼 확장 등의 이슈로 추가 구축이 이루어지고 있고, 상대적으로 도입이 늦은 곳들은 개인정보보호 시장 활성에 맞추어 문서보안까지 도입이 진행되고 있습니다. 또한 스마트폰과 스마트 패드의 보급 증가에 따라 업무환경이 모바일로 확산되면서 기업을 중심으로 모바일 환경에서도 DRM이 적용된 상태에서 문서를 볼 수 있는 환경을 요청하고 있으며 이로 인해 모바일 DRM도 확산되고 있습니다.

(2) 애플리케이션보안 시장

애플리케이션보안 시장은 동적분석 시장을 위주로 시작되었고 정적분석 시장은 삼성전자, 현대자동차, LG전자 등 임베디드 SW분야에서 대기업 위주로 외산제품만 일부

도입 되어 국내 시장 형성이 제대로 되지 않았습니다. 과거에는 외산 정적분석도구의 품질 경쟁력이 높고 국산 대체제품이 없다보니 국내 대기업은 외산제품이 고가임에도 불구하고 도입을 하였습니다. 그러나 품질도구의 특성상 기술적 접근방법에 따라 오탐이 불가피하며, 이러한 점을 시장이 인지하기 시작하여 이를 보완할 도구의 추가 도입이 필요하게 되었습니다. 최근에는 당사가 제품라인업을 완료하고 지원 언어를 늘려가면서 지속적으로 영업을 하고 외산도구 대비 경쟁력을 확보함에 따라 당사의 제품이 임베디드 SW시장의 정적분석 품질도구의 추가 표준으로 채택되어가고 있습니다.

시큐어코딩 시장은 공공기관에서 시작하여 점차 금융권 및 일반 기업으로 확대될 것으로 예상되며, 정부 규제도 확대 시행될 것으로 보입니다. 또한 지속되는 사이버 해킹으로 인해 고객개인정보 유출 사고 등 보안 사고가 끊임없이 발생하면서 웹 또는 모바일 애플리케이션에 대한 보안 니즈가 점점 확대되고 있습니다. 이를 위해서는 소프트웨어 개발단계부터 보안을 고려해서 해커의 출입구가 되는 보안취약점을 막아야 합니다. 최근에는 소프트웨어가 중심이 되는 IoT 기술이 전 산업분야는 물론 개인의 일상생활까지 확대 적용되면서, 소프트웨어보안의 중요성이 더욱 강조되고 있습니다.

최근에는 IoT(Internet of Things), IoE(Internet of Everything)에 기반한 수많은 플랫폼과 다양한 연결 기술, 그리고 많은 센서와 디바이스의 연결로 보안 취약점도 과거에 비해 훨씬 다양화 되고 많아졌으며, 기존의 보안 솔루션만으로는 이를 감당하기 어려워 SoT(Security of Things)라는 새로운 보안 이니셔티브의 등장을 이끌게 되었습니다. SoT는 IoT전체를 아우르는 모든 부분, 즉 네트워크와 플랫폼은 물론 이를 운용하고 사용하는 사람에 이르기까지 모든 부분에 보안을 적용해야 한다는 것이며, 물리적인 보안에서 네트워크 보안, 정보 보안을 모두 아우르는 차세대 보안의 큰 그림이라고 볼 수있습니다. 따라서 앞으로도 물리보안 및 자동차, 통신업계 외에도 네트워크, 클라우드, 빅데이터, AI와 머신러닝에 걸친 보안 기술이 꾸준히 요구될 것으로 보이며, 이는 앞으로도 무한한 기회와 발전 가능성이 있을 것임을 시사한다고 볼 수 있습니다.

(3) 정보보호컨설팅 시장

정보보안컨설팅 서비스에는 취약점 분석평가(기반시설, 전자금융기반시설), 인증(IS

MS, ISO27001, BS10012), 진단 및 모의해킹, 개인정보보호 컨설팅(GDPR, PIMS), 기타 보안컨설팅이 포함됩니다.

1) 취약점 분석평가

취약점 분석평가 서비스는 정보통신기반보호법에 의해 주요정보통신기반시설로 지정된 대상과 전자금융거래의 안전성과 신뢰성을 확보해야 하는 전자금융기반시설 대상으로 매년 실시하고 있습니다. 주요정보통신기반시설로 지정된 주요정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰과 같은 정보통신서비스제공자는 정보통신망에 대한 침해사고 예방을 위한 관리대책과 이행여부를 정보보호전문서비스 기업에게 확인받도록 의무화되어 있으며, 금융회사와 전자금융업자의 전자금융기반시설에 대한 분석평가 결과를 전문성이 확보된 정보보호전문서비스 기업에게 요청하고 있어 공급 가능한 규모 이상의 수요가 지속적으로 증대 및 확대된다고 기대할 수 있습니다.

2) 인증(ISMS, ISO27001)

인증(ISMS, ISO27001)은 조직이 수립 및 운영하는 관리체계가 정보보호 측면에서 적합한지를 판단하는 제도로 인증을 통해 정보보호 관리에 대한 인식을 제고해 보호해야 할 정보통신망 및 정보자산의 안전성과 신뢰성을 향상시키는 것이 목적입니다. 조직에 적합한 수준의 정보보호를 제공하기 위해 정책 및 조직을 수립하고 위험관리, 대책 구현, 사후 관리 등의 정보보호관리과정을 통해 여러 정보보호대책들이 유기적으로 통합되어 구현, 운영되는 체계입니다. 인터넷 세상이 확산될수록 정보보안의 중요성이 부각되고 그에 따른 ISMS 인증 필수 대상 기업과 자율 신청 기업이 늘어나게 되며 ISMS 인증 유지 기업은 약 600개 기업, 국제 규격인 ISO27001은 거의 800여 개 기업이 인증을 지속적으로 유지하고 있습니다.

3) 기술적 취약점 진단(인프라, 모바일, IoT) 및 모의해킹

고객이 운용하고 있는 인프라(서버, 네트워크, DBMS, 응용 프로그램의 취약점), 모바일(iOS, Android), IoT(Internet of Things)를 대상으로 한 기술적 취약점 진단은 위협/취약성에 대한 보호대책을 제시하여 침해사고 발생 가능성을 낮추고 가용성을 높일 수 있도록 합니다. 특히 스마트폰을 통한 모바일 서비스와 IoT가 적용된 기기 증대에 따라 진단 범위 및 종류가 다양해지고 있습니다. 모의해킹은 실제 해커가 사용하는 최신 해킹기법 및 도구를 이용하여 보안담당자의 사전 승인을 취득한 후 취약

점을 찾고 내· 외부자 관점에서 침투테스트(Penetration test)를 시도하여 해킹 위협들을 심층적으로 분석하는 것으로 최근에는 시나리오 기반의 모의해킹이 주류를 이루고 있습니다.

4) 개인정보보호 컨설팅(GDPR, ISMS-P)
개인정보보호컨설팅이란 온라인상에서 개인의 신용정보 등 중요한 개인정보를 보호하는 것을 목적으로 개인의 허락 없이 개인의 정보가 유출되어 도용되는 것을 방지하기 위한 서비스입니다. 국내에서는 인터넷과 정보통신기술이 발전되면서 과거 단순 신분정보가 금융거래, 전자상거래, 고객관리를 위한 필수 요소 정보가 되었습니다. 2011년 9월에 개인정보보호법이 제정된 이후 개인정보보호인증(ISMS-P), 개인정보영향평가, 개인정보실태점검과 같은 다양한 서비스가 창출되어 유지되고 있습니다. 특히 GDPR이라는 2018년 5월 25일부터 시행된 EU(유럽연합)의 개인정보보호 법령은 EU의 모든 회원국이 의무적으로 준수해야 하는 강행 규정입니다. GDPR의 시행으로 EU내 사업장을 운영하는 국내 기업 뿐만 아니라 전자상거래 등을 통해 해외에서 EU주민의 개인정보를 처리하는 기업에게도 적용되어 국내외 글로벌회사를 대상으로 한 컨설팅 서비스 확대가 예상되고 있습니다.

5) 종합보안컨설팅
종합보안컨설팅이란 조직의 목적을 달성하는데 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 자문 서비스입니다.

6) 내부정보유출방지컨설팅
내부정보유출방지컨설팅이란 고객정보, 핵심기술, 영업정보 등 기업의 내부 중요정보가 전산시스템, 사람 등에 의해 유출 될 수 있는 위협을 분석하고 이에 대한 대책을 수립하여 지원하는 자문 서비스입니다.

나. 회사의 현황

(1) 영업개황 및 사업부문의 구분

(가) 영업개황

(1) 데이터보안 사업

데이터보안 사업은 전자문서를 암호화하여 외부자는 물론, 허가된 내부자에 의한 기밀문서 유출까지 방지하는 강도 높은 기업용 문서보안솔루션을 제공하는 사업입니다. 이와 같은 기능은 최근 이슈가 되고 있는 개인정보 유출과 같은 내부자에 의한 문서유출을 미연에 방지하고 사이버 공격에 의한 원전 설계자료 유출 등과 같은 외부자에 의한 문서유출에도 대응할 수 있는 최적의 솔루션으로 각광받고 있습니다.

당사는 세계 최초로 DRM 기술을 상용화하고 국내 기업용 DRM 시장을 개척하였습니다. 국내 최다 레퍼런스를 갖춘 DRM 1위 기업 파수는 경쟁력 높은 기술력과 서비스로 국내 시장에서 업계 선두주자로서의 위상을 유지하고 있습니다.

정보보호산업의 최신 동향에 적극 대응하기 위해 가장 강력한 데이터보안 솔루션인 "Fasoo Enterprise DRM" 제품을 중심으로, 사용자가 보유한 모든 데이터를 탐지하여 예외상황에 대한 보안의 빈틈을 방지하는 "Fasoo Data Radar"제품과 보안리스크를 관리하는 "Fasoo RiskView" 제품이 상호 긴밀하게 연관되어 단계별로 보안을 강화하는 "Fasoo Data Security Framework"를 완성하였습니다. 향후 컨설팅 역량 강화를 통해 추가적인 매출 확대를 추진할 계획입니다.

또한, 당사는 블록체인 기반의 진본 증명 플랫폼인 '파수블록(FasooBlock)'을 개발하여 제공하고 있습니다. 파수블록은 문서의 해시값을 블록체인에 저장하고, 블록체인에 등록된 해시와 거래시간에 대한 위・변조를 불가능하게 하여 지적자산이 생성된 시점과 이후 변경이 없음을 영구히 증명할 수 있습니다. 이러한 진본 등록 및 검증 기능을 통해 문서의 무결성 및 보안성 확인이 필요한 보험, 의료정보, 물류, 유통, 전자계약 등의 전 분야로의 진출을 확대할 계획입니다.

당사의 데이터보안 사업 경쟁력은 다음과 같습니다.

1) 높은 고객충성도

데이터보안 제품은 다른 보안제품과 달리 고객충성도가 높습니다. 기업내 문서의 호환이 가장 중요하므로 한번 도입된 데이터보안 제품이 그룹사 및 시스템 확장에 지속적으로 들어가고 있어, 표준으로 한번 선정되면 큰 문제가 없는한 지속적인 매출이 발생하게 됩니다. 당사는 삼성그룹, 포스코, CJ, 롯데, 동부, 금호 등 국내 대기업 대

부분의 데이터보안 표준제품으로 선정되어 안정적인 고객기반을 확보하고 있으며 정부 공공기관도 중앙부처의 대부분에 도입이 되어 그 산하기관과 자치단체에 파급되는 사업효과를 가져가고 있습니다. 후발업체 및 신생업체들이 중소기업 중심으로 영업을 하고 있으나 국내 데이터보안 시장에서 차지하는 비율은 미미한 수준입니다.

2) 높은 진입장벽

기존 시스템의 문서와의 호환문제로 충성도가 높을뿐 아니라, E-DRM은 제품의 기술진입장벽이 높고, OS와 각종 문서 Application의 잦은 버전 업그레이드, PC, 모바일, 태블릿 등 각종 플랫폼 지원 등 유지관리와 신규투자 이슈가 많아서 신생업체들이 시장에 진입을 못하고 있습니다. 과거 대기업뿐 아니라 유수의 중견 보안업체들이 E-DRM시장에 뛰어들었으나 성공하지 못하여, 2000년부터 시작한 3개사만이 지금도 경쟁사로 남아있습니다.

3) 글로벌 수준의 제품 경쟁력

E-DRM은 보안분야에서 유일하게 외산업체가 국내 진입을 못하고, 국내업체만 시장에서 사업을 하고 있습니다. 국내시장이 해외시장보다 훨씬 일찍 성숙되어 제품의 수준이 해외업체 제품보다 앞서있으며, 실제로 해외업체들이 존재하나 국내 고객들의 기업환경과 요구사항에 대응할 수 있는 제품이 전무한 상황입니다.

4) 안정적인 유지관리 매출

타 SW 대비 OS 및 문서 Application 업그레이드, 끊임없이 쏟아지는 악성코드와 타 보안 솔루션들과의 충돌 및 호환 이슈, PC교체 등의 문제로 E-DRM은 도입 후 유지관리가 필수인 SW입니다. 따라서 타 제품들 대비 유상유지관리 계약율이 90%가 넘고, 최근 SW의 유지관리 제값받기에 대한 정부의 관심과 정책 등에 힘입어 유지관리 요율이 현실화 되어가는 분위기입니다. 실제로 유지관리 계약 시에는 보안 SW로서 유지관리 이슈가 많은 점을 고객과 협의하여 요율을 과거 계약대비 상향 책정하여 평균 14%로 계약하고 있습니다. 유지관리 시장은 고객사가 늘어남에 따라 누적으로 매출이 증가하는 구조로, 매출의 안정화와 기존고객의 추가도입을 위한 영업전략으로 중요한 역할을 하고 있습니다.

(2) 애플리케이션보안 사업

애플리케이션보안 제품인 Sparrow는 정적 프로그램 분석(Static Program Analysis)

기술을 응용하여, 프로그램이 실행되기 전에 프로그램 소스에 있는 치명적인 오류 및 보안 취약점을 자동으로 검출해 주는 솔루션입니다. 이는 소스코드만 있으면 프로그램을 실행하지 않고도 모든 실행사항을 마치 사람이 눈으로 분석하는 것처럼 깊고 상세하게 분석하여 반드시 고쳐야 하는 오류를 검출하기 때문에 결과적으로 프로그램 테스팅 시간은 물론, 오류수정 비용에 대한 절감효과를 볼 수 있습니다.

그동안 임베디드 SW와 금융권 위주로만 형성되던 품질 시장이 일반 기업들의 품질에 대한 의식제고로 점차 시장 영역이 확대되고 있으며, 2013년 시큐어코딩을 위한 버전을 출시한 이후 2014년 1월 국내 최초의 CC인증 확보를 통해 보안 시장에 빠른 속도로 진입하여 공공분야 중심으로 시큐어코딩에 대한 도입이 활발히 진행 중입니다. 코드분석을 통한 테스트자동화 및 자동 오류 검출 기술은 계속 발전 중이지만, 국내의 정적분석 기반의 기초 기술력은 높은 편이며 당사는 Active Suggestion 등 차별화된 기능 구현으로 선두 제품과의 기술적 격차도 크지 않습니다. 또한 정부로부터 GCS(Global Creative SW)과제로 선정되어 2015년 9월부터 2017년 9월까지 신규 솔루션 개발을 진행하였으며 그 결과, 정적/동적분석의 모든 기능을 통합 제공하는 정적분석솔루션(SAST)와 동적분석솔루션(DAST), 웹애플리케이션에 대한 공격을 실시간으로 탐지 및 차단하는 자기방어솔루션(RASP), 효율적인 소프트웨어 공급망 관리를 위한 라이선스 식별 및 보안취약점 진단 도구(SCA) 그리고 이를 모두 통합 관리하는 플랫폼인 인터렉티브허브(InteractiveHUB)를 개발하였습니다. 다만 외산 Leading Vendor 대비 시장 진입이 늦은 관계로 글로벌 경쟁력을 높이기 위한 노력을 경주하고 있으며, 그 일환으로 2018년 5월 애플리케이션 보안 사업을 영위하는 PA사업부문을 단순· 물적분할 방식으로 분할하여 자회사인 주식회사 스패로우를 설립하여 사업 경쟁력을 강화하였습니다.

주식회사 스패로우의 애플리케이션보안 사업 경쟁력은 다음과 같습니다.

1) 시큐어코딩을 위한 최적의 소스코드 보안약점 분석 도구
- 행정자치부 '소프트웨어 개발보안(시큐어코딩)' 47개 항목 지원
- 국제표준 레퍼런스 검출 (CWE/SANS Top 25, OWASP Top 10, CERT 등)

2) 실행오류와 코딩표준을 함께 지원하는 실행의미 기반의 정적 분석 도구
- 코딩 단계부터 런타임 오류의 검출 및 수정이 가능하여 개발 시간 단축

- 융합SW 관련 국제 코딩 표준에 적합한 소프트웨어 개발 (MISRA, HIS, HICPP, JPL, BSSC)

3) 다양한 차별화 기능을 통한 높은 편의성과 검출 성능
- Active Suggestion(액티브 서제스쳔)
- Advanced lssue Filtering(어드밴스드 이슈 필터링)
- Intelligent Alarm Clustering(인텔리전트 알람 클러스터링)

4) 유연한 구축 및 운영
- 웹 기반의 통합관리 시스템을 통해 진행 중인 모든 프로젝트를 서버에서 통합 관리
- C/C++, JAVA, JSP, PHP, ASP, C#, HTML, Android 등 다양한 언어에 대한 소스 코드 분석을 지원

5) 새로운 통합 품질 솔루션의 제공 (GCS과제 선정)
- 정적/동적분석의 모든 기능을 통합 제공하는 정적분석솔루션(SAST)와 동적분석솔루션(DAST)
- 웹애플리케이션에 대한 공격을 실시간으로 탐지 및 차단하는 자기방어솔루션(RASP)
- 신규 솔루션들을 통합 관리하는 플랫폼(InteractiveHUB)

6) 오픈소스 관리도구 제공
효율적인 소프트웨어 공급망 관리를 위한 오픈소스 소프트웨어 라이선스 식별 및 보안 취약점 진단 도구 (SCA)

(3) 정보보호컨설팅 사업
당사는 조직의 비즈니스 연속성 보장 및 보안사고로 인한 영향을 최소화하기 위해 위험분석, 대책수립, 이행 및 점검과 같은 일련의 보안활동을 지속적으로 수행 할 수 있도록 지원하는 정보보안 컨설팅을 제공합니다.
ISMS, ISMS-P, ISO27001 심사원 자격을 보유한 전문 컨설턴트들이 정보보호 관련 다양한 컨설팅 경험과 데이터・애플리케이션 보안 솔루션 구축 및 운영 노하우를 기반으로 새롭게 개발 완성된 컨설팅 방법론을 통해 종합 정보보호 컨설팅 서비스가 가능합니다.

당사의 정보보호컨설팅 사업 경쟁력은 다음과 같습니다.

1) 풍부한 경험과 우수한 역량을 지닌 전문 컨설턴트 보유
- ISMS, ISO27001, ISMS-P 체계구축 및 인증획득, 기반시설 및 IT보안 실태점검 등 다양한 분야의 보안컨설팅 경험이 풍부한 컨설턴트 보유
- ISMS, ISO27001, ISMS-P 인증 심사원 유자격자 다수 보유
- 대규모 사업수행 및 관리경험이 풍부한 PM급 인력 다수 보유

2) 최상의 컨설팅 방법론과 솔루션 구축 및 운영 경험 접목
- 다년간의 정보보호 전문서비스 사업을 통해 검증된 컨설팅 방법론(Fasoo_USIM)을 적용하여 최적의 컨설팅 산출물 도출 가능
- 국내 최고 수준의 데이터 보안 및 애플리케이션 보안 분야의 기술력 및 운영 경험을 접목하여 고객 요구사항 만족 및 산출물 품질 고도화 가능

3) 다양한 고객 및 분야에 대한 컨설팅 경험 보유
- 미래창조과학부 지정 정보보호 전문서비스기업으로서 다수의 공공· 민간 주요정보통신 기반시설 컨설팅 이력 보유
- 공공, 금융, 통신, 제조, IT 등 다양한 산업분야의 대기업부터 중소기업을 대상으로 정보보호 및 개인정보보호 관련 컨설팅 다수 수행

(3) 시장점유율
국내 데이터보안 시장의 주요 경쟁 회사는 마크애니와 소프트캠프가 있습니다. 마크애니와 소프트캠프의 경우 데이터보안 이외의 사업도 영위하고 있으나 사업부문별매출 비중을 파악할 수 없어 정확한 시장 점유율을 산출할 수 없습니다.
국내 애플리케이션보안 시장은 국내 업체로써는 주식회사 스패로우가 독보적인 위치를 점유하고 있으며, 공공 및 금융 시장을 중심으로 외산 솔루션과 경쟁하고 있습니다.

(4) 신규 사업 등의 내용 및 전망

1) 엔터프라이즈 문서 플랫폼

종합 기업 문서 플랫폼인 Wrapsody는 ECM(Enterprise Contents Management)을 타겟으로 개발된 콘텐츠 중심의 지속적인 문서공유/협업/관리 솔루션입니다. 기존 문서관리 개념에서 벗어나, 서버 또는 개인 PC 등 콘텐츠가 보관되는 위치에 상관없이 콘텐츠를 항상 최신 상태로 유지하여 효율적인 협업환경을 제공합니다.
Wrapsody는 2015년에 국내 시장에 첫 출시된 이후 많은 관심과 기대를 모으고 있으며 미국 내 ECM 시장에서의 성공가능성이 더 높다고 판단되어 관련 IP를 2017년 12월 31일 기준으로 미국법인에 이관 하였습니다.
2018년에는 Wrapsody 기반의 외부 협업 솔루션인 Wrapsody eCo 를 개발하였으며, 2019년에는 블록체인 기반 기술을 접목하여 모든 버전의 문서의 자동 수집/관리/기록/원본증명 및 검증이 가능한 종합 Document Platform 으로 발전하였습니다.

2) Analytic DID
빅데이터를 활용한 Analytic DID는 '비식별화' 기술을 기반으로 최적의 알고리즘이 적용된 개인정보 비식별화 솔루션 및 전문 컨설팅 서비스로서, 효율적인 비즈니스 프로세스 지원은 물론 의사결정에 도움을 줄 수 있도록 분석의 효용성과 위험에 대한 다양한 지표를 가시화하여 제공합니다. 2018년에는 과학기술정보통신부의 GCS과제에 선정되어 다양한 컴플라이언스 기준에 부합하면서도 데이터의 유용성이 저하되지 않는 모듈을 확장 개발하고 있습니다. 또한, 2020년 1월 데이터3법이 국회 본회의를 통과하고 같은 해 8월 5일부터 시행되었습니다.

3) 해외사업
당사는 신시장 개척을 위한 노력도 지속적으로 추진하고 있습니다. 해외 데이터보안 시장의 성장에 발빠르게 대처하여 기회를 선점하고, 해외 IT서비스회사 및 Reseller와의 협력 강화를 통해 의미있는 레퍼런스를 확보해 나가기 위해 노력하고 있습니다. 이를 지원하기 위해 우수 인력을 영입하고 해외법인의 독자적인 관리 권한을 보장하고 있으며 이러한 해외 신시장을 개척하기 위한 전략을 통해 안정적인 시장 확대 및 수익성을 확보하고자 합니다.

(5) 조직도



조직도 공시용

2. 주주총회 목적사항별 기재사항

기타 주주총회의 목적사항

가. 의안 제목

- 자본준비금 감액을 통한 이익잉여금 전입의 건

나. 의안의 요지

- 주식회사 파수는 상법 제461조의2에 의거하여 자본준비금(289억원)이 자본금의 1.5배(87억원)를 202억원 초과하므로, 회사의 자본준비금 중 주식발행초과금 200억원을 감액하여 이익잉여금으로 전환하고, 배당 재원 등으로 활용하고자 함.

IV. 사업보고서 및 감사보고서 첨부

가. 제출 개요

제출(예정)일	사업보고서 등 통지 등 방식
-	-

나. 사업보고서 및 감사보고서 첨부

금번 주주총회는 임시주주총회이므로 사업보고서 및 감사보고서 첨부는 해당사항 없습니다. 제 22기 사업보고서 및 감사보고서는 전자공시시스템(http://dart.fss.or.kr)에 게재되어 있어 참고 가능합니다.

참고사항

코로나바이러스 감염증-19(COVID-19)에 관한 안내

- 당사는 주주총회장에 체온계와 손소독제를 비치할 예정이오니 주주총회장 입장시 반드시 열 체크 및 손소독을 부탁드립니다.

- 코로나바이러스 감염증-19(COVID-19)의 감염 및 전파를 예방하기 위하여 발열, 기침 등 감염증세가 있거나 미완치자, 자가격리자, 위험지역 방문자 및 마스크 미착용자는 주주총회장 출입이 제한될 수 있습니다.

- 감염병에 따른 총회장의 불가피한 변경시 총회장소 변경의 권한은 대표이사에게 있으며 동사실 발생시 지체없이 재공시할 예정입니다.